Implementação de um Sistema Centralizado de Gestão de Logs com Wazuh para a Universidade Aberta

José Ribeiro[1], Silvana Oliveira[2], Sofia Teixeira[3], Vitor Rocio[4]
[1] Universidade Aberta,— 1601792@estudante.uab.pt
[2] Universidade Aberta,— 2102785@estudante.uab.pt
[3] Universidade Aberta,— 2103022@estudante.uab.pt
[4] Universidade Aberta, INESC TEC, LE@D — vitor.rocio@uab.pt

Resumo

Este artigo descreve a implementação experimental de um sistema centralizado de gestão de *logs* baseado na plataforma *open-source Wazuh*, desenvolvido no contexto da Universidade Aberta. O principal objetivo consistiu em estudar e configurar uma solução distribuída capaz de consolidar e monitorizar dados de segurança provenientes de diferentes origens, contribuindo para a deteção precoce de anomalias e o reforço da cibersegurança institucional. A metodologia envolveu a criação de uma arquitetura em três camadas (Wazuh *Manager, Indexer e Dashboard*) em ambiente *cloud*, com validação das comunicações e análise de logs simulados. Os resultados obtidos demonstram a viabilidade da solução e evidenciam o potencial da abordagem para futuras integrações com os sistemas reais da Universidade Aberta.

Palavras-chave: gestão de logs, cibersegurança, monitorização de segurança, Wazuh, Universidade Aberta

Title: Implementation of a Centralized Log Management System with Wazuh for Universidade Aberta

Abstract: This paper describes the experimental implementation of a centralized log management system based on the open-source Wazuh platform, developed within the context of Universidade Aberta. The main goal was to study and configure a distributed solution capable of consolidating and monitoring security data from multiple sources, contributing to the early detection of anomalies and the strengthening of institutional cybersecurity. The methodology involved designing a three-layer architecture (Wazuh Manager, Indexer, and Dashboard) in a cloud environment, with communication validation and analysis of simulated logs. The results demonstrate the feasibility of the solution and highlight its potential for future integration with Universidade Aberta's real systems.

Keywords: log management, cybersecurity, security monitoring, Wazuh, Universidade Aberta

1. Introdução

Vivemos numa era digital em que a informação é um dos ativos mais valiosos das organizações. Esta realidade exige soluções eficazes que garantam a segurança e a integridade dos dados. A crescente incidência de ciberataques e violações de privacidade reforça a importância de sistemas capazes de realizar monitorização contínua e deteção precoce de incidentes [ENISA, 2023].

Na Universidade Aberta (UAb), que ministra a sua oferta formativa em modalidade online, a forte dependência de plataformas como o Moodle, o WordPress e bases de dados administrativas origina diariamente um elevado volume de logs e eventos de segurança. Paralelamente, o cumprimento de normas como o RGPD impõe exigências acrescidas de integridade, confidencialidade e disponibilidade da informação [ENISA,2023]. Neste artigo descreve-se a implementação de uma solução centralizada de gestão de logs baseada numa plataforma SIEM (*Security Information and Event Management*), desenvolvida para otimizar a recolha, correlação e análise de eventos de segurança na Universidade Aberta. A Secção 1 enquadra o problema, os objetivos e a solução proposta; a Secção 2 descreve a metodologia de implementação e os testes realizados; e a Secção 3 apresenta as conclusões e perspetivas futuras.

1.1. Problema

Os Serviços de Informática da Universidade Aberta identificaram a necessidade de uma solução eficaz para centralizar e gerir os logs gerados pelos diversos sistemas e aplicações da instituição. Estes registos automáticos documentam o funcionamento, os acessos e os erros ocorridos nos diferentes componentes tecnológicos [Stallings, 2012].

A dispersão dos logs por múltiplos servidores e bases de dados dificultava a correlação de eventos e a deteção atempada de incidentes, reduzindo a visibilidade sobre a infraestrutura e comprometendo o cumprimento de requisitos de auditoria e conformidade, nomeadamente no âmbito do Regulamento Geral de Proteção de Dados (RGPD) e das normas relativas à segurança da informação (ISO 27001).

A inexistência de uma solução centralizada implicava uma dependência acrescida de processos manuais de análise, o que diminuía a eficiência das ações de monitorização e resposta a incidentes. A ausência de mecanismos automáticos de recolha e correlação de eventos também limitava a capacidade de identificar padrões de comportamento anómalos ou potenciais ameaças, de forma proativa.

Face a estas limitações, tornou-se necessário conceber uma abordagem que permitisse centralizar a recolha, o armazenamento e a análise dos logs provenientes de diferentes fontes, proporcionando uma visão global e integrada da infraestrutura tecnológica e reforçando a segurança e a fiabilidade dos serviços institucionais.

1.2. Estado da arte e trabalho relacionado

As práticas atuais de *logging* enfrentam desafios tais como implementação arbitrária e suporte inadequado para tarefas operacionais. Existe uma necessidade de abordagens mais sistemáticas, que contemplem várias questões: porquê registar (log), onde registar, o que registar e qual a qualidade dos registos [Gu et al., 2022].

