SIEM - Gestão e Análise de Eventos de Segurança nas Organizações **(Parte II)**

Mestrado de Cibersegurança e Informática Forense
UC: Gestão e Análise de Relatórios de Segurança
Docente: Beatriz Piedade

Pedro Marques
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220562@my.ipleiria.pt

Filipe Bagagem
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220558@my.ipleiria.pt

***Abstract*— As plataformas SIEM recolhem e processam um grande volume de dados. A apresentação desses dados de forma rápida e inteligível para o analisa é fundamental. A complementaridade conseguida com a integração de várias ferramentas faz com que as plataformas SIEM sejam cada vez mais completas.**

Keywords—SIEM, logs, incidents, segurança, análise, ataques,

I. Introdução e Enquadramento

A implementação de um sistema SIEM é uma tarefa que requer uma planificação detalhada e cuidada dos objetivos a que o sistema se propõe. A escolha das ferramentas e do funcionamento tem de ser dimensionada tendo em consideração a dimensão do sistema a monitorizar. A capacidade de monitorização em tempo real, deteção de ameaças, resposta a incidentes e recursos de geração de relatórios de conformidade são uma mais valia de peso neste tipo de sistemas.

Ao longo deste relatório, e no seguimento do trabalho realizado na fase I, será explorada a implementação de um sistema SIEM, neste caso o Security Onion.

No presente documento será abordada a instalação e configuração do sistema tendo em consideração o ambiente de testes que será detalhadamente apresentado, as eventuais ligações do sistema SIEM a outros sistemas ou equipamentos, será realizada uma simulação de monitorização e análise, definidos e configurados alertas para situações de alertas comprometimento de segurança através do tratamento de eventos recolhidos através de logs. Posteriormente será criada e efetuada uma análise a partir de um dataset criado dos logs exportados da plataforma.

Neste artigo, exploraremos os fundamentos do SIEM e como ele pode fortalecer a postura de segurança das organizações. Discutiremos as principais funcionalidades de um SIEM. Além disso, abordaremos as principais vantagens e desafios na implementação de um SIEM, bem como as melhores práticas para maximizar o seu valor.

Ao compreender os benefícios de um SIEM e adotar as estratégias corretas, as organizações podem elevar o seu nível de segurança e estar melhor preparadas para enfrentar as ameaças cibernéticas em constante evolução. Vamos mergulhar no mundo do SIEM e descobrir como essa poderosa solução pode proteger os ativos vitais das empresas e proporcionar tranquilidade no mundo digital cada vez mais complexo e perigoso.

II. Instalação e Configuração do "Security Onion"

A instalação e configuração do Sistema SIEM está documentada no anexo[1].

III. Ligação do Security Onion a Outros Sistemas/Equipamentos

O "Security Onion" é uma plataforma completa que conta nativamente com a integração de diversas ferramentas, nomeadamente:

Kibana

O Kibana é uma plataforma de análise e visualização de dados desenvolvida pela Elastic. Ele é usado em conjunto com o Elasticsearch, um mecanismo de recolha e análise de dados, para fornecer uma interface de utilização intuitiva para explorar, analisar e visualizar grandes volumes de dados.

O Kibana oferece várias funcionalidades:

1. O Kibana permite criar painéis e gráficos interativos para visualizar dados de várias fontes. Ele oferece uma ampla gama de opções de visualização, como gráficos de barras, gráficos de linhas, mapas geográficos e tabelas.
2. Permite realizar pesquisas avançadas e filtrar dados de forma flexível usando a linguagem de consulta do Elasticsearch. Isso permite explorar e analisar dados específicos com base em critérios personalizados.

[1] anexo_I_instalacao_configuracao_securityOnion.pdf

3. O Kibana permite a exploração de dados em tempo real, permitindo aos utilizadores visualizar informações atualizadas instantaneamente à medida que os dados são atualizados no Elasticsearch.
4. É possível criar painéis personalizados com vários gráficos e visualizações para acompanhar métricas e indicadores importantes. Os painéis podem ser compartilhados com outras pessoas ou incorporados em outras aplicações.
5. O Kibana suporta a configuração de alertas com base em condições específicas dos dados. Os utilizadores podem definir regras de alerta e receber notificações por e-mail ou Slack.
6. O Kibana fornece recursos de autenticação e autorização para controlar o acesso aos dados e às funcionalidades do sistema. Isso ajuda a garantir a segurança e a privacidade dos dados sensíveis.

Grafana

O Grafana é uma plataforma de visualização e monitorização de dados de código aberto. Ele permite criar painéis interativos e gráficos para analisar e visualizar dados de várias fontes, como bases de dados, logs e serviços cloud.

Algumas das principais características e funcionalidades do Grafana incluem:

1. Visualização de dados: O Grafana oferece uma ampla variedade de opções de visualização, como gráficos de linhas, barras, medidores, tabelas, mapas e painéis interativos. Isso permite a criação de painéis personalizados e intuitivos para monitorizar e analisar dados.
2. Permite suporte para múltiplas fontes de dados como bases de dados SQL, sistemas de monitorização, como Prometheus e Graphite, serviços cloud como AWS CloudWatch e Azure Monitor.
3. O Grafana possui recursos de criação de alertas com base em métricas e condições predefinidas. Ele pode enviar notificações via e-mail, Slack, PagerDuty e outros serviços, ajudando os utilizadores a responder rapidamente a eventos críticos.
4. Com a funcionalidade de exploração de dados do Grafana, é possível executar consultas interativas, filtrar e agrupar dados para análises mais aprofundadas. Ele também suporta linguagens de consulta populares, como SQL e PromQL.
5. O Grafana pode ser integrado a várias ferramentas e serviços, permitindo uma integração contínua com fluxos de trabalho existentes. Ele suporta autenticação única (SSO), integração com ferramentas de controle de versão como o Git, e é altamente personalizável por meio de plugins e APIs.
6. O Grafana possui uma comunidade ativa de utilizadores e desenvolvedores, o que resulta em uma ampla gama de recursos adicionais, plugins e integrações disponíveis para estender a sua funcionalidade.

CyberChef

O CyberChef é uma ferramenta gratuita e de código aberto usada para manipular, transformar e analisar dados de forma rápida e eficiente. É especialmente útil na área da cibersegurança, análise digital forense e análise de dados.

O CyberChef foi desenvolvido pela GCHQ, a agência de inteligência do governo do Reino Unido, e é projetado para lidar com uma ampla variedade de tarefas relacionadas com dados. Ele fornece uma interface de drag and drop, onde os utilizadores podem combinar e aplicar uma variedade de operações em cadeia para executar transformações nos dados.

Algumas das funcionalidades e características do CyberChef incluem:

1. O CyberChef oferece uma extensa lista de operações pré-definidas para executar tarefas como codificação e decodificação de diferentes formatos, criptografia e descriptografia, manipulação de strings e conversão de formatos de data e hora.
2. Possui recursos úteis para análise digital forense, como análise de ficheiros, extração de metadados, decodificação de strings ocultas, descompressão de ficheiros e análise de registos.
3. O CyberChef pode exibir visualmente dados em diferentes formatos, como imagens, gráficos ou mapas, ajudando a identificar padrões e informações relevantes nos dados processados.
4. É possível criar dados personalizadas no CyberChef, combinando várias operações numa sequência específica. Isso permite automatizar tarefas complexas e repetitivas.
5. O CyberChef suporta a importação e exportação de dados, o que facilita a colaboração e a partilha de fluxos de trabalho com outros utilizadores. Também é possível integrá-lo em outros aplicativos e scripts através da API.

ATT&CK Navigator

O ATT&CK Navigator é uma ferramenta de visualização interativa desenvolvida pela equipe MITRE ATT&CK. Ela foi projetada para auxiliar na exploração, análise e compreensão da Framework ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

O ATT&CK é um modelo de conhecimento utilizado na área da cibersegurança, que descreve as táticas, técnicas e procedimentos (TTPs) utilizados em ataques. Ela oferece uma visão detalhada dos passos que um atacante pode seguir durante um comprometimento de segurança.

O ATT&CK Navigator permite que os profissionais de segurança visualizem e interajam com o Framework ATT&CK de forma mais intuitiva e eficiente. Ela oferece recursos como:

1. O ATT&CK Navigator organiza as táticas, técnicas e procedimentos numa estrutura hierárquica, permitindo uma navegação simplificada através do Framework ATT&CK.
2. A ferramenta permite explorar as relações entre diferentes TTPs, mostrando como uma técnica pode levar a outra e fornecendo links para informações detalhadas sobre cada TTP.
3. Os utilizadores podem adicionar marcadores e anotações aos itens do ATT&CK, permitindo a personalização e o registo de observações relevantes para casos específicos.
4. É possível importar dados do ATT&CK Navigator para criar ou partilhar visualizações personalizadas. Além disso, os utilizadores podem exportar as visualizações para partilha e colaboração com outros profissionais de segurança.
5. A ferramenta é atualizada regularmente com as mais recentes informações e atualizações do Framework ATT&CK, garantindo que os utilizadores tenham acesso às informações mais recentes sobre as táticas e técnicas utilizadas.

