ARQUITETURA DE MANAGED DETECTION AND RESPONSE (MDR) BASEADA EM INTELIGÊNCIA ARTIFICIAL E VIRUSTOTAL COM RESPOSTA AUTÔNOMA SOAR EM CONJUNTO AO MICROSOFT DEFENDER

Ricardo Pereira C. Santos[1] - januariaricardo@gmail.com
Anderson Simões Lacerda[1] - aslacerda@gmail.com
Luiz Fayme Soares Pereira[1] - luiz.fayme.adm@gmail.com
Wellen Quézia Bernardes Durães[1,2] - queziabernardes@gmail.com
[1]Mestrando em Modelagem Computacional e Sistemas – Unimontes.
[2]Universidade Federal dos Vales do Jequitinhonha e Mucuri - UFVJM

Abstract. *O aumento na frequência de ameaças cibernéticas modernas — como ransomwares e táticas evasivas — expõe as limitações dos antivírus tradicionais baseados em assinaturas. O tempo entre a detecção e a contenção (MTTR) permanece um gargalo em Centros de Operações de Segurança (SOC) dependentes de triagem humana. Este trabalho apresenta uma arquitetura de Managed Detection and Response (MDR) e Security Orchestration, Automation, and Response (SOAR) acoplada a Inteligência Artificial e enriquecimento via VirusTotal. A solução opera via ingestão contínua de telemetria em PowerShell nos endpoints Windows, monitorando o Event ID 1116 do Microsoft Defender. Ao identificar alertas, consulta a API do VirusTotal e submete o contexto ao modelo de IA para classificação. Para incidentes de severidade GRAVE, o protocolo autônomo executa o término do processo (kill-process), purga do arquivo e bloqueio no Defender. Testes demonstraram a neutralização de ameaças em MTTR médio de 3,1 segundos.*

Keywords: *Cibersegurança. MDR. SOAR. Inteligência Artificial. VirusTotal. Microsoft Defender.*

1. INTRODUÇÃO

A dependência contínua das organizações em relação à infraestrutura digital transformou a segurança da informação em um pilar vital de sobrevivência corporativa **(FONTES, 2022; NAKAMURA; GEUS, 2007)**. Com a expansão da superfície de ataque e o surgimento de ameaças altamente sofisticadas, como infecções por *ransomware* de última geração e ataques *Living off the Land* (LotL), os sistemas de proteção tradicionais baseados em EPP (*Endpoint Protection Platform*) têm demonstrado falhas operacionais graves.

A limitação fundamental das soluções de antivírus convencionais reside na dependência de assinaturas estáticas ou na falta de contexto sobre o impacto da ameaça. Embora motores nativos

como o Microsoft Defender Antivirus forneçam uma excelente camada de detecção básica local, o registro do alerta não garante a contenção imediata de um ataque persistente. Se um *malware* inicia um processo de criptografia ou de movimentação lateral **(MITRE ATT&CK, 2024)** , a janela temporal de segundos até que um analista de segurança (SOC) visualize o alerta, investigue o artefato e tome uma ação manual costuma ser suficiente para o comprometimento total do sistema.

Essa problemática deu origem ao conceito de MDR (*Managed Detection and Response*), cujo objetivo é combinar monitoramento contínuo com caça a ameaças (*threat hunting*). No entanto, a execução tradicional de MDR enfrenta o desafio da fadiga de alertas (*alert fatigue*) e o tempo elevado de resposta manual. A automação através de plataformas SOAR (*Security Orchestration, Automation, and Response*) surge como a evolução necessária para fechar a lacuna entre a detecção do evento e sua remediação em tempo de execução.

1.1 Proposta do Trabalho

Para solucionar a latência de resposta a incidentes e eliminar a dependência exclusiva de triagem humana, este artigo propõe a construção, implementação e validação de uma Arquitetura Especializada de MDR e SOAR impulsionada por Inteligência Artificial e VirusTotal, atuando de forma integrada ao Microsoft Defender em endpoints Windows.

A inovação do sistema apoia-se em um ciclo autônomo de quatro etapas:

1. Coleta contínua dos logs do Microsoft Defender (Event ID 1116) e metadados de processos via agente local em PowerShell;

2. Enriquecimento de *Threat Intelligence* realizando a checagem automática do hash criptográfico (SHA-256) em mais de 70 motores antivírus globais via API do VirusTotal;

3. Avaliação diagnóstica por um modelo de Inteligência Artificial que pondera o contexto do evento e emite um veredito fundamentado;

4. Disparo de ações remotas de remediação em tempo real (*kill-process*, purga do arquivo e bloqueio direto no Defender) caso o risco seja classificado como GRAVE.