As finalidades dos logs são variadas: auditoria dos sistemas, recolha de dados e estatísticas de operação, análise da eficiência, conhecimento da base de utilizadores, etc. Uma das aplicações mais importantes é permitir a resposta eficaz a incidentes, como erros de operação ou ciberataques [Nguyễn, 2022].

Os logs são normalmente registados junto do serviço que os gera, o que numa organização minimamente complexa, significa que estão dispersos por vários servidores, lógica e, muitas vezes, fisicamente dispersos. Havendo sistemas que concentram a informação dos logs num único local ou serviço, são frequentemente dependentes de tecnologias específicas e têm dificuldade em compatibilizar sistemas operativos ou vários serviços de natureza diferente [Strileț chi et al., 2025].

Por outro lado, a informação a registar e a sua qualidade é também muito variável, o que levanta questões relativas à uniformidade e granularidade da informação num repositório central de dados.

A centralização dos logs numa organização é assim uma etapa fundamental para a gestão da informação, da resposta eficaz a ocorrências ou incidentes e da consequente melhoria da cibersegurança. No campo da educação a distância, que depende do fornecimento de serviços online, a centralização de logs é uma preocupação que não é recente [Peled & Rashty, 1999], e soluções específicas para esta área de atividade abordam aspetos particulares, como a previsão do desempenho dos estudantes [Latif et al., 2023] ou deteção de fraude [Alsabhan, 2023].

1.3. Objetivos

O objetivo geral deste trabalho consiste no estudo e implementação experimental de uma solução de gestão centralizada de logs que melhore a monitorização e a segurança dos sistemas da UAb. Os objetivos específicos incluem:

1. Identificar requisitos funcionais (recolha, armazenamento, consulta, relatórios e alarmística);
2. Definir requisitos não funcionais (retenção de dados, segurança, desempenho e escalabilidade);
3. Desenhar a arquitetura de centralização e integração dos logs;
4. Instalar e configurar os componentes necessários à recolha e análise dos logs;
5. Implementar mecanismos de deteção automática de incidentes;
6. Simular cenários de falha e resposta;
7. Testar e validar o desempenho do sistema;
8. Produzir documentação técnica para manutenção e evolução futura.

2. Metodologia

O trabalho desenvolvido segue uma metodologia de engenharia: análise de requisitos, desenho da solução, desenvolvimento e testes. Na fase de análise de requisitos, foram entrevistados dois elementos dos Serviços de Informática da UAb, tendo sido identificados os sistemas que geram logs e os seus formatos. Além da centralização, foram identificados alguns requisitos não funcionais: solução open source, interface web e integração de diversos sistemas operativos. A solução desenhada é resultado de uma pesquisa e comparação de vários sistemas existentes que respondem minimamente aos requisitos enunciados.

2.1. Solução Proposta

A solução proposta baseia-se na plataforma open-source Wazuh, que permite a gestão centralizada de logs e a monitorização contínua da segurança de infraestruturas tecnológicas. O Wazuh enquadra-se na categoria de soluções SIEM (*Security Information and Event Management*), integrando num único sistema a recolha, correlação e análise de eventos de segurança [Rash, 2017].

A sua implementação visa assegurar a recolha, armazenamento, visualização e monitorização de logs provenientes de diferentes origens, aliando-se à deteção automatizada de incidentes através de mecanismos de alarmística configuráveis e ajustados ao contexto organizacional.
A escolha desta ferramenta resultou da comparação com outras alternativas open-source, sendo justificada pela sua arquitetura distribuída, elevada capacidade de integração e comunidade ativa de suporte e atualização contínua.

A arquitetura adotada é composta por três componentes principais: o Wazuh Manager, responsável pela análise e correlação de eventos; o Wazuh Indexer, encarregado do armazenamento e indexação de dados; e o Wazuh Dashboard, que fornece uma interface gráfica para visualização e monitorização [Wazuh, 2025]. Esta abordagem distribuída facilita a escalabilidade e assegura maior fiabilidade no processamento dos logs institucionais.

Combinando correlação de eventos, monitorização de integridade e deteção de vulnerabilidades, o Wazuh reforça a capacidade de identificação atempada de comportamentos anómalos e potenciais ameaças. A configuração de alertas automáticos e regras personalizadas permite uma atuação proativa na prevenção e mitigação de incidentes de segurança [Jumiaty et al., 2024].

Na secção seguinte, descrevem-se as etapas de implementação do sistema, bem como os testes realizados para validar o seu funcionamento. Dada a natureza experimental do projeto, optou-se por incluir um nível de detalhe técnico superior ao habitual, de forma a assegurar a reprodutibilidade do trabalho.

3. Implementação e testes

3.1. Implementação do Modelo

A implementação decorreu num ambiente de testes controlado em infraestrutura cloud (*DigitalOcean*), com três instâncias virtuais dedicadas (*droplets*) que alojaram, respetivamente, o Wazuh Manager, o Wazuh Indexer e o Wazuh Dashboard. Cada máquina virtual foi configurada com 2 vCPUs, 4 GB de RAM e 80 GB SSD, recursos adequados para suportar as cargas de ingestão e indexação de logs em ambiente experimental [DigitalOcean, 2025].