Snort

O Snort é um sistema de detecção de intrusões (IDS) de código aberto. Ele foi desenvolvido inicialmente por Martin Roesch em 1998 e continua a ser mantido pela Cisco Systems.

O Snort foi projetado para monitorar e analisar o tráfego de rede em tempo real, a fim de identificar e alertar sobre possíveis atividades maliciosas ou intrusivas. Ele atua como uma solução de segurança para detetar e prevenir ameaças, como ataques de hackers, explorações de vulnerabilidades e malware.

Principais características e funcionalidades do Snort:

1. O Snort utiliza um mecanismo de deteção baseado em assinaturas para comparar o tráfego de rede com um conjunto de padrões pré-definidos. Esses padrões representam características de ataques conhecidos ou comportamentos suspeitos, permitindo que o Snort identifique atividades maliciosas.
2. O Snort examina pacotes de rede individualmente em tempo real, analisando cabeçalhos, cargas úteis e outros atributos para identificar padrões suspeitos ou correspondências com assinaturas conhecidas.
3. Oferece flexibilidade para personalizar as regras de deteção de acordo com as necessidades do ambiente e das ameaças específicas enfrentadas. Os administradores podem criar e modificar regras para melhorar a deteção de ameaças específicas ou comportamentos anômalos.
4. Suporta uma ampla gama de protocolos de rede, como TCP/IP, HTTP, FTP, DNS, ICMP, entre outros. Isso permite que ele analise e detete atividades maliciosas em diversos tipos de tráfego de rede.
5. Quando uma atividade maliciosa é detetada, o Snort gera alertas e regista informações detalhadas sobre a atividade suspeita. Esses alertas podem ser enviados por e-mail, registados em logs ou integrados em sistemas de gestão de segurança.

Zeek

O Zeek é um sistema de monitorização de rede de código aberto usado para análise de tráfego de rede em tempo real. Ele foi desenvolvido pelo International Computer Science Institute (ICSI) e é mantido pela comunidade Zeek.

O Zeek foi projetado para fornecer uma visão detalhada do tráfego de rede, recolhendo informações valiosas sobre as ligações, os protocolos usados e o comportamento do tráfego. Ele opera em modo passivo, monitorizando o tráfego de rede sem interferir na sua transmissão.

Principais características e funcionalidades do Zeek:

1. O Zeek captura e analisa o tráfego de rede à medida que passa pela interface de rede, fornecendo uma visão em tempo real das ligações, protocolos e fluxos de dados.
2. Possui recursos avançados de deteção de ameaças, identificando atividades suspeitas e maliciosas com base em padrões pré-definidos, como assinaturas de malware, anomalias de tráfego e comportamentos incomuns.
3. Suporta uma ampla variedade de protocolos de rede, permitindo a análise de tráfego em várias camadas, incluindo IP, TCP, UDP, HTTP, DNS, FTP, entre outros.
4. Regista informações detalhadas sobre o tráfego de rede em formato de log, permitindo a análise posterior, investigação forense e correlação de eventos. Os logs podem incluir informações sobre ligações, sessões, URLs visitados, ficheiros transferidos.
5. É altamente personalizável e extensível. Os utilizadores podem desenvolver e integrar os seus próprios scripts e plugins para adicionar funcionalidades personalizadas e adaptar o sistema às necessidades específicas do ambiente.

Suricata

O Suricata é um sistema de deteção e prevenção de intrusões (IDPS) de código aberto. Foi projetado para monitorizar o tráfego de rede em tempo real, detetar ameaças e prevenir ataques.

Assim como o Snort, o Suricata utiliza um mecanismo de deteção baseado em assinaturas para comparar o tráfego de rede com um conjunto de padrões pré-definidos, conhecidos como regras, a fim de identificar atividades maliciosas. No entanto, o Suricata oferece recursos adicionais e aprimorados em comparação com o Snort.

Principais características e funcionalidades do Suricata:

1. O Suricata utiliza regras de deteção baseadas em assinaturas para identificar atividades maliciosas, tais como exploração de vulnerabilidades, ataques de rede e malware. Essas regras podem ser personalizadas e atualizadas para se adequarem a ameaças específicas.
2. Além da deteção baseada em assinaturas, o Suricata também pode identificar comportamentos anómalos no tráfego de rede. Ele utiliza técnicas como análise de fluxo, deteção de fluxos incompletos e análise de padrões de tráfego para identificar atividades suspeitas que não correspondem a assinaturas conhecidas.
3. É capaz de analisar uma ampla variedade de protocolos de rede, incluindo IP, TCP, UDP, HTTP, DNS, FTP e muitos outros. Ele pode inspecionar o tráfego em várias camadas para detetar atividades maliciosas em diferentes níveis do protocolo.
4. Conhecido pela sua capacidade de processar grandes volumes de tráfego de rede em tempo real, mantendo um desempenho eficiente. Ele é projetado para aproveitar recursos de hardware, como múltiplos núcleos de CPU, para melhorar a velocidade de processamento.
5. Quando uma atividade maliciosa é detetada, o Suricata gera alertas e regista informações detalhadas sobre o incidente. Isso inclui informações sobre os pacotes envolvidos, as regras correspondentes e outros dados relevantes para análise posterior.

Devido aos amplos recursos que a solução disponibiliza não verificamos a necessidade de integração com outros sistemas.

IV. Definição do Cenário de Testes

Atualmente os sistemas e redes de TI das empresas são um dos principais vetores de ataque tendo em vista o ganho de vantagem através de acesso a dados ou o comprometimento total dos sistemas.

O cenário de testes SIEM refere-se ao ambiente no qual serão realizados testes e simulações para avaliar a eficácia e o desempenho do SIEM em detetar e responder a ameaças de segurança.

O objetivo principal do cenário de testes é verificar se o SIEM está configurado corretamente, se as regras de deteção estão a funcionar adequadamente e se as respostas a incidentes estão a ser executadas conforme o esperado. Isso envolve a simulação de eventos de segurança, como tentativas de invasão, malware, atividades suspeitas de utilizadores e outros incidentes relevantes.

Recorremos a um servidor físico, com um CPU Core i5, 16 GB de RAM e 1TB de Disco, para montar todo o cenário. Optamos por criar três máquinas virtuais, no Virtual Box, uma dedicada ao SIEM - Security Onion, e as outras duas dedicadas a serviços. Não dispondo de mais recursos no Servidor Físico para alocar a outras máquinas virtuais, preferimos disponibilizar serviços também no servidor físico. Tentámos ao máximo disponibilizar vários serviços em vários equipamentos para enriquecer os Datasets que iriam ser criados posteriormente com esta diversidade.

O cenário final que preparamos para o ambiente de testes, encontra-se ilustrado na figura 1.

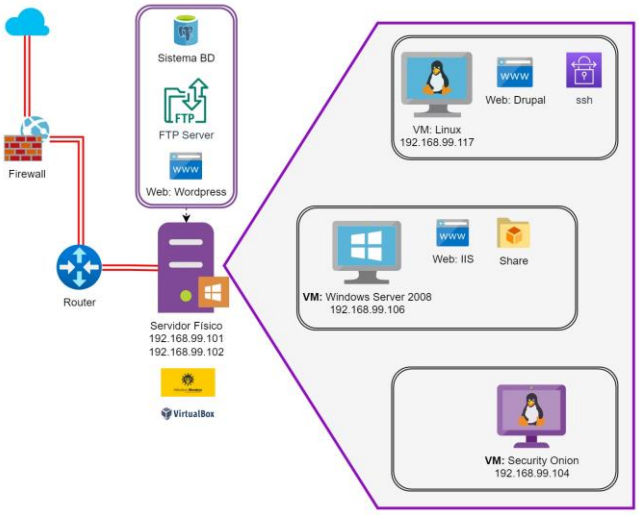


Figura 1 - Cenário de testes

Especificação - Ambiente de Testes Detalhado

Servidor Físico

- S.O. Windows 10 PRO
- Oracle Virtual Box 7.0
  - **[1]** VM Linux
  - **[2]** VM Windows Server 2008
  - **[3]** VM Security Onion
- 2 Interfaces Ethernet GB
  - 192.168.99.101
  - 192.168.99.102
- Serviços:
  - Sistema de Base Dados PostgreSQL
  - FTP Server (Filezilla)
  - WEB [apache] > Wordpress
- Software: Infection Monkey

