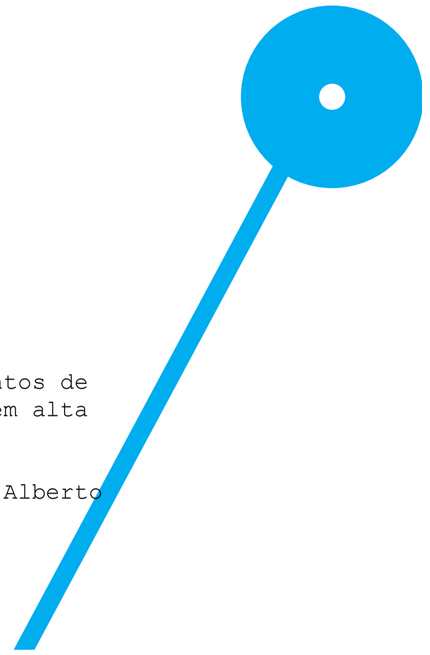
ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

P.PORTO

M

MESTRADO
ENHENHARIA INFORMÁTICA

Sistema de gestão de eventos de segurança de informação em alta disponibilidade
Hélio Sousa
Professor Doutor António Alberto dos Santos Pinto



02/2019

Sistema de gestão de eventos de segurança de informação em alta disponibilidade. Hélio Sousa; Professor Doutro António Alberto dos Santos Pinto

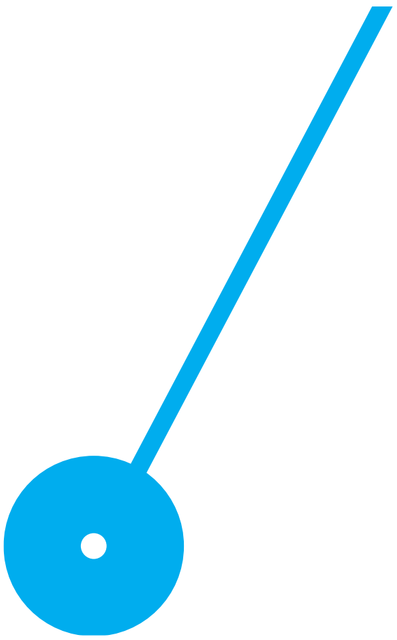
P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M

MESTRADO
ENGENHARIA INFORMÁTICA

Sistema de gestão de eventos de segurança de informação em alta disponibilidade
Hélio Sousa
António Alberto dos Santos Pinto



02/2019

P.PORTO

Sistema de gestão de eventos de segurança de informação em alta disponibilidade

Politécnico do Porto
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia Informática

Autor
Hélio Sousa

Orientador
Professor Doutor António Alberto dos Santos Pinto

Novembro de 2018

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Listagens

Siglas

ACL Access Control List. 36, 50, 69

AD Activity Director. 43, 45

APT Ameaças Persistentes Avançadas. 9

ARP Address Resolution Protocol. 20

CIDR Classless Inter-Domain Routing. 19

CLI Command Line Interface. 50

CPU Central Processing Unit. 57

CSV Comma Separated Value. 60

CVEs Common Vulnerabilities and Exposures. 19

DAC Direct Attach Cable. 50

DHCP Dynamic Host Configuration Protocol. 43

DNS Domain Name System. 33, 61

EPS Events Per Second. 57

ERP Enterprise Resource Planning. 8

FEED Front-End Engineering and Design. 19

FQDN Fully Qualified Domain Name. 61

GUI Graphical User Interface. 50

HIDS Host-based Intrusion Detection System. 18

HIMS Host Integrity Monitoring System. 21

IDS Intrusion Detection Systems. 6

IOCs Indicadores de Comprometimento. 19

IP Internet Protocol. 10, 61

IPS Intrusion Prevention Systems. 6

ISP Internet Service Provider. 45, 50

LDAP Lightweight Directory Access Protocol. 43

LMS Log Management System. 5

MAC Media Access Control. 20

MB Megabyte. 63

MITM Man-in-the-Middle. 20

NIDS Network Intrusion Detection Systems. 18

NTP Network Time Protocol. 50

OCS-NG Open Computer and Software Inventory Next Generation. 22

OSI Open System Interconnection. 43

OSSIM Open Source Security Information Management. 12

OTX ™ Open Threat Exchange®. 18

PCAP Packet Capture. 21

RAM Random-Access Memory. 48

RFI Radio Frequency Interference. 46

RGPD Regulamento Geral sobre a Proteção de Dados. 55

SEC Security Event Correlation. 5

SEM Security Event Management. 5

SIEM Security Information and Event Management. 2

SIM Security Information Management. 5

SMTP Simple Mail Transfer Protocol. 56

SNMP Simple Network Management Protocol. 6

SOC Centro de Operações de Segurança. 9

SSD Solid State Disk. 49

SSH Secure Socket Shell. 8

SSIC Serviços de Sistemas de Informação e Comunicação. 40

SYSLOG System Log. 6

TCP Transmission Control Protocol. 21, 56

TCP/IP Transmission Control Protocol/Internet Protocol. 20

TI Tecnologias de Informação. 1

UDP User Datagram Protocol. 56

URI Universal Resource Identifier. 19

URL Universal Resource Locator. 19

USB Universal Serial Bus. 22

UTP Unshielded Twisted Pair. 46

VLAN Virtual Local Area Networks. 43

VPN Virtual Private Network. 36, 43

WMI Windows Management Instrumentation. 6

XML Extensible Markup Language. 11, 64, 69

Capítulo 1

Introdução

As Tecnologias de Informação (TI) têm viabilizado soluções disruptivas que acontecem com velocidades cada vez mais rápidas. A disponibilidade, rapidez, forma de acesso e modo de processamento dos dados e informação, afetam diretamente a operacionalidade das empresas, bem como as formas de comunicar, socializar e trabalhar das pessoas. A segurança informática nasce da necessidade das organizações garantirem e salvaguardarem os seus ativos de forma segura, tendo vindo a ser compreendida ultimamente como sendo fulcral na continuidade dos seus negócios. Esta consciencialização deve-se ao facto de nestas organizações a informação se encontrar maioritariamente em suporte digital. Outra nota relevante e de grande importância, esta tomada de consciência prende-se com o facto de os ataques informáticos terem aumentado exponencialmente tanto em número como em sofisticação [1][2][3].

A necessidade de segurança dos ativos das organizações e a existência de ameaças à sua disponibilidade, integridade e confidencialidade leva à necessidade de estudar e potenciar ferramentas eficazes que possibilitem o controlo e monitorização destes ativos. Segundo Tankard [4], assim como Friedberg, Ivo and Skopik, Florian and Settanni, Giuseppe and Fiedler, Roman [5], as tecnologias de segurança, tais como *firewalls*, sistemas de deteção/prevenção de intrusões, sistemas de *proxy* ou antivírus, utilizadas tradicionalmente nas organizações, começam a deixar de ser suficientes por si só para identificar e prevenir ataques da melhor forma.

Do ponto de vista de gestão de segurança da informação observam-se problemas relacionados com a recolha de registos de atividade (ou *logs*)[6], com a monitorização da rede, com a correlação de eventos e com deteção de falsos positivos. A quantidade de *logs* e outros registos de atividade, gerados das atividades monitorizadas pelos sistemas de segurança e do próprio funcionamento das mesmas, é avassaladora e requer um esforço de normalização. Tipicamente as várias fontes de registos usam formatos de registo diferentes. A monitorização é também complexa já que as consolas de monitorização

são heterogéneas, oferecendo visões isoladas sobre o estado de segurança do ambiente. Há ainda dificuldade em correlacionar eventos reportados pelas diversas soluções. Finalmente, surgem frequentemente falsos positivos, decorrente das análises isoladas das várias soluções por estas não possuírem a visão de todo o ambiente. Numa tentativa de controlar toda esta situação caótica, recorrem-se a soluções que passam pela utilização de ferramentas (*software*) de gestão de redes [7], sendo estas as principais armas para sanar os problemas que têm vindo a surgir nestes últimos tempos.

Tecnologia de gestão de eventos de segurança de informação, ou Security Information and Event Management (SIEM), visam colmatar as falhas anteriormente evidenciadas. Um SIEM consiste numa solução de *software* que possibilita a monitorização da rede e seus ativos, a concentração, correlação e gestão de eventos, bem assim como a vertente de alarmística alicerçada em motores que correlacionam múltiplas fontes em tempo real [8]. A adoção de SIEM nas organizações começa a ser uma realidade cada vez mais presente. Este tipo de tecnologias não vem de alguma forma substituir as tecnologias acima elencadas e já existentes, mas sim o seu complemento[9].

1.1 Objetivos

O atual projeto nasce com necessidade de garantir a monitorização de segurança de uma infraestrutura de rede de alta complexidade, assente numa solução disponível, escalável e financeiramente ajustada. Pretende-se com esta solução monitorizar e detetar eventos de segurança de informação de modo a assegurar uma resposta eficaz e em tempo útil aos mesmos. Como objetivo pretende-se que a proposta de solução registe e gere eventos catalogados por grau de perigosidade, gere alertas para as situações mais graves e que opere em modo altamente disponível, permitindo o seu funcionamento mesmo com parte da infraestrutura indisponível. A solução deverá ser balizada pelo contexto real da entidade onde esta vai ser instalada.

1.2 Metodologia

Tecnologias de gestão de eventos de segurança de informação, por regra geral tem elevada complexidade, tendo uma abrangência muito grande desde as camadas de rede aos serviços aplicacionais, passando por uma panóplia multifacetada de dispositivos e serviços que geram *logs*[10]. Estas tecnologias exigem um nível de conhecimento alargado das tecnologias usadas na sua implementação e a necessidade da concertação de esforços de vários especialistas, para se obter uma implementação eficaz que se irá traduzir num aumento de visibilidade da segurança das infraestruturas tecnológicas da organização.

O trabalho depende da qualidade e relevância dos dados recolhidos, da quantidade de dispositivos agregados à solução, e das regras definidas para gerarem eventos para poderem ser consultados para *troubleshooting* ou para gerar alertas de segurança. A solução deverá ser implementada por fases e constantemente monitorizada de forma a validar resultados e possíveis impactos negativos que possa causar tanto a nível de rede como na infraestrutura de servidores.

1.3 Organização do documento

Nesta secção apresenta-se uma descrição de como o presente documento se encontra organizado, explicando sucintamente os capítulos que os compõem.

Neste primeiro capitulo é efetuado o enquadramento relativo ao tema do projeto desenvolvido, e a principal motivação para a sua realização. É ainda especificado os objetivos para o presente projeto e qual a metodologia utilizada de forma a atingir os objetivos delineados.

O Capítulo 2 debruça-se sobre o funcionamento dos sistemas de gestão de eventos de segurança de informação, assim como um enquadramento de conceitos teóricos relativos ao problema inicialmente identificado.

O Capitulo 3 consiste na especificação e explicitação da ferramenta escolhida para a implementação do projeto, o OSSIM.

O Capitulo 4 especifica considerações para a implementação de um sistema SIEM Neste capitulo, são abordados o planeamento, âmbito, processos e procedimento, assim como a importância de um plano de resposta a incidentes.

No Capitulo 5 escreve a implementação da solução, utilizando um sistema de gestão de eventos de segurança de informação de código livre.

O Capitulo 6 descreve a validação e avaliação de resultados da solução implementada. Apresenta-se os principais alertas detetados, relatórios entre a informação de maior relevo.

Por fim, o Capitulo 7 resume as principais conclusões deste projeto, assim como a definição de trabalhos futuros a desenvolver.

Capítulo 2

Sistemas de gestão de eventos de segurança de informação

O termo SIEM, cunhado em 2005 por Mark Nicolett e Amrit Williams[11], descreve-o como um sistema capaz de recolher, analisar e apresentar informações dos dispositivos de segurança de rede, softwares de controle de acesso, softwares gestão de vulnerabilidades, ferramentas de conformidade, *logs* de sistemas operativos, base de dados e aplicações, e por último, dados de ameaças externas. Um SIEM permite então que os eventos registados pelas diversas tecnologias e soluções já existentes nas organizações, sejam recolhidos, normalizados, armazenados e correlacionados, permitindo desta forma a rápida identificação de incidentes de segurança. Por seu lado, a rápida identificação deste tipo de incidentes potencia a sua rápida resolução. Segundo Kavanagh [12], o mercado dos SIEM tem um crescimento lento mas a aposta nestes sistemas parece ser visível já que a maioria das empresas da lista Fortune 500 já implementou soluções deste tipo para garantir a segurança da sua informação.

SIEM é uma solução que providencia uma visão panorâmica de uma infraestrutura TI. Cumpre dois objetivos primordiais; Primeiro, detetar incidentes de segurança praticamente em tempo real e segundo, gerir com eficiência os registos. Estes dois objetivos são conhecidos como gestão de eventos de segurança ou Security Event Management (SEM), e gestão de informações de segurança ou Security Information Management (SIM), sendo que hoje em dia essas funções foram mescladas num único sistema conhecido como SIEM [12][11], que além destas tecnologias também incorpora tecnologias complementares como o Log Management System (LMS) e Security Event Correlation (SEC). Segundo [13], o LMS veio corrigir uma série de problemas e unificar, centralizar o registo de *logs*, de forma a conseguirmos de um determinado ponto aceder aos *logs* de vários sistemas e dispositivos

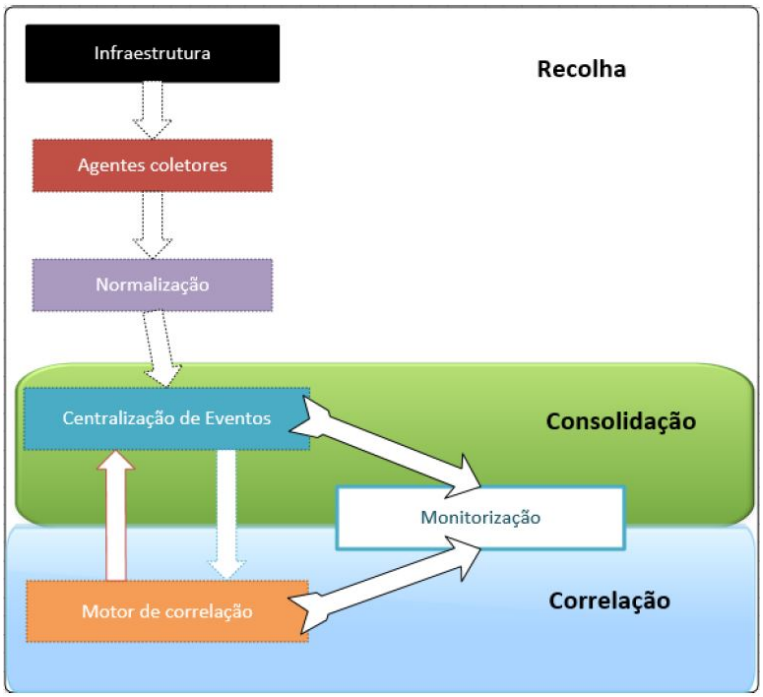


Figura 2.1: Arquitetura genérica de um SIEM

sem a necessidade de acesso físico a esses mesmos dispositivos e sistemas.

A capacidade de recolher registos é a base de operação de um SIEM, devendo então suportar vários formatos de registos (System Log (SYSLOG), Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), etc). A Figura 2.1 apresenta uma arquitetura genérica de um SIEM. Os *logs* são então gerados pelos ativos de rede e outros equipamentos dentro da infraestrutura, sendo enviados para agentes que concentram estes *logs*, passando de seguida por um processo de normalização para assim possibilitar o seu armazenamento numa base de dados relacional. Sobre estes eventos, guardados na base de dados, executa-se um processo de correlação dos mesmos para assim identificar eventos que sejam suportados por vários registos de várias fontes. Desta forma o sistema obtém uma maior certeza da correta identificação de eventos dignos de alerta.

Segundo David Swift [14] a implementação e configuração bem sucedida de um SIEM permitirá ao departamento de TI:

- **Identificar ameaças internas e externas.** Todos os dias são descobertos e identificados novos ataques e novas vulnerabilidades informáticas. Dispositivos do tipo *Firewall*, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) e Anti-vírus, concentram-se na atividade maliciosa entre os vários pontos da infraestrutura baseando-se em assinaturas de ameaças conhecidas para a sua deteção,

sendo manifestamente ineficientes na deteção de novas ameaças. Apesar de novas tecnologias também tendo vindo a ser incorporadas nos sistemas anteriores, acabam por funcionar de forma isolada, com base de conhecimento limitado, apesar de existência de mais informação nas infraestruturas, gerada por outros dispositivos. A tecnologia SIEM pode ser pensada e configurada para detetar atividade associada a ataques e não a um *exploit* específico, tornando mais eficiente a deteção deste tipo de ameaças.

- **Monitorizar atividades de toda a infraestrutura e principalmente dos equipamentos críticos.** Recorrendo a inteligência artificial para analisar e combinar eventos, aumenta exponencialmente a capacidade de deteção de ameaças em toda a infraestrutura.

- **Consolidação de *logs* e Investigação forense.** Armazena de forma centralizada eventos de dispositivos e sistemas. A prática forense tem como uma das suas principais características, ser processo demoroso e longo. O processo de recolha, preservação e análise de evidencias deixados nos sistemas por um atacante pode ser facilitado pelas ferramentas de pesquisa, armazenamento e correlação de registos da tecnologia SIEM.

- **Monitorizar atividade de utilizadores privilegiados.**

- **Disponibilizar relatórios de conformidade, segurança e forense.** Um SIEM tem a capacidade de gerar relatórios de eficiência operacional, forense e de conformidade com normas como *PCI-DSS* e *ISO 27001*.

- **Gestão de incidentes e suporte.** O sistema após a deteção de incidentes é parametrizado para despoletar uma ação. Esta ação pode ser um simples mail, a criação de um *ticket* de suporte e escala-lo para uma determinada equipa ou responsável. Também pode ser parametrizado de forma a executar ações automáticas como correr determinado script.

Com estes pontos, torna-se evidente que o administrador de sistemas ou administrador de segurança, pode recorrer a um sistema deste género para monitorizar, identificar, registar e responder a ameaças de segurança. No entanto por se tratar de uma ferramenta complexa, ela dependerá do bom conhecimento da infraestrutura e da sua integração, nomeadamente:

- ***Networking***, com a integração nos dispositivos de rede como *routers*, *switchs*, etc.

- **Dispositivos de segurança**, tais como *IDS/IPS*, *firewalls*, etc.

- **Servidores**, como *Web servers*, email, aplicacionais, etc.
- **Aplicações**, tais como o Enterprise Resource Planning (ERP), gestão documental, etc.

2.1 *Logs* e eventos

Um sistema SIEM faz uso de diversos tipos de informação, sendo a principal o *log* de dados. *Log* de dados consiste num arquivo de texto gerado por um software para descrever eventos de funcionamento, interações de utilizadores, interações de sistemas, entre outras. Com várias finalidades, é utilizado normalmente para depuração, administração de sistemas assim como auditorias de segurança. Basicamente no *log* são escritas unidades de informação com indicação do horário em que foi inserida, identificação do responsável que motivou a sua escrita e informação respetiva a uma modificação no estado de um sistema ou periférico.

Outro tipo de informação que pode ser recuperada por um SIEM são eventos. Os eventos normalmente são produzidos por dispositivos de segurança ou de controlo, como sistemas *IDS/IPS*. A título de exemplo temos, falhas de validação de entrada, nomes / valores de parâmetros inválidos, violações de protocolo, ou erros de aplicativo e eventos de sistemas, tais como erros de tempo de execução, problemas de conectividade, problemas de desempenho, etc. Os eventos podem ser correlacionados com outras informações para fornecer maior inteligência na gestão de *logs*.

O SIEM pode recorrer a várias condições de forma a verificar se determinados eventos correspondem a uma regra e, dependendo da última, poderá despoletar um alarme. Exemplo prático, considerando a execução de um *scanner* na rede para enumerar as portas abertas disponíveis, quando uma *firewall* receber um pacote na porta 22, ela registará um *log* como tentativa de conexão ao serviço Secure Socket Shell (SSH). No entanto se continua a receber pacotes por exemplo entre as portas 20 e 200 em fração de segundos, todos estes eventos enviados para o SIEM poderão corresponder a uma regra de "*scanner* na rede", podendo acionar um alerta de segurança.

2.2 A ponderação

A implementação de uma solução de SIEM pode ser bastante complexa e financeiramente dispendiosa. O preço dos equipamentos, o tempo de configuração e ajustes, o conhecimento necessário para o seu uso quotidiano podem ser barreiras dissuasoras do arranque da implementação deste tipo de projeto. Após a implementação, um trabalho constante de acompanhamento é obrigatório, para poder ajustar a plataforma a novos eventos, para que o recursos TI possam atuar em tempo útil.

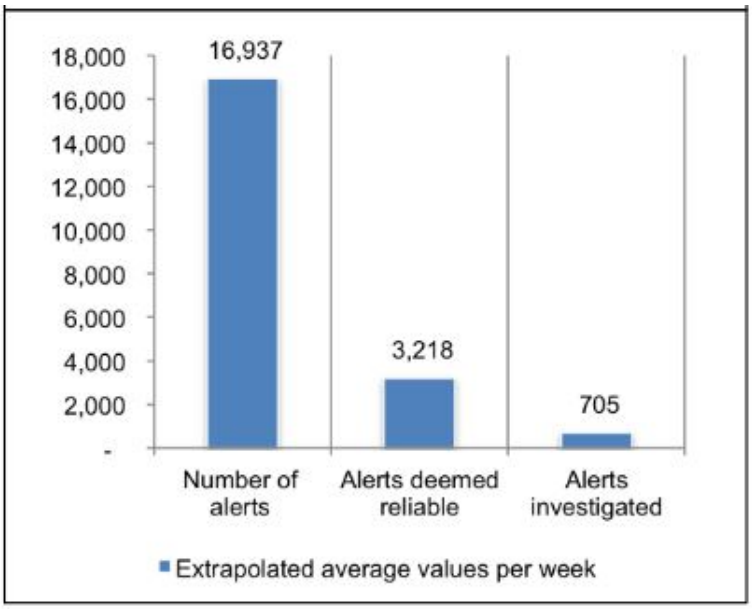


Figura 2.2: Média de alertas gerados por semana de *Malware*, nas empresas participantes do estudo

Ao usar o SIEM numa abordagem de defesa baseada em assinatura, a equipa de segurança monitorizará as atividades e atualizará regularmente os dispositivos de segurança com assinaturas de ameaças conhecidas. Após a deteção, a equipa investigará o alerta e o encaminhará à equipa de resposta a incidentes, caso eles não consigam resolver o problema diretamente (exemplo, interromper o ataque se ainda existir problemas com sistemas comprometidos), e finalmente reportar às chefias. Esse processo geral pode levar algum tempo, sendo que "tempo é dinheiro", especialmente quando se trata de segurança.

Como verificamos no exemplo anterior, nem qualquer empresa de dimensões médias ou mesmo grande, poderá ter no seu quadro equipas ou pessoas qualificadas e disponíveis para manter um sistema deste género. Os SIEM como *services* também já são uma realidade hoje em dia, sendo que a empresa envia os *logs* para empresas de segurança onde existem Centro de Operações de Segurança (SOC), que monitorizará as atividades do cliente, e intervindo quando houver necessidade. Desta forma a empresa terá o custo do serviço sem ter que se preocupar com tecnologia e manutenção da mesma.

Um estudo da Ponemon Institute publicado em 2015 [15](ver Figura 2.2) mostra-nos que em média, uma empresa terá 170.000 alertas por semana e somente 4% desses serão investigados. Este mesmo estudo diz-nos que as empresas gastam US $1,27 milhões em média anual desperdiçando tempo respondendo a informações erróneas, e além disso, existe um aumento de ataques direcionados, chamadas de Ameaças Persistentes Avançadas (APT).

Todos estes pontos têm que ser bem ponderados e a postura tradicional de segurança reativa não é suficiente. Com a redução de orçamentos TI e de segurança, as empresas necessitam de encontrar soluções eficientes a custos ajustados à sua realidade.

2.3 Uso de Inteligência nas ameaças

As tecnologias que dispomos dentro das nossas instalações fornecem-nos informações sobre os atacantes e suas capacidades, sendo valiosa para melhorar o nível de segurança. Se utilizarmos essa inteligência poderemos concentrar-nos em pontos fulcrais de forma a criarmos uma segurança eficiente e com menos desperdício de esforços. Segundo vários autores[16], ao questionar vários pontos chaves podemos proteger a nossa organização mais eficientemente:

- **Quem é o atacante?** As tecnologias de informação, sistemas e ferramentas ajudam a atribuir ataques ou atividades maliciosas a grupos de cibercrime, ativistas, agências governamentais, etc.
- **Porque está a atacar?** Sabendo quem está por de trás de um ataque ou atividade maliciosa, ajuda-nos a compreender as motivações do adversário, quanto esforço ele está investir nessas atividades, se se trata de uma ameaça persistente avançada ou de um ataque de oportunidade , se trata-se de um ataque específico à tipologia do nosso negócio ou se direcionado à nossa organização.
- **O que eles procuram?** Sabendo os alvos dos atacantes, informação ou mesmo dispositivos, podemos organizar esforços e priorizar ações com base da importância dos ativos que estão tentando comprometer.
- **Qual o seu método de ataque?** Táticas, técnicas e procedimentos fornecem-nos uma visão de como eles irão proceder, que tipos de ferramentas e infraestruturas vão ou estão utilizando.
- **Qual a origem do ataque?** Situar geograficamente o atacante, dá-nos informação preciosa para uso nas técnicas de defesa.
- **Pegada digital.** Endereços de Internet Protocol (IP), *hashes*, etc, fornecem informações claras que poderemos utilizar para detetar e identificar presença maliciosa.
- **Mitigação.** Identificarmos e documentarmos procedimentos e etapas que poderemos adotar para nos protegermos.