O Ubuntu Server 24.04 LTS foi o sistema operativo selecionado pela sua estabilidade, segurança e suporte prolongado [Canonical, 2025]. O acesso administrativo foi estabelecido via SSH com autenticação por chaves públicas a fim de garantir comunicações seguras desde o início da instalação.

Após o primeiro acesso, foram aplicadas medidas de reforço de segurança: definição de palavra-passe de emergência para o utilizador *root* (restrita à consola da cloud), atualização integral do sistema e sincronização horária entre servidores (fuso Europe/Lisbon com NTP ativo). Esta sincronização assegura a coerência temporal dos logs e a correta correlação entre eventos.

A instalação seguiu a documentação oficial do Wazuh: primeiro o Manager, depois o Indexer e por fim o Dashboard. De maneira que as dependências entre serviços fossem corretamente resolvidas.

O Dashboard ficou acessível via HTTPS, protegido por certificado TLS autoassinado, para permitir validar a encriptação sem necessidade de autoridade externa. A topologia lógica manteve o isolamento funcional de cada componente e definiu as portas padrão de serviço (1514–1516/55000 TCP para o Manager; 9200–9400 TCP para o Indexer; 443 TCP para o Dashboard).

Para mitigar riscos de exposição pública, reforçou-se a segurança da infraestrutura com a substituição imediata das credenciais predefinidas (*admin*, *filebeat*, *kibanaserver*), a revisão das regras de *firewall* na DigitalOcean e a limitação do acesso apenas às portas estritamente necessárias.

O serviço SSH foi deslocado da porta 22 para a 5522, reduzindo a incidência de varrimentos automáticos, uma medida de *security through obscurity* complementar à *firewall*.

Ao nível do Wazuh Manager, utilizou-se exclusivamente o conjunto de regras nativas disponibilizado pelo projeto, sem personalizações adicionais [GitHub, 2025]. Estas regras classificam eventos por severidade de 0 a 15. Por predefinição, o Dashboard exibe eventos com severidade ≥ 3, mas foi ajustado para ≥ 2, de modo a incluir logs informativos relevantes. O ajuste foi realizado através da diretiva alerts.log_level no ficheiro *ossec.conf*.
Para validar as integrações e gerar eventos controlados, foram preparadas duas máquinas-alvo num ambiente isolado:

- um Windows Server 2008 R2, para simular um ambiente corporativo Microsoft (serviços RDP, IIS, AD DS e partilhas SMB);
- e um Ubuntu Server 20.04 LTS, com serviços SSH, Apache/PHP, MySQL, WordPress, Docker e MariaDB.

Em ambos o sistema foi instalado o agente Wazuh, para garantir a recolha, indexação e visualização dos logs no Manager. Foram ainda ativados módulos nativos do Wazuh que ampliam significativamente as capacidades de deteção, análise e correlação de eventos:

- File Integrity Monitoring (FIM): deteta alterações em ficheiros e diretórios sensíveis, registando utilizador, processo e conteúdo modificado;
- Security Configuration Assessment (SCA): avalia automaticamente a conformidade dos sistemas com *benchmarks* reconhecidos, produzindo relatórios e *scores* de segurança;
- Vulnerability Detection: realiza varreduras periódicas e cruza resultados com bases de dados como NVD e CVE, classificando vulnerabilidades por severidade;
- MITRE ATT&CK: associa eventos a táticas e técnicas documentadas na *framework* MITRE ATT&CK, contextualizando o propósito de cada alerta;

- Compliance: mapeia alertas para controlos de normas e *standards* internacionais, como o RGPD e o NIST 800-53, assegurando conformidade com boas práticas de segurança;
- Integração com VirusTotal: verifica ficheiros suspeitos via API pública, enriquecendo alertas com dados de múltiplos motores antivírus.

A combinação destes módulos conferiu ao sistema uma camada adicional de análise e correlação, transformando o Wazuh num centro de monitorização unificado capaz de detetar, classificar e contextualizar eventos de segurança de forma automática e contínua.

3.2. Validação do Modelo e Resultados Experimentais

3.2.1. Arquitetura e Comunicação entre Componentes

Numa primeira fase, a validação concentrou-se na comunicação entre os três componentes principais do sistema Wazuh e na ligação dos agentes instalados nos sistemas monitorizados.

O objetivo foi confirmar a integridade do pipeline de recolha, indexação e visualização de logs, garantindo que a arquitetura distribuída operava de forma estável e segura.

A metodologia combinou a observação direta no Wazuh Dashboard com a análise dos ficheiros de log de cada componente, comparando o comportamento observado com o esperado de acordo com a documentação oficial [Wazuh, 2025].

Cada teste abordou uma etapa distinta da comunicação, desde a origem dos eventos até à sua representação visual.