[1] VM Linux

- S.O. Debian
- Memória: 1 GB
- Disco: SATA 4 GB
- 1 Interface Ethernet Gb
  - IP: 192.168.99.117

- Serviços:
    - WEB [apache] > Drupal
    - SSH

[2] VM Windows Server 2008

- S.O. Windows Server 2008 R2
- Memória: 2 GB
- Disco: SATA 32 GB
- 1 Interface Ethernet Gb
    - IP: 192.168.99.106
- Serviços:
    - WEB [iis] > index.html
    - Partilha de Ficheiros (SMB)

[3] VM Security Onion

- Versão: 2.3.250
- S.O. Ubuntu (64 bits)
- Memória: 8 GB
- Disco: SATA 200 GB
- 2 Interfaces Ethernet Gb
    - Captura: 172.17.0.1
    - Administração: 192.168.99.104

No Servidor Físico optamos por instalar e configurar o software Infection Monkey para simular ataques ao cenário apresentado. O Infection Monkey utiliza uma variedade de técnicas de ataque, como exploração de vulnerabilidades e bruteforce – pesquisa por senhas fracas. O principal objetivo é verificar se o Security Onion consegue identificar e alertar a equipa de resposta a incidentes, se existiu por exemplo uma tentativa de acesso a um dos sistemas que está a ser monitorizado. A instalação e configuração do Infection Monkey está documentada no anexo[2].

V. SIMULAÇÃO, MONITORIZAÇÃO E ANÁLISE DO CENÁRIO DE TESTES

Para além das ferramentas que já foram descritas no Capítulo III, o Security Onion conta com vários módulos, que formam o menu da solução, nomeadamente: *Alerts*, *Dashboards*, *Hunt*, *Cases*, *PCAP*, *Grid*, *Downloads* e por último a *Administration*. Segue-se uma breve descrição de cada uma das opções.

A. ALERTS (Alertas)

A interface de alertas permite rever e gerir os alertas de segurança do Security Onion, que podem ter origem nas diversas ferramentas (suricata, zeek, wazuh, etc).

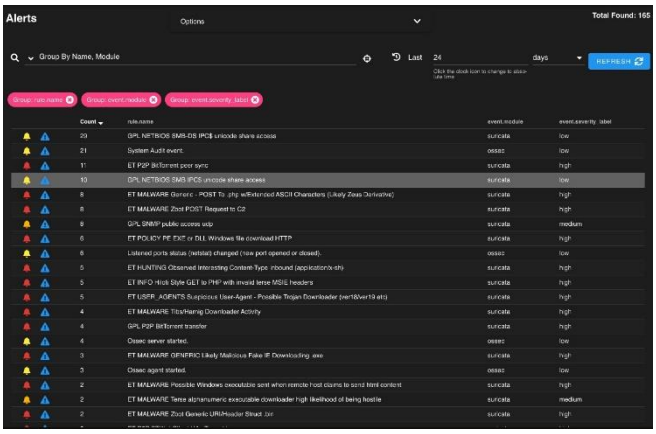


Figura 2 - Lista de Alertas

Caso de estudo - Alertas

Foram identificados 2 alertas, um do módulo Suricata (IDS) e outro do módulo OSSEC. Ambos de severidade BAIXA. O primeiro já ocorreu por 98 vezes e o segundo apenas com uma ocorrência, conforme é possível verificar na ilustração seguinte.

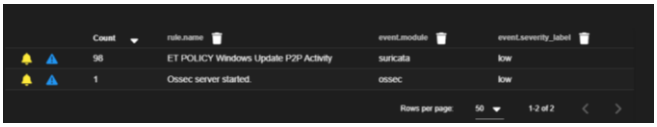


Figura 3 - Alertas (1)

Para ignorar o alerta, é só clicar sobre o "sino" e o mesmo deixa de ser apresentado na grelha, conforme é possível verificar na ilustração seguinte.

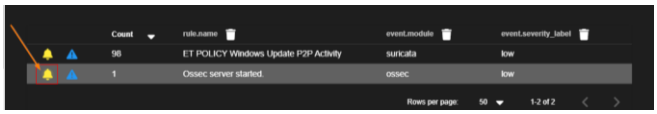


Figura 4 - Alertas (2)

Se o alerta tiver de ser analisado pela equipa de resposta a incidentes, o mesmo terá de ser escalado, conforme é possível verificar na ilustração seguinte.

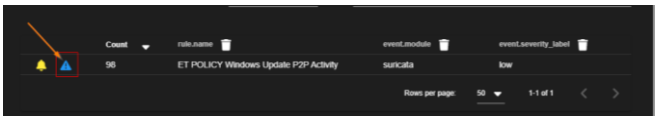


Figura 5 - Alertas (3)

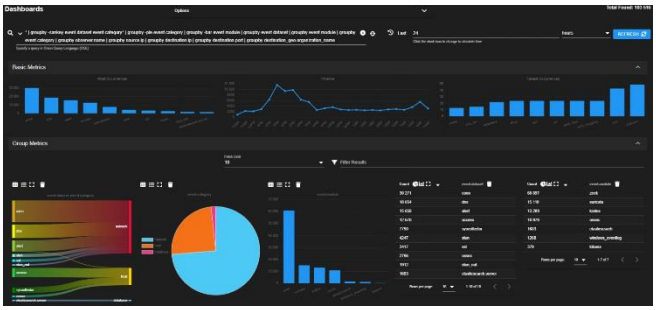
O mesmo pode dar lugar a um novo caso (ponto 1), ou pode ser associado a um caso já existente (ponto 2), conforme é possível verificar na ilustração seguinte.

Figura 6 - Alertas (4)

[2] anexo_II_instalacao_configuracao_InfectionMonkey.pdf

B. DASHBOARDS (Painéis)

Permite personalizar os painéis à medida das necessidades. Com tabelas, gráficos e diagramas intuitivos e atraentes.



Caso de estudo – DASHBOARDS

Gráficos de eventos por Categoria.

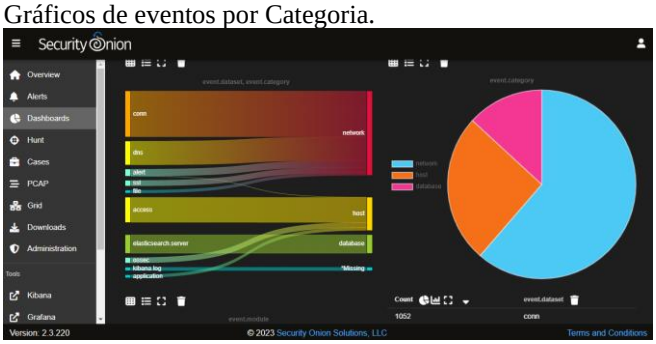


Figura 7 - Dashboard (1)

Contagem de eventos - Ferramenta [Zeek, Suricata, Ossec, Windows EventLog, Wazuh, etc] (Ponto 1 – da imagem abaixo). Contagem de eventos – Categoria [network, host, database, etc] (Ponto 2 – da imagem abaixo).

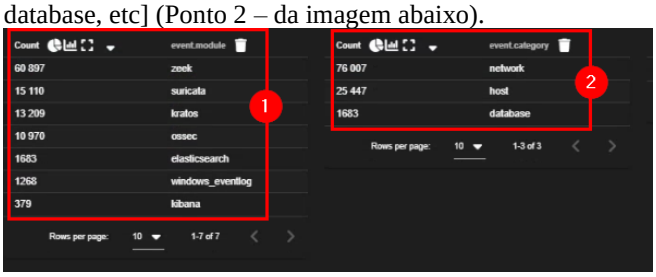


Figura 8 - Dashboard (2)

Contagem de eventos – IP de Origem (Ponto 1 – da imagem abaixo). Contagem de eventos – IP de Destino (Ponto 2 – da imagem abaixo). Contagem de eventos – Porto de Destino (Ponto 3 – da imagem abaixo).

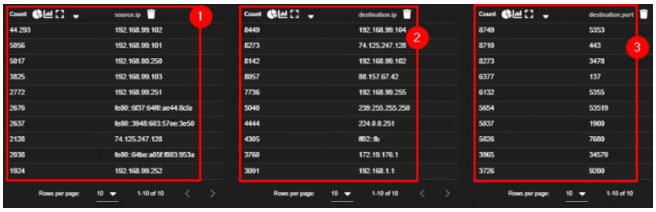


Figura 9 - Dashboard (3)

Contagem de eventos – Nome da organização de Destino, conforme é possível verificar na ilustração seguinte.