As questões levantadas podem correlacionar-se diretamente umas às outras. Ao mapear toda a informação obtida, e sendo correlacionada por uma

solução SIEM, teremos visibilidade do panorama dos acontecimentos reais, podendo atuar pro-ativamente contra essas ameaças.

Segundo Friedman[16] entre outros autores a inteligência de ameaças pode ser apresentada em dois níveis diferentes, dependendo do público-alvo. Inteligência a Nível estratégico, sendo neste legível pelo Homem, não sendo técnico e destinado a ser processado exclusivamente por humanos, de forma a dar a estes uma visão do impacto da ameaça sobre o negócio ou organização. Desta forma permite aos decisores tomarem as decisões mais assertivas, sendo o formato típico de inteligência estratégica os relatórios informativos.

Por outro lado, a inteligência poderá estar no nível operacional, após recolha de informação pelos analistas, esses dados legíveis por máquina são absorvidos pelos dispositivos de forma a torna-los capazes de agir sob ameaças. A inteligência operacional, normalmente utiliza o formato Extensible Markup Language (XML) para facilitar o processamento e a fácil interação com sistemas heterogéneos.

O uso deste tipo de inteligência traduz-se em muitos ganhos nomeadamente quando podemos automaticamente dispensar informação irrelevante. Ou seja, vulnerabilidades direcionadas a sistemas e aplicações que não estão presentes nas nossas infraestruturas, podem ser automaticamente descartados diminuindo o tempo gasto em análise de alertas relacionados com ameaças irrelevantes. Com boa inteligência, uma organização pode facilmente dispensar indicadores inválidos para eliminar falsos positivos e, portanto, concentrar-se nas ameaças reais.

Num relatório do SABS Institute [17], Dave Shackleford após questionar organizações de todo o mundo de como estavam a alavancar a inteligência de ameaças na utilização de TI, obteve os dados como apresentados no gráfico na Figura 2.3. Num total de resposta de 326 empresas de varias dimensões e sectores, como governamentais, finanças, bancos do qual se pode retirar a seguinte conclusão. Entre 50% e 60% das organizações que responderam ao inquérito, usam um SIEM de forma a agregar e analisar dados TI de múltiplas fontes, ou seja as TI e o SIEM devem ser combinados.

As vantagens de usar TI com SIEM são indiscutíveis, e nos dias que correm, uma boa solução de SIEM vem com integração de inteligência de ameaças, e todos os fornecedores estão conscientes que para as suas soluções terem sucesso, e serem levados a sério precisam de responder a crescente rapidez e fluidez que o mercado exige de forma a facilitar e integrar as suas soluções.

2.4 Soluções SIEM

Segundo a Gartner [18], SIEM, define-se pela necessidade do cliente em analisar dados de eventos em tempo real, para deteção antecipada de ataques

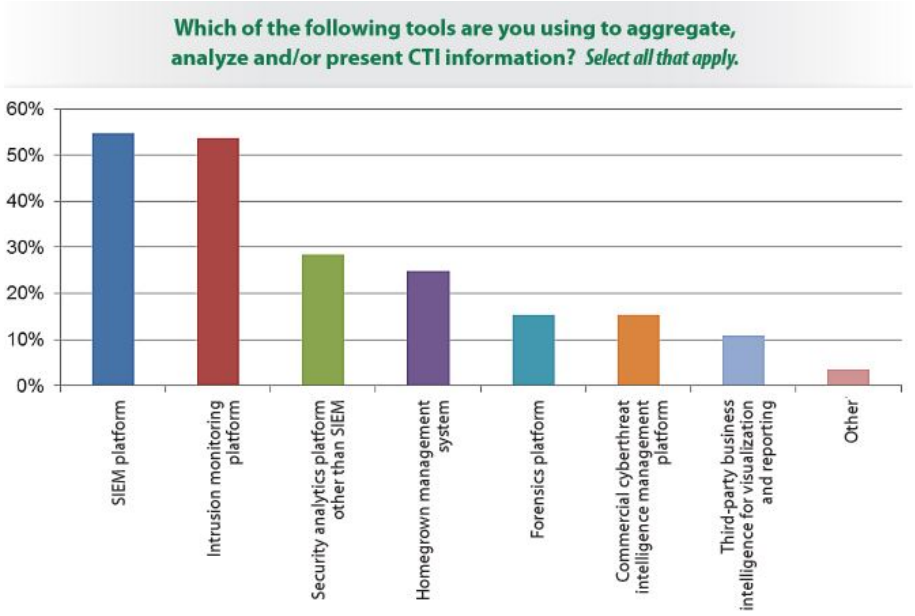


Figura 2.3: Sistema para agregar e utilizar a inteligência de ameaças

direcionados e violações de dados. O SIEM servirá para recolher, armazenar, analisar, investigar e reportar dados de eventos de incidentes de forma a responder a análises forenses ou conformidades regulamentares. As ferramentas SIEM agregam dados de eventos produzidos por dispositivos de segurança, infraestrutura de rede, sistemas e aplicativos. A fonte de dados primária são dados de registo (*logs*), mas as ferramentas SIEM também podem processar outras formas de dados, como *NetFlow* e pacotes de rede, ou informações contextuais sobre utilizadores, ativos, ameaças e vulnerabilidades que podem ser encontradas dentro ou fora da organização podendo ser útil para enriquecer *logs* e dados em bruto [10].

Podemos ver as principais soluções de SIEM na Figura 2.4, Magic Quadrant de 2017 da Gartner, empresa que disponibiliza uma análise detalhada sobre diversas áreas e tecnologias existentes no mercado. Ressalva-se que o Quadrante Mágico é considerado como sendo umas das principais fontes de informação para as instituições, sendo que para uma solução estar presente no Quadrante mágico tem de cumprir com um certo nível de requisitos bastante elevados.

Soluções presentes no quadrante mágico em 2017: AlienVault, BlackStratus, Dell Technologies (RSA), EventTracker, Exabeam, FireEye, Fortinet, IBM, LogRhythm, ManageEngine, McAfee, Micro Focus (ArcSight), Micro Focus (NetIQ), Rapid7, Securonix, SolarWinds, Splunk, Trustwave e Venustech. O sistema de gestão de eventos de segurança de informação mais popular é o Open Source Security Information Management (OSSIM) da

Figura 2.4: *Magic Quadrant for SIEM* (Gartner, 2017)

AlienVault. Este foi considerado como a solução *open source* mais viável e completa por João Alves [19] em estudo comparativo das principais soluções de mercado. Será a plataforma escolhida para a implementação no projeto pelo que não será feito uma análise mais exaustiva das restantes.

Capítulo 3

OSSIM

3.1 Introdução ao software

O OSSIM (*Open Source Security Information and vent Management*), é descrito pela própria Alienvault no seu *site* [21] como um SIEM de código aberto rico em recursos completos com recolha, normalização e correlação de eventos. Lançado por engenheiros de segurança devido à falta de produtos de código aberto disponíveis, o AlienVault OSSIM foi criado especificamente para lidar com a realidade que muitos profissionais de segurança enfrentam. Um SIEM, seja de código aberto ou comercial, é praticamente inútil sem os controlos básicos de segurança necessários para visibilidade de segurança. Podemos constatar isso mesmo na Figura 3.1 onde num comparativo da AlienVault do seus produtos, OSSIM com a sua versão comercial USM Anywhere^{TM}, mostra-nos que os principais recursos e capacidades de segurança estão disponíveis na sua versão de código aberto.

"Our Open Source SIEM (AlienVault OSSIM) addresses this reality by providing one unified platform with many of the essential security capabilities you need like: Figura 3.2

- **Asset discovery**.
- **Vulnerability assessment**.
- **Intrusion detection**.
- **Behavioral monitoring**.
- **SIEM event correlation**.

O OSSIM oferece como base as seguintes funções [20]:

- O OSSIM descobre recursos no ambiente da organização, deteta alterações nos ativos e descobre ativos não autorizados na rede.

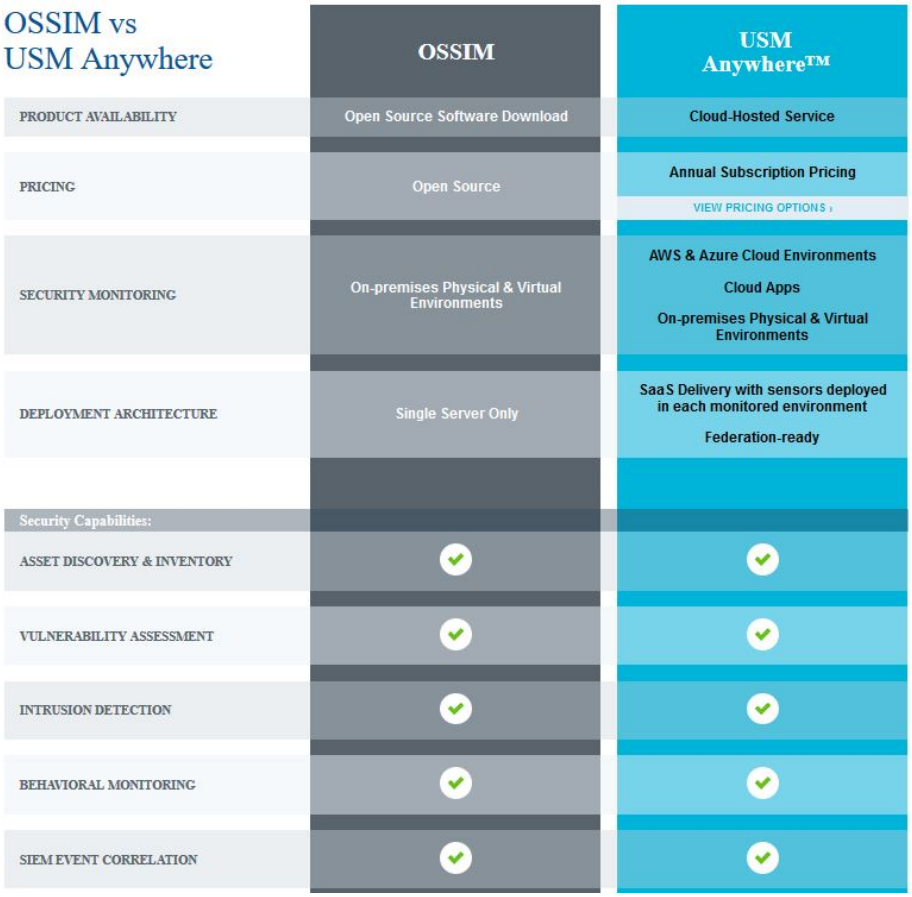


Figura 3.1: Comparativo do OSSIM com USM Anywhere
Fonte: AlienVault - Documentation Center [20]

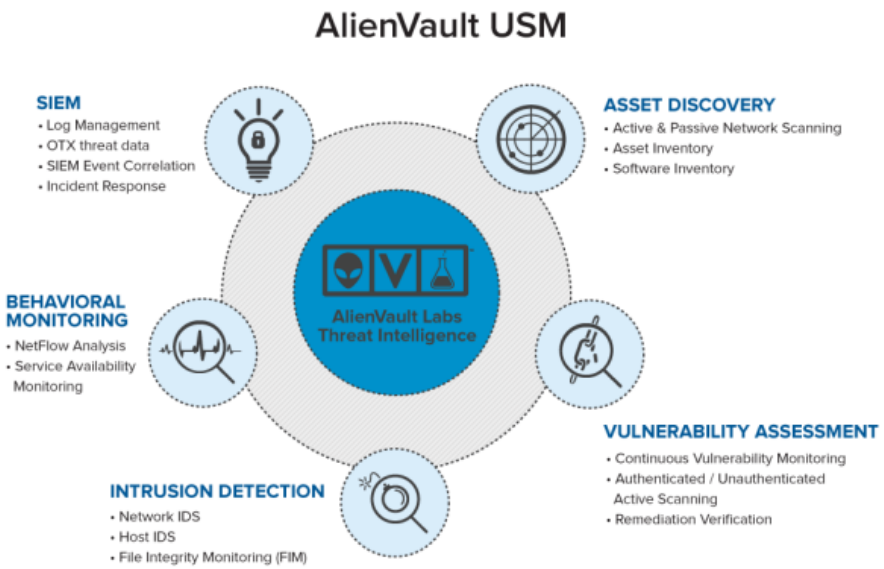


Figura 3.2: AlienVault USM
Fonte: AlienVault - Documentation Center [20]

- A descoberta de ativos utiliza ferramentas passivas, como a impressão digital do sistema operativo passivo e a descoberta de serviço passivo. A descoberta de ativos também utiliza o scanner da rede ativo, que pode ser programado para ser executado periodicamente ou executado manualmente.

- A avaliação de vulnerabilidades, que pode ser feita em modos não autenticados ou autenticados, identifica vulnerabilidades ou conformidade comparando o software instalado em ativos com uma base de dados de vulnerabilidades conhecidas. Com o *scanner* autenticado e o uso de uma conta de utilizador administrativo, o OSSIM pode verificar os ativos com mais eficiência. As verificações de vulnerabilidades também podem ser agendadas para serem realizadas periodicamente ou executadas manualmente.

- A deteção de intrusões monitoriza o tráfego de rede em busca de atividades mal-intencionadas, monitoriza as mensagens de registo do sistema e monitoriza a atividade do utilizador. A deteção de intrusão do OSSIM consiste em Host-based Intrusion Detection System (HIDS) e Network Intrusion Detection Systems (NIDS).

  O HIDS pode ser utilizado para detetar problemas em terminais de *hosts* e pode incluir monitorização de integridade de arquivos, verificações de *rootkit* e registo. As interfaces de deteção *sniffing* passivas do NIDS podem analisar dados de carga útil da rede para monitorizar atividades potencialmente mal-intencionadas.

- A monitorização comportamental fornece visibilidade sobre padrões de tráfego e fluxos de rede (dados do *NetFlow*), que são usados para detetar anomalias que podem indicar violações da política de segurança. Os dados usados para monitorização e análise comportamental são recolhidos de dispositivos de rede, fluxos baseados em tráfego espelhado *(Port mirroring)* e monitorização de disponibilidade de ativos.

- A inteligência de segurança do SIEM combina e correlaciona de *logs* coletados e outros dados para encontrar padrões mal-intencionados no tráfego da rede e na atividade do *host*.

Conforme informação da organização que desenvolve o produto [22], o AlienVault OSSIM aproveita o poder do AlienVault Open Threat Exchange® (OTX ™), permitindo que os utilizadores contribuam e recebam informações em tempo real sobre *hosts* maliciosos. Além disso, fornecem um desenvolvimento continuo do produto, porque acreditam na visão que todos devem ter acesso a tecnologias de segurança sofisticadas, para melhorar a segurança de todos.

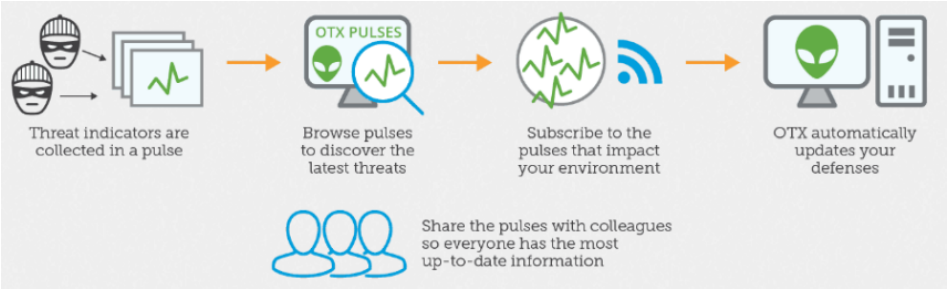


Figura 3.3: Fluxograma dos indicadores de comprometimento
Fonte: AlienVault - Documentation Center [20]

3.2 Tecnologia OTX

O AlienVault OTX é uma rede de análise a nível mundial de partilha de informações sobre ameaças. A OTX fornece acesso a uma comunidade global de investigadores de ameaças e profissionais da segurança de TI, com mais de 50.000 participantes em 140 países, que contribuem com mais de quatro milhões de indicadores de ameaças diáriamente. O OTX permite que qualquer pessoa na comunidade de segurança discuta, pesquise, valide e partilhe ativamente os dados, tendências e técnicas de ameaças mais recentes.

A comunidade OTX informa e recebe dados de ameaças em forma de pulsos. Um pulso OTX consiste num ou mais Indicadores de Comprometimento (IOCs) Figura 3.3 que constituem uma ameaça ou definem uma sequência de ações que podem ser usadas para realizar ataques em dispositivos e computadores de rede. Os pulsos OTX também fornecem informações sobre a fiabilidade das informações sobre ameaças, quem relatou uma ameaça e outros detalhes das investigações sobre ameaças.

O OTX reconhece, entre outros tipos, os blocos de endereços *IPv4*, *IPv6*, *Classless Inter-Domain Routing (CIDR)*, *Common Vulnerabilities and Exposures (CVEs)*, domínios, *hashes*, endereços de e-mail, nomes de *host* e *Universal Resource Identifier (URI) / Universal Resource Locator (URL)*.

Os membros do OTX recebem informações de pulso por Front-End Engineering and Design (FEED) de atividade do OTX, além de receber atualizações sobre os mesmos por email. Essas informações aparecem assim que se abre uma conta do OTX. Os dados OTX podem ser usados para aprimorar os recursos de deteção de ameaças, não apenas de sistemas de monitorização de segurança, como o OSSIM, mas também de outros sistemas de monitorização e gestão de segurança de terceiros.

O AlienVault também fornece um painel de controlo de ameaças global gratuito com tecnologia OTX, disponível em `https://www.alienvault.com/open-threat-exchange/dashboard#/threats/top` (ver Figura 3.4), que mostra alguns dos dados de ameaças provenientes da comunidade OTX. Pode-se visualizar um *feed* ao vivo de atividades maliciosas gravadas pelo

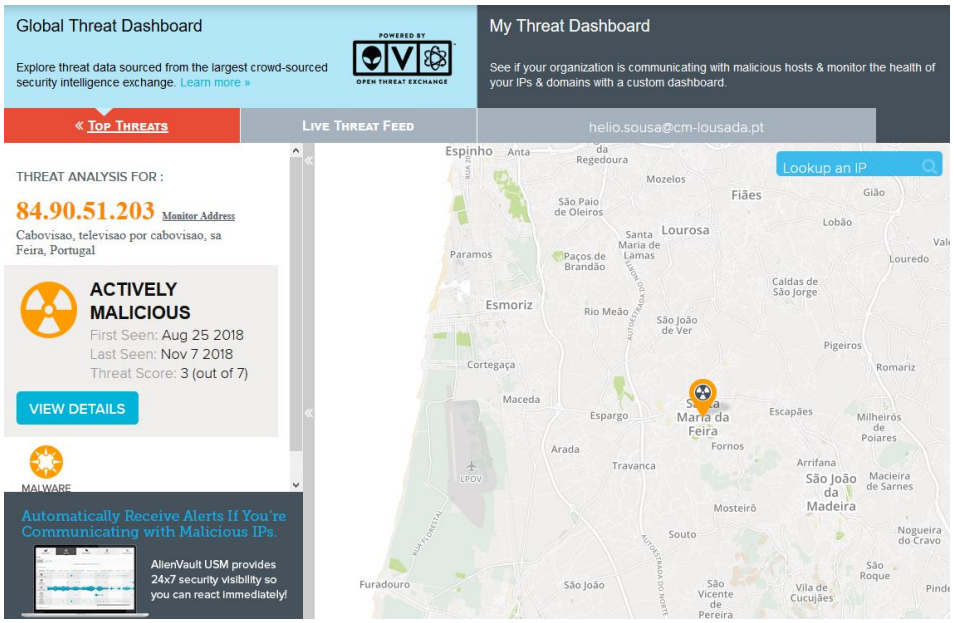


Figura 3.4: Global Threat Dashboard

OTX de todo o mundo e ver as principais ameaças ativas.

3.3 Características e ferramentas do OSSIM

O OSSIM é um sistema centralizado de eventos e gestão de informações de segurança, composto por diversas ferramentas de código aberto integradas e com o sistema operativo assente na distribuição GNU/Linux Debian. O OSSIM encontra-se na versão 5 e pode ser descarregado gratuitamente em: `https://dlcdn.alienvault.com/AlienVault\_OSSIM\_64bits.iso`

Algumas das ferramentas que integram o OSSIM são:

- **ArpWatch** - É uma ferramenta que monitoriza a atividade numa rede *ethernet*, mantendo atualizada uma tabela com endereços *ethernet* Media Access Control (MAC) e seus respetivos endereços IP. O Arpwatch é uma ferramenta importante na monitorização da rede contra ataques de Address Resolution Protocol (ARP), *Arp Poisoning* ou *Arp Spoofing* usados para realizar ataques mais sofisticados como *Man-in-the-Middle (MITM)* [23].

- **P0f** - Segundo Zalewski [24], é uma ferramenta que utiliza uma matriz de sofisticados mecanismos de impressão digital de tráfego puramente passivo, de forma a identificar os intervenientes por traz de qualquer comunicação Transmission Control Protocol/Internet Protocol (TCP/IP) acidental.

- **Nmap** - É uma ferramenta para descoberta de rede e auditoria de segurança. O nmap permite identificar quais os dispositivos que estão a ser executados nos seus sistemas, descobrindo os *hosts* disponíveis e que serviços correm, descobrindo portas abertas e detetando riscos de segurança [25].

- **Nessus** - É um dos scanners de vulnerabilidades mais populares e capazes da atualidade. O Nessus é uma ferramenta constantemente atualizada, com mais de 70.000 *plugins*. Os principais recursos incluem verificações de segurança remota e local, uma arquitetura cliente/servidor com uma interface web e uma linguagem de script incorporada para gravar seus próprios *plugins* ou compreender os existentes [26].

- **Snort** - É um sistema de prevenção de intrusões de código aberto capaz de analisar o tráfego em tempo real e o registo de pacotes. Snort pode ser configurado para operar em três modos de funcionamento nomeadamente: *Sniffer mode* - Lê os pacotes da rede e exibe-os continuamente na consola; *Packet Logger mode* - Regista os pacotes para disco; *NIDS mode* - Realiza deteção e analise no tráfego de rede [27].

- **Spade** - É utilizada para obter conhecimentos sobre os ataques sem assinatura. A ferramenta deteta conexões anómalas analisando as portas utilizadas e o destino.

- **Tcptrack** - É um *sniffer* que mostra as informações sobre conexões Transmission Control Protocol (TCP) num interface especifico para correlação de ataques. O tcptrack fornece informações úteis para os administradores rastrearem cada conexão única aos seus servidores. O tcptrack também tem um recurso de filtragem, ele utiliza o padrão de filtragem Packet Capture (PCAP) - idêntico ao usado no tcpdump.

- **Ntop** - É uma ferramenta para monitorizar e gerir sistemas de rede, além dos imensos recursos que providencia tem a capacidade de o demonstrar através de gráficos e informações detalhadas, permitindo uma melhor interação com o utilizador [28].

- **Nagios** - É uma ferramenta poderosíssima de monitorização de sistemas, permitindo às organizações identificar e solucionar problemas nas infraestruturas de TI antes de estes afetarem os processos críticos do negócio [29].

- **Osiris** - Host Integrity Monitoring System (HIMS) é utilizada para monitorizar equipamentos Windows e recolher em tempo real dados sobre alterações em arquivos utilizando *checksums*, alterações em portas, alterações de utilizadores e de *kernel*.

- **Snare** - É utilizado para monitorizar equipamentos Microsoft Windows e recolher em tempo real dados sobre criação, modificação e acesso de arquivos assim como utilização de Universal Serial Bus (USB), *Login*, *Logoff*, e, instalação e execução de programas.

- **Open Computer and Software Inventory Next Generation (OCS-NG)** é um *software* que permite inventariar os ativos de TI. O OCS-NG recolhe informações sobre o *Hardware* e o *Software* dos dispositivos conectados, executando um cliente de OCS - *OCS Inventory Agent"*. O OCS tem a capacidade de disponibilizar o inventário por interface web.