Testes de Comunicação entre os Componentes

A comunicação entre os componentes principais do sistema foi verificada de forma sequencial a fim de garantir a integridade do fluxo de dados desde a geração dos logs até à sua visualização final no Dashboard.

*Manager → Indexer***:**

Foi confirmada a transmissão de eventos do Manager para o Indexer. Após a inicialização dos serviços, observaram-se os índices wazuh-alerts-* e wazuh-monitoring-*, responsáveis pelo armazenamento dos eventos. A atualização contínua destes índices demonstrou o envio regular de logs e a correta indexação dos dados, validando a integridade do canal TCP entre ambos os serviços.

Dashboard → Indexer:

Validou-se a comunicação do Dashboard com o Indexer através da visualização dos mesmos índices em estado green, indicador de integridade e sincronização. A consulta direta a esses índices confirmou a leitura e filtragem de eventos em tempo real, assegurando a ligação estável entre as duas camadas.

Dashboard → Manager (API):

A interação entre Dashboard e Manager foi testada via API do Wazuh (porta 55000). No painel Server Management → Status, foi possível visualizar a versão instalada, os processos ativos e o estado *Up to date* do Manager, comprovando a autenticidade e fiabilidade da comunicação entre os componentes.

Testes de deteção e resposta
Durante a fase inicial de monitorização, o sistema detetou múltiplas tentativas de ligação SSH não autorizadas provenientes da Internet. Os eventos foram processados pelo Manager, transmitidos para o Indexer e visualizados no Dashboard em tempo quase real, confirmando a integridade do fluxo de recolha e correlação de logs. Este episódio permitiu identificar uma vulnerabilidade associada à exposição da porta 22/TCP, o que levou à aplicação imediata de medidas corretivas: restrição de acessos, reforço da firewall e endurecimento das políticas de segurança. Após a mitigação, as tentativas de intrusão cessaram, comprovando a eficácia das ações implementadas.

Validação da Comunicação com os Agentes
Após confirmada a estabilidade da comunicação entre os componentes centrais, procedeu-se à verificação da ligação dos agentes instalados nos sistemas monitorizados. No Windows Server 2008 R2, o agente foi instalado a partir do pacote oficial do Wazuh e manteve o estado Active no Dashboard, enviando corretamente eventos do *Security Log*, incluindo registos de autenticações via RDP. No Ubuntu Server 20.04 LTS, o agente foi instalado a partir do repositório oficial do Wazuh, com conectividade validada ao Manager através da porta 1514/TCP, dedicada à receção de eventos.
Em ambos os casos, o campo *Last Keep Alive* foi atualizado de forma periódica, confirmando a transmissão contínua de logs e a sincronização entre os agentes e o Manager.

Sincronização Horária e Consistência Temporal
Para assegurar a coerência temporal das correlações entre eventos, foi implementada a sincronização horária através do *Network Time Protocol* (NTP) em todos os servidores da infraestrutura. Esta configuração garantiu a correspondência dos timestamps entre máquinas distintas, evitando discrepâncias que poderiam comprometer a análise cronológica dos incidentes de segurança.

Conclusão da Validação Estrutural
A fase de validação confirmou que a arquitetura distribuída implementada cumpre integralmente os requisitos de comunicação, ingestão e indexação de logs. O modelo revelou-se tecnicamente estável e preparado para suportar fases posteriores de integração e teste, nomeadamente a correlação prática de eventos e alertas de segurança nos ambientes Windows Server 2008 R2 e Ubuntu Server 20.04 LTS.

3.2.2. Windows Server — Testes de Integração de Logs e Geração de Alertas
Esta fase avaliou a integração do Windows Server 2008 R2 com o Wazuh e a capacidade do sistema para recolher, correlacionar e visualizar eventos de segurança provenientes de diferentes serviços. Após a instalação do agente, foram ativados os principais componentes do sistema operativo: Remote Desktop (RDP), Windows Firewall, Serviços de Ficheiros (SMB), Task Scheduler, Internet Information Services (IIS) e Active Directory (AD) - com o objetivo de testar o comportamento da solução em cenários de uso real e de ataque controlado. Os testes combinaram a observação no Wazuh Dashboard com a análise de eventos no *Event Viewer*, permitindo validar a comunicação entre o agente e o Manager e confirmar a correta classificação e severidade dos alertas.

Remote Desktop (RDP)
O sistema detetou tentativas de autenticação com credenciais inválidas (Event ID 4625), apresentando corretamente no Dashboard o utilizador, o endereço IP de origem e a severidade do alerta.

Windows Firewall
Os eventos de pacotes bloqueados e permitidos foram registados e correlacionados em tempo real, confirmando a integração entre o serviço de firewall do Windows e o Wazuh.

Serviços de Ficheiros (SMB)
A monitorização de partilhas de rede permitiu identificar operações de criação, modificação e eliminação de ficheiros, comprovando a eficácia do módulo de auditoria do Windows na deteção de atividades suspeitas.

Task Scheduler
Eventos de criação, atualização e eliminação de tarefas foram corretamente processados e exibidos no Dashboard, ainda que os de eliminação não tenham gerado alerta nativo: um ponto a melhorar através de regras personalizadas.