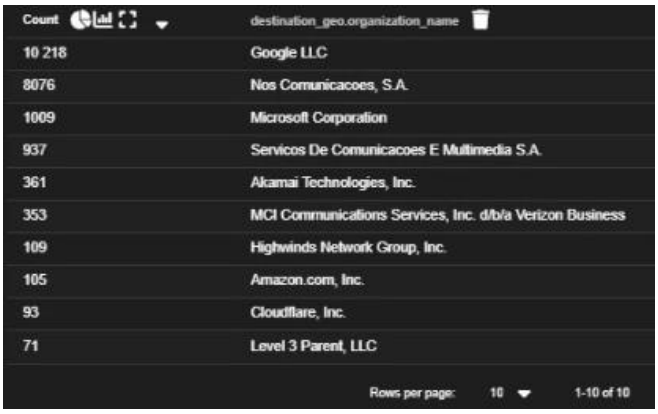


Figura 10 - Dashboard (4)

E na parte inferior do Dashboard é possível verificar todos os eventos, com a possibilidade de Escalar um evento para ser analisado por uma equipa de nível superior (Ponto 1 – da imagem abaixo). A grelha é dinâmica e permite a ordenação por qualquer um dos campos, embora os campos com maior relevo é o timestamp (Ponto 2 – da imagem abaixo) e o log_level (Ponto 3 – da imagem abaixo).

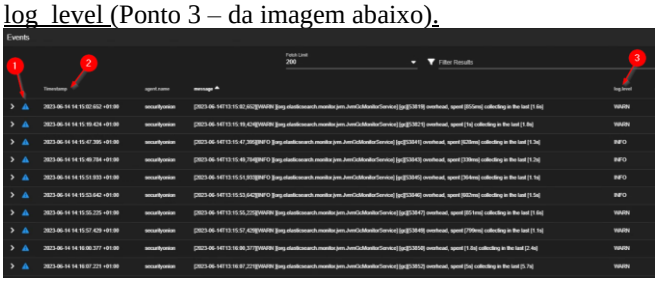
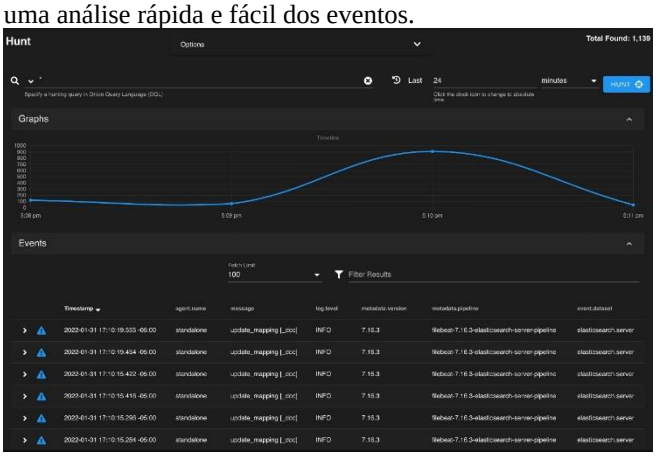


Figura 11 - Dashboard (4)

C. HUNT (Análise Rápida)

A interface **Hunt** foi criada especificamente para permitir uma análise rápida e fácil dos eventos.



Caso de estudo – HUNT

Aceder a "Hunt" através do menu Principal e selecionar qual a consulta (query) pretendida, bem como o período, conforme é possível verificar na ilustração seguinte.

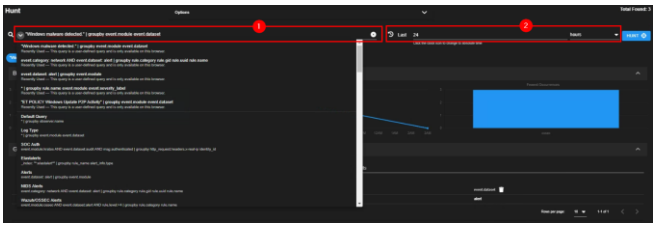


Figura 12 - Hunt (1)

Existe uma lista extensa de consultas já pré-configuradas, como por exemplo: por protocolo (HTTP, FTP, DNS, SMB, etc), por ligação, por módulo (wazuh, zeek, etc). E para o mesmo protocolo existem várias consultas, conforme é possível verificar na ilustração seguinte.

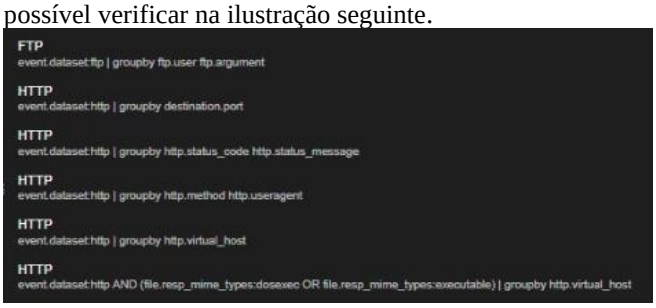
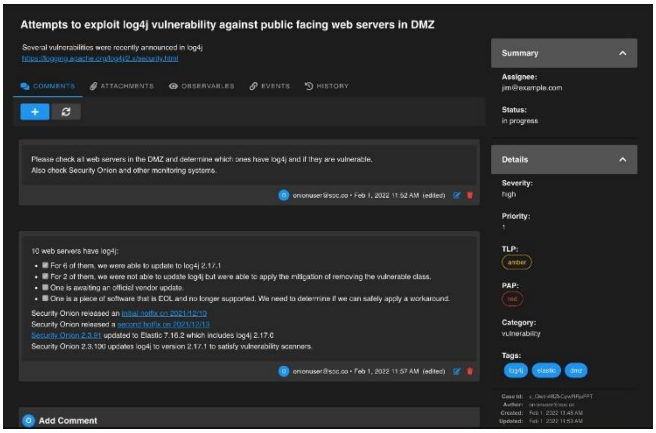


Figura 13 - Hunt (2)

*D. **CASES (Casos)***

A interface nativa de casos oferece uma plataforma de resposta a incidentes que se integra totalmente com os módulos **Hunt** and **Alerts**.



Caso de estudo – CASES

Aceder a "Cases" através do menu Principal e verificar qual é o caso a analisar, conforme é possível verificar na ilustração seguinte.

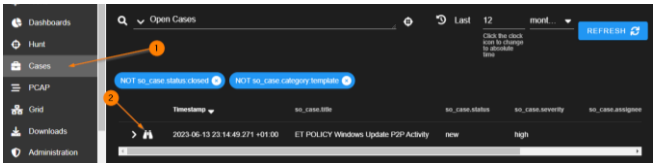


Figura 14 - Casos (1)

No topo da página é possível aplicar o filtro por casos em aberto, fechado,

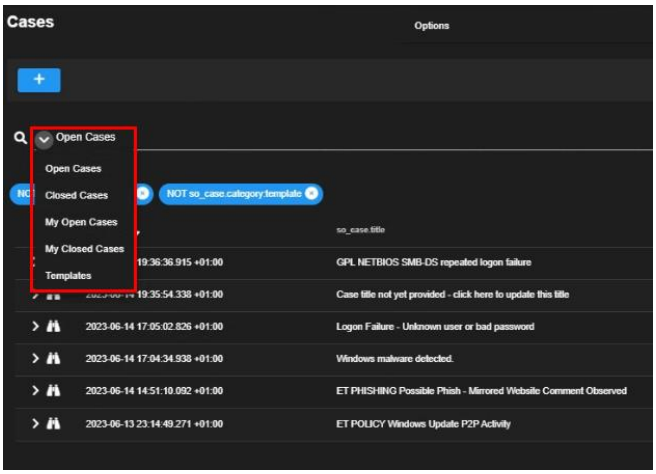


Figura 15 - Casos (2)

Verificar o detalhe de um caso (incidente), conforme é possível verificar na ilustração seguinte.

Figura 16 - Casos (3)

O caso pode ser atribuído a um membro da equipa de resposta a incidentes e este tem um estado associado que pode ser "*new*", "*in progress*" ou "*closed*" (Ponto 1 – da imagem abaixo).

Bem como a classificação do incidente (Ponto 2 – da imagem abaixo), com a definição da Severidade (*low*, *médium*, *high*, *critical*), Prioridade, o TLP (*red*, *amber+strict*, *amber*, *green e clear)*, a PAP *(White, green, amber e red)* a Categoria (geral e com a possibilidade de registar novas categorias) e por último as TAGS (*confirmed*, *false-positive*, *pending*), conforme é possível verificar na ilustração seguinte.

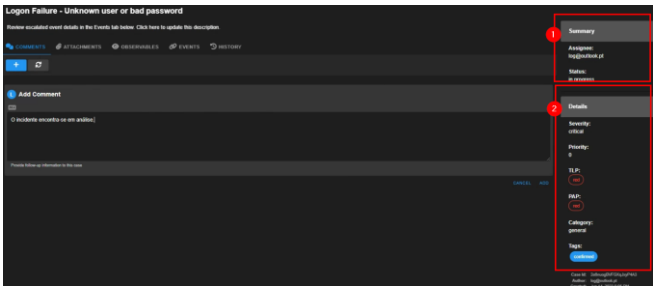


Figura 17 - Casos (4)

Se necessário, é possível recolher toda a informação do caso em análise, conforme é possível verificar na ilustração seguinte.