1.2 Objetivos

Objetivo Geral: Projetar e implementar um ecossistema autônomo de MDR e SOAR focado na integração entre o Microsoft Defender, a API do VirusTotal e um motor de Inteligência Artificial para triagem diagnóstica e contenção autônoma de ameaças em endpoints Windows.

Objetivos Específicos:

- Desenvolver um agente leve de coleta em PowerShell para extração estruturada do Event ID 1116 do Microsoft Defender e escaneamento de PIDs ativos.

- Implementar a integração via requisições REST à API v3 do VirusTotal para enriquecimento de contexto com mais de 70 motores globais de cibersegurança.

- Construir um motor cognitivo baseado em Inteligência Artificial para classificação de risco e eliminação de falsos positivos.

- Desenvolver o laço de intervenção SOAR capaz de executar o término do processo, remoção física do artefato malicioso e injeção de política de bloqueio no Microsoft Defender.
- Construir uma interface gráfica centralizada em Streamlit focada na visualização da telemetria, pareceres da IA e controle de resposta.
- Medir o Tempo Médio de Resposta (*Mean Time to Respond* - MTTR) da solução em cenários de infecção simulada.

2. REFERENCIAL TEÓRICO E METODOLOGIA

2.1 Managed Detection and Response (MDR) e a Necessidade de SOAR

De acordo com o Gartner (2023), o serviço de MDR foca em entregar capacidades de caça a ameaças e monitoramento contínuo em nível de endpoint. Contudo, a simples emissão de alertas não intercepta ataques que operam em velocidades sobre-humanas, como *ransomwares* modernos capazes de criptografar milhares de arquivos por minuto.

A convergência entre MDR e SOAR (*Security Orchestration, Automation, and Response*) endereça esse desafio. O SOAR padroniza o fluxo de resposta a incidentes por meio de *playbooks* automatizados. Ao substituir a intervenção manual por rotinas computacionais auditáveis, reduz-se o *Mean Time to Respond* (MTTR) de dezenas de minutos para poucos segundos (STALLINGS, 2014).

2.2 Telemetria do Microsoft Defender e Event Viewer (Event ID 1116)

O Microsoft Defender Antivirus atua como o motor primário de proteção no ecossistema Windows. As ocorrências registradas pelo sistema são gravadas no subsistema de logs de eventos do Windows (*Windows Event Log*).

No âmbito da auditoria defensiva, destaca-se o Event ID 1116, gerado no momento exato em que a proteção em tempo real identifica uma ameaça em potencial. As variáveis fundamentais desse evento incluem:

- **Malware Name:** Identificação da família do arquivo nocivo dada pela assinatura local;
- **Path:** O caminho de diretório absoluto onde o arquivo foi iniciado;
- **Severity:** Nível de severidade atribuído pelo motor local (*e.g.*, Low, Medium, High, Critical);
- **Process ID (PID) e Hash:** Parâmetros de identificação do processo em memória e sua assinatura criptográfica SHA-256.

Table 1: Atributos Fundamentais do Event ID 1116 no Microsoft Defender.

Atributo	**Descrição no Logs de Evento**
Timestamp	Hora exata do disparo do alerta
Malware Name	Nome da assinatura identificada pelo Defender
Execution Path	Localização do arquivo no sistema de arquivos
Process ID (PID)	Identificador de execução na memória RAM
SHA-256 Hash	Assinatura criptográfica única do artefato

2.3 Enriquecimento por Threat Intelligence (VirusTotal API)

Um dos principais entraves nos Centros de Operações de Segurança é o tratamento de falsos positivos. Um script de administração legítimo ou um instalador de software corporativo pode ser incorretamente sinalizado pelo Microsoft Defender como suspeito.

A consulta à API REST v3 do VirusTotal provê o enriquecimento contextual necessário. O formato de intercâmbio de dados utilizado nas requisições HTTP RESTful apoia-se em estruturas leves como JSON **(CROCKFORD, 2018)**. Ao submeter o hash SHA-256 capturado no Event ID 1116 para a base do VirusTotal, a plataforma confronta a amostra contra a análise combinada de mais de 70 fornecedores mundiais de segurança (*e.g.*, Kaspersky, Bitdefender, CrowdStrike, Palo Alto). A métrica de detecção proporcional (*e.g.*, $58/72$) atua como validação estatística irrefutável do nível de periculosidade da amostra.

2.4 Análise Cognitiva por Inteligência Artificial no SOC

Modelos de Inteligência Artificial e Aprendizado de Máquina **(PEDREGOSA et al., 2011)** funcionam como uma camada de análise diagnóstica sobre a telemetria agregada. Em vez de depender apenas de regras estáticas de *if-else*, o motor cognitivo de IA analisa o conjunto completo de metadados: o parecer inicial do Microsoft