Internet Information Services (IIS)
A recolha e correlação de logs web demonstraram que o agente interpreta corretamente o formato IIS, permitindo a visualização imediata de pedidos HTTP e erros 404.

Active Directory (AD)
Durante a promoção do servidor a Domain Controller, foram registados e correlacionados eventos de autenticação, criação de utilizadores e gestão de privilégios, nomeadamente *Kerberos Service Ticket* (4769), validando a integração com o domínio uab.lab.

Simulação de ataque
Foi ainda conduzida uma simulação de ataque ao Windows Server 2008 R2 com o objetivo de avaliar a resposta do sistema em contexto adverso. A ofensiva envolveu três fases: reconhecimento, exploração e pós-exploração. Foram utilizadas ferramentas como *Nmap*, *Metasploit* e *Mimikatz*. O Wazuh detetou e correlacionou múltiplos eventos críticos, incluindo criação e alteração de contas, autenticações privilegiadas e manipulação de políticas de segurança. Os alertas foram automaticamente mapeados na framework MITRE ATT&CK, correspondendo às táticas *Valid Accounts*, *Pass-the-Hash* e *Account Manipulation*, com severidades entre 5 e 8. A coerência temporal entre os sistemas confirmou a eficácia da sincronização horária e a robustez do fluxo de correlação.

Conclusão
Os testes demonstraram que o Wazuh é uma solução eficaz e fiável para ambientes Windows, assegurando visibilidade operacional, contextualização de eventos e suporte à resposta a incidentes. A solução cumpriu integralmente os objetivos definidos, validando a sua capacidade de deteção e correlação de eventos em tempo real.

3.3. Ubuntu Server — Testes de Integração de Logs e Geração de Alertas

Nesta fase foi avaliada a integração do Ubuntu Server 20.04 com o Wazuh e a capacidade do sistema para recolher, correlacionar e apresentar eventos de segurança em diferentes

camadas de serviços. Após a instalação e configuração do agente, foram realizados testes sobre múltiplos componentes do sistema operativo e de aplicações, incluindo SSH, Apache2 com PHP, MySQL, WordPress, Docker e MariaDB, de modo a validar a correta ingestão e análise dos logs. Os resultados foram observados no Wazuh Dashboard e comparados com os registos locais, assegurando a correlação e severidade adequadas dos alertas.

SSH
A monitorização dos acessos remotos demonstrou que o Wazuh deteta corretamente tentativas de autenticação falhadas e conexões suspeitas, gerando alertas imediatos no Dashboard a partir dos registos do auth.log.

Apache2 e PHP
A integração entre o servidor Apache2 e o módulo PHP permitiu validar a recolha e análise de eventos web. Foram simulados acessos indevidos a ficheiros sensíveis e tentativas automatizadas com cabeçalhos maliciosos (User-Agent: sqlmap).
O sistema gerou alertas de severidade média e alta, comprovando a eficácia das regras de deteção aplicadas a ataques web.

MySQL
Os testes ao MySQL confirmaram a monitorização de autenticações falhadas, erros de sintaxe e tentativas de SQL Injection.
A correlação entre os logs de base de dados e os alertas do Dashboard validou a capacidade do Wazuh para identificar comportamentos anómalos no acesso e manipulação de dados.

WordPress
Com o WordPress instalado sobre Apache e MySQL, foi avaliada a deteção de eventos em contexto de aplicação real.
O sistema identificou falhas de autenticação, acessos a páginas inexistentes e consultas à base de dados, demonstrando a integração funcional entre as diferentes camadas da aplicação.

Docker
A utilização do módulo docker-listener permitiu monitorizar o ciclo de vida dos containers: criação, execução, pausa e eliminação.
Cada ação originou eventos distintos detetados e exibidos no Dashboard, comprovando a capacidade do Wazuh para supervisionar ambientes virtualizados em tempo real.

MariaDB (em container)
A integração do MariaDB num container Docker validou a recolha de eventos administrativos e de segurança em ambientes isolados. O sistema registou tentativas de autenticação falhadas, erros de sintaxe e alterações administrativas, revelando a eficácia do Wazuh em monitorizar bases de dados distribuídas e virtualizadas.

Simulação de reconhecimento e exposição de serviços
Foi realizada uma simulação de reconhecimento a partir de uma máquina externa (*Kali Linux*), recorrendo à ferramenta Nmap para varrer serviços expostos no Ubuntu Server. O cenário incluiu a exposição intencional de um serviço FTP com login anónimo,

representando uma configuração insegura. O Wazuh registou 44 alertas na primeira varredura, incluindo a deteção de portas abertas e autenticações anónimas.
Após a aplicação de políticas de firewall que restringiram o tráfego apenas à porta SSH (22/TCP), observou-se uma redução substancial dos eventos registados e do ruído de segurança. A comparação entre os dois momentos confirmou o impacto positivo do endurecimento da rede (*hardening*) na diminuição da superfície de ataque e na carga de alertas.