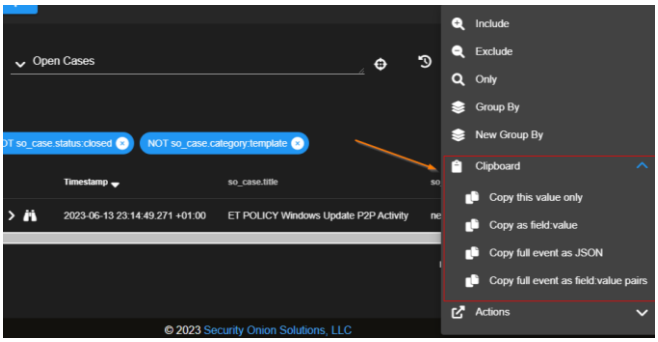


Figura 18 - Casos (5)

Exemplo da recolha da informação do evento no formato JSON:

{"@timestamp":"2023-06-13T22:14:49.27193344Z","so_case.assigneeId":"","so_case.category":"","so_case.completeTime":null,"so_case.createTime":"2023-06-13T22:14:49.271927763Z","so_case.description":"Review escalated event details in the Events tab below. Click here to update this description.","so_case.pap":"","so_case.priority":0,"so_case.severity":"high","so_case.startTime":null,"so_case.status":"new","so_case.tags":null,"so_case.template":"","so_case.title":"ET POLICY Windows Update P2P Activity","so_case.tlp":"","so_case.userId":"log@outlook.pt","so_kind":"case","soc_id":"Nk7TtogBlir0xRjTb1Xc","soc_score":3.3862944,"soc_type":"","soc_timestamp":"2023-06-13T22:14:49.271Z","soc_source":"securityonion:so-case"}

E possível realizar várias ações sobre a informação do evento, como por exemplo, pesquisar no motor de busca do Google (figura 11) ou no Virus Total, conforme é possível verificar na ilustração seguinte.

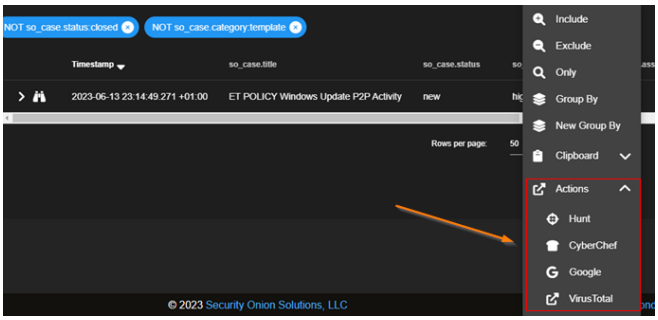


Figura 19 - Casos (6)

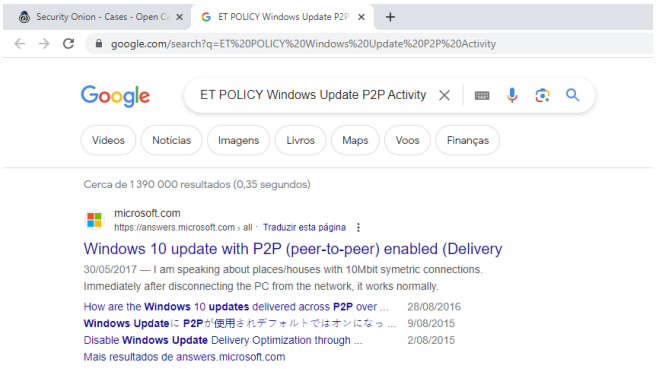


Figura 20 - Casos (Pesquisa no Google)

E. PCAP (Análise Rápida de Pacotes)

Esta interface permite aceder à captura completa de pacotes que foram gravados pelo Stenographer.

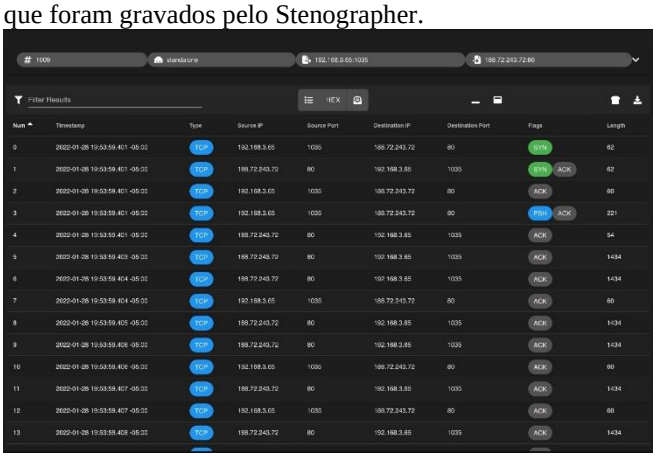


Figura 21 - Opçãp PCAP

Caso de estudo – PCAP

A partir de uma das opções "Dashboards", "Alerts" ou "Hunt" é possível enviar um determinado evento para análise do PCAP, conforme é possível verificar na ilustração seguinte.

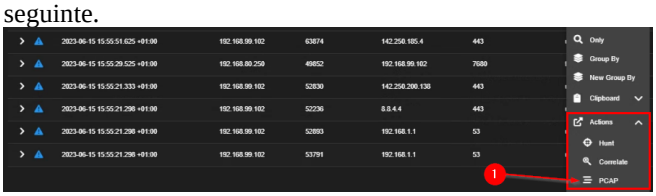


Figura 22 - Ação PCAP

Ao clicar na ação "PCAP", será adicionado um novo registo para análise de toda a comunicação sobre aquele evento, conforme é possível verificar na ilustração seguinte.

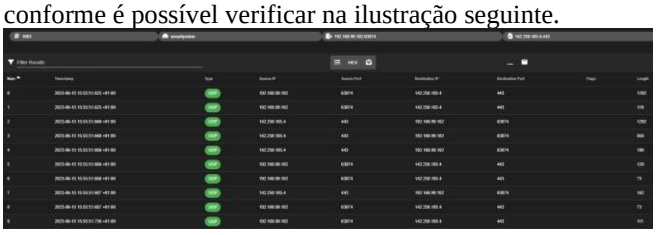


Figura 23 - Analisar comunicação

Para além da análise, é possível descarregar um ficheiro para analise externa, como por exemplo no Wireshark ou NetworkMiner.

F. Grid

Permite verificar o estado de todos os equipamentos Security Onion. No cenário de testes, existe apenas uma instância do Security onion, conforme é possível verificar na ilustração seguinte.

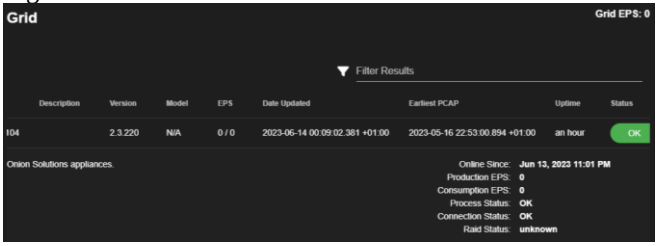


Figura 24 - Grid - Security Onion

G. *Downloads*

É possível descarregar do SecurityOnion os agentes dos diversos módulos (Elasticsearch, wazuh, etc) para instalar nos equipamentos a monitorizar.

Caso de estudo – Downloads

Um dos utilitários que utilizámos no cenário de testes, foi o Wazuh Agent. (Ponto 1 – da figura 21)

Figura 25 - Downloads dos utilitários

Após o download, o aplicativo foi instalado no Servidor Físico (192.168.99.101) e no VM Windows Server 2008 (192.168.99.106).

Concluída a instalação dos agentes tivemos de realizar algumas configurações no Security Onion, através de uma ligação ssh, para o efeito recorremos ao PuTTy, conforme é possível verificar na ilustração seguinte.