- **OSSEC** - É uma ferramenta de deteção de intrusão baseada em *hosts* que monitoriza *logs* de serviços e sistemas, faz verificação de integridade de arquivos, monitorização de políticas, deteção de *rootkits*, envia alertas em tempo real e resposta ativa, ou seja, permite a execução de uma ação baseada num evento [30]. O OSSEC é uma ferramenta muito granular e personalizável podendo correr praticamente em todos os sistemas operativos. O OSSEC possui quatro tipos de instalação, nomeadamente em modo Servidor, Local, agente e híbrido. No modo servidor ele atua como servidor do serviço, concentra toda a gestão e correlacionar os eventos, envio de alertas e resposta ativa.

  O modo Agente funciona basicamente como um encaminhador de eventos para o OSSEC server, onde os eventos serão analisados e correlacionados. Este Agente está otimizado para correr com uma menor impacto na maquina cliente, utilizando pouquíssimos recursos e necessitando de privilégios mínimos. As configurações do Agente podem ser maioritariamente realizadas pelo servidor de OSSEC.

  O modo Local basicamente é utilizado quando pretendemos usar o OSSEC em *Standalone*, sem pertencer a uma estrutura de servidor/-cliente. Todas as operações são realizadas localmente, analise e correlação de *logs*, verificação de arquivos, deteção de rootkits, envio de alertas e restantes funcionalidades.

  O modo Híbrido é o modo de operação mais recente da ferramenta, permitindo a uma infraestrutura de maior dimensão, balancear cargas dos servidores evitando que um OSSEC server fique em sobrecarga.

3.4 Ativos, Risco e Ameaças

O princípio fundamental do OSSIM é que ele monitoriza os ativos. Os ativos são todos os dispositivos de uma organização que tem valor para a mesma, normalmente, são ativos que podem ser monitorizados, recolher informações

sobre, status, integridade ou disponibilidade, configuração atividade e eventos. O valor prende-se com o custo do próprio dispositivo, o valor dos dados que ele armazena ou a informação que aí circula.

- Um ativo é definido como um endereço IP exclusivo.
- Os ativos são organizados em redes com base no endereçamento IP.
- As redes são organizadas em locais ou regiões, com base da sua localização geográfica.

Quando a nossa organizarão é geograficamente dispersa, geralmente recorre-se a utilização de pelo menos um sensor para monitorizar cada local geograficamente independente. Cada sensor monitorizará o seu site e enviará informações para o OSSIM server sobre os ativos que estão no mesmo local. *Plugins* são usados no Sensor OSSIM para extrair e normalizar dados de diferentes fontes de dados em eventos de formato padrão. O OSSIM fornece uma ampla variedade de *plugins* que podem ser usados para recolher eventos para as fontes de dados mais comummente encontradas. Podemos ativar até 10 *plugins* por ativo e até 100 *plugins* por Sensor.

Na maioria das organizações, as prioridades das operações de segurança de rede são determinadas principalmente pelo risco, ou seja, fatores como o valor dos ativos, o dano potencial que as ameaças específicas representam aos ativos e as vulnerabilidades desses ativos às ameaças e a probabilidade de que os ataques reais serão tratados.

No OSSIM os valores de risco são calculados para cada evento recebido do sensor OSSIM, bem como para eventos de segurança adicionais gerados como resultado de correlação ou correlação cruzada de vários eventos. O OSSIM gera um alarme para qualquer evento que tenha um valor de risco calculado maior ou igual a 1.

A fórmula usada pelo OSSIM para calcular o risco de eventos individuais é a seguinte:

$$Risco = (Ativo * Prioridade * Fiabilidade)/25$$

Na fórmula, Valor do Ativo é um valor compreendido entre **(0 e 5)** que a organização atribui a cada ativo. Prioridade de evento é uma classificação de prioridade compreendida entre **(0 e 5)** baseada no tipo de evento, como falha de autenticação, ataque na Web ou negação de serviço, que indica a urgência com a qual um evento deve ser investigado. A AlienVault fornece uma taxonomia de eventos para classificar vários eventos por categoria e subcategoria. Fiabilidade do evento é uma classificação de fiabilidade compreendida entre **(0 e 10**) que especifica a probabilidade de um evento ser um ataque real ou um evento falso positivo.

Ameaças e vulnerabilidades são o que correlacionam a ocorrência de certos eventos com o risco e geram alarmes quando os valores de risco dos

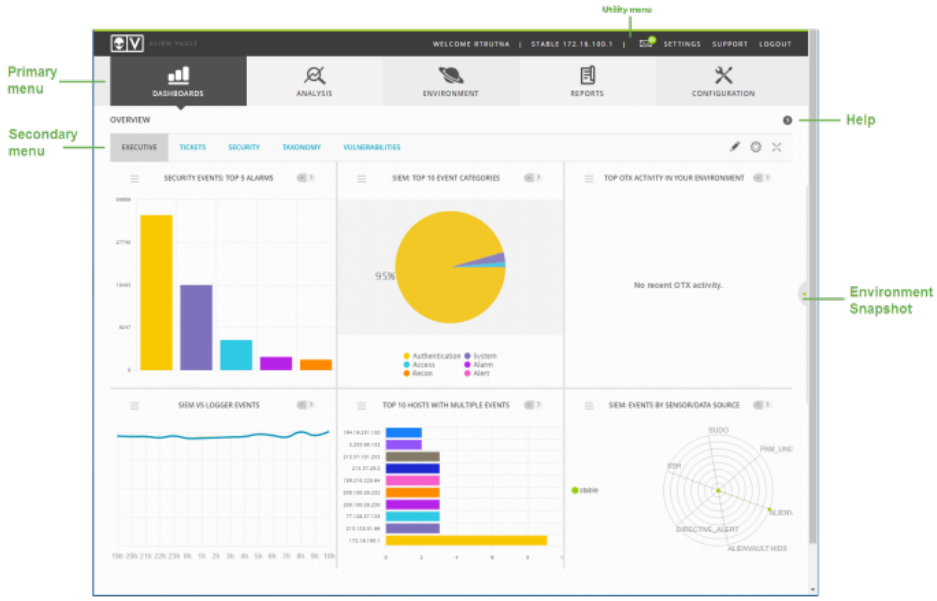


Figura 3.5: OSSIM frontend

eventos excedem um valor limite específico (maior que ou igual a 1). Informações sobre ameaças específicas são obtidas de fontes como as relatadas pelo AlienVault Labs e pelo OTX. Por exemplo, o OTX fornece indicadores de comprometimento e notificações de *hosts* maliciosos, que podem vincular ativos por suas vulnerabilidades a ameaças específicas e notificação sobre eventos que envolvam *hosts* mal-intencionados conhecidos ou suspeitos. O OSSIM também pode executar verificações que identificam as vulnerabilidades dos ativos a ameaças específicas e identificadas, pois como descrito no secção anterior, ele conta com um conjunto de ferramentas para executar este tipo de ações.

3.5 A Arquitetura

O OSSIM é composto por quatro blocos principais: sensores, *Management Server*, base de dados e *Frontend*[31]. Os sensores fazem a recolha da informação de segurança, de forma passiva, e de modo a não afetarem o tráfego da rede. Os sensores têm a capacidade também de recolher informação de *routers, firewalls e IDS/IPS*. O agente, incorporado no sensor, é o responsável pelo envio da informação ao *Management Server*. Por seu lado, o *Management Server* é o responsável por tratar, analisar e correlacionar informação com o intuito de encontrar atividades maliciosas. Faz esta análise com base em regras ou políticas de segurança. Na Base de dados são alojados todos os eventos e restante informação útil para a gestão do sistema.

O interface de utilizador *(Frontend)* é uma aplicação web que permite a visualização, parametrização e interação do utilizador com todo o OSSIM Figura 3.5.

A interface do utilizador é muito completa e fornece acesso a todas as ferramentas e recursos que o OSSIM disponibiliza para gerir a segurança da rede, dos computadores e de outros dispositivos da organização na rede. Na interface Web do utilizador pode-se visualizar todas as informações essenciais sobre dispositivos de rede, aplicativos, atividade do utilizador e tráfego de rede. À medida que se monitoriza informações vindas de dispositivos, pode-se definir e refinar políticas e diretivas de correlação para ajustar o comportamento do sistema OSSIM para alertar sobre possíveis problemas e vulnerabilidades de segurança.

3.6 Recolha de dados de *log*, análise e normalização

Os recursos de gestão de monitorização de segurança do OSSIM resulta da capacidade geral da recolha de dados de dispositivos, transformar os dados num conjunto comum de campos de dados que definem eventos e processar, filtrar e correlacionar esses eventos para identificar possíveis ameaças e vulnerabilidades, ou mesmo a ocorrência de ataques reais. O OSSIM avalia a importância dos eventos atribuindo valores de risco com base nos ativos subjacentes, na origem e natureza da ameaça identificada e na probabilidade de um ataque bem sucedido.

A recolha de *logs* está na raiz da gestão de segurança OSSIM. O OSSIM recolhe dados de várias fontes, dispositivos de rede, como *firewalls* e *routers*, servidores e sistemas *host* e aplicativos de software em execução nos servidores. Dispositivos que suportam o protocolo *Syslog* podem ser configurados para enviar seus registos diretamente para o OSSIM server evitando duplicação de informação e maior eficiência na gestão desses *logs*. Para outra tipologia de dispositivos o OSSIM utiliza várias formas para recolher essas fontes de dados.

Em ambas as situações, os dados de *logs* são normalizados para extrair e armazenar informações em campos de dados comuns que definem um evento; endereços de IP, nome do *host*, identificação do utilizador, nome do interface e outros de relevância. Estes são os eventos que o analista de segurança pode utilizar no OSSIM para descobrir ameaças e vulnerabilidades e avaliar o risco na organização.

Após instalação do OSSIM na organização, os eventos começam a fluir pelo OSSIM (ver Figura 3.6) e começamos a ganhar visibilidade sobre a atividade normal ou não ameaçadora e quais atividades preocupantes, indicando possíveis ataques que podem estar a ocorrer. O OSSIM Sensor combina deteção de ativos, avaliação de vulnerabilidade, deteção de ameaças e monitorização comportamental para fornecer reconhecimento completo da

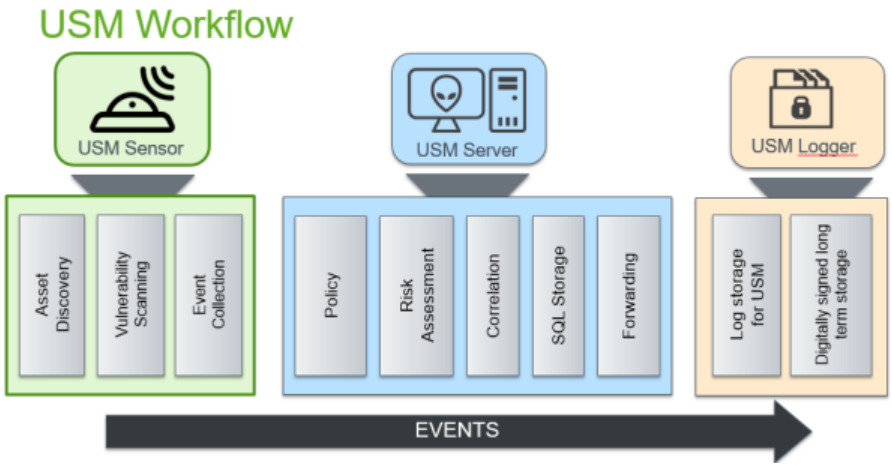


Figura 3.6: OSSIM *workflow*

situação. Este fornece visibilidade detalhada do ambiente da organização, vulnerabilidades, metas e vetores de ataque e serviços. Normaliza os dados de *log* brutos e outras informações de atividade ou *status* dos dispositivos num formato de evento OSSIM padronizado [**?**]. Esses eventos normalizados são então enviados para o componente OSSIM Server.

O OSSIM server fornece uma interface de gestão unificada web, que combina automação de segurança e inteligência de ameaças OTX e AlienVault Labs para correlacionar dados, identificar anomalias, reduzir riscos e melhorar a eficiência operacional [32]. Recebe eventos do OSSIM Sensor e executa a avaliação da política. A política define o que acontecerá com os eventos. Por padrão, os eventos são enviados para o mecanismo de correlação , a partir do módulo de avaliação de riscos, e armazenados numa base de dados SQL interno.

A correlação (ver Figura 3.7) pode ser feita logicamente, onde os eventos podem ser comparados a padrões e várias condições podem ser conectadas usando operadores lógicos como *OR* e *AND*. A correlação também pode ser calculada usando correlação cruzada, em que os eventos são correlacionados com os dados de vulnerabilidade. Depois dos eventos serem processados e correlacionados, o OSSIM server realiza análises de risco e dispara um alarme se o risco do evento for alto o suficiente.

A seguir podemos verificar um exemplo do funcionamento de uma diretiva de correlação (ver Figura 3.8). Esta diretiva é utilizada para detetar eventos de autenticação recorrendo a força bruta, ligando dois tipos de eventos, *login* bem sucedido e os sem sucesso. Neste exemplo baseado no número de ocorrências individuais o motor de correlação consegue perceber se um utilizador se enganou a digitar a sua *password* (um evento de *login* sem sucesso seguido de um bem sucedido) ou no caso de um ataque por força bruta

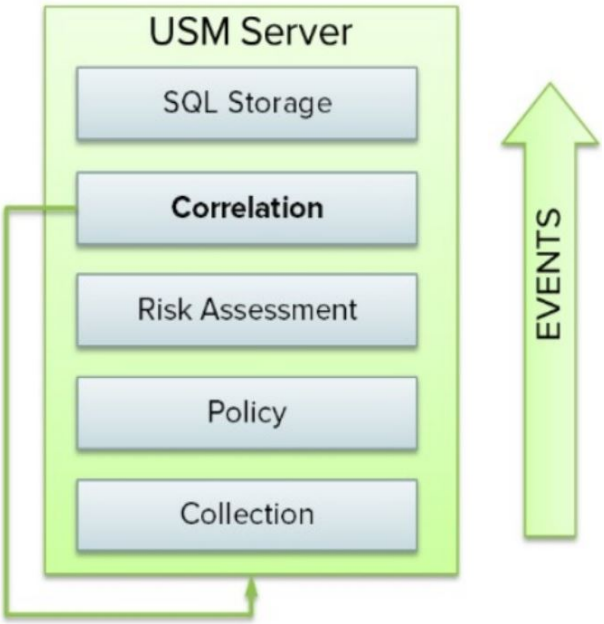


Figura 3.7: Mecanismo para efetuar registos de sistema

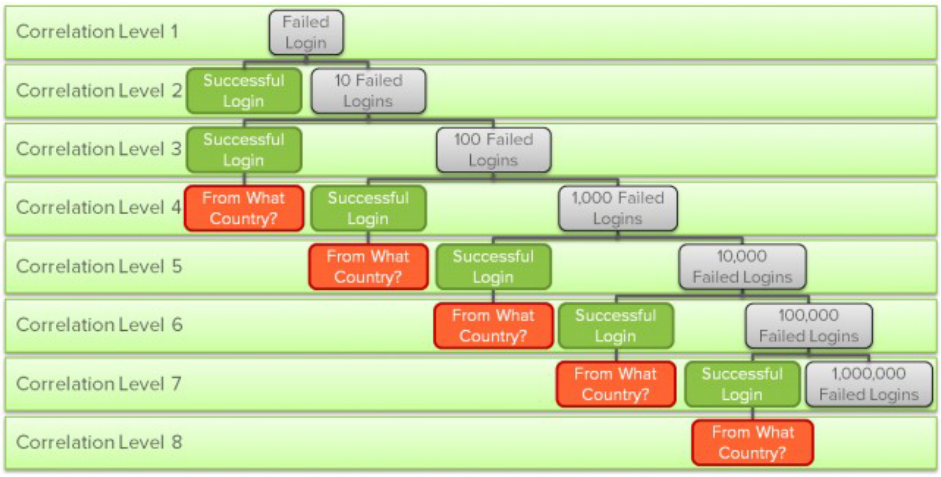


Figura 3.8: Controlo de entrada num sistema através de credenciais.

Figura 3.9: Painel geral OSSIM.

de alta fiabilidade em que ocorrem 100000 *logins* sem sucesso, seguido de um bem sucedido. Estes eventos devem ter origem no mesmo IP e serem destinados também a um único endereço IP de destino para que a diretiva seja criada. O motor de correlação também pode usar tabelas de reputação sobre os endereços de origem e destino a fim de gerar eventos de segurança.

3.7 *Dashboards*

O OSSIM apresenta um *dashboard* (ver Figura 3.9) parametrizável, desempenhando um papel de grande relevo na monitorização e análise de segurança do ambiente de rede da nossa organização, fornecendo visibilidade geral da atividade da rede e métricas de segurança da rede.

A exibição Visão geral mostra vários *widgets* (gráficos, tabelas e gráficos) que resumem vários aspetos da segurança da rede e outros status, atividades e eventos que ocorrem na rede. Opções adicionais da página Visão geral fornecem exibições do painel para Tickets, Segurança, Taxonomia e Vulnerabilidades.

- **Tickets** - Fornece métricas de tickets criados dentro do próprio sistema de tickets do OSSIM.

- **Segurança** - Fornece métricas sobre diferentes medidas de segurança no ambiente, por exemplo, *hosts* ativos, alarmes mais frequentes e tendências de relatórios de eventos de segurança.
- **Taxonomia** - Fornece métricas de eventos com base em diferentes classificações de eventos de taxonomia do OSSIM, por exemplo, deteção de vírus, *logins* bem-sucedidos e sem sucesso, *malware* e tipos de evento de exploração.
- **Vulnerabilidades** - Fornece métricas sobre características de vulnerabilidade, como gravidade e *hosts* mais afetados. Também exibe detalhes dos relatórios de digitalização disponíveis.

Cada *widget* no painel fornece sua própria representação de informações junto com uma legenda ou descrição de pontos de dados.

3.8 Políticas

O OSSIM utiliza políticas para configurar como os eventos são processados. As políticas definem uma ou mais condições que são avaliadas para cada evento de entrada para determinar se a ação associada é acionada. As políticas desempenham um papel fundamental na gestão da resposta efetiva a incidentes e influenciam muitos aspetos do OSSIM. As políticas usam condições para determinar quais os eventos a serem processados pela política e consequentemente para definir o que ocorrerá quando os eventos corresponderem às condições especificadas [33].

Há várias formas de utilizar políticas para gerir e controlar o processamento de eventos no OSSIM, dependendo das necessidades do utilizador, da organização e do fluxo de trabalho. Pode ser criada uma política para acionar automaticamente um e-mail para administradores ou outras pessoas sempre que ocorra um alarme de alto risco. Aumentar a importância de eventos específicos para um endereço IP específico ou uma porta específica, utilizando políticas para gerar um alarme sempre que ocorram eventos que incluam o endereço IP ou essa porta, sem gravar uma regra de correlação. Armazenar eventos no OSSIM sem correlaciona-los, quando por exemplo há o uso de um *honeypot* pela equipa de TI. A existência de um *honeypot* na rede, não precisa do OSSIM para gerar alarmes ao mesmo, pois este será atacado. Pode-se utilizar as políticas para filtrar os eventos para reduzir o número de alarmes criados.

Capítulo 4

Considerações para a implementação de um SIEM

Neste capítulo serão analisados os pontos chaves para se compreender as necessidades de monitorização de segurança de uma organização.

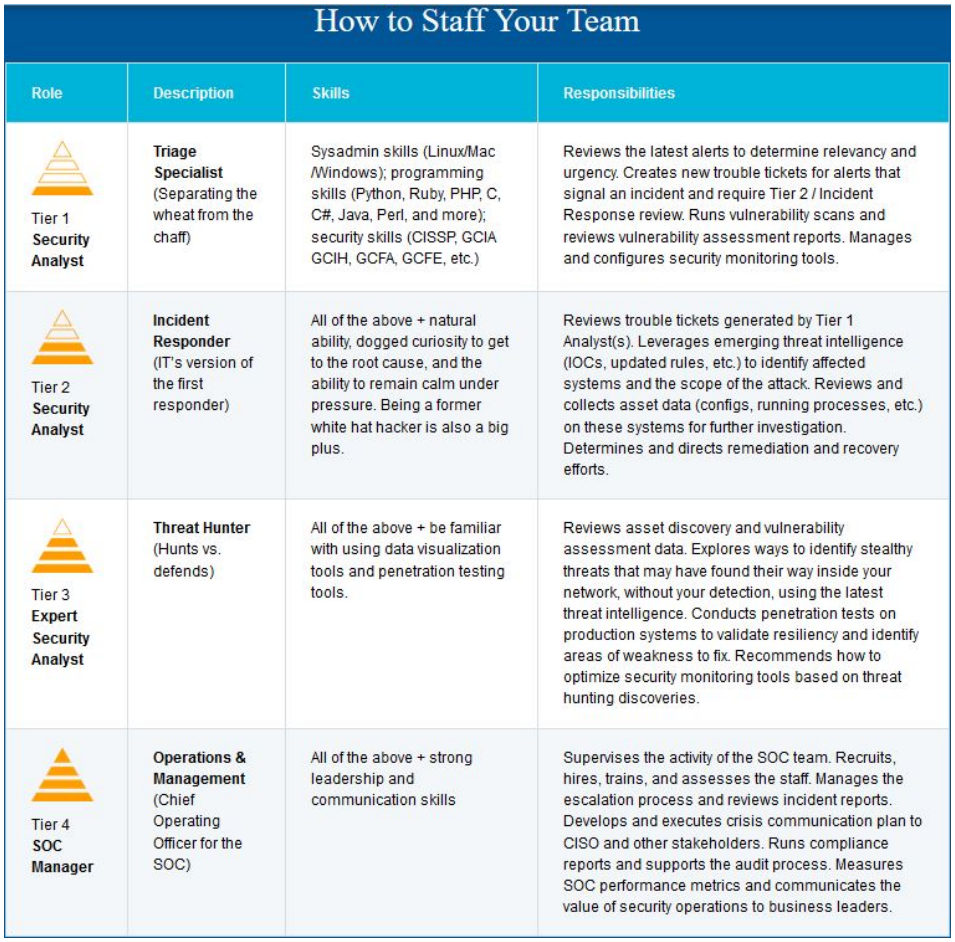
4.1 Planeamento e Pessoas

A fase de planeamento é de extrema importância e é também a fase mais extensa de um projeto de implementação de um SIEM. Segundo [34], os projetos de implementação de SIEMs continuam a ser repletos de dificuldades, com falhas graves no processo de implementação, acabando por não corresponder às expetativas iniciais.

Assim como as pessoas, todas as organizações são diferentes. Nalgumas empresas, a equipa de direção ou executiva, reconhece a importância da segurança cibernética para o resultado final no negócio, para o bom funcionamento da organização ou como uma questão legal e de transparência com o publico. Nesses casos, a equipa de TI está uma ótima posição, com orçamento suficiente para boas ferramentas, recursos humanos suficientes para geri-los, visibilidade e apoio do executivo. Infelizmente, esta não é a realidade na maioria das empresas.

A maioria da equipas de TI lutam diariamente para apagar "incêndios", com pessoas insuficientes, sem os recursos humanos com as competências adequadas, sempre sem tempo suficiente, certezas suficientes e visibilidade do que está ocorrendo. Por isto é importante consolidar as ferramentas já existentes e organizar efetivamente a equipa. Deverá ter como objetivo, dispor de uma equipa de TI que tenha as competências certas e utilize a menor quantidade de recursos, enquanto ganha visibilidade sobre ameaças ativas e emergentes.

Segue um exemplo, recomendação Alienvault Figura 4.1 sobre como poderemos organizar uma equipa de segurança com 4 a 5 membros. Sucinta-



How to Staff Your Team

Role	Description	Skills	Responsibilities
Tier 1 **Security Analyst**	**Triage Specialist** (Separating the wheat from the chaff)	Sysadmin skills (Linux/Mac /Windows); programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more); security skills (CISSP, GCIA GCIH, GCFA, GCFE, etc.)	Reviews the latest alerts to determine relevancy and urgency. Creates new trouble tickets for alerts that signal an incident and require Tier 2 / Incident Response review. Runs vulnerability scans and reviews vulnerability assessment reports. Manages and configures security monitoring tools.
Tier 2 **Security Analyst**	**Incident Responder** (IT's version of the first responder)	All of the above + natural ability, dogged curiosity to get to the root cause, and the ability to remain calm under pressure. Being a former white hat hacker is also a big plus.	Reviews trouble tickets generated by Tier 1 Analyst(s). Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack. Reviews and collects asset data (configs, running processes, etc.) on these systems for further investigation. Determines and directs remediation and recovery efforts.
Tier 3 **Expert Security Analyst**	**Threat Hunter** (Hunts vs. defends)	All of the above + be familiar with using data visualization tools and penetration testing tools.	Reviews asset discovery and vulnerability assessment data. Explores ways to identify stealthy threats that may have found their way inside your network, without your detection, using the latest threat intelligence. Conducts penetration tests on production systems to validate resiliency and identify areas of weakness to fix. Recommends how to optimize security monitoring tools based on threat hunting discoveries.
Tier 4 **SOC Manager**	**Operations & Management** (Chief Operating Officer for the SOC)	All of the above + strong leadership and communication skills	Supervises the activity of the SOC team. Recruits, hires, trains, and assesses the staff. Manages the escalation process and reviews incident reports. Develops and executes crisis communication plan to CISO and other stakeholders. Runs compliance reports and supports the audit process. Measures SOC performance metrics and communicates the value of security operations to business leaders.