Conclusão
Os testes realizados demonstraram que o Wazuh assegura uma monitorização eficaz de sistemas Linux com capacidade para correlacionar eventos em diferentes serviços e camadas de aplicação. A simulação de reconhecimento demonstrou a importância de combinar a monitorização contínua com políticas de segurança preventivas, reforçando o papel do Wazuh como ferramenta de deteção e mitigação de riscos operacionais.

3.4. Dashboards de Monitorização e Visualização de Eventos

Concluída a fase de testes de integração e validação nos sistemas Windows e Ubuntu, procedeu-se à análise dos resultados através do Wazuh Dashboard, a interface gráfica que centraliza a visualização de eventos e alertas recolhidos pelo sistema. Esta componente é essencial para transformar grandes volumes de logs técnicos em informação operacional clara e acionável, permitindo uma perceção imediata do estado de segurança da infraestrutura monitorizada.

O Dashboard oferece a possibilidade de criar painéis personalizados compostos por visualizações interativas: gráficos, tabelas dinâmicas, métricas e contadores agregados, que permitem correlacionar dados provenientes de diferentes origens (*hosts*, serviços e módulos). Estes elementos facilitam tanto a monitorização em tempo real como a análise retrospetiva de incidentes.

No contexto deste projeto foi criado o painel "Visão Geral de Segurança da Infraestrutura Simulada", concebido para agregar, num único espaço visual, as métricas mais relevantes obtidas durante as simulações. Este painel fornece uma visão consolidada do comportamento global do sistema, permitindo identificar rapidamente anomalias, picos de atividade ou padrões de ataque. As principais visualizações incluídas foram:

- Total de alertas por agente (host): identifica os sistemas que geraram maior volume de alertas, facilitando a priorização da análise;
- Evolução temporal dos eventos: mostra a variação da atividade maliciosa ao longo do tempo, destacando períodos de maior incidência;
- Distribuição da severidade por máquina: relaciona o nível de criticidade dos eventos com a origem, apoiando a resposta a incidentes;
- Técnicas de ataque detetadas (MITRE ATT&CK): mapeia automaticamente os eventos às táticas reconhecidas pela framework, proporcionando contexto estratégico às deteções;
- Eventos críticos recentes: apresenta os alertas de maior relevância, funcionando como resumo executivo da atividade;
- Top IPs de origem: evidencia as principais fontes internas e externas de eventos, contribuindo para o controlo de ameaças de rede.

A análise destes indicadores confirmou que o sistema é capaz de fornecer visibilidade contínua e contextualizada sobre o estado de segurança da infraestrutura. Os painéis do Wazuh revelaram-se uma ferramenta eficaz de apoio à decisão, permitindo o acompanhamento em tempo real e a produção de relatórios úteis para auditorias e conformidade com normas como o Regulamento Geral sobre a Proteção de Dados (RGPD) e a Diretiva NIS2.

4. Considerações Finais e Trabalho Futuro

4.1. Conclusões Gerais

O presente projeto teve como objetivo conceber e validar uma solução centralizada de gestão e monitorização de logs, tecnicamente robusta, economicamente viável e alinhada com as necessidades dos Serviços de Informática da Universidade Aberta (UAb).

Através de uma arquitetura distribuída composta por três componentes: Wazuh Manager, Wazuh Indexer (baseado em OpenSearch) e Wazuh Dashboard, instalados em máquinas virtuais distintas, foi possível demonstrar a eficácia da solução na recolha, correlação e visualização de eventos de segurança provenientes de múltiplas fontes.

O projeto comprovou a capacidade do Wazuh para integrar e analisar logs de diferentes origens (sistemas operativos, serviços web, bases de dados e ambientes containerizados), assegurando correlação automática de eventos e visualização clara através de dashboards dinâmicas.

Foi igualmente demonstrada a viabilidade de criar um ambiente de testes seguro e realista, no qual se simularam incidentes e ataques controlados, permitindo avaliar a resposta e a eficácia da plataforma em cenários próximos da realidade institucional.

O protótipo integrou duas máquinas-alvo: Windows Server e Ubuntu Server, executando serviços reais (Apache, MySQL, FTP, Active Directory) e simulando ataques a partir de um sistema Kali Linux. Os resultados confirmaram a capacidade do Wazuh para detetar e correlacionar eventos em tempo quase real. A arquitetura revelou-se leve, modular e escalável, constituindo uma base sólida para o desenvolvimento de um sistema institucional de monitorização de segurança.

De forma global, a solução proposta demonstrou ser tecnicamente válida e operacionalmente fiável, respondendo de modo eficaz às necessidades identificadas e estabelecendo as fundações para futuras evoluções da infraestrutura de deteção e resposta a incidentes da UAb.