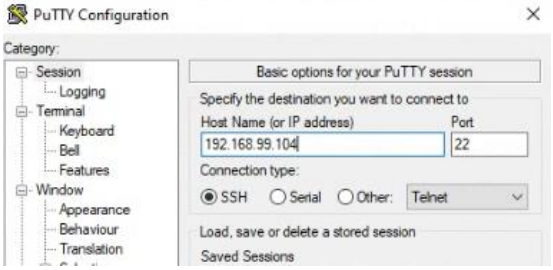


Figura 26 – Iniciar ligação ssh (PuTTy)

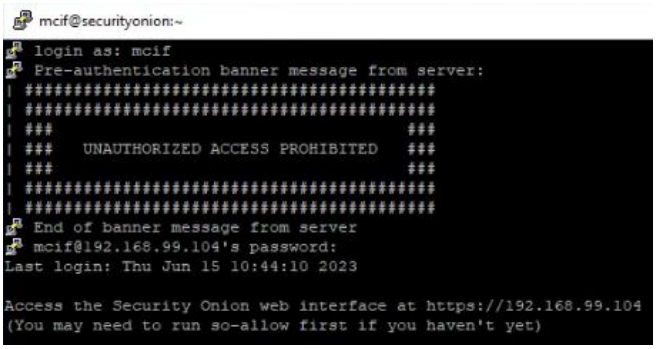


Figura 27 - Ligação estabelecida (ssh)

Tarefas a realizar no Security Onion (via ssh)

1) Autorizar os agentes do Wazuh, de uma determinada rede ou IP, a comunicar com o porto 1514 (TCP e UDP)

$ sudo so-allow

Opção: w

IP ou Rede: 192.168.99.0/24

Figura 28 - Autorizar comunicação dos agentes do Wazuh

2) Registar um novo Agente no Security Onion e consultar a key para introduzir posteriormente no agente.

$ sudo so-wazuh-agent-manage

Opção: A

Nome Equipamento: ServidorFísico

IP do Agente: 192.168.99.101

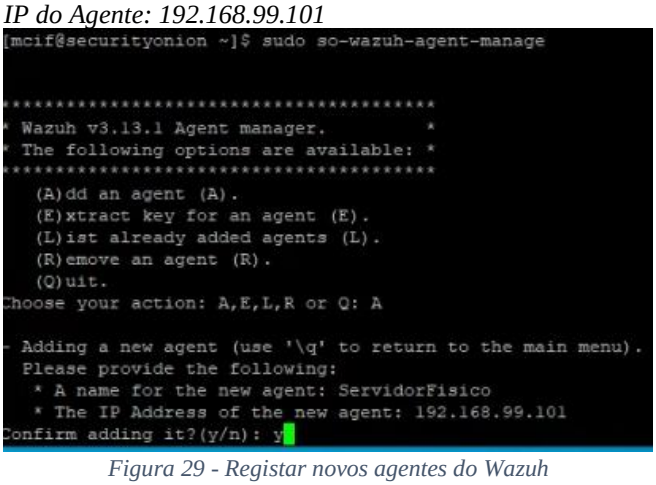


Figura 29 - Registar novos agentes do Wazuh

Concluído o registo dos agentes, voltar ao menu e selecionar a opção "L", para listar todos os equipamentos que estão registados, conforme é possível verificar na ilustração seguinte.

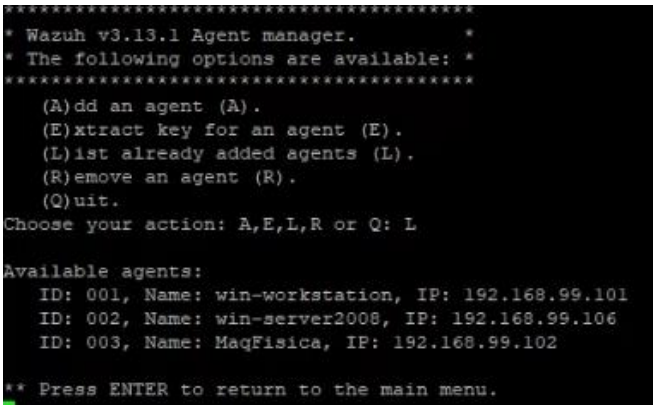


Figura 30 - Listar agentes Wazuh registados

O passo seguinte, foi a extração das key's dos agentes, registados anteriormente no Security Onion (Ponto 1 e 2 da figura 27), para concluir a instalação dos agentes nos dois equipamentos.

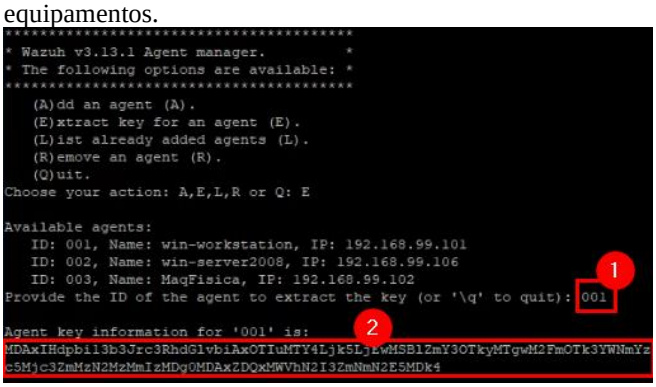


Figura 31 - Extrair key do Agent 001

Voltámos aos equipamentos (Servidor Físico e à máquina virtual Windows Server 2008) para configurar os agentes. O agente foi instalado na diretoria "C:\Program Files (x86)\ossec-agent", e nesta tivemos de executar o ficheiro "win32ui.exe" e introduzir o IP do Security Onion e a key que foi extraída para aquele equipamento especifico, e para concluir clicar em "*Save*", conforme é possível verificar na ilustração seguinte.

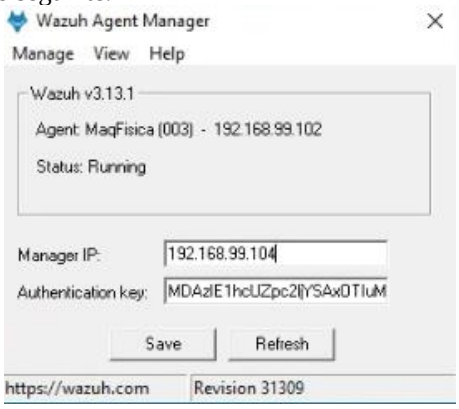


Figura 32 - Configurar Agent Wazuh

Para finalizar, foi necessário aceder ao serviços locais do Windows (services.msc) e reiniciar o serviço "Wazuh", conforme é possível verificar na ilustração seguinte.

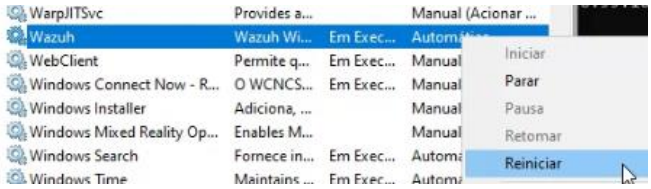


Figura 33 - Reiniciar agent Wazuh

*H. **Administration (Administração)***

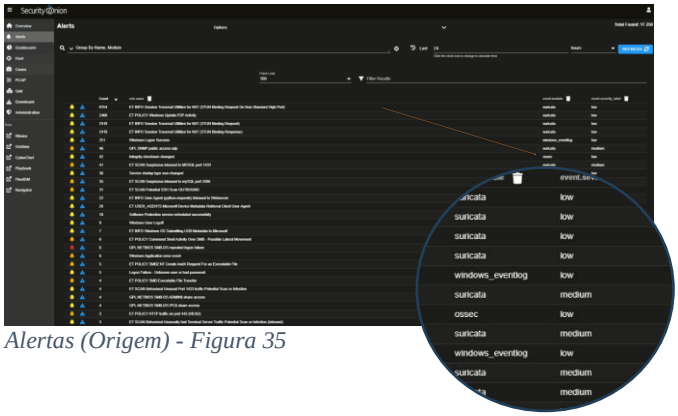
É possível verificar os utilizadores que estão criados no sistema e qual o nível de acesso que está atribuído, conforme é possível verificar na ilustração seguinte.

Figura 34 - Lista de Utilizadores

A gestão das contas é via linha de comandos. Por exemplo, para criar uma nova conta de utilizador terá de ser executado o seguinte comando:
$ sudo so-user-add "nome-utilizador".

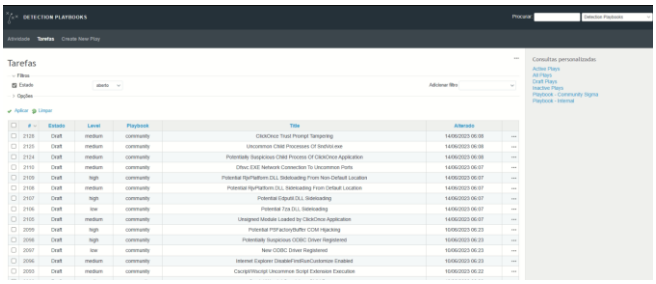
VI. DEFINIÇÃO E CONFIGURAÇÃO DE ALERTAS DE SEGURANÇA

No "Security Onion" os alertas de segurança podem ter como origem qualquer um dos módulos de deteção já descritos no capítulo II como podemos verificar na figura 21.