Figura 4.1: Como organizar a equipa.
Fonte: Alienvault [20]

mente, existe a necessidade num primeiro nível a ser desempenhado por um Analista de segurança com a principal função de triagem, revendo os alertas mais recentes, determinando relevância e urgência. Este analista deverá utilizar ferramentas de *scanning* de vulnerabilidades e analisar os relatórios de avaliação de vulnerabilidades, escalando através de *tickets* de problemas ou incidentes que exijam nível de resposta nível superior.

Num segundo nível, um perfil idêntico ao do primeiro nível é exigido tendo como competências a resposta aos incidentes criados e escalonados pelo de primeiro nível. Correlaciona com informação sobre ameaças emergentes (IOCs, regras atualizadas, etc.) para identificar os sistemas afetados e âmbito dos ataques. Organiza esforços de remediação e recuperação.

Num terceiro nível, temos alguém que se preocupará em rever os novos ativos descobertos e avaliação de vulnerabilidades. Correrá testes de penetração em sistemas de produção para validar a resiliência e identificar áreas de fraqueza a serem corrigidas. Faz recomendações para otimizar as ferramentas de monitorização de segurança com base em resultados das descobertas alcançadas.

No topo da hierarquia, teremos um responsável de forma a supervisionar a equipa. O seu papel é de extrema importância pois será o responsável por fazer a ponte entre vários serviços, nomeadamente dando os relatórios com as métricas de desempenho e relevância da equipa para a organização aos líderes na organização/negócio.

4.2 Âmbito

Após consciencialização das recursos humanos e definidos os objetivos deve-se proceder à definição do âmbito. A abrangência do âmbito terá grande impacto em todo o projeto. A implementação de um SIEM é um projeto de grande abrangência, que deverá envolver múltiplas pessoas, pelo que, uma boa definição do âmbito terá um percentagem muito significativa no sucesso do projeto. Uma boa definição do âmbito ajudará na previsão de custos, dependências, requisitos e restrições.

O SIEM pode abranger todos os equipamentos da infraestrutura, ou apenas partes dela de acordo com os objetivos que se definiu anteriormente, sendo que duas funções criticas no projeto de um SIEM passarão por:

- Primeiro configurar as ferramentas de monitorização de seguranças para receber dados brutos relevantes para a segurança da organização (por exemplo, eventos de *login* / *logoff*, transferências de dados, permissões de *firewall*, etc.). Garantir que os dispositivos de críticos da infraestrutura (*firewall*, servidor de Base de dados, servidor de ficheiros, controlador de domínio, Domain Name System (DNS), email, web, etc.) estejam a enviar *logs* para o SIEM.

- A segunda função é utilizar essas ferramentas para encontrar atividades suspeitas ou mal-intencionadas, analisando alertas, investigando indicadores de compromisso (IOCs como *hashes* de ficheiros, endereços de IP, domínios, etc.), reavaliando e editando regras de correlação de eventos, realizando a triagem destes alertas, determinando a sua criticidade e impacto, partilhando as descobertas com a comunidade de inteligência contra ameaças, etc.

Nem todos os equipamentos têm a mesma relevância, considerando os resultados que se pretendem alcançar e as atividades que se pretendem monitorizar. Descartar informação inútil que esteja a ser registada pelos sistemas, é tão ou mais importantes para a implementação com sucesso do projeto, como a escolha dos ativos críticos da nossa rede. Assim não haverá degradação de performance do SIEM, não ocupando recursos no tratamento de informação menos interessante, e eliminar-se-á o tempo gasto em análise de alertas de pouca relevância.

4.3 Processos e procedimentos

Uma lista de verificação enumera todas as coisas que devem ser feitas para manter a segurança, evitar riscos e proteger a organização. Devem fazer parte dos principais processos de um projeto de implementação de um SIEM:

- **Classificação e Triagem de Eventos**

  O valor de recolher, correlacionar e analisar dados de registo, só é real quando se encontram sinais ou evidências [35]. Os principais indicadores de comprometimento podem ser encontrados dentro da atividade do utilizador, eventos do sistema, *firewall* / Anti-vírus, etc. Além disso, sequências específicas e combinações desses eventos em padrões específicos também podem sinalizar um evento que requer atenção. O sucesso é obtido ao conseguirmos obter uma forma de classificar cada evento rapidamente, para podermos priorizar e escalar eventos de criticidade elevada e que exijam investigação adicional.

  Aqui, os analistas de primeiro nível, analisam os eventos mais recentes que apresentam os de maior criticidade ou severidade. Depois de verificar esses eventos e estes exigirem investigação adicional, eles então irão escalar o problema para um analista de segurança de resposta a incidentes. Claro que numa equipa de menores dimensões, pode ter que ser o mesmo analista a investigar os problemas. O sucesso nesta etapa é documentar todas as atividades.

- **Priorização e Análise**

  O sucesso passa por identificar a atividade do invasor nos estágios iniciais de um ataque, antes que dados e sistemas confidenciais sejam

afetados [36]. À medida que um atacante avança nesses estágios da cadeia de destruição, fica mais provável e que eles sejam bem-sucedidos nos seus ataques. A priorização é a chave para o sucesso na segurança cibernética [37] [38]. As apostas são altas e o ritmo dos ataques continuam aumentando, não havendo sinais de abrandamento. Enquanto isso, os ativos que temos para proteger face aos recursos disponíveis são sempre limitados. Deste modo devemos dar atenção e concentrar esforços sempre nas ameaças e vulnerabilidades que possam criar mais impacto na organização, assim como nos ativos de maior criticidade da nossa infraestrutura. No final do dia, manter a continuidade do negócio é o mais importante para a organização e deverá ser a responsabilidade mais importante para a equipa de TI.

Ao priorizar os alarmes nas categorias corretas como exploração, instalação e comprometimento do sistema, os analistas conseguem escalar os incidentes para o nível certo, ou para as pessoas corretas, pois as ameaças em estado avançado, além das defesas de segurança primárias têm que ser contidas e remediadas o mais rápido possível, evitando maior consequências.

Neste processo é de extrema importância o conhecimento de todo o ambiente e ativos, sendo que a descoberta e inventário de ativos é um dos mais importantes e negligenciados recursos de segurança TI como referenciado pelos autores do Artigo [39]. Deverão existir rotinas de verificação contínua do ambiente, de forma a descobrir todos os ativos que devem ser monitorizados. Estes dispositivos deverão ser catalogados, verificado quais os *softwares* que disponibilizam assim como serviços que estão a ser executados e validar se incluem vulnerabilidades.

Algumas questões que se pode colocar que podem ajudar neste ponto.

- Quais os sistemas críticos para a operação contínua de empresa?
- Quais os sistemas críticos para as tarefas do dia-a-dia?
- Quais são os outros sistemas, dispositivos ou redes que estão dependentes os serviços críticos?
- Quais sistemas gerem ou armazenam informações confidenciais?

- **Remediação e Recuperação**

  Quanto mais rápido puder ser detetado e intervido, um incidente, maior será a probabilidade de conter os danos e evitar que um ataque semelhante aconteça no futuro. Várias decisões são tomadas ao investigar um incidente, principalmente se a organização está mais interessada em recuperar do dano/incidente ou de investigá-lo por crime. Deve ser realizado um trabalho em estreita colaboração com a equipa

de gestão. A comunicação deve ser realizada com clareza e frequentemente, assim como documentar tudo. Cada ataque será diferente em termos das etapas de correção apropriada, para aplicar nos sistemas afetados, mas normalmente envolverá uma ou mais das seguintes etapas:

  - Reposição de imagens de sistemas e restaurar backups.
  - *Patch* ou atualização de sistemas, exemplo: aplicativos e atualizações do sistema operativo.
  - Reconfiguração de acesso aos sistemas, exemplo: a eliminação de conta de utilizador, reconfiguração de *passwords*, etc.
  - Reconfiguração de acessos à rede, exemplo: regras de Access Control List (ACL), politicas de *firewall*, acessos Virtual Private Network (VPN), etc.
  - Revisão dos ativos monitorizados e realização de ajustes, exemplo, configuração de sistema HIDS, etc.
  - Validação dos procedimentos de *patch* e outros controlos de segurança existentes, recorrendo a *scanners* de vulnerabilidades.

- **Avaliação e Auditoria**

  É importante encontrar e corrigir vulnerabilidades antes que alguém mal intencionado as explore de forma a obter acesso ao ambiente corporativo da organização. Uma forma de o fazer, passa por executar avaliações periódicas de vulnerabilidades e reavaliar essas descobertas em detalhes [40]. Estas avaliações identificarão vulnerabilidades técnicas, nunca esquecendo que as vulnerabilidades podem ser de carácter procedimental, também podendo expor e comprometer a organização.

Existe uma longa lista de atividades que o departamento de TI necessita de fazer, e fazer corretamente, para que os ativos da organização sejam protegidos e para que ameaças de criticidade elevada sejam detetadas rapidamente e com impacto mínimo.

4.4 Criar um plano de resposta a incidentes

Segundo Richard Bejtlich [41] um incidente é um evento não planeado que requer medidas de investigação, de tempo e recursos para o corrigir. Eventualmente, um sistema interno para classificação de incidentes, será a medida com a qual a maioria das organizações devem iniciar.

Os incidentes no mundo da segurança normalmente implicam que uma parte hostil externa ou mesmo interna tenha acesso não autorizado, ou controlo de sistemas que suportam os processos centrais da organização [42].

Figura 4.2: 6 fases de resposta a incidentes
Fonte: https://www.sans.org/

Muitas organizações podem ficar comprometidas por muito tempo antes de serem descobertas.

Segundo a SANS [43] assim como o artigo Computer security incident handling [44], referenciam seis fases principais de um Plano de Resposta a Incidentes, nomeadamente, Preparação, Identificação, Contenção, Erradicação, Recuperação e Lição aprendida (ver Figura 4.2).

Como o objetivo final de um plano de resposta a incidentes não é apenas abordar efetivamente incidentes únicos, mas também identificar possíveis ameaças originadas de uma sequência de eventos ou incidentes que poderiam ser usados para realizar um ataque mais amplo. Ter um plano, completo com procedimentos e processos para lidar com diferentes cenários é importante, porque, mesmo que se aceite que nada irá acontecer de acordo com o planeado, ele ainda fornecerá uma lista de verificação valiosa e será referência para tudo que precisa ser realizado. Isto poderá fornecer um valor acrescido inigualável, especialmente durante momentos de crise quando toda a gente fica sobre stress e o raciocínio poderá não ser o mais coerente.

Algumas organizações de segurança e grupos de normas diferentes publicam recomendações ou diretrizes para os processos de resposta a incidentes que as empresas devem seguir para a investigação, remediação ou mitigação de incidentes de segurança de rede e acompanhamento. Essas recomendações geralmente incluem elementos muito semelhantes a:

- **Preparação** Preparar a equipa de TI e uma equipa de resposta a incidentes com recursos, procedimentos, prioridades e escalonamento para lidar com possíveis incidentes, caso eles ocorram. Implementação e monitorização da configuração para estabelecer o comportamento de linha de base, configurando alarmes, eliminando falsos positivos.
- **Análise, deteção e identificação** Desenvolvimento de ferramentas e fornecimento de instruções e procedimentos específicos para analisar incidentes, analisar sua gravidade, identificar explorações reais e

potenciais associadas a incidentes, determinar a prioridade e possível escalonamento na correção ou mitigação de ameaças e vulnerabilidades.

- **Contenção, Erradicação e Recuperação** Diretrizes para isolar sistemas afetados por incidentes de segurança, para evitar mais danos, localizar e eliminar a causa raiz dos ataques e remediar ou atenuar as ameaças. Permitir que os sistemas afetados voltem ao ambiente de produção após resolver os problemas e monitorizar os sistemas para futuros incidentes repetidos.

- **Atividade pós-incidente e lições aprendidas** Recolha de dados pós-incidentes e relatórios após a resolução de problemas. Documentação das atividades e resultados no tratamento de incidentes e manutenção de registos para avaliações de conformidade. Revisão e discussão com todos os membros da equipa de resposta a incidentes, para melhorar os futuros esforços de resposta a incidentes.

Capítulo 5

Caso de uso C.M.Lousada

5.1 Enquadramento da instituição

A instituição na qual se desenvolve o projeto, Figura 5.1, concelho que está inserido na região do Vale do Sousa, é um concelho com uma população maioritariamente jovem. É um concelho com um crescimento e desenvolvimento sustentados e com uma grande margem de progressão.

5.1.1 História

O topónimo Lousada deriva do antigo latim "(Villa) Lausada", ou seja, a quinta das lousas. Segundo informação oficial do site do site da autarquia, o concelho caracteriza-se por[45]:

O concelho de Lousada localiza-se no noroeste de Portugal – unidade natural definida pelo predomínio dos caracteres atlânticos, na região geográfica do Minho, estando situado no seio do distrito do Porto.

Possui uma superfície de 94,89 km^2 de área, que se encontra subdividida em 25 freguesias. Tem como limites administrativos, a norte, o concelho de Vizela; a nordeste, Felgueiras; e a este, Amarante; a sudeste e sul Penafiel; a sudoeste, Paredes, a oeste, o concelho de Paços de Ferreira e, por último,

Figura 5.1: Instituição - CM Lousada

a noroeste, Santo Tirso.

A matriz económica do concelho de Lousada encontra-se ainda fortemente marcada pela agricultura, embora o desenvolvimento de outros sectores económicos se comecem afirmar, nomeadamente o têxtil e, mais recentemente, a reorganização da produção vinícola.

A área onde se implanta o concelho lousadense, apesar da pretensa homogeneidade, apresenta-se profundamente marcada pela orogenia, o que permite individualizá-la do quadro Minhoto, interiormente, pelas características muito próprias do vale do Sousa, que lhe conferem uma certa unidade espacial.

No concernente aos recursos aquíferos, Lousada é um concelho beneficiado pela natureza. Abundantemente irrigado, o seu território é abrangido por duas grandes bacias hidrográficas. Na parte mais setentrional do concelho, com limite na serra dos Campelos, temos a bacia hidrográfica do rio Ave, de que são subsidiários o rio Porto e a ribeira de Sá, que nascem na citada serra; a restante área concelhia é ocupada pela bacia hidrográfica do Sousa, tendo como subsidiários um conjunto alargado de ribeiros e regatos. O rio Sousa nasce em Friande (Felgueiras) e é subsidiário do rio Douro, desaguando em Foz do Sousa, freguesia do concelho de Gondomar.

A situação litológica de Lousada caracteriza-se por uma cobertura quase total de rochas granitóides, que corresponde ao extenso cordão orientado NW-SE, que se estende do Minho às Beiras.

Do ponto de vista climático, o concelho implanta-se numa região de influência atlântica, para o qual muito contribuem os corredores naturais dos rios Sousa e Mezio, traduzindo-se deste modo num clima temperado marítimo húmido, a super húmido, de invernos e verões com variações climáticas de tipo fresco a moderado, com temperaturas médias anuais entre 10-12,5º.

5.1.2 Enquadramento dos serviços TI na organização

Na Figura 5.2 apresenta-se parte da organização interna da Câmara Municipal de Lousada, com particularidade dos serviços de TI aqui identificados como Serviços de Sistemas de Informação e Comunicação (SSIC). Os SSIC do Município de Lousada têm um responsável do serviço com funções de gestão e coordenação do mesmo. Estes serviços inserem-se no Departamento de Obras Municipais e Ambiente tendo como responsável um Diretor, reportando este diretamente à Presidência do Município. Os SSIC são constituídos atualmente por 7 colaboradores, sendo que os recursos Humanos afetos aos serviços dividem-se, um cargo de chefia e duas equipas de três colaboradores cada, com competências e responsabilidades diferentes, sendo as principais sintetizadas nos pontos apresentados de seguida com base em documento interno:

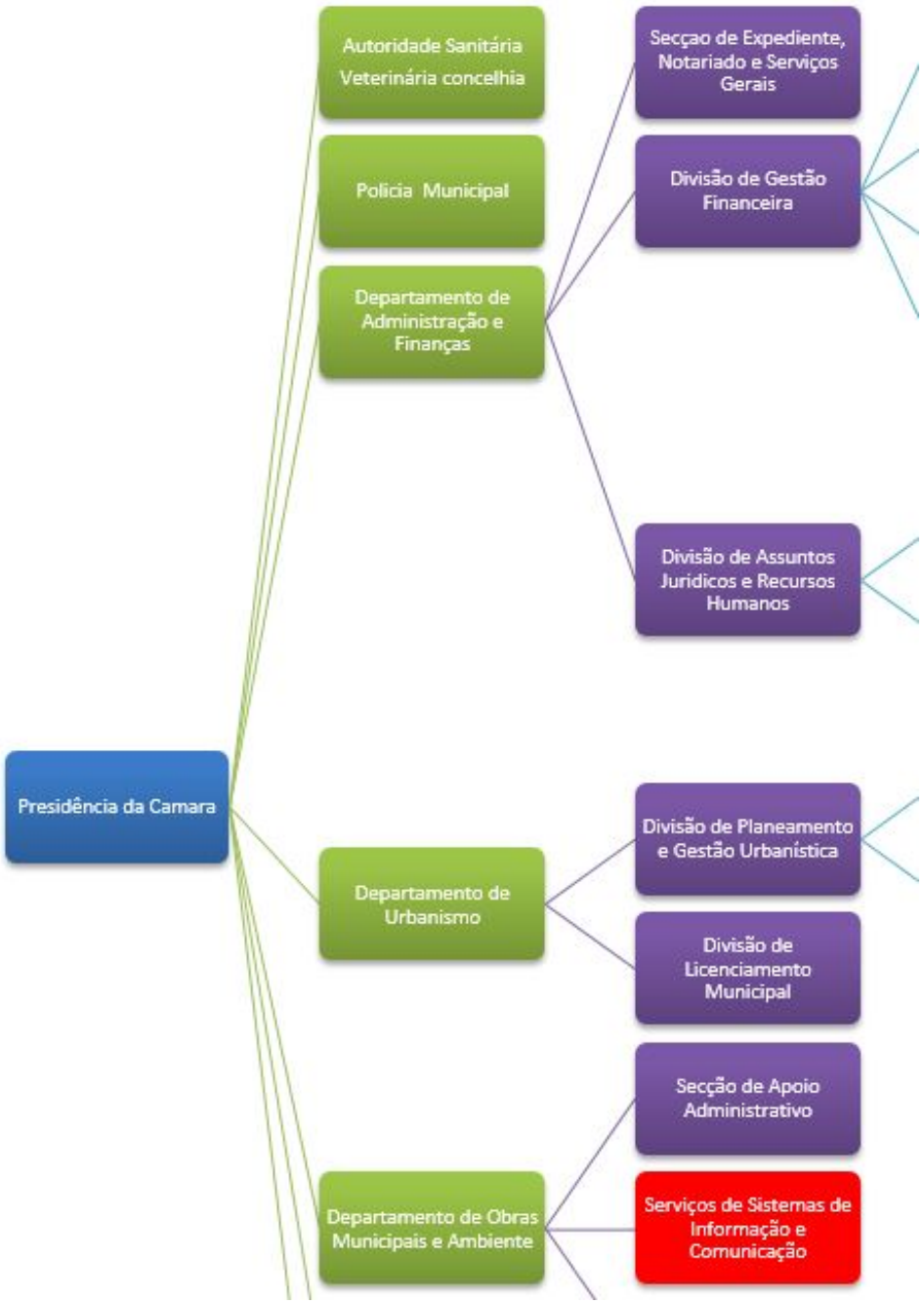


Figura 5.2: Organograma CM Lousada

- Equipa de Modernização e Sistemas de Informação
  - Garantir a manutenção, o desempenho do *ERP* de gestão autárquica do Município (Aplicações SIGMA Medidata), dando suporte à operação otimizando-o de acordo com as necessidades de utilizadores e cidadãos;
  - Garantir o Suporte técnico em *Helpdesk* do *ERP* de gestão autárquica do Município (Aplicações SIGMA Medidata) bem como da Gestão Documental e outras aplicações;
  - Gerir e aperfeiçoar continuamente os Portais, melhorando a oferta de serviços online disponíveis e criando incentivos e facilitando o uso de serviços eletrónicos;
  - Aumentar a oferta de serviços em novos canais de atendimento, nomeadamente através de utilização serviços de atendimento online e de aplicações para smartphones;
  - Desenvolver em coordenação com as necessidades indicadas pelas restantes orgânicas e executivo municipal, ferramentas e plataforma de análise de dados e apoio à decisão.
- Equipa de Administração de Sistemas, Infraestruturas e Comunicações
  - Gestão de redes de dados da autarquia ao nível de *switching* e *routing*;
  - Gestão e manutenção dos postos trabalho dos colaboradores (computadores). Compete-lhes assegurar a gestão e manutenção dos equipamentos, garantindo o seu correto e normal funcionamento. Devem assegurar o planeamento da substituição/reparação dos equipamentos elaborando relatórios de apoio a decisão com vista à planificação da aquisição de equipamentos, componentes, software e serviços para assegurar o funcionamento contínuo da infraestrutura técnica da autarquia;
  - Gestão e manutenção do parque de servidores físicos e virtuais, assegurar a correta implementação das políticas de segurança definidas e garantir a execução das tarefas de atualização e cópia de segurança de todos os sistemas;
  - Gestão e manutenção do Sistema de comunicações IP (VOIP) implementado na autarquia, devendo garantir o seu correto e normal funcionamento;
  - Gestão e manutenção dos equipamentos informáticos instalados nas escolas e Jardins de infância sobre a tutela da autarquia, bem como da definição de políticas de segurança e normas de utilização destes.

O presente projeto insere-se nas funções e competências atribuídas à equipa de Administração de Sistemas, Infraestruturas e Comunicações. A equipa suporta os ativos internos da CM Lousada totalizando aqui neste segmento de rede por volta dos 500 dispositivos, desde equipamentos de segurança (*Firewall's, IDS, VPN,* Sistemas de controlos de acesso fisico às instalações, etc), servidores (*Activity Director (AD), DNS, Dynamic Host Configuration Protocol (DHCP)*, *Radius*, WebServers, Aplicacionais, Base de dados, *Backup*, Arquivos, Impressão, etc.), cluster de servidores, *Storages*, *Routers, Switche's, Access Point's*, Sistemas de vigilância, etc. Ativos de rede externa de utilização pública, estando disponíveis para consulta e lazer do público, totalizando aqui cerca de 50 computadores e cerca de 50 dispositivos para acesso wireless, segurança, *switching e routing.* Por último e não menos importante, a rede de escolas espalhada por todo o concelho, que conta com 26 sites remotos, quer sejam jardins de infância, escolas básicas ou centro escolares, no global com cerca de 400 equipamentos ativos.

5.2 Levantamento da infraestrutura

A rede é segmentada tanto ao nível 2 Open System Interconnection (OSI), com recurso a Virtual Local Area Networks (VLAN), como ao nível 3. Incluí ainda *firewalls*, programas anti-vírus, servidores de autenticação (Lightweight Directory Access Protocol (LDAP) e *Radius*) e acessos remotos por VPN. Todos estes dispositivos e tecnologias geram eventos que ficam registados isoladamente nas suas plataformas, não existindo uma correlação entre os mesmos. Também não existe uma plataforma que possibilite uma visão unificada e centralizada do estado da rede. Cada solução tem a sua própria consola de gestão.

A instituição para a qual se apresenta esta proposta de solução possui uma infraestrutura de rede e sistemas como se pode ver na Figura 5.3, com mais de 1000 ativos onde se incluem computadores fixos, servidores, telefones IP, *switches, routers*, entre outros, ligados entre si através de uma rede maioritariamente cablada. Os edifícios geograficamente separados estão dotados de conetividade em fibra ótica própria da instituição, assim como de algumas ligações rádio redundantes á exceção do parque escolar onde existe alguns acesso *VPN* e *software* de gestão para acesso remoto.