4.2. Desafios e Mitigações

Durante a implementação, foram identificados diversos desafios técnicos e operacionais que exigiram ajustes à abordagem inicial. Entre os mais relevantes destacam-se:

- Limitação no acesso ao Dashboard devido a certificado TLS autossinado, solucionada através da importação manual do certificado no sistema operativo. Em ambiente de produção, recomenda-se a utilização de certificados emitidos por autoridades reconhecidas ou de uma infraestrutura de chave pública (PKI) interna.
- Dificuldade na obtenção de logs realistas e correlacionáveis, ultrapassada através da simulação de incidentes em máquinas reais (Windows e Ubuntu) e da geração

controlada de eventos a partir de um sistema Kali Linux, garantindo uma validação mais fidedigna das capacidades de deteção e correlação.

- Exposição involuntária da porta SSH (22/TCP), mitigada pela reconfiguração da firewall e alteração da porta de acesso, reforçando as práticas de segurança na fase inicial de configuração.
- Falhas de comunicação entre componentes devido à inconsistência de credenciais, resolvidas através de diagnóstico detalhado e sincronização das configurações entre o Manager, o Indexer e o Dashboard.

A superação destes desafios contribuiu para o amadurecimento técnico do sistema e reforçou a importância de práticas de configuração seguras, gestão cuidadosa de credenciais e monitorização contínua de vulnerabilidades em ambientes distribuídos.

4.3. Trabalho Futuro

A solução desenvolvida constitui um ponto de partida sólido para a implementação de um sistema centralizado de gestão e monitorização de logs na Universidade Aberta, com diversas oportunidades de evolução e aprofundamento técnico.

Entre as principais linhas de desenvolvimento futuro destacam-se:

- Alinhamento com a Diretiva NIS2 e com frameworks de referência (NIST 800-53, ISO/IEC 27001), assegurando conformidade com as novas exigências legais e normativas;
- Expansão das fontes de logs para incluir plataformas como Moodle, servidores de correio eletrónico, proxies, firewalls e serviços em cloud;
- Automatização da integração de agentes e serviços, permitindo maior escalabilidade e facilidade de manutenção;
- Adoção da funcionalidade Active Response do Wazuh para execução automática de ações de mitigação (ex.: bloqueio de IPs ou interrupção de processos);
- Evolução para capacidades de XDR (Extended Detection and Response), integrando módulos como o *osquery* ou soluções EDR já existentes na instituição;
- Reestruturação da arquitetura para produção, através de escalabilidade horizontal, balanceamento de carga, clusters de OpenSearch com replicação e mecanismos de *failover* automático;
- Personalização das regras de deteção e alarmística por tipo de serviço e integração com APIs REST para recolha avançada de logs;
- Garantia de imutabilidade e retenção prolongada dos dados, com políticas *Write Once Read Many* (WORM) e *snapshots* protegidos;
- Reforço da auditabilidade e autenticidade dos próprios registos, com suporte em tecnologia *blockchain*.

Recomenda-se ainda a implementação de rotinas automáticas de backup e redundância, complementadas por infraestruturas tolerantes a falhas energéticas (UPS ou datacenters resilientes), assegurando a continuidade operacional em cenários críticos.

Em suma, este trabalho demonstrou que o Wazuh, quando corretamente parametrizado e integrado numa arquitetura distribuída, pode assumir um papel central na monitorização e correlação de eventos de segurança em contexto académico, conciliando eficiência técnica, sustentabilidade e conformidade institucional.

A solução aqui desenvolvida constitui não apenas uma prova de conceito funcional, mas também um alicerce estratégico para a consolidação da cibersegurança e da governança digital da Universidade Aberta e de outras instituições com oferta de ensino a distância,

abrindo caminho a futuras evoluções em direção a um ecossistema de monitorização inteligente e resiliente.

REFERÊNCIAS

Alsabhan, W. (2023). Student cheating detection in higher education by implementing machine learning and LSTM techniques. *Sensors*, *23*(8), 4149.

Burgess, M. (2017). *Inside the WannaCry ransomware attack that hit the NHS – and why it's a sign of things to come.* Wired UK.

Canonical Ltd. (2025). *Ubuntu Server 24.04 LTS Documentation.* Disponível em: https://ubuntu.com/server/docs

Delpy, B. (2019). *Mimikatz: tool for credential extraction and Windows security testing.* GitHub Repository.

DigitalOcean LLC. (2025). *Droplet Technical Specifications and Networking Guide.* Disponível em: https://www.digitalocean.com/docs

ENISA — European Union Agency for Cybersecurity. (2023). *Threat Landscape 2023: ENISA Annual Report on Cybersecurity Trends.* Publications Office of the European Union.

GitHub, Inc. (2025). *Wazuh Ruleset Repository.* Disponível em: https://github.com/wazuh/wazuh-ruleset

Gu, S., Rong, G., Zhang, H., & Shen, H. (2022). Logging practices in software engineering: A systematic mapping study. IEEE transactions on software engineering, 49(2), 902-923.

Jumiaty, E., & Soewito, B. (2024). *Implementation of Wazuh SIEM for Security Monitoring on Cloud Infrastructure. International Journal of Information Technology and Systems*, 13(2), 45–53.

Latif, G., Abdelhamid, S. E., Fawagreh, K. S., Brahim, G. B., & Alghazo, R. (2023). machine learning in higher education: students' performance assessment considering online activity logs. *IEEE access*, *11*, 69586-69600.