Alertas (Origem) - Figura 35

Para além dos módulos de deteção é possível adicionar regras de deteção através do módulo "Playbook".



Palybook - Figura 36

As regras adicionadas ao playbook são totalmente independentes e surgem como uma estratégia de deteção especifica.

Um playbook refere-se a uma sequência de ações automatizadas executadas em resposta a eventos de segurança. Um playbook é projetado para lidar com um tipo específico de incidente ou atividade maliciosa e contém instruções detalhadas sobre como responder a esse evento.

Os playbook´s no Security Onion geralmente são criados utilizando uma linguagem de programação chamada YAML (YAML Ain't Markup Language). Ela contém uma série de etapas ou tarefas que são executadas automaticamente quando um determinado evento de segurança é acionado. Por exemplo, um playbook pode ser criado para lidar com um alerta de invasão num sistema específico.

As tarefas em um playbook podem incluir a execução de comandos em sistemas afetados, a recolha de informações relevantes, a notificação de pessoal de segurança, a criação de registos e a implementação de medidas corretivas. O objetivo de um playbook é automatizar o processo de resposta a incidentes, economizando tempo e garantindo uma resposta consistente e eficiente.

Os playbooks no Security Onion podem ser personalizados para atender às necessidades específicas de uma organização e são uma parte importante de um programa abrangente de cibersegurança. Eles ajudam a garantir que as ameaças sejam tratadas de forma consistente e eficaz, reduzindo o tempo de resposta e minimizando o impacto de um incidente de segurança.

Exemplo da Estrutura de um Playbook (YAML):

```
- name: Playbook de Detecção de Malware
  hosts: security-onion
  tasks:
    - name: Recolha de Informações
      command: <comando para recolher informações relevantes do sistema afetado>

    - name: Notificar a Equipa de Segurança
      command: <comando para enviar notificação por e-mail ou mensagem>

    - name: Isolar o Sistema Afetado
      command: <comando para isolar o sistema afetado da rede>

    - name: Analisar Logs
      command: <comando para analisar logs do sistema afetado>

    - name: Tomar Ações Corretivas
      command: <comando para executar ações corretivas no sistema afetado>

    - name: Gerar Registo do Incidente
      command: <comando para gerar um registo detalhado do incidente>

    - name: Notificar a Equipa de Resposta a Incidentes
      command: <comando para notificar a equipa de resposta a incidentes>

    - name: Limpar Evidências
      command: <comando para limpar evidências no sistema afetado>

    - name: Restaurar Conectividade
      command: <comando para restaurar a conectividade do sistema afetado>

    - name: Finalizar Playbook
      command: <comando para registar o término do playbook>
```

VII. RECOLHA, TRATAMENTO E ANÁLISE DE EVENTOS (LOGS)

O Security Onion utiliza várias ferramentas, como IDS (sistema de deteção de intrusão), NSM (monitorização de segurança de rede) e análise de registos, para recolher eventos de segurança da rede.

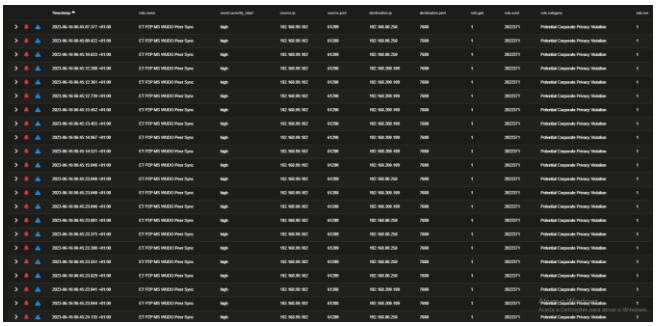


Figura 37 - Lista de eventos

Essas ferramentas monitorizam o tráfego de rede em tempo real e registam eventos detalhados suspeitos ou maliciosos.

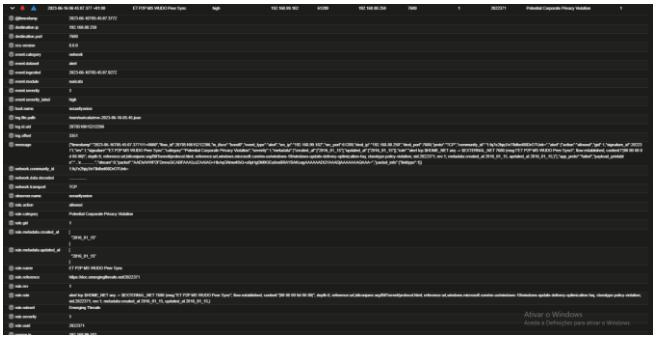


Figura 38 - Evento Detalhado

Esses eventos de segurança recolhidos são armazenados em um ou mais repositórios de dados, como bases de dados ou sistemas de ficheiros. O Security Onion utiliza o Elastic Stack (Elasticsearch, Logstash e Kibana) como uma das opções de armazenamento e visualização dos eventos. Os eventos armazenados são processados e analisados para identificar atividades suspeitas, indicadores de comprometimento (IOC) e padrões de comportamento malicioso. Isso pode envolver a aplicação de regras de deteção, algoritmos de análise comportamental e a correlação de eventos para obter uma compreensão abrangente do ambiente de segurança. Com base na análise dos eventos, o Security Onion pode gerar alertas e notificações para informar sobre possíveis ameaças de segurança. Quando um evento suspeito é identificado, a equipa de segurança pode realizar investigações adicionais usando recursos como análise forense, visualização de dados e consulta de logs.

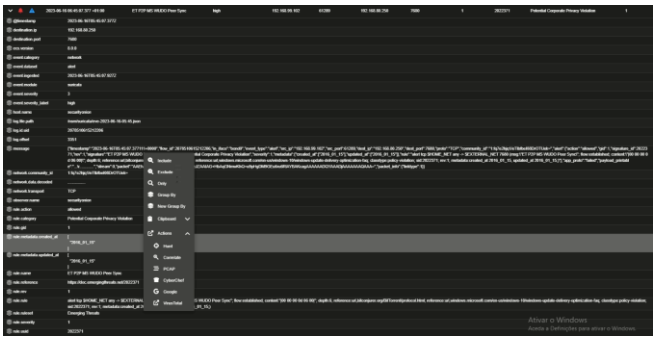


Figura 39 - Investigações dos Eventos

Com base nas descobertas, podem ser tomadas medidas corretivas para mitigar o impacto do incidente e evitar futuras ocorrências. Durante todo o processo, é importante manter registos detalhados de eventos, ações tomadas e resultados das investigações. Esses registos são essenciais para posterior análise, revisão de segurança e conformidade regulatória. O Security Onion oferece recursos de geração de relatórios e registos para facilitar essa documentação.

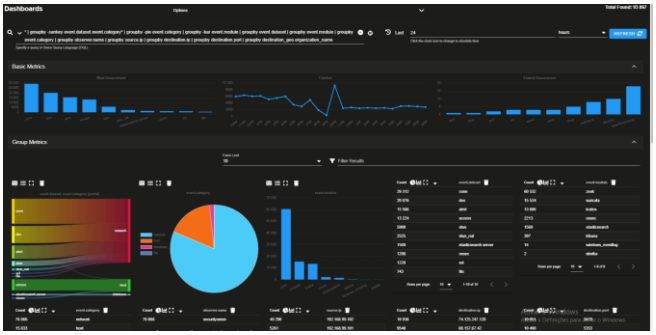


Figura 40 - Relatórios

A análise de eventos no Security Onion é baseada em regras pré-definidas e personalizadas, que permitem a rápida deteção de possíveis ameaças. É possível definir diferentes níveis de prioridade para os eventos, de forma a garantir uma resposta mais rápida a incidentes críticos.
Em resumo, o Security Onion permite recolher, tratar e analisar eventos de segurança de forma integrada, proporcionando uma abordagem proativa à deteção de possíveis ameaças.

VIII. TÉCNICAS UTILIZADAS NA CRIAÇÃO E ANÁLISE DE UM DATA SET

O Security Onion possui uma completa e poderosa estrutura de criação e análise de log´s. O processamento de log´s externamente à plataforma torna-se um trabalho pouco atrativo uma vez que toda a informação está disponível em tempo real e relacionada entre ela, da análise que fizemos aos log´s e disponibilização da informação pareceu-nos que cobriam as necessidades com bastante eficácia. Os dados que compõem os log´s são recolhidos pelos módulos (agentes), aos quais não temos acesso, e são logo manipulados pelo security onion. Os dados que conseguimos extrair já têm tratamento pelos algoritmos da plataforma. Apresentamos de seguida alguns exemplos de dataset's gerados pela plataforma.
Na figura 41 e 42 podemos observar os datasets disponíveis na plataforma e os módulo que geram os dados.