5.3 Proposta de Solução

A infraestrutura física de cablagem e equipamentos de *networking* constitui um ponto crítico no bom e estável funcionamento do sistema informático, sendo por isso extremamente importante a sua correta configuração e otimização. Os equipamentos de segurança e servidores que suportam o funcionamento da organização assim como servidores ou serviços dos quais estes

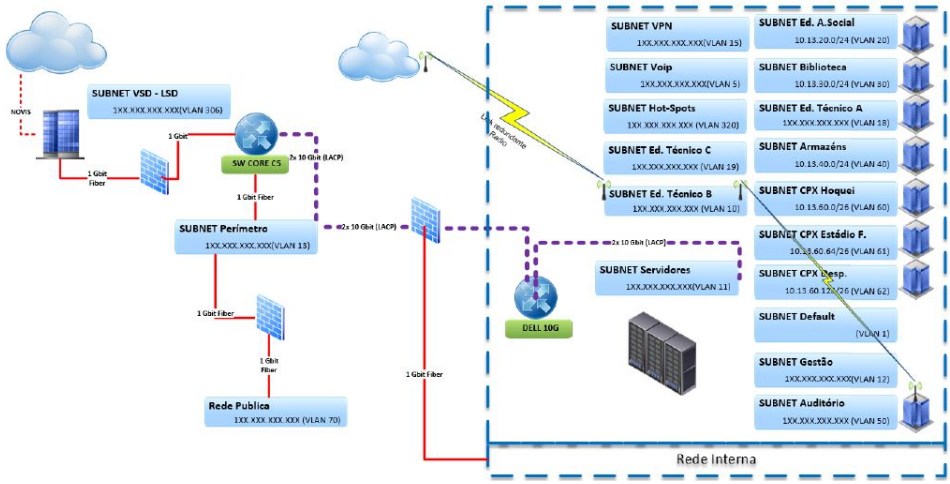


Figura 5.3: Diagrama de rede

dependem, foram identificados de forma criteriosa, sendo estes os que alimentarão com os seus *logs* o sistema SIEM a implementar. Com base nos objetivos pretendidos para a organização, face às limitações de carácter financeiro e de escassos recursos humanos para o desenvolvimento do projeto, assim como a literatura analisada, propôs-se a instalação e configuração do SIEM OSSIM. Deste modo e neste ponto não haverá necessidade de verbas financeiras para avanço do projeto.

Para testar a solução sem criar impactos na rede organizativa, decidiu-se instalar um protótipo em ambiente virtual, proceder à sua configuração para recolha, monitorização e análise de tráfego de um ponto da rede, assim como a sua integração com dois servidores de criticidade baixa. Desta forma a solução poderia ser validada sem grandes impactos no ambiente de produção da organização. Após realização deste cenário inicial, e validado o seu sucesso, será implementado em ambiente produtivo o SIEM OSSIM .

Pretende-se, como tal, dotar a infraestrutura existente de uma solução SIEM de forma a recolher os logs dos servidores, dispositivos de segurança, dispositivos de rede, atividades nas aplicações principais, informação de vulnerabilidades e atividade de utilizadores, e tratar os dados de forma a catalogá-los por perigosidade e apresentar a informação realmente importante à equipa de administração de sistemas. A proposta de solução como se pode verificar na Figura 5.4, passa então pela implementação de SIEM com Requisitos de Alta Disponibilidade, dois servidores OSSIM, em redundância, configurados para receberem uma cópia de todo tráfego de rede com origem na rede pública, na rede interna e na rede core.

Como se verifica na Figura 5.4, existirá a necessidade de instalação de sistemas NIDS em pontos estratégicos da rede possibilitando a análise de todo o tráfego. A localização da instalação do NIDS é um ponto importante

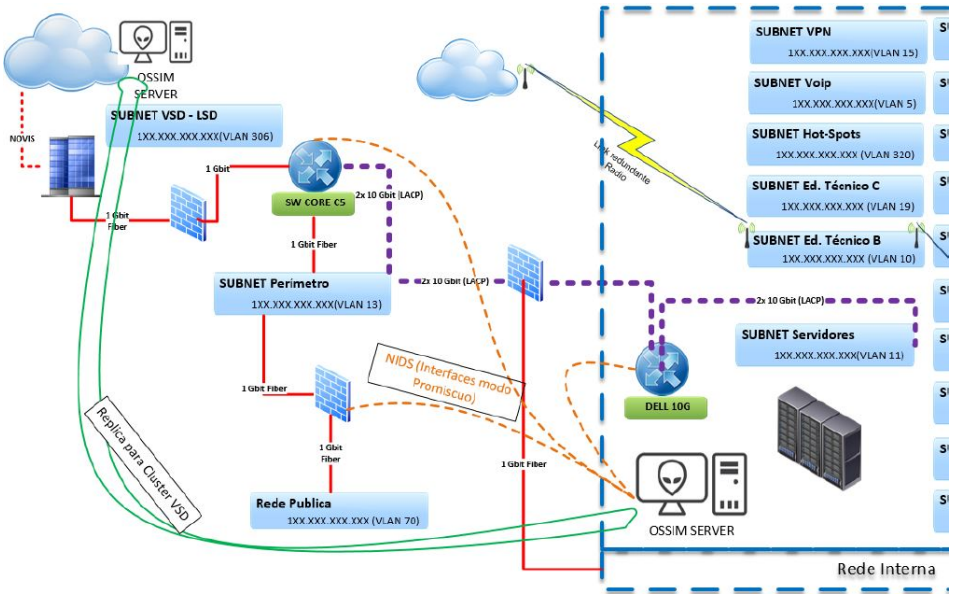


Figura 5.4: Diagrama de rede

assim a forma como receberá o tráfego a monitorizar.

Atendendo à quantidade de sistemas existentes na organização e prevendo a existência de uma quantidade elevada de tráfego a circular na rede, optou-se pela instalação dos sistemas de NIDS no OSSIM server, com a interface em modo promíscuo e os equipamentos de *switch* a replicarem todo o tráfego de todas as portas para encaminharem para o interface do NIDS. De forma a recolher mais informação e poder eliminar falsos positivos, definiu-se configurar em modo promíscuo as portas à entrada da *Firewall*, no link para o Internet Service Provider (ISP) como à entrada da rede, permitindo avaliar a realidade do tráfego nos dois lados da rede.

Tal permite suprimir a necessidade de monitorizar todo o tráfego da rede interna, da rede pública, assim como dos pontos de acesso wireless dispostos pelo concelho. Permitirá ainda monitorizar todos os eventos gerados pelo servidor de autenticação AD, pelas *firewalls* e sistema de anti-vírus.

O OSSIM inclui a funcionalidade de IDS e os sensores já vêm devidamente configurados para integrarem os eventos com a plataforma de SIEM. Assim, serão instalados os componentes de sensor do OSSIM, como resposta à necessidade de analisar o tráfego da rede, e instalados agentes OSSIM nos controladores de domínio e nos servidores que detêm as aplicações consideradas críticas para a instituição. O sistema, de forma a garantir a sua disponibilidade e resiliência, será configurado em modo réplica.

5.4 Implementação

O OSSIM server foi implementado no edifício dos Serviços Técnicos, sendo este o edifício central de toda a estrutura da Câmara. Este edifício é constituído por 5 pisos, estando nele inserido todos os serviços de atendimento ao público, bem como quase todos os departamentos da estrutura organizativa do Município.

Todo o suporte de comunicações do edifício assenta numa infraestrutura de rede de cablagem estruturada, com cabos do tipo Unshielded Twisted Pair (UTP) – Categoria 5E. A organização de toda a rede de comunicações do edifício assenta em 3 bastidores que fazem a distribuição das comunicações por todos o edifício sendo o presente projeto implementado na sala aqui identificada como "Bastidor A". A nível de comunicação, estes bastidores estão ligados por fibra ótica e por *switches ópticos Gigabit Ethernet*. A ligação aos diversos pontos de acesso é feita através da rede de cablagem estruturada e de *switches – FastEthernet*. Para garantir uma maior flexibilidade, economia de espaço e energia optou-se pela instalação do OSSIM server num ambiente virtualizado.

As entidades públicas, privadas e os cidadãos estão dependentes do funcionamento ininterrupto da tecnologia de informação e comunicações. Isto apenas é possível com a implementação de medidas de segurança, que passa pela criação da alta disponibilidade de todos os sistemas de tecnologias de informação, acompanhados por uma supervisão e formação de todas as pessoas que lidam com dados e recursos sensíveis. Por questões de salvaguarda da confidencialidade e quebra de segurança, não serão descritas ao pormenor todas as políticas e mecanismos de segurança aplicados.

5.4.1 Bastidor A

Esta sala é de acesso reservado através de fechadura mecânica com sensor biométrico e cartão Radio Frequency Interference (RFI), registando todos os acessos físicos à mesma, com climatização redundante, alimentação elétrica com quadro próprio e alimentação por gerador a gasóleo. Esta sala conta com 3 bastidores de *rack*, estando organizado do seguinte modo:

- 1 bastidor para cablagens de conetividade para todos os equipamentos de rede.
- 1 bastidor para ativos de rede *(switchs e routers)*.
- 1 bastidor para servidores.

Além dos bastidores, a sala contempla duas secretárias com um *desktop* e um portátil funcionando como suporte à instalação e configuração de novos equipamentos, assim como centro de crise para resolução de problemas

Figura 5.5: Bastidor A

Dell PowerEdgeR515	
CPU	2xAMD Opteron 4280, 8C, 2.8GHz
RAM	128GB Memory for 2CPU 1600MHz
RAID	PERC H200, Internal Controller for 8x HDD
Storage	3 x300GB SAS 15k (Raid 1 + Hot-Spare) + 2 x 500 SSD
Power	750 Watt Redundant Power Supply (2 PSUs Included)
Lan1	2 x Gigabit Port Cooper
Lan 2	1 xIntel® X520 DA2 Dual Port SFP+ 10GbE Server Adapter

Tabela 5.1: Dell PowerEdge R515

Dell PowerEdge R710	
CPU	2 x CPU Intel XeonQuad Core E5520
RAM	48GB DDR3-1600 RDIMM ECC
Storage	3 x 300GB SAS 15k (Raid 1 + Hot-Spare)
Power	750 Watt Redundant Power Supply(2 PSUs Included)
Lan1	2 x Gigabit Port Cooper
Lan 2	1 x Intel® X520 DA2 Dual Port SFP+ 10GbE Server Adapter

Tabela 5.2: Dell PowerEdge R710

críticos que possam ocorrer nos servidores ou infraestrutura de redes. Algumas imagens ilustrativas da infraestrutura são apresentadas na Figura 5.5

5.4.2 Instalação da plataforma

Nesta fase do projeto foi efetuada toda a componente de instalação e configuração base de todos os componentes da arquitetura anteriormente definidos. De forma a compreender toda a implementação apresenta-se os componentes utilizados ou equipamentos intervenientes para a implementação do projeto, como as suas principais caraterísticas.

Os requisitos de *Hardware* para correr o OSSIM server são baixos, segundo a AlienVault [21] 2GB de memória Random-Access Memory (RAM) e um espaço de armazenamento de 200GB são os requisitos mínimos recomendados para correr a solução. Ressalva-se que a quantidade de eventos gerados assim como a quantidade de tráfego, definirá a necessidade de ajustes dos recursos de *hardware*.

Identifica-se nas Tabelas 5.1, 5.2, 5.3 e 5.4 os principais recursos e suas características que fazem parte direta da instalação do OSSIM e seus dependentes.

Como referido anteriormente, de forma avaliar a solução, inicialmente foi realizada uma instalação e configuração da solução num ambiente minimalista, após validação deste passou-se à instalação do ambiente de produção. O ambiente de inicial de avaliação mantém-se em funcionamento como cenário

Switch Dell Force10 S4810P
Switch c\48 portas SFP+ e 4 QSFP 40GbE Ports
1,28Tbps switch fabric capacity
Switching latency: 800ns
40GB stacking, Jumbo Frames e DCB
Fontes de alimentação Redundantes
Cpu memory: 2GB

Tabela 5.3: Switch Dell Force10 S4810P

Switch Enterasys C5K175-24
Layer 3 Switch
24 x Gigabit Ethernet SFP
2 x 10 Gigabit Ethernet SFP+
Fontes de alimentação Redundantes
Switch Core

Tabela 5.4: Switch Core - Enterasys C5K175-24

de testes.

Alguns ajustes no *hardware* do município foram realizados, sendo que com as alterações realizadas ficou-se com o equipamento da Tabela 5.1 para correr a versão de ambiente de testes, ambiente de produção e outros servidores necessários. Neste equipamento físico optou-se por instalar e configurar o *VMware vSphere Hypervisor* (ESXi) na versão 6.5 Figura 5.6. Uma tecnologia de virtualização baseada em *Hypervisor*. O *Hypervisor* é a plataforma de processamento de virtualização que permite que múltiplos Sistemas Operativos partilhem uma única plataforma de hardware. Isto permitiu aproveitar os recursos de todo o equipamento, dando-nos a flexibilidade necessária para correr os vários ambientes.

Na plataforma de virtualização foram configurados vários tipos de armazenamento, sendo que os volumes mecânicos suportam os ambientes de teste, por estes serem menos críticos e requererem menos desempenho. Os volumes em Solid State Disk (SSD) configurados em *mirroring*, suportam os ambientes de produção oferecendo a resiliência esperada e o performance adequado a este tipo de ambiente.

A nível de *networking* foram realizadas as seguintes configurações dentro da plataforma de virtualização, de forma suportar ambos os ambiente (ver Figura 5.7). Foram criados 2 *virtual switches* identificados como "Switch 10G_01_Blue"e "Switch 10G_01_Red. Ambos os *virtual switches* funcionam sobre placas de 10Gbit, eliminando qualquer tipo de congestionamento de rede e evitando ser um ponto de*Bottleneck*.

Foi configurado um interface de rede e segmentada em VLANs, sendo

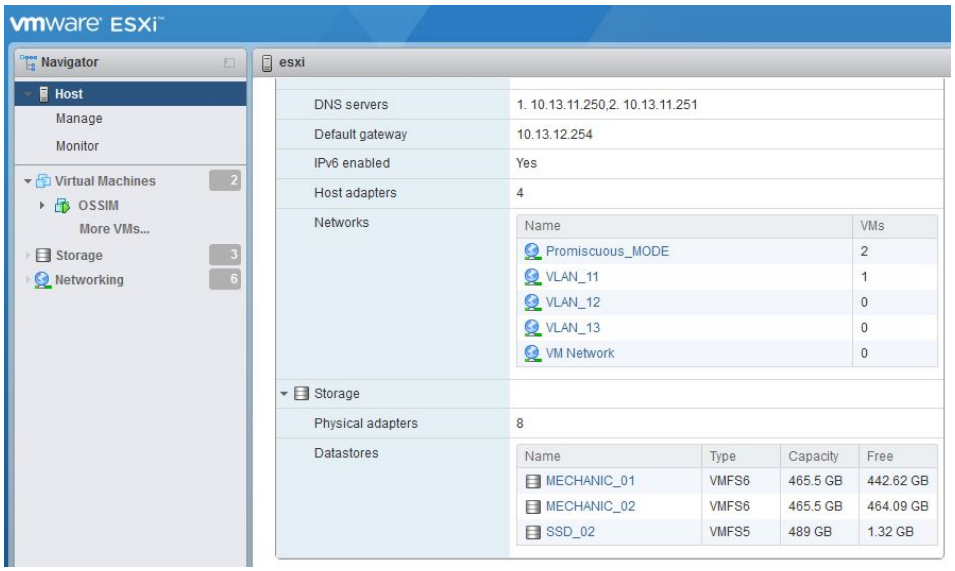


Figura 5.6: VMware vSphere Hypervisor (ESXi) V6.5

este o interface de gestão e comunicação do OSSIM server. Foi criado um interface no equipamento 5.3 na mesma VLAN e mesma rede, sendo este a *Gateway* para que o OSSIM comunique com as restantes redes e VLANs. Foram configuradas as respetivas portas inerentes a toda a comunicação em *untagging mode* ou *trunk*, assim como ACL de forma que tráfego desta VLAN proliferasse em toda a rede. Uma segundo interface foi configurado em modo Promíscuo (ver Figura 5.8), sendo conectado fisicamente através de um Direct Attach Cable (DAC), interligando o interface físico "Intel® X520 DA2 Dual Port SFP+ 10GbE"com o switch de core 5.4. No switch de *core* 5.4 foram configuradas as portas, à entrada do tráfego na rede, link de dados do ISP, assim como a porta após passagem pela *firewall* de perímetro em modo *mirroring*, fazendo que todo este tráfego fosse de igual forma replicado para o interface em modo promiscuo no OSSIM server.

Tendo o ambiente preparado como descrito nas secções anteriores, procedeu-se a instalação do OSSIM server. Este processo está bastante automatizado e é realizado através dum *wizard* com Graphical User Interface (GUI), onde se vai colocando os parâmetros do que se pretende, sem a necessidade de recorrer à Command Line Interface (CLI). Como nota relevante pode-se identificar que no mesmo instalador existe a opção de instalar o OSSIM server e a versão OSSIM sensor.

Após a instalação, o OSSIM server dispõe de um GUI na consola que permite parametrizar e gerir o equipamento, (ver Figura 5.9). Um ponto de extrema importância desde a instalação para colocação em produção do OSSIM é a configuração do servidor de Network Time Protocol (NTP). A exatidão dos relógios dos sistemas é de vital importância para a segurança,

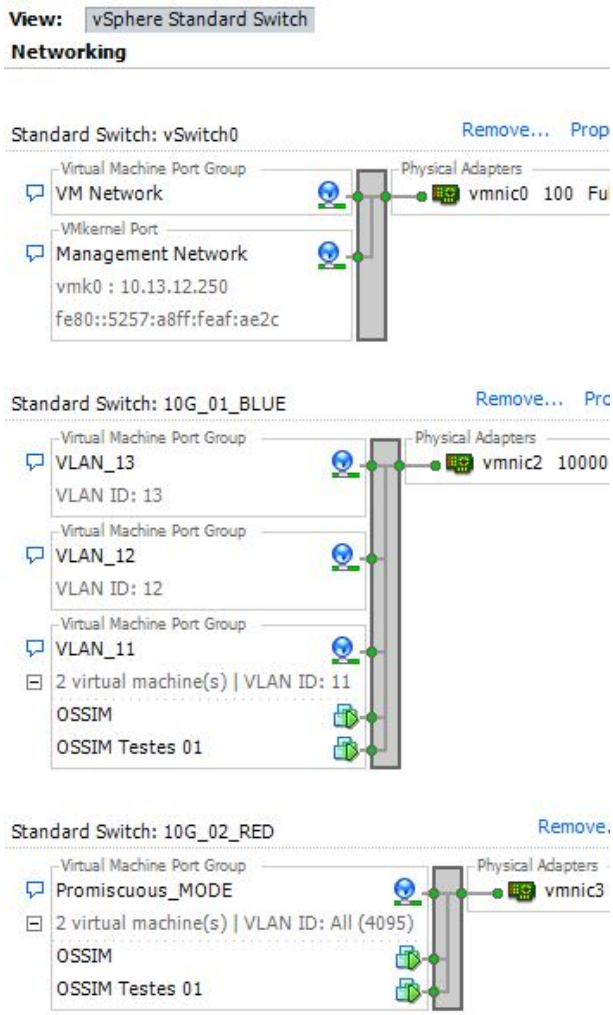


Figura 5.7: Rede em - vSphere ESXi starndard switch

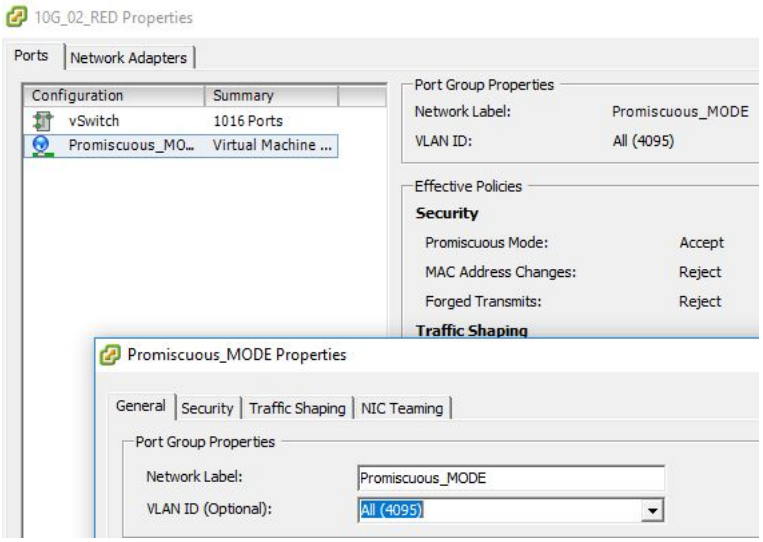


Figura 5.8: Interface modo promiscuo - vSphere ESXi

Listagem 5.1: Enterasys Port Mirroring

```
C5(su)->show port mirroring
Port Mirroring
==============
Source Port      = ge.1.16
Target Port      = tg.1.25
Frames Mirrored = Rx and Tx
Port Mirroring status enabled
Source Port      = ge.1.18
Target Port      = tg.1.25
Frames Mirrored = Rx and Tx
Port Mirroring status enabled
```

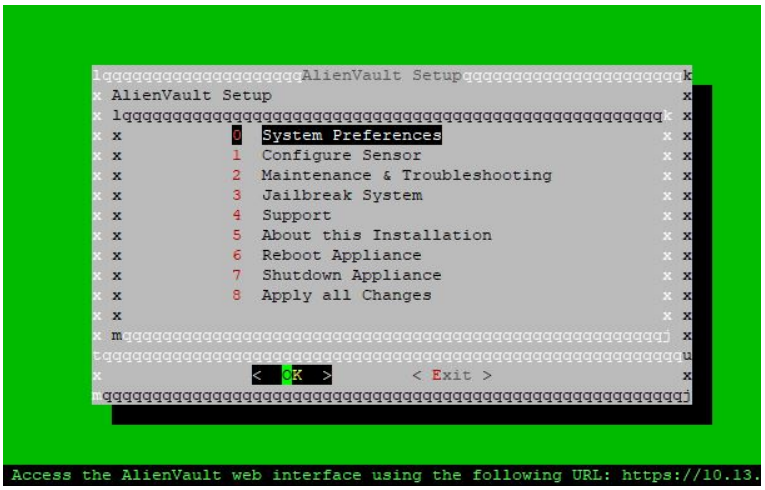


Figura 5.9: Interface GUI OSSIM

principalmente para o tratamento de incidentes de segurança. Relógios exatos, devidamente sincronizados com servidores NTP fiáveis, permitem manter a consistência dos logs, o que é imprescindível nas investigações e identificação de responsáveis, assim como a possibilidade de reconstruir historicamente um evento ocorrido. A organização interna dispõe dos próprios servidores de NTP, tendo sido estes utilizados e configurados no OSSIM. No final da instalação de forma a configurar os interfaces de rede como descrito na secção anterior, procedeu-se a essa alteração ficando da seguinte forma:

Listagem 5.2: /etc/network/interfaces

```
Starting shell
alienvault:~# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet manual
   up ifconfig $IFACE 0.0.0.0 up
   up ip link set $IFACE promisc on
   down ip link set $IFACE promisc off
   down ifconfig $IFACE down
auto eth1
iface eth1 inet static
```

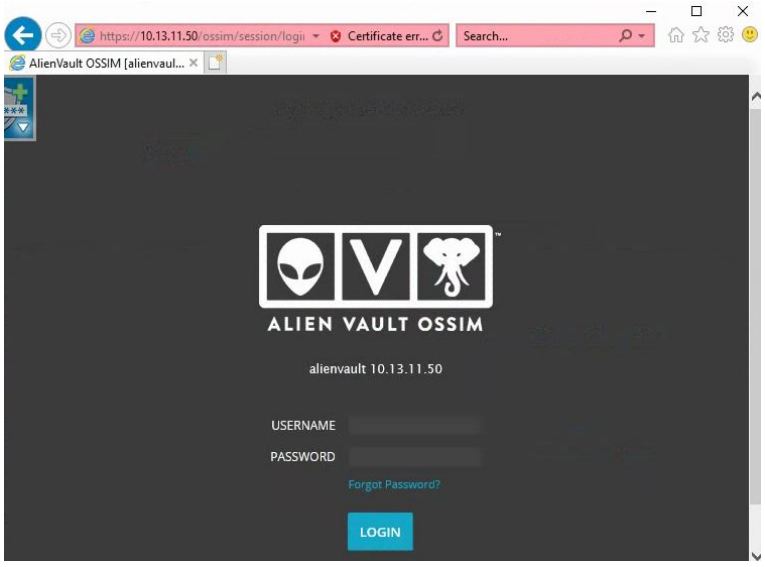


Figura 5.10: Interface Web OSSIM

```
address 10.13.11.50
netmask 255.255.255.0
network 10.13.11.0
broadcast 10.13.11.255
gateway 10.13.11.254
dns-nameservers 10.13.11.250
dns-search alienvault
```

Terminado os passos da instalação passou-se à configuração do OSSIM server. O OSSIM server como elencado no capitulo da descrição da ferramenta, dispõe de um FrontEnd acessível por *Web browser*, Figura 5.10 acessível pelo endereço de gestão configurado anteriormente.

Foram criados vários utilizadores com diferentes níveis de acesso como se verifica na Figura 5.11. De salientar a flexibilidade de atribuição de permissões e parametrização dos mesmos, permitindo criar utilizadores com acesso somente a determinados menus do *dashboard*,*"Allowed Menus"* como utilizadores que somente têm aceso a determinados ativos dentro da nossa infraestrutura, em "Assets Filters". Foi criado um utilizador "TV"onde este tem visibilidade somente sobre determinados dashboards, dos quais faz parte um esquema lógico da rede, mostrando em tempo real a disponibilidade e degradação de serviços dos servidores críticos da infraestrutura, assim como os pontos de rede críticos, estando disponível numa TV de 42"polegadas, dando uma maior visibilidade à equipa de infraestruturas do estado atual da rede.