Lyon, G. F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.* Insecure.Org Press. ISBN 978-0979958717.

Manzoor, M., Hasan, S., & Rehman, S. (2024). *Comparative Study of Open-Source SIEM Tools: Wazuh, ELK and Graylog. Journal of Information Security and Applications*, 78, 103-118.

MITRE Corporation. (2025). *MITRE ATT&CK Framework v14.0: Tactics, Techniques and Procedures for Enterprise Networks.* Disponível em: https://attack.mitre.org

Nguyễn, T. H. (2022). Cybersecurity Logging & Monitoring Security Program. School of Computer Science & Engineering, Sacred Heart University. https://digitalcommons.sacredheart.edu/computersci_stu/3/

NIST — National Institute of Standards and Technology. (2024). *NIST Special Publication 800-53 Rev. 6: Security and Privacy Controls for Information Systems and Organizations.* U.S. Department of Commerce.

O'Brien, L. (2022). *Proof-of-Concept Environments for Cyber Range Simulation. IEEE Access*, 10, 21445–21458.

OpenSearch Project. (2025). *OpenSearch Dashboards and Index Management Guide.* The OpenSearch Foundation.

Peled, A., & Rashty, D. (1999). Logging for success: Advancing the use of WWW logs to improve computer mediated distance learning. *Journal of Educational Computing Research*, *21*(4), 413-431.

Rash, M. (2017). *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management.* Syngress Publishing. ISBN 978-0124158153.

Stallings, W. (2012). *Network Security Essentials: Applications and Standards* (5th ed.). Pearson Education. ISBN 978-0133370430.

Strilețchi, C., Pop, P. G., & Gavrilă, C. (2025). A Centralized Approach to the Logging Mechanisms of Distributed Complex ERP Applications. *Information*, *16*(3), 216.

Wazuh, Inc. (2025). *Wazuh Documentation: Architecture, Modules and Deployment Guide.* Disponível em: https://documentation.wazuh.com

Yamin, M., Katt, B., & Gkioulos, V. (2020). *Cyber Ranges and Security Testbeds: Scenarios, Taxonomies, and Future Directions. Computers & Security*, 88, 101636.

José Ribeiro, Licenciado em Engenharia Informática pela Universidade Aberta (2025) e titular de um Bachelor of Science (Honours) in International Studies pela Open University, Reino Unido (2011). Coautor do projeto Sistema Centralizado de Gestão de Logs com Wazuh, desenvolvido em ambiente académico em colaboração com os Serviços de Informática da UAb. As suas áreas de interesse incluem cibersegurança, machine learning, inteligência artificial, sistemas distribuídos e análise de dados.

Silvana Oliveira, Licenciada em Criminologia (2017) pela Faculdade de Direito da Universidade do Porto e também licenciada em Engenharia Informática (2025) pela Universidade Aberta. É Mestre em Medicina Legal e Ciências Forenses (2016) pelo Instituto de Ciências Biomédicas Abel Salazar e especialista em Cibersegurança (2021) pela Academia Nacional de Cibersegurança. Atualmente é especialista em Cibersegurança na empresa portuguesa CyberS3c, onde colabora em projetos técnicos e estratégicos e atua como formadora e docente convidada na área. Coautora do projeto Sistema Centralizado de Gestão de Logs com Wazuh, desenvolvido em colaboração com os Serviços de Informática da Universidade Aberta. Os seus interesses de investigação centram-se na cibersegurança, em particular na segurança ofensiva, na análise de vulnerabilidades e na aplicação de inteligência artificial à deteção de ciberameaças.

Sofia Teixeira, Licenciada em Engenharia Biotecnológica (2011) pelo Instituto Politécnico de Bragança e a terminar a Licenciatura em Engenharia Informática pela Universidade Aberta. Frequentou o curso de Especialista em Cibersegurança da ANCIBER e é detentora de certificados profissionais na área, com destaque para cibersegurança ofensiva. Atualmente, desempenha funções como Especialista em Cibersegurança na empresa Next-IT, onde realiza auditorias técnicas e avaliações de vulnerabilidades em ambientes corporativos. O seu trabalho alia a vertente operacional à consultoria estratégica. Coautora do projeto "Sistema Centralizado de Gestão de Logs com Wazuh", desenvolvido em colaboração com os Serviços de Informática da Universidade Aberta. As suas principais áreas de interesse incluem a análise de vulnerabilidades, testes de intrusão, monitorização e deteção de ameaças, e a integração de práticas de segurança ofensiva e defensiva no contexto corporativo.

Vitor Rocio, Professor Associado da Universidade Aberta (UAb). Doutorado em Informática pela Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa (2002), e Licenciado em Engenharia Informática pela FCT-UNL (1993). É diretor do Departamento de Ciências e Tecnologia da UAb. Os seus principais interesses são as tecnologias das linguagens humanas, o processamento automático de línguas naturais, os sistemas de análise sintáctica evolutivos, e as tecnologias de elearning.