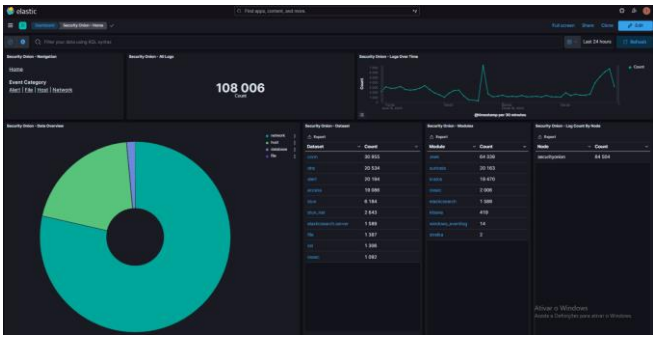


Figura 41 - Dataset´s e Módulos

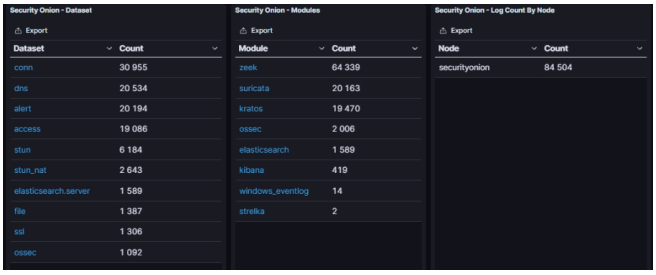


Figura 42 - Dataset´s e Módulos (Detalhe)

Na figura 43 são apresentados os detalhes do dataset "conn".

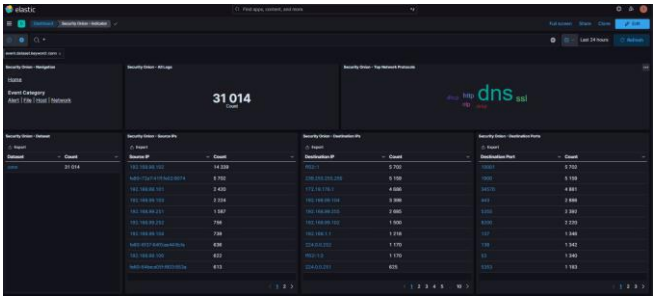


Figura 43 - Ligações

Na figura 43 são apresentados os detalhes do dataset "alerts".

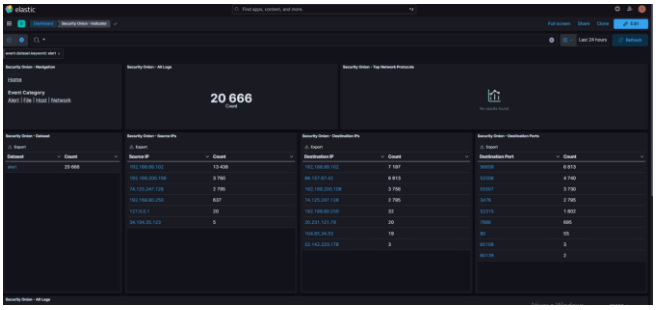


Figura 44 - Dataset alerts

Na figura 45 é possível ver a informação disponibilizada pelo dataset “Alerts” para o endereço ip 34.104.35.123.

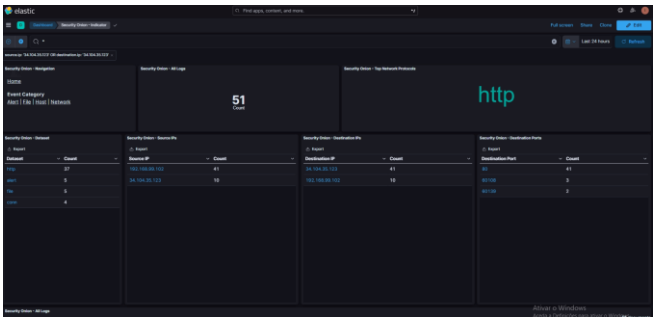


Figura 45 - Informação IP 34.104.35.123

Os dados dos vários datasets estão relacionados entre eles pelos ID (log.id.uid) que permite correlacionar os log´s acrescentando uma profundidade de análise bastante grande ao longo de todos os módulos do Security Onion.

Figura 46 - Relação Entre Registos (log.id.uid)

Da plataforma Security Onion foi extraído o log de ligações (conn) o qual foi entregue para análise na aplicação Rapid Miner, o objetivo era conseguir perceber quais os endereços IP e portos mais solicitados (porto destino).

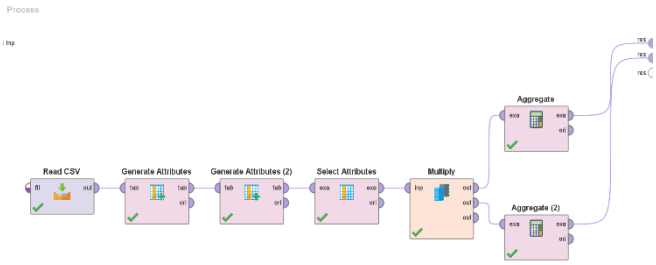


Figura 47 – Tratamento do Dataset no Rapid Miner

Row No.	destination.ip	percentage_count(destinat...
4	192.168.99.104	21.674
1	192.168.99.102	15.053
3	239.255.255.250	13.804
10	192.168.1.1	9.307
2	192.168.99.255	8.307
21	8.8.8.8	3.373
19	95.100.135.187	3.186

Figura 48 - Resultado da Análise (Endereço IP)

Row No.	destination.ip	destination.port	percentage_cou...
48	192.168.99.102	7680	15.053
51	192.168.99.104	9200	13.866
87	239.255.255.250	1900	13.741
46	192.168.1.1	53	9.307
50	192.168.99.104	1514	4.685
52	192.168.99.255	137	4.372
53	192.168.99.255	138	3.935

Figura 49 - Resultado da Análise (Portos)

IX. CONCLUSÃO

O SIEM - Security Onion é uma opção bastante interessante para quem deseja garantir a proteção dos sistemas e redes de uma organização de forma efetiva e eficiente. Com uma ampla gama de ferramentas e recursos, é possível integrar diferentes funcionalidades num único ambiente, o que possibilita uma monitorização constante e por sua vez a identificação de ameaças em tempo real.

Além disso, a implementação do Security Onion oferece uma série de benefícios adicionais, como a possibilidade de personalização e adaptação às necessidades específicas de cada organização, a automação de processos e a otimização do fluxo de trabalho dos profissionais de segurança.

O Security Onion é uma solução de monitorização e análise bastante completa. Permite a implementação de uma solução que garante uma resposta eficaz e de baixo custo de implementação em relação aos SIEM proprietários. A complementaridade conseguida entre os módulos e a correlação entre os registos garantem-nos uma profundidade de informação significativa e de grande mais valia em termos técnicos. A apresentação de dados é atrativa, clara e objetiva, sendo de grande facilidade a utilização dos interfaces nos diferentes módulos.

As conclusões deduzidas de um cenário de testes como o apresentado podem não ser escaladas para um ambiente de produção real. O desempenho do sistema em cenário de testes mostrou-se por vezes instável porque as condições mínimas ao nível do Hardware não estavam reunidas. O volume das amostras de comunicações são limitadas derivado à dimensão do cenário de testes.

Portanto, a implementação do Security Onion é uma excelente opção para quem deseja adotar uma abordagem abrangente e proativa em relação à segurança da informação, mas deve ser parte de um conjunto de medidas e estratégias adotadas pela equipa de segurança, a fim de garantir uma proteção sólida e completa para seus sistemas e redes.

Deixamos algumas sugestões para quem tiver interesse em instalar e configurar o Security Onion:

1) Documentação: o Security Onion tem uma documentação completa e detalhada que pode ajudar a entender melhor cada funcionalidade e as opções de parametrização. https://docs.securityonion.net/en/2.3/index.html

Certifique-se de ler a documentação relevante antes de iniciar uma configuração.

2) Hardware: Para evitar problemas com o desempenho da solução, garanta no mínimo os seguintes recursos: 16 GB de RAM, 4 núcleos de CPU e 200 GB de armazenamento.
3) Modo básico: Caso disponha de poucos conhecimentos em segurança de redes ou em ferramentas como o Security Onion, comece com as configurações e parametrizações básicas antes de avançar para as opções mais avançadas.
4) Ambiente de Testes: Uma solução como o Security Onion, antes de ser colocada em Produção, tem de ser muito bem testada. O ambiente de testes permite-lhe experimentar diferentes opções de parametrização e ao mesmo tempo verificar o desempenho e resultados obtidos, e ajustar caso seja necessário.

X. REFERÊNCIAS

[1] S. Onion, "securityonion.net," [Online]. Available: https://docs.securityonion.net/en/2.3/.