Após a criação e disponibilização das credenciais aos utilizadores que

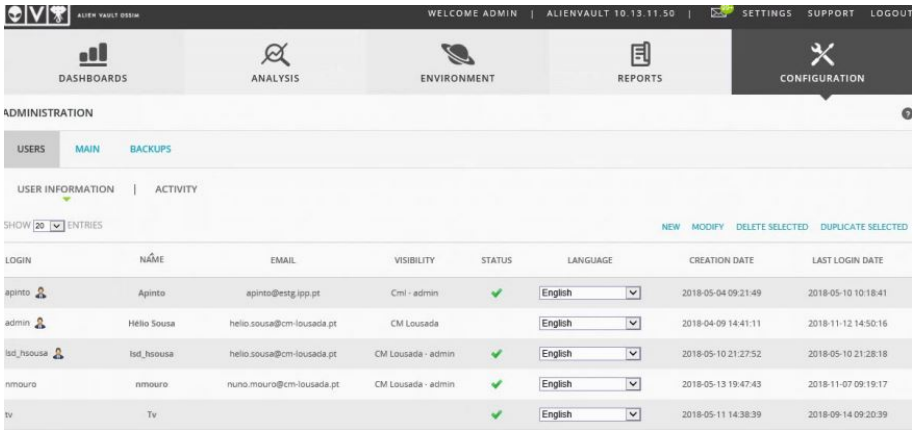


Figura 5.11: Administração OSSIM - Configuração de Utilizadores

terão acesso ao OSSIM procedeu-se às configurações de outros parâmetros de algum relevo nomeadamente:

- ***Backup*** - Foi criada uma política de cópias e segurança da base de dados a ser executada no período noturno a partir da 1:00, tendo sido definido como a retenção de 5 dias das configurações de sistema, política já utilizada internamente com outros sistemas servidores. Definiu-se manter os eventos na base de dados por um período de 15 dias, sendo um valor razoável para a equipa poder, havendo necessidade olhar para o evento. O tempo de expiração dos alarmes foi definido em 45 dias. Também neste ponto foi definido uma password de encriptação dos backups, de forma a somente poderem ser utilizados por pessoas devidamente autorizadas. As políticas de cópia de segurança aqui definidas são o resultado de ajustes ao longo do tempo, de acordo com a validação de necessidades, de consulta de eventos antigos, quantidade de eventos e alarmes em aberto assim como espaço ocupado pela quantidade de informação, logs em análise,

- ***Password Policy*** - Foi definido uma política de password de forma a cumprir com as normas do Regulamento Geral sobre a Proteção de Dados (RGPD), requisitos mínimos, nomeadamente:

  - Dimensão - Mínimo de 9 caracteres e um máximo de 16
  - Histórico - A password não deverá ser repetida num período de 1 ano.
  - Bloqueio conta - Bloqueio automático de conta de utilizador após 5 tentativas sem sucesso de autenticação.
  - Duração de bloqueio - Desbloqueio automático da conta após 60 minutos.

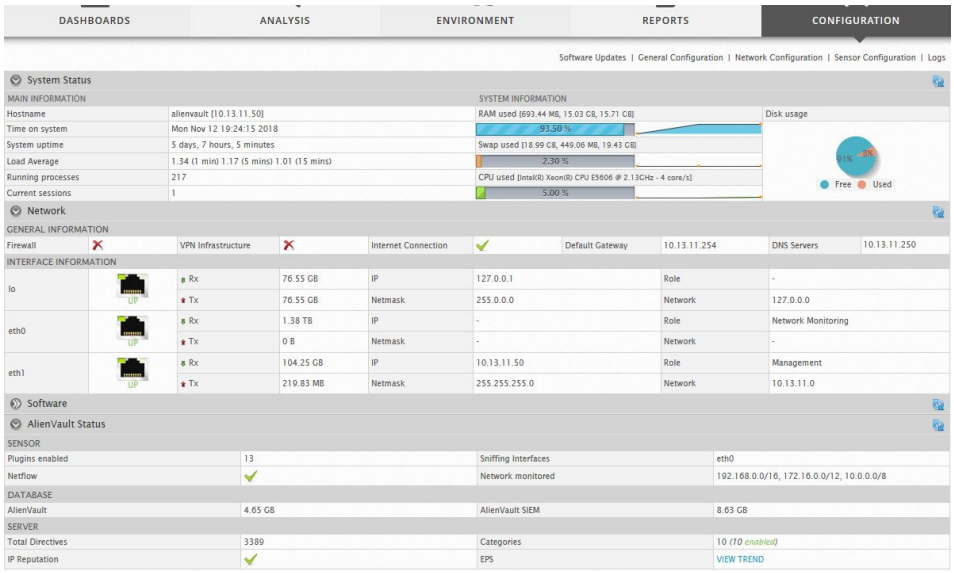


Figura 5.12: Administração OSSIM - Deployment

  - Complexidade - Ser uma password forte: Requer 3 características das 4 identificadas:
    * Caracteres minúsculos (a – z)
    * Caracteres maiúsculos (A - Z)
    * Números (0-9)
    * Caracteres especiais (@ $ % ^ * - _ ! + = [ ] — : ‘ , . ? / ‘ “ ( ) ;)

- ***NetFLOW*** - Foram definidos parâmetros que servem de base, para aplicação de políticas de correlação, nomeadamente valores para TCP e User Datagram Protocol (UDP) tanto para download e upload.

Aqui neste ponto, foram também realizadas e ajustadas outras configurações como *user login timeout*, configurações bases do sistema de *tickets*, métodos de autenticação, atividades dos utilizadores, servidor de Simple Mail Transfer Protocol (SMTP) e seus parâmetros para o envio de notificações, etc.

As configurações gerais relativas ao OSSIM server também podem ser realizadas diretamente no ficheiro ossim_setup.conf localizado na diretoria /etc/ossim/. Aquando qualquer tipo de alteração, estas só surtirão efeito após reiniciar os serviços, podendo ser realizado através do comando *ossim-reconfig*.

No menu *Deployment*, como se verifica na Figura 5.12, dá-nos uma visibilidade sobre o estado do sistema, assim como a possibilidade de o parametrizar. Neste menu consegue-se verificar de forma fácil e intuitiva os

seguintes dados:

- Estado de todos os componentes do sistema.
- Consumos de memoria RAM, (Atual e médias históricas).
- *Uptime* do sistema.
- Utilização do processador, (Atual e médias históricas).
- Ocupação do armazenamento.
- Utilização de tráfego por interface.
- Necessidades de *updates*.
- Quantidade de *plugins* ativos.
- Total de diretivas existentes e suas categorias.
- Informação gráfica, atual, diária, mensal e anual dos Events Per Second (EPS).

Com base nesta informação, o sistema foi sendo ajustado principalmente no que concerne aos recursos de Central Processing Unit (CPU) e memória *RAM*, resultando num dimensionamento para a atualidade de 4 virtual cores em termos de CPU e 16 GB de memoria *RAM*. Relativo a espaço em disco, verifica-se que os 500GB de armazenamento atribuído cumpre para já com as necessidades do sistema.

Ainda nas configurações gerais, foram realizadas várias ajustes ao sistema, sendo neste menu onde se procedem a *updates* de software, alterações de configuração de componente *networking*, configuração de sensores e consulta de *logs* das vários componentes que compõem a aplicação, nomeadamente os *logs* de sistema, dos sensores, da componente web e do Servidor. No que concerne a atualizações, seja do próprio core do sistema do OSSIM, assim como toda a panóplia de ferramentas embutidas na aplicação, a AlienVault lança em muitos curtos períodos de tempo imensos *updates*, sendo possível de uma forma fácil a sua atualização através deste menu.

A configuração dos sensores é realizada aqui também, onde se procedeu a ativação de vários *plugins* para recolha de dados, nomeadamente do HIDS, NIDS, availability_monitoring, etc. Aqui podemos encontrar um total de 478 *plugins* disponíveis pela ferramenta, sendo possíveis de ativar e configurar. Todos os *plugins* encontram-se no diretório /etc/ossim/agent/-plugins/, e as configurações aqui executadas ficam registadas no ficheiro /etc/ossim/agent/config.cfg como se pode verificar de seguida assim como os *plugins* ativos no sistema em produção.

Procedeu-se ao registo de uma conta de utilizador para a posterior integração dos *feeds OTX*, permitindo aos sistema detetar ataques ou tentativas

Listagem 5.3: /etc/ossim/agent/plugins/

```
alienvault:~# cat /etc/ossim/agent/config.cfg | grep
    plugins
[plugins]
apache=/etc/ossim/agent/plugins/apache.cfg
aruba=/etc/ossim/agent/plugins/aruba.cfg
dell-force=/etc/ossim/agent/plugins/dell-force.cfg
dhcp=/etc/ossim/agent/plugins/dhcp.cfg
iis=/etc/ossim/agent/plugins/iis.cfg
kaspersky=/etc/ossim/agent/plugins/kaspersky.cfg
kaspersky-sc=/etc/ossim/agent/plugins/kaspersky-sc.cfg
kaspersky-sc-db=/etc/ossim/agent/plugins/kaspersky-sc-
    db.cfg
nagios=/etc/ossim/agent/plugins/nagios.cfg
nmap-monitor=/etc/ossim/agent/plugins/nmap-monitor.cfg
ossec-single-line=/etc/ossim/agent/plugins/ossec-
    single-line.cfg
ping-monitor=/etc/ossim/agent/plugins/ping-monitor.cfg
softether=/etc/ossim/agent/plugins/softether.cfg
squid=/etc/ossim/agent/plugins/squid.cfg
suricata=/etc/ossim/agent/plugins/suricata.cfg
whois-monitor=/etc/ossim/agent/plugins/whois-monitor.
    cfg
wmi-monitor=/etc/ossim/agent/plugins/wmi-monitor.cfg
```

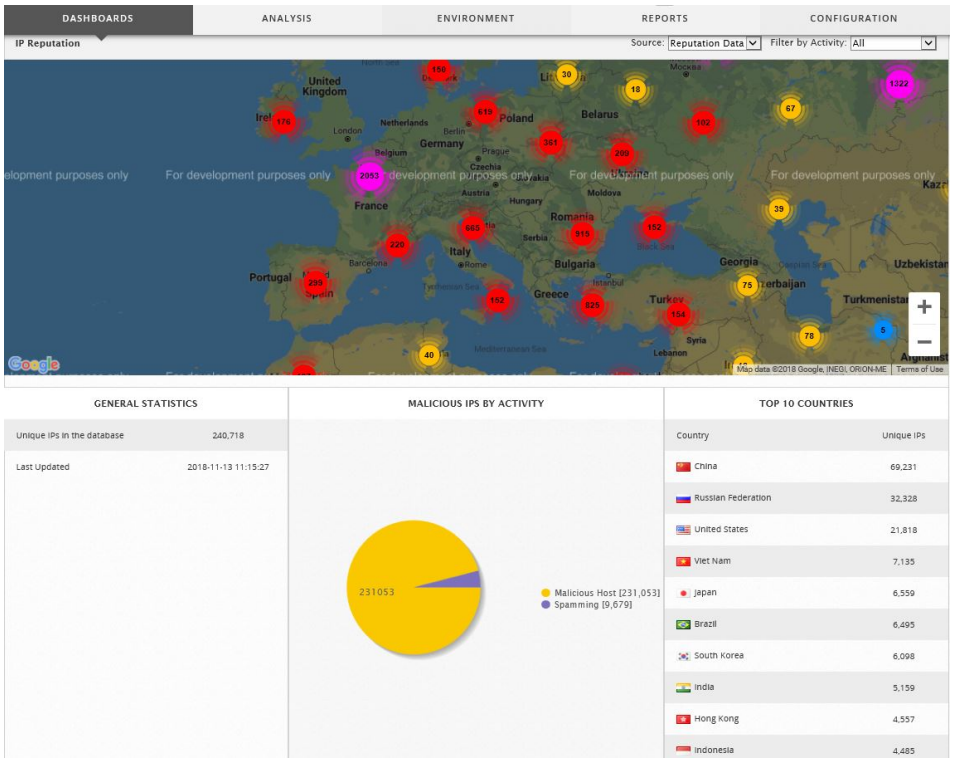


Figura 5.13: Dashboard OSSIM - OTX

com base na reputação dos IPs e URLs reportados pela comunidade. Esta funcionalidade permite receber as referências de toda a comunidade podendo assim ter uma visão, (ver Figura 5.13) geral dos ataques e vulnerabilidades atuais permitindo-nos antecipar aos mesmos, com regras de alerta ou bloqueio dos IPs com a reputação comprometida.

Foi identificada a necessidade de instalação e configuração de um OSSIM sensor no segmento da rede publica. Para não realizar alterações e possível comprometimento da rede existente este equipamento colocou-se no segmento da rede pública, com um interface na mesma rede e um de gestão com comunicação ao OSSIM *server*. Este OSSIM *sensor* foi instalado sobre o equipamento 5.2, utilizando a mesma metodologia do OSSIM *server*, recorrendo a virtualização vSphere ESXi e o mesmo ISO de instalação do OSSIM *server*. Este sensor ficou a receber os *logs* da *firewall* de perímetro desta rede, assim como dos equipamentos críticos que a suportam, nomeadamente ativos de rede *routing, switching e access points*.

De forma a integrar o sensor com o OSSIM *server* existente, procedeu-se a definições nomeadamente de especificação do endereço de IP de *Server* e *Framework* do já existente. As configurações podem ser realizadas diretamente no ficheiro /etc/ossim/ossim_setup.conf editando a secção [server] e [framework]. Após a configuração do sensor, procede-se no servidor a adição do mesmo no menu CONFIGURANTION > DEPLOYMENT > SENSORS. Finalizando esta integração, todos os eventos recolhidos pelo sensor passam a ser integrados no OSSIM *server* e assim correlacionados, estando visíveis no mesmo através da interface web.

5.4.3 Ambiente - Parametrizações

Tendo o OSSIM as configurações anteriormente concretizadas, é necessário carregar os ativos de rede que se pretende monitorizar, podendo ser realizado de forma manual, introduzindo os respetivos identificadores de cada ativo, carrega-los por ficheiro Comma Separated Value (CSV), importa-los de outro SIEM ou realizar uma procura na rede. Esta última opção foi a metodologia adotada. Apesar de não ser necessário, mas devido ao conhecimento detido sobre a infraestrutura da rede, criaram-se os vários segmentos de rede, de forma a poder correr os *scans* nestes segmentos e agendar procuras periódicas semanais de forma a registar novos equipamentos existentes.

Na Figura 5.14 podem-se verificar as redes configuradas, assim como o sensor responsável pela mesma, a indicação se essas redes produzirão alarmes, eventos, assim como se está configurado os *scanners* de vulnerabilidades aos ativos da mesma. Neste Menu ENVIRONMENT > Assets & Groups, pode-se configurar as redes e agrupa-las sempre que fizer sentido, assim como avaliar os ativos registados e agrupa-los consoante as necessidades. Exemplos de grupos criados de forma a facilitar as tarefas posteriores foram:

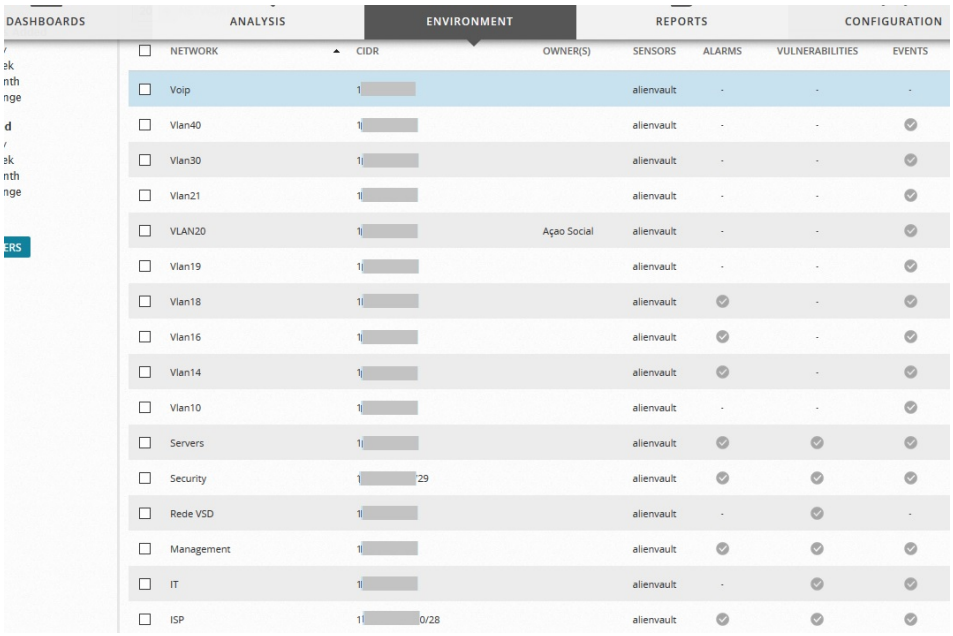


Figura 5.14: Environment OSSIM - Assets Groups

- Servers - Agrupa os equipamentos categoria servidor não críticos. A operacionalidade da CML mantém-se com possíveis falhas nestes servidores.
- Storage - Agrupa os vários equipamentos de armazenamento existentes.
- Wireless - Agrupa os ativos de infraestrutura da rede Wireless.
- Network-Core - Agrupa os ativos de *routing e switching* da redes de core.
- Critical-Servers - Agrupa os equipamentos servidores dos quais dependem operacionalidade da CML.

Inventário dos ativos

Os ativos foram de forma gradual e automática inventariados, e posteriormente analisados individualmente, sendo editado vários parâmetros de forma a concretizar-se os objetivos pretendidos, como elenca a Figura 5.15. O ativo depois de inventariado, e como se está a utilizar os recursos de DNS, é apresentado com o seu *hostname* e Fully Qualified Domain Name (FQDN)/Aliases assim como endereço de IP entre outras informações. No entanto procedeu-se à edição individual de cada ativo na medida que:

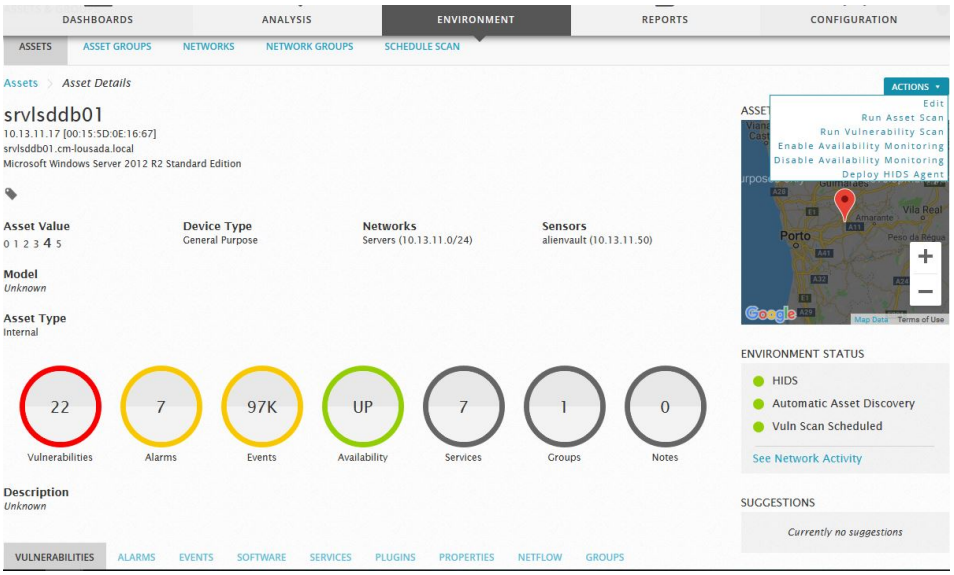


Figura 5.15: Environment OSSIM - Detalhes de um ativo

- Valor do ativo - Como descrito no Capitulo 3, o OSSIM utiliza valores entre **0 e 5** por ativo, como um dos parâmetros para cálculo do risco. Este valor por defeito tem um valor de 2, tendo que se ajustar em consideração do seu real valor para a CML.

  Assim aos ativos dos quais dependem a normal operacionalidade da CML foi-lhes atribuído um valor máximo de 5. Ativos de criticidade alta mas dos quais não está dependente a operacionalidade ou funcionamento dos serviços da autarquia foram atribuídos um valor de 4.

- Ativo externo - É recorrente, porque as normas do regulamento interno da CML assim o permitem, a utilização de equipamentos pessoais, sendo a catalogação destes ativos como externos, podendo-se tratar de um equipamento da equipa de TI, ou mesmo do grupo de executivo que apesar de ter uma utilização profissional, é de carácter pessoal, e nestes dispositivos não se possui gestão dos mesmos, mas o conhecimento da existência de vulnerabilidades e possíveis comprometimentos á infraestrutura interna torna-se vital para o sucesso da segurança na CML.

- Localização do Ativo - Permitiu georreferenciar os ativos para facilitar a sua localização no mapa com identificação do site a que pertence.

- Sensor - Permite alterar o sensor ao qual o ativo está "agregado".

- Tipo de Dispositivo - Permite de uma forma mais granular especificar

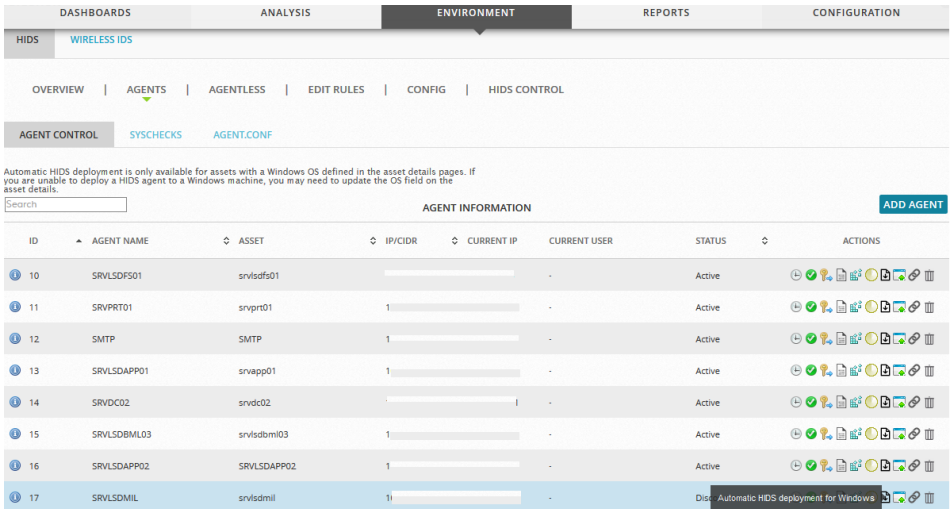


Figura 5.16: Environment OSSIM - HIDS

o tipo de equipamento.

Outros parâmetros como modelo, descrição, propriedades e softwares foram utilizados consoante as necessidades. Aqui também existe a opção de correr um *scan* de vulnerabilidades sobre o ativo, adiciona-lo à monitorização de disponibilidade, passando desta forma a estar contido na lista do Nagios pertencente ao OSSIM.

HIDS - OSSEC

Nos servidores de plataforma Microsoft Windows Server, foram instalados agentes OSSEC para recolha de *logs*, verificação da integridade dos ficheiros, e realização de verificações do *registry*. No menu ENVIRONMENT > DETECTION > AGENTS, dispõe-se de várias formas de configurar este agente. O OSSIM permite fazer o download do binário pré-configurado apropriado ao servidor que se deseja adicionar, podendo de seguida através de armazenamento amovível, e-mail ou partilhas disponibiliza-lo para instalação no servidor destino. O OSSIM também permite fazer um *deploy* remoto e automatizado em *silent mode* (ver Figura 5.16) tendo sido a opção utilizada nos servidores da autarquia.

Do lado do servidor monitorizado é possível aceder por interface ao gestor de cliente do OSSEC, como se pode verificar na Figura 5.17. Verificou-se que o cliente mesmo em equipamentos que produzem uma imensidão de *logs* como a Actie Directory, os recursos utilizados pelo mesmo são baixíssimos, sem percentagem significativa de processamento assim como a ocupação de memoria situa-se na ordem dos 3 a 5 Megabyte (MB). O cliente, alem das opções de *Start/Stop* e *Restart* do serviço também permite aceder ao

Figura 5.17: Environment OSSIM - HIDS OSSEC Cliente

ficheiro de configurações (ossec.conf) onde se pode realizar parametrizações da informação que se pretende recolher. As configurações, como se pode verificar de seguida, com excertos da parametrização do ossec.conf de um dos servidores, trata-se de um ficheiro em XML com uma flexibilidade muito grande no que efetivamente se pretende recolher e monitorizar.

NIDS

No que concerne ao IDS baseado em Snort presente no próprio OSSIM, não foi necessárias configuração adicionais de relevo. Na interface web dispomos apenas das opções de configurar, quais interfaces serão utilizadas para monitorizar e as mesmas serão colocadas em modo promíscuo, estas opções já foram escolhidas no momento da instalação e configuração inicial.

Estas configurações podem ser realizadas ou alteradas através do menu Configuration e posteriormente nas parametrizações do sensor. No caso da atualização das regras do Snort, as mesmas serão atualizadas sempre que se atualizar o OSSIM server, logo não é necessária a instalação de programas adicionais para realização da tarefa. Para criação de regras personalizadas pode-se fazê-lo através do menu Threat Intelligence nas opções Policy e Actions, inclusive para eliminação de falso-positivos e falso-negativos.

Vulnerabilidades

Foi criado um plano (ver Figura 5.18) sobre os grupos de ativos criados anteriormente, para serem executadas baterias de testes de vulnerabilidades, com uma periodicidade semanal. Estes testes produzirão relatórios, como toda a informação recolhida. Desta forma a verificação ativa de vulnerabilidades

Listagem 5.4: ossec.conf

```
<ossec_config>
<!-- One entry for each file/Event log to monitor. -->
<localfile>
 <location>Application</location>
 <log_format>eventlog</log_format>
</localfile>
...
<localfile>
 <log_format>full_command</log_format>
 <command>wmic logicaldisk where "drivetype=2␣AND␣NOT␣deviceid␣
     like␣"a:"" get deviceid, volumename, description,
     FileSystem, Size, VolumeSerialNumber</command>
 <frequency>60</frequency>
</localfile>
  ...
<!-- Rootcheck - Policy monitor config -->
<rootcheck>
 <windows_audit>./shared/win_audit_rcl.txt</windows_audit>
 <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
 <windows_malware>./shared/win_malware_rcl.txt</windows_malware
     >
</rootcheck>>
  ...
<!-- Default files to be monitored - system32 only. -->
<directories check_all="yes">%WINDIR%/win.ini</directories>
<directories check_all="yes">%WINDIR%/system.ini</directories>
<directories check_all="yes">C:\autoexec.bat</directories>
<directories check_all="yes">C:\config.sys</directories>
<directories check_all="yes">C:\boot.ini</directories>
<directories check_all="yes">%WINDIR%/System32/CONFIG.NT</
    directories>
<directories check_all="yes">%WINDIR%/System32/AUTOEXEC.NT</
    directories>
    ...
<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</
    windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</
    windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</
    windows_registry>
```

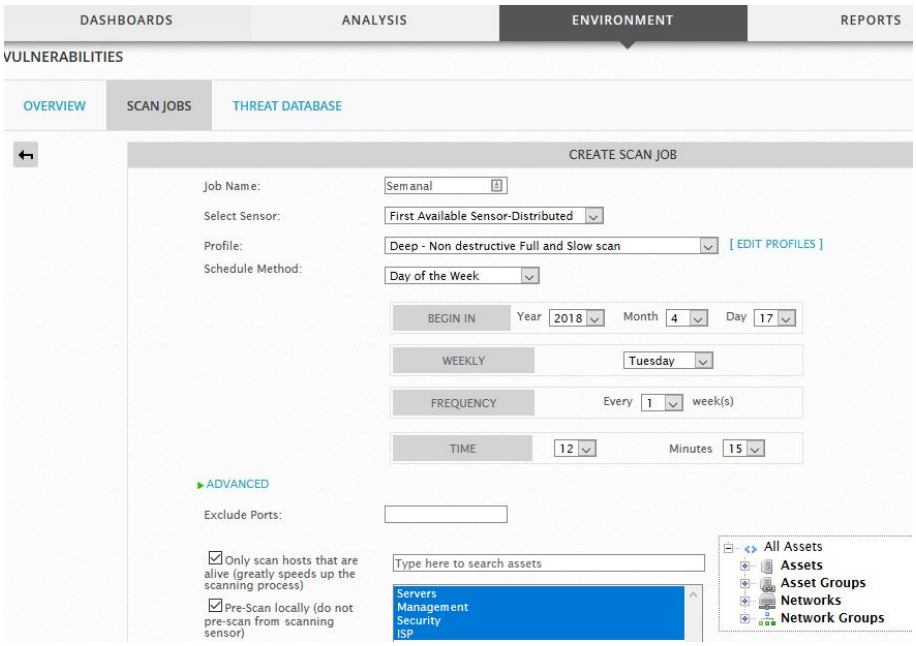


Figura 5.18: Environment OSSIM - Vulnerabilidades

existentes na infraestrutura fica implementada, passo bastante importante para manter a segurança da autarquia. Ferramentas como o OpenVas e Nessus, funcionam para esta análise. Toda esta integração de ferramentas demonstra a importância do sistema SIEM, sendo que neste ponto após análise de vulnerabilidades o OSSIM poderá além dos relatórios gerados:

- Abrir *tickets* - O sistema tem a capacidade de criar *tickets* automaticamente ao detetar uma vulnerabilidade, por defeito quando forem do tipo *high* e *serious*.
- Correlacionar dos dados - Ao identificar a existência de uma falha no sistema, o OSSIM é capaz de gerar alertas críticos caso formas de exploração da mesma seja detetada. Caso exista uma ameaça de uma vulnerabilidade inexistente ele deteta a tentativa, mas gera alertas imediatos.

Com esta implementação dispõe-se de um maior controlo sobre as falhas da infraestrutura, inclusive com capacidade para acompanhar as soluções para elimina-las ou mitiga-las, como se pode verificar na Figura 5.19.

Mapas de Risco

Uma potencialidade do OSSIM bastante interessante e em plena produção na autarquia, são mapas de risco, contendo indicadores de risco, disponibilidade e vulnerabilidade.

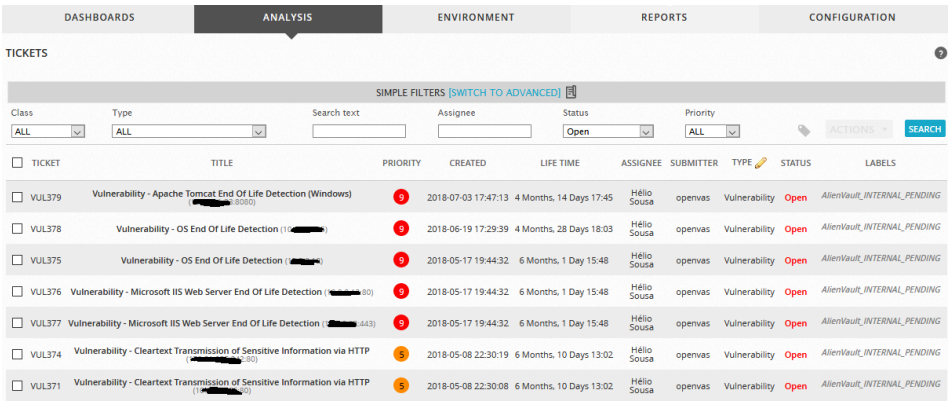


Figura 5.19: ANALYSIS OSSIM - Tickets

O objetivo destes mapas passa por agrupar as informações mais importantes que podem ser obtidas a partir do interface OSSIM, em mapas simples de gerir e simples de analisar. Os mapas podem ser construídos da seguinte forma:

- Background shape - Normalmente será o mapa de rede da infraestrutura monitorizada ou parte da infraestrutura, mapas geográficos, em branco ou outro que cumpra as necessidades pretendidas. No caso prático optou-se por criar três mapas, contendo no principal um mapa lógico representante da infraestrutura de core e dispositivos críticos da autarquia, da qual depende para o sua normal operacionalidade, um segundo mapa representante dos ativos de rede e um mapa que agrupa-se todos os servidores da autarquia.

- Configurable icons - Existe um conjunto razoável de *ícones* para representação dos equipamentos físicos, serviços, países, ou utilizadores monitorizados. Existe a possibilidade de carregar novos icoes na plataforma.

- Cada elemento pode ser arrastado, sempre que o modo de configuração esteja ativo.

- Cada elemento pode ser ligado a um ativo, serviço, utilizador, etc (alguma parte do OSSIM, outro mapa, ou mesmo recurso externo).

- Cada elemento é de fácil compreensão (verde / amarelo / vermelho) Indicadores de risco / vulnerabilidade / disponibilidade.

Durante a configuração, como mencionado acima, dispõe-se da opção de upload de mapas que no caso prático foram elaborados recorrendo ao Microsoft Visio e depois carregados na plataforma. Posteriormente passamos à definição dos indicadores para o mapa definido, onde se pode definir

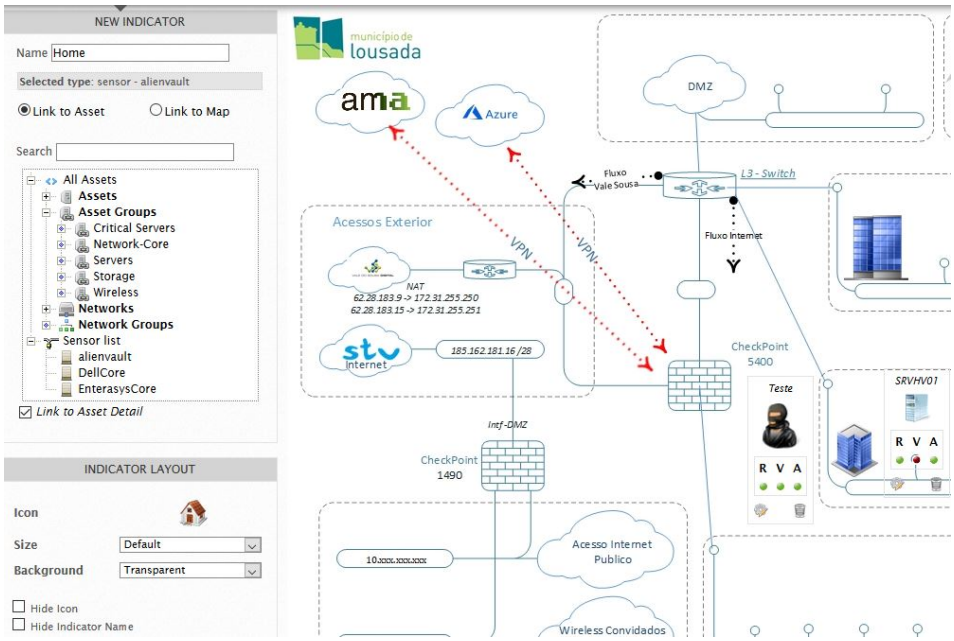


Figura 5.20: Mapas de Risco - Configuração

um ícone, o objeto monitorizado, atribuição de uma designação, Link para outro mapa ou para uma URL assim como outras definições relativas à apresentação do *ícon* (ver Figura 5.20.

Quanto aos objetos utilizáveis para colocação poderão ser do tipo:

- *Hosts*
- Redes
- Grupos de *hosts*
- Grupos de redes
- Sensores

Uma vez escolhido o objeto, procede-se à opção de criar novo indicador. Desta forma irá ser colocado o ícone junto com o indicador no mapa, permitindo que seja movido para o local exato pretendido.

Por fim, quando o mapa objetivado estiver finalizado, para que este esteja acessível a outros utilizadores deverá ser salvo e editado em termos de permissões, podendo desta forma ser visualizado por outros utilizadores ou grupos.

5.4.4 Threat Intelligence

No que concerne à componente de *Threat Intelligence* do OSSIM, depreende-se ao navegar entre os vários menus existentes que a aplicação já vem reche-

ada de "inteligência", contemplando uma base de conhecimento com imensas parametrizações, desde o reconhecimento de vulnerabilidade por assinatura até a forma de responder aos incidentes, das várias tipologias que possam ocorrer, acessos de ACL, acessos *Firewall*, alarmes de *Bruteforce*, etc.

Para o trabalho realizaram-se alterações a nível de ações, diretivas de correlação e políticas. O OSSIM possui um número muito baixo de diretivas de correlação, revelando-se insuficientes ao identificar apenas um pequeno número reduzido de ataques, mas pode-se personalizar e criar as próprias diretivas com base nas necessidades. Neste ponto e comparativamente com a versão comercial verificou-se uma discrepância de algumas diretivas existentes na versão open source para milhares da versão AlienVault USM. As diretivas podem ser criadas no interface web no painel de gestão do OSSIM ou diretamente em ficheiro pois trata-se de informação em XML.

De forma a detetar outros problemas de segurança com base na correlação dos eventos, após investigação e com informação disponível na comunidade de suporte do OSSIM, conseguiu-se para já criar uma centena de diretivas, passando por comprometimento de portas, conflitos de endereços de IP, IP *spoofing*, serviços a correrem em portas não standards, downloads de ficheiros do tipo suspeito, deteção de scanners na rede, tentativas de intrusão, tentativas de quebra de segurança por *Bruteforce*, tentativas de SQL *injection*, bloqueio de contas, etc. Desta forma pretende-se abranger o maior leque de possibilidades de ataques, que comprometam a infraestrutura critica da autarquia assim como os ativos mais importantes.

O OSSIM utiliza políticas para configurar como os eventos são processados. As políticas definem uma ou mais condições que são avaliadas para cada evento de entrada para determinar se a ação associada é acionada. As políticas desempenham um papel fundamental na gestão e resposta a incidentes. As políticas utilizam condições para determinar quais os eventos a serem processados pela política e consequências para definição do que acontecerá quando os eventos corresponderem às condições especificadas.

Nesta funcionalidade foram criadas imensas políticas, de forma a responder a eventos do tipo, comprometimento de credenciais, utilizadores com contas bloqueadas, equipamentos desativos da *Active Directory*, falhas de hardware em servidores, falhas de equipamentos críticos, etc. das quais passa-se a exemplificar como se criam.

A maior parte das políticas aqui definidas, culminam no envio de um e-mail com a gravidade do evento para a pessoa ou equipa responsável, sendo que para isso criou-se nas *Actions*, várias ações personalizadas correspondendo à política que iria ser associada. Pode-se verificar no exemplo da Figura 5.21, a configuração do envio de um e-mail identificado como "ossim@cm-lousada.pt", para o "helpdesk.si@cm-lousada.pt"sendo este um grupo de Administradores com privilégios sobre equipamentos críticos, recebendo a informação que um dos sistemas críticos da organização está indisponível, assim como a identificação do ativo afetado. Neste caso colocou-se

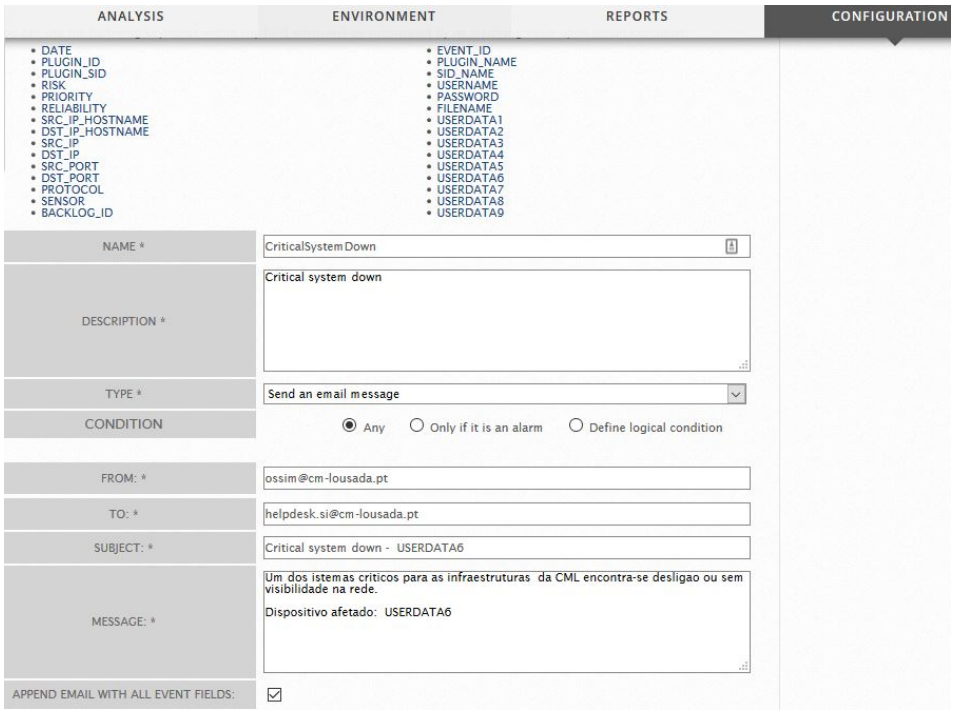


Figura 5.21: Configuration OSSIM - Actions - SystemDown

em anexo todos os campos do evento para que a equipa de uma forma fácil consiga despistar a causa desse acontecimento e intervir imediatamente.

Comparativamente à ação anterior temos o exemplo da Figura 5.22, que será utilizada quando uma conta de utilizador da *Active Directory* for bloqueada, despoletando um e-mail para "informatica@cm-lousada.pt", grupo de utilizadores com acesso administrativos sobre utilizadores de domínio, recebendo a informação que o utilizador bloqueou a conta, identificando o equipamento utilizado na tentativa de acesso, assim como a razão do bloqueio da conta.

Com as ações configuradas passou-se à configuração das políticas. Ressalva-se que as políticas consistem em regras numeradas que o OSSIM aplica em ordem decrescente sempre que processa um evento. Quando um evento corresponde a uma regra, o OSSIM para de procurar outras correspondências, mesmo que elas existam. Por esse motivo, as regras mais específicas e restritivas devem ser ordenadas no topo da lista de regras e as regras genéricas devem ser ordenadas na parte inferior da lista de regras.

Ilustra-se um exemplo da criação de uma política, entre muitas criadas, na qual informa o Administrador da falha de ativo crítico da infraestrutura. Opta-se por este exemplo por ser bastante completo abordando várias componentes do sistema e podendo-se traduzir para outras políticas.

- 1º Passo - O ativo terá que estar monitorizado, como se falou aquando

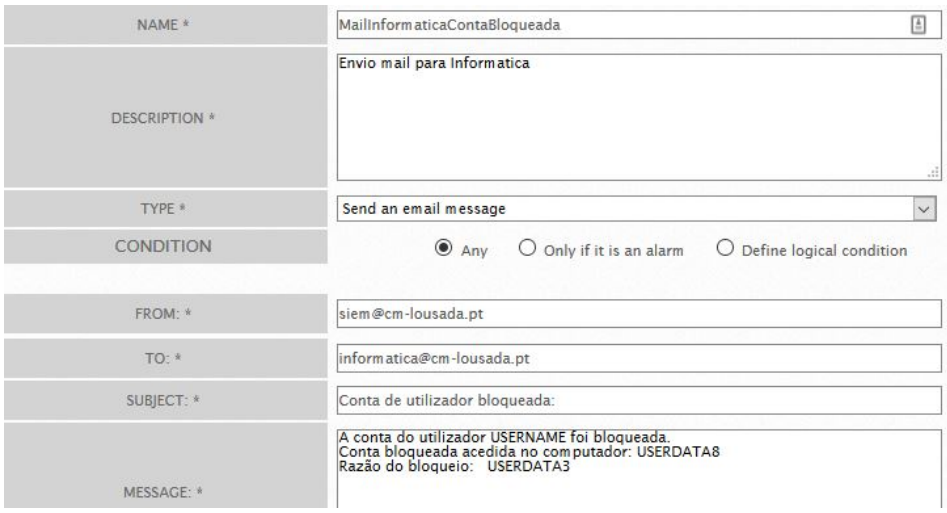


Figura 5.22: Configuration OSSIM - Actions - Lockout

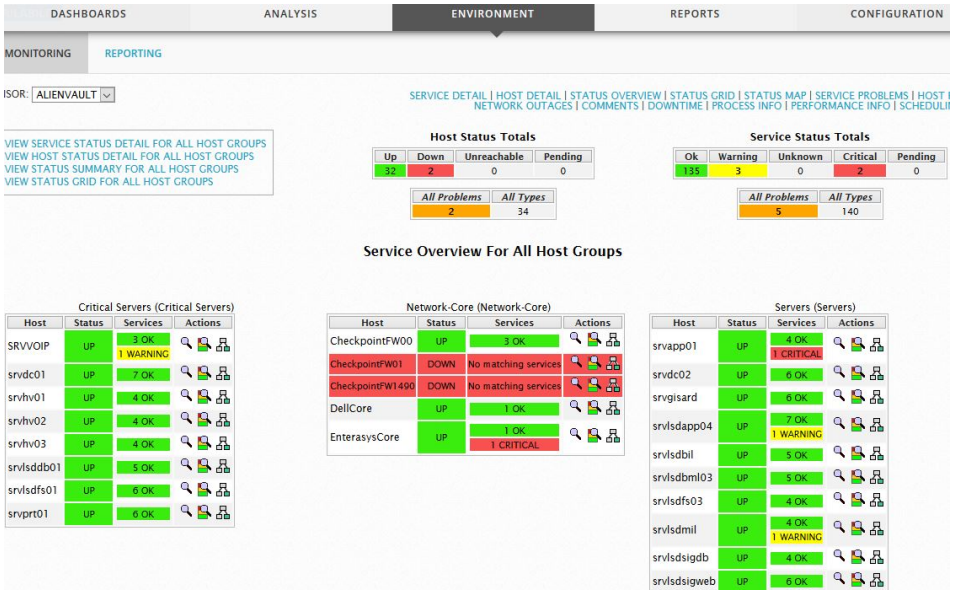


Figura 5.23: ENVIRONMENT OSSIM - Availability

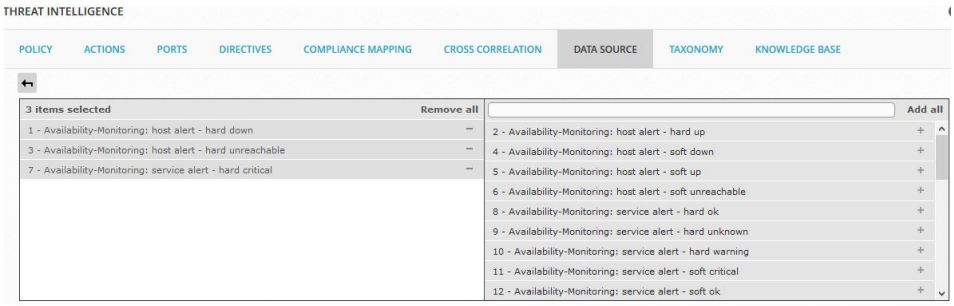


Figura 5.24: Configuration OSSIM - Disponibilidade de Serviço

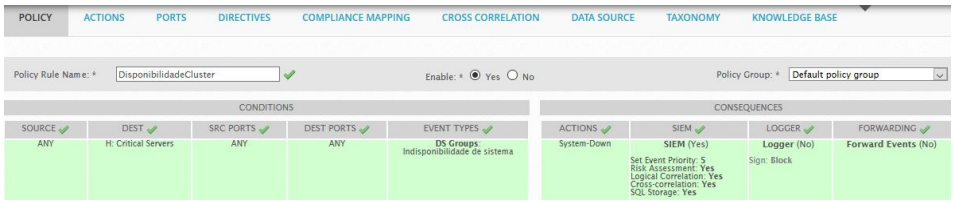


Figura 5.25: Configuration OSSIM - Políticas

da parametrização do ativo, e este passará a estar disponível em ENVIRONMENT > Availability > Monitoring, (ver Figura 5.23)

- 2º Passo - De seguida, necessita-se de informar ao sistema o que monitorizar no ativo. No caso de um domínio, alguns serviços principais devem estar ativos e em execução para que o ativo seja considerado "Active". Esta parametrização também é realizada nas definições do ativo em *Services*.

- 3º Passo - Regressando ao Menu CONFIGURATION > THREAT INTELLIGENCE, pode-se criar um grupo de fontes de dados que poderá ser utilizado para aplicar as políticas. Criou-se em "DATA SOURCE"um grupo com a identificação "indisponibilidade de sistema", recorreu-se ao ID da fonte de dados 1525 (Availability-Monitoring), e adicionou-se as opções como se verifica na Figura 5.24 de *Hardware Down, unreachable, e Critical*.

- 4º Passo - Cria-se a política, como na Figura 5.25, onde a identificamos com um nome, na *SOURCE* neste caso deixou-se "ANY", em *DESTINATION* colocou-se o ativo ou neste caso concreto o grupo anteriormente criado que contêm os ativos considerados críticos para o funcionamento da organização, e configuramos em *EVENT TYPES* a tipologia de evento criado acima com a identificação "Indisponibilidade de sistema".

  Na componente de consequências, em *ACTIONS* vamos adicionar a

ação anteriormente criada identificada como "System-Down"que fará as ações aí delineadas, pela gravidade do evento definiu-se prioridade máxima de "5"com risco associado para o ativo.

- 5º Passo - No final colocamos a política na ordem correta, e procedemos com a aplicação clicando em *"Reload Policies"* devendo a política ficar a verde com o status de *"Enable"*.

Capítulo 6

Avaliação de Resultados

Este projeto trouxe uma nova **visibilidade** sobre os ativos e sobre a infraestrutura que até à data era desconhecida, apresentam-se alguns resultados da avaliação da solução implementada e do trabalho realizado, através dos *dashboards* e relatórios gerados pelo OSSIM.

Logo após a autenticação, observa-se uma grande quantidade de informação, disponibilizada num único local como se verifica na Figura 6.1. Através de gráficos consegue-se saber o estado geral da nossa infraestrutura, quais os principais alarmes que estão a ser despoletados, principais eventos de SIEM por categorias, principais *hosts* com maior atividade de eventos, etc. Ainda dentro do primeiro painel podemos navegar entre as várias abas e temos acesso sempre de forma gráfica ao sistema de *tickets*, um painel reservado para segurança, taxonomia e no ,final, reportes sobre as vulnerabilidades por ativo de rede. Todos estes painéis destacam-se pela positiva, pela quantidade de informação que transmitem, com simplicidade e de fácil interpretação, e ainda pela possibilidade de acesso à informação detalhada que suporta determinado gráfico, através do simples clique do rato na barra, gráfico ou *host* pretendido.

Com o inventário das ativos realizado de forma automática, passou-se a verificar as vulnerabilidade encontradas com o OpenVas, assim como exploração das mesmas com o nmap e Nessus. Este inventário veio mostrar uma realidade por vezes desconhecida ou menosprezada, a quantidade de equipamentos ativos utilizados dentro da nossa infraestrutura de rede, é superior ao dobro dos ativos pertencentes à rede corporativa, sendo estes ativos a principal fonte de vulnerabilidades, *malwares* e vírus. Dentro da infraestrutura interna de rede o OSSIM registou atualmente 1033 dispositivos, sendo por volta de 500 os efetivamente da organização e geri-veis pela mesma.

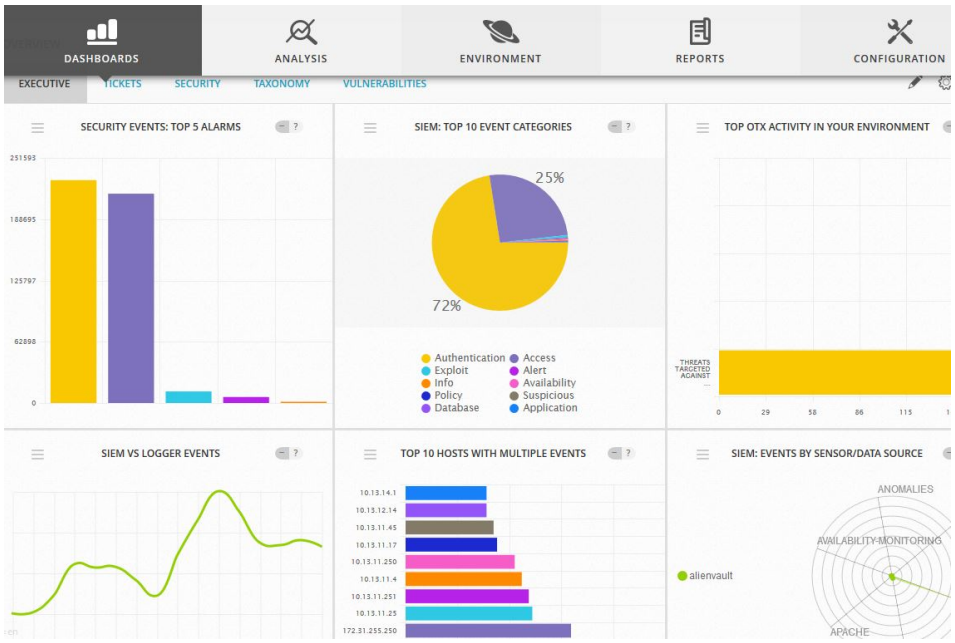


Figura 6.1: Dashboards - Overview

6.1 Principais alertas detetados

O OSSIM deu **visibilidade** a uma quantidade de atacantes com permanentes *scans* às *firewall* de perímetro da infraestrutura de rede. O OSSIM permitiu identificar máquinas potencialmente infetadas com vários tipos de *malware* e serviços com vulnerabilidades. Com toda uma nova informação foi possível proceder a correções desde bloqueio de endereços de IP's que constantemente faziam ataques deliberados à rede, criar políticas de quarentena para equipamentos potencialmente comprometidos, isolar equipamentos detentores de *malware*, entre uma panóplia de novas metodologias que foram, e vão sendo criadas, de forma a responder perante esta nova visibilidade/realidade.

A informação gerada pelo OSSIM, além de alterar metodologias internas, serviu de fundamentação base para solicitar a parceiros, para procederem a correções nos seus sistemas, serviços e aplicações. Sistemas estes que se encontram em produção na infraestrutura existente como se pode verificar pela Figura 6.2. Este ativo tratava-se de um servidor, apesar de não crítico para a autarquia, que providencia serviços assentes numa aplicação de um parceiro externo que estavam a comprometer e colocar em risco informação da organização.

As ações despoletadas pela definição de políticas, nomeadamente de envio de e-mails para a equipa de TI aquando ocorre bloqueios de computadores, contas de utilizadores e dispositivos críticos com falhas, criou um

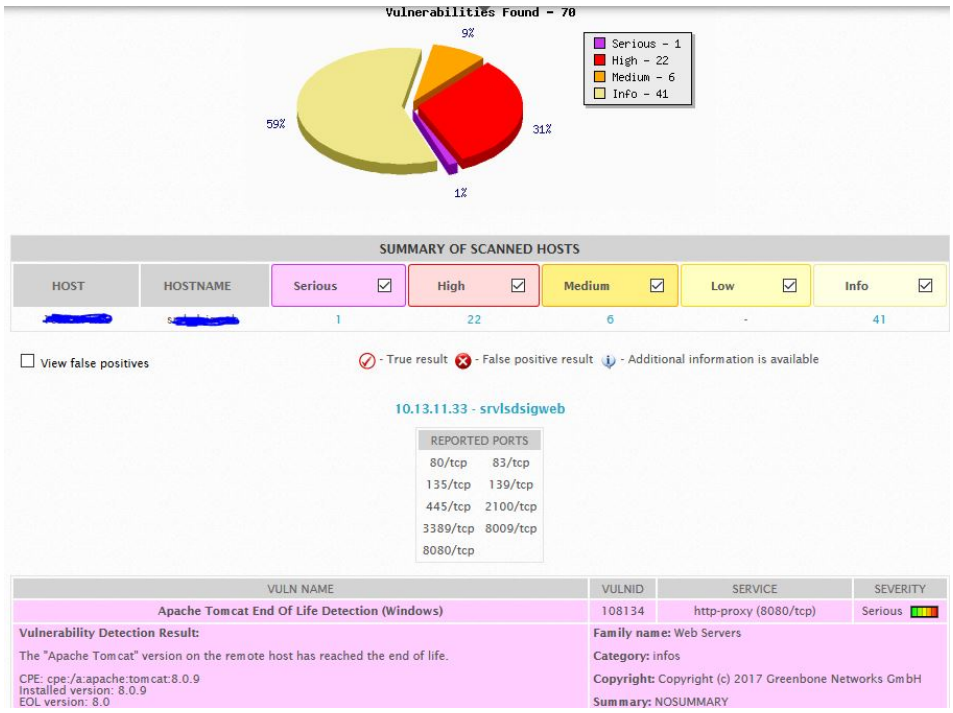


Figura 6.2: Environment - Vulnerabilidades de um ativo

Figura 6.3: Alerta de bloqueio de conta

significativo impacto positivo nas metodologias de trabalho assim como rapidez de resposta ao utilizador final, como por exemplo:

Com bastante frequência existe o bloqueio de contas de utilizador, acontecendo isto diariamente em média entre 4 a 5 utilizadores por dia. Anteriormente estes bloqueios no caso do utilizador reportar um engano de sucessivas entradas inválidas da sua *password*, era procedido ao desbloqueio da conta e em caso de necessidade a reposição de uma nova *password*. No entanto um número percentual significativamente alto dos utilizadores reportam desconhecer o motivo do bloqueio, motivando à equipa de TI uma série de diligencias de forma a tentar compreender a causa do acontecimento e se tratava efetivamente de uma tentativa de acesso ilegítimo. Por vezes este processo em alguns casos poderiam demorar horas.

Como se verifica na Figura 6.3, com o OSSIM estes acontecimentos passaram a ser tratados de forma completamente diferente. Com a informação que a equipa de TI recebe em tempo útil, quando um utilizador faz um contacto de bloqueio de conta, a equipa sabe imediatamente todas as evidencias significativas para avaliação do caso.

- Conta está referencia como bloqueada?
- A hora do acontecimento em causa.
- O dispositivo do qual foi realizada a tentativa de autenticação de sessão e que servidor foi responsável pelo bloqueio.
- Razão/Causa que originou o bloqueio.

Com estes dados a equipa de TI antevê a necessidade do contacto do utilizador, assim como consegue providenciar informação útil do acontecimento sanando o problema em poucos minutos senão segundos.

6.2 Visibilidade para todos

Com a implementação do OSSIM foi possível criar mapas de risco, e disponibilizar estes de forma permanente em painéis de grande dimensão, desta forma a equipa de TI tem facilmente a perceção de problemas na infraestrutura, assim como facilidade no *troubleshooting* e resolução desses mesmos problemas, como podemos visualizar na Figura 6.4. Estes mapas permitenos criar por ativo, indicadores de risco, disponibilidade e vulnerabilidade e consequentemente o acesso ao ativo através de um simples click do rato.

6.3 Informação do *hacker*

Tendo por base a informação mantida pelo OSSIM, a organização passou a efetuar bloqueios de endereços de IP de países estrangeiros, uma vez que,

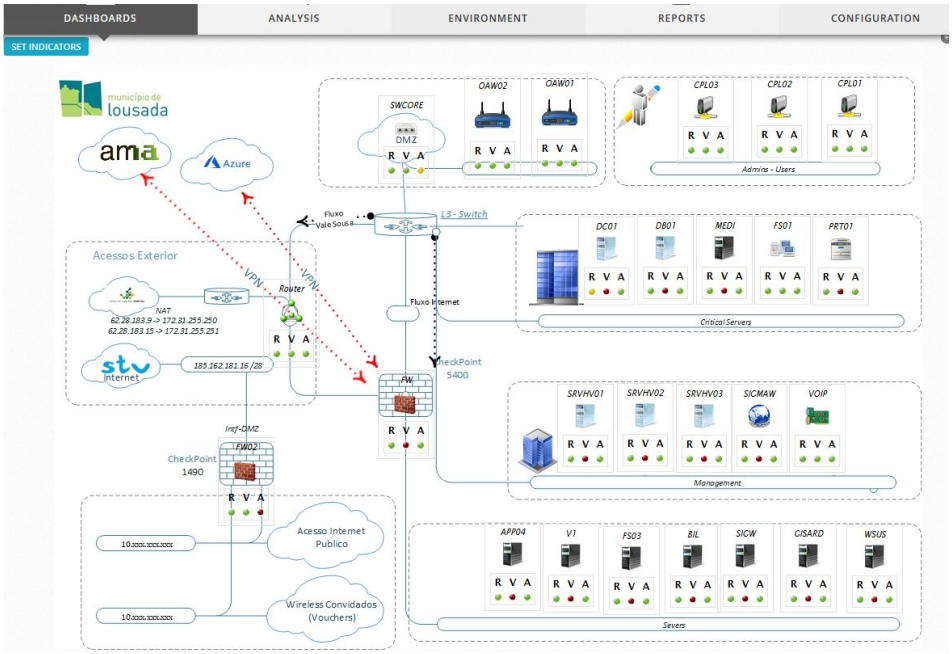


Figura 6.4: Dashboards - Risk Maps

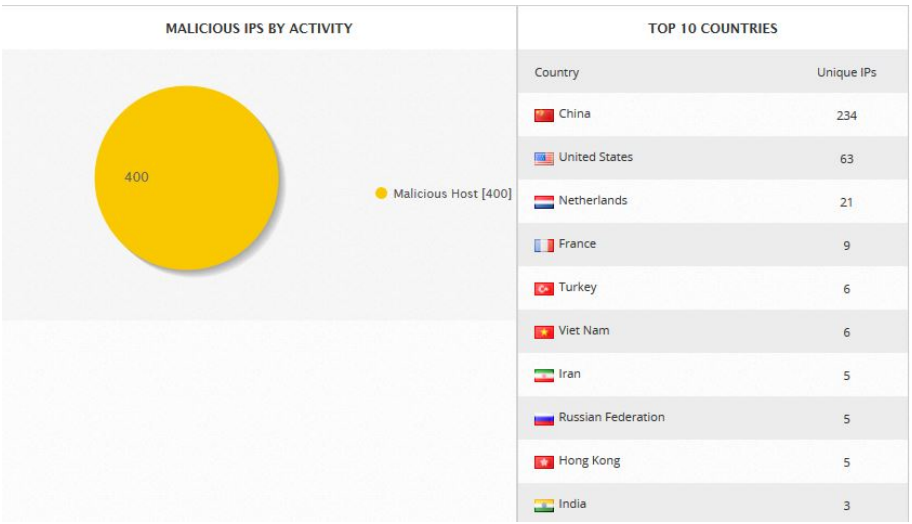


Figura 6.5: Dashboards - Open Threat Exchange

como se pode ver na Figura 6.5, estes IPs estavam continuamente a efetuar tentativas/intrusões nos sistemas e estando referenciados na comunidade OTX como *hosts* maliciosos. Esta metodologia permitiu reduzir o risco de ataques com sucesso uma vez que o IP quando identificado como um IP de Top Attacker passa a fazer parte de uma *black list* e consequentemente bloqueado pelas firewall's de perímetro.

6.4 Relatórios

Com os OSSIM em produção, a autarquia passou a ter acesso a relatórios no que concerne a segurança e estado da infraestrutura de rede, estes relatórios servem de base para correções, informações para melhorias da segurança da infraestrutura, dar conhecimento aos superiores hierárquicos da maturidade de segurança da infraestrutura, assim como fundamento de estudo e análise para planeamento de evolução da segurança da infraestrutura do município, entre outros. Com os OSSIM passou-se a disponibilizar relatórios periodicamente do tipo:

- Alarm Report.
- Asset Details.
- Availability Report.
- Business & Compliance ISO 27001.
- Geographic Report.
- Tickets Status.
- Tickets Report.
- User Activity Report.
- Vulnerabilities Report.

6.5 Atualizações do OSSIM

No que concerne a atualizações seja do próprio core do sistema do OSSIM, assim como toda a panóplia de ferramentas embutida na aplicação, a ferramenta é uma agradável surpresa. O AlienVault Labs oferece periódica e regularmente atualizações de inteligência de ameaças para a plataforma. Essas atualizações geralmente incluem:

- Regras de Correlação.
- Regras de correlação cruzada.

- Assinaturas de IDS na Rede.
- Assinaturas do IDS do *host*.
- Base de dados de ameaças de vulnerabilidade .

O AlienVault Labs também fornece uma atualização periódica de *feed* de *plugin* para a plataforma. Nestas atualizações incluem-se novos *plugins*, correções para *plugins* existentes, bem assim como, descodificadores e regras para o AlienVault HIDS.

Capítulo 7

Conclusão

Este trabalho oferece uma visão geral e técnica do que é um SIEM e discute a recolha de dados, o armazenamento de dados, o processamento de dados e, por fim, a implementação do projeto. O SIEM tem na sua essência a correlação de eventos e *logs*. Para a recolha de dados é importante descobrir quais os *logs* a analisar e de que ativos devem ser realizadas as recolhas. Regras de negócio e identificação dos ativos dos quais a organização depende para a sua operacionalidade são excelentes questões para começar.

A recolha de dados requer conhecimentos técnicos para consequentemente atingir os objetivos definidos. Como se verifica na implementação do projeto, os *logs* são providenciados de uma multiplicidade de fontes e, por cada tipologia de ativo, terá a sua forma de recolha dos dados. Já o processamento de dados é diretamente influenciado pela quantidade de informação recolhida, pela sua complexidade ou que exijam correlação entre muitos dispositivos e eventos. A nível de processador e memoria verificou-se que os recursos mínimos propostos pela AlienVault seriam para o tratamento de informação numa escala de dimensões muito menores, sendo que neste caso pratico não foram suficientes.

O SIEM OSSIM está organizado em duas partes: um *frontend*/consola de gestão e um conjunto de relatórios. O *frontend* fornece uma visão geral. Ilustra o estado de segurança atual (baseado em alarmes e eventos), permite ao administrador ou equipa de segurança alterar políticas e configurações. Fornece ferramentas para análise de eventos de segurança e arquivos de *log* brutos. Os relatórios estão disponíveis também no *fronttend*, mas podem ser configurados para serem enviados a pessoas específicas ou a um grupo de pessoas. Os relatórios têm um intervalo de datas, um intervalo de recursos a incluir, alarmes e eventos personalizados que significam algo digno de nota. Estes relatórios podem ser construídos com especificações personalizadas, baseadas, por exemplo, nas regras de negócio estabelecidas pela organização ou pelas metodologias de trabalho adotadas.

7.1 Resultados

A implementação do OSSIM na instituição em causa trouxe inúmeras vantagens no que diz respeito à unificação das plataformas de monitorização, com especial destaque para a monitorização de eventos de segurança de informação, que se resumia a plataformas isoladas e sem nenhum tipo de correlacionamento de informação. Em resultado foram consolidados uma panóplia de *logs* de tipologias de fontes diferentes, e apresentados de uma forma a dar **visibilidade** do estado geral em tempo real da segurança da informação da organização.

O sucesso da realização do trabalho foi reconhecido pelos colegas do serviços de TI, assim como, pelos dirigentes. Para além do projeto desenvolvido, houve ainda possibilidade de aplicar esta implementação como suporte a projetos, a decorrer na autarquia, apoiar a implementação das ações necessárias para a adequação ao RGPD a nível de infraestrutura e sistemas de informação, assim mesmo como suporte base para inicio de certificação de segurança de informação (ISO 27001/2). Este trabalho é importante na medida em que ajudará a sensibilizar, antever e evidenciar os problemas de segurança, consequentes da falta de visibilidade dos risco, vulnerabilidades e disponibilidade dos ativos das infraestruturas de TI.

Os objetivos propostos foram cumpridos. A plataforma OSSIM implementada corresponde às necessidades de monitorização evidenciadas pela organização. A componente de alta disponibilidade do OSSIM não foi implementada porque que esta componente não é suportada na versão *open source*. Assim, a alta disponibilidade foi garantida através de ativação de uma replica do ambiente virtual de produção para o *DataCenter* externo.

7.2 Trabalho futuro

Como trabalho futuro, prevê-se o desenvolvimento de processos relativos à manutenção e continuidade da solução desenvolvida. Continuidade na criação de diretivas de correlação, de forma a abranger outras potencias novas vulnerabilidades, ataques e riscos. Continuidade na definição de políticas, para a execução de tarefas de alarmística, assim como de enfoque mais técnico como a execução de *scripts* para uma mitigação de riscos de segurança de forma mais célere.

Bibliografia

[1] M. Garnaeva, F. Sinitsyn, Y. Namestnikov, D. Makrushin, and A. Liskin, "Kaspersky security bulletin. overall statistics for 2016," *Kaspersky Lab, Dec*, 2016.

[2] R. Power and R. Foreword By-Farrow, *Tangled Web: Tales of digital crime from the shadows of cyberspace*. Macmillan Press Ltd., 2000.

[3] L. Coppolino, S. D'Antonio, V. Formicola, and L. Romano, "Integration of a system for critical infrastructure protection with the ossim siem platform: A dam case study," in *International Conference on Computer Safety, Reliability, and Security*, pp. 199–212, Springer, 2011.

[4] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network security*, vol. 2011, no. 8, pp. 16–19, 2011.

[5] I. Friedberg, F. Skopik, G. Settanni, and R. Fiedler, "Combating advanced persistent threats: From network event correlation to incident detection," *Computers & Security*, vol. 48, pp. 35–57, 2015.

[6] A. Chuvakin, "The complete guide to log and event management," *White Paper*, 2010.

[7] A. Chuvakin, "Practical strategies to compliance and security with siem," *Vendor T" webinar, available at http://goo. gl/kifj2*, 2012.

[8] H. F. Tipton and M. K. Nozaki, *Information security management handbook*. CRC press, 2007.

[9] B. Binde, R. McRee, and T. J. O'Connor, "Assessing outbound traffic to uncover advanced persistent threat," *SANS Institute. Whitepaper*, p. 16, 2011.

[10] D. Luckham, *The power of events*, vol. 204. Addison-Wesley Reading, 2002.

[11] K.-O. Detken, T. Rix, C. Kleiner, B. Hellmann, and L. Renners, "Siem approach for a higher level of it security in enterprise networks.," in *IDAACS*, pp. 322–327, 2015.

[12] K. M. Kavanagh, O. Rochford, and T. Bussa, "Magic quadrant for security information and event management," *Gartner Group Research Note*, 2015.

[13] A. Kanda, E. Akagawa, and Y. Ishii, "File server, file server log management system and file server log management method," Mar. 17 2009. US Patent 7,506,375.

[14] D. Swift, "A practical application of sim/sem/siem automating threat identification," 2006 (accessed August 24, 2018). https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781.

[15] P. Institute, "The cost of malware containment," 2015 (accessed August 24, 2018). https://www.ponemon.org/local/upload/file/Damballa\%20Malware\%20Containment\%20FINAL\%203.pdf.

[16] J. Friedman and M. Bouchard, "Definitive guide to cyber threat intelligence," 2015.

[17] D. Shackleford, "Who's using cyberthreat intelligence and how," *SANS Institute*, 2015.

[18] Gartner, "Best security information and event management (siem) software as reviewed by customers," 2018 (accessed August 24, 2018). https://www.gartner.com/reviews/customers-choice/security-information-event-management.

[19] D. A. Pinto, "Gestão de eventos de segurança de informação-siem," 2015.

[20] AlienVault, "Alienvault - documentation center," 2018 (accessed June , 2018). https://www.alienvault.com/documentation/.

[21] AlienVault, "Alienvault ossim: The world's most widely used open source siem," 2018 (accessed June , 2018). https://www.alienvault.com/products/ossim.

[22] AlienVault, "Documentation - alienvault® open threat exchange®," 2018 (accessed June , 2018). https://www.alienvault.com/documentation/otx.htm.

[23] C. Leres, "The arpwatch manual page," 1992.

[24] M. Zalewski, "p0f v3 (version 3.08 b)," 2014.

[25] G. F. Lyon, *Nmap network scanning: The official Nmap project guide to network discovery and security scanning.* Insecure, 2009.

[26] J. Beale, R. Deraison, H. Meer, R. Temmingh, and C. V. D. Walt, *Nessus network auditing*. Syngress Publishing, 2004.

[27] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks.," in *Lisa*, vol. 99, pp. 229–238, 1999.

[28] L. Deri and S. Suin, "Effective traffic measurement using ntop," *IEEE Communications Magazine*, vol. 38, no. 5, pp. 138–143, 2000.

[29] W. Barth, *Nagios: System and network monitoring*. No Starch Press, 2008.

[30] R. Bray, D. Cid, and A. Hay, *OSSEC host-based intrusion detection guide*. Syngress, 2008.

[31] J. M. Madrid, L. E. Munera, C. A. Montoya, J. D. Osorio, L. E. Cardenas, R. Bedoya, and C. Latorre, "Functionality, reliability and adaptability improvements to the ossim information security console," in *Communications, 2009. LATINCOM'09. IEEE Latin-American Conference on*, pp. 1–6, IEEE, 2009.

[32] G. Suarez-Tangil, E. Palomar, J. M. de Fuentes, J. Blasco, and A. Ribagorda, "Automatic rule generation based on genetic programming for event correlation," in *Computational Intelligence in Security for Information Systems*, pp. 127–134, Springer, 2009.

[33] M. Alamanni, "Ossim: A careful, free and always available guardian for your network," *Linux Journal*, vol. 2014, no. 242, p. 2, 2014.

[34] J. K. Pinto and S. J. Mantel, "The causes of project failure," *IEEE transactions on engineering management*, vol. 37, no. 4, pp. 269–276, 1990.

[35] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE security & Privacy*, no. 5, pp. 35–41, 2014.

[36] K. Geers, *Strategic cyber security*. Kenneth Geers, 2011.

[37] A. Conklin and G. B. White, "E-government and cyber security: the role of cyber security exercises," in *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, vol. 4, pp. 79b–79b, IEEE, 2006.

[38] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[39] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," *Information Management & Computer Security*, vol. 22, no. 5, pp. 410–430, 2014.

[40] G. Gearhart, "Method and system for cyber-security vulnerability detection and compliance measurement (cdcm)," June 16 2005. US Patent App. 10/737,503.

[41] R. Bejtlich, *The Tao of network security monitoring: beyond intrusion detection*. Pearson Education, 2004.

[42] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers & Security*, vol. 25, no. 7, pp. 522–538, 2006.

[43] M. Bromiley, "Incident response capabilities in 2016: The 2016 sans incident response survey," *SANS Institute, June*, 2016.

[44] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, pp. 1–147, 2012.

[45] C. lousada, "Lousada - a história," 2018 (accessed June , 2018). `http://www.cm-lousada.pt/pt/historia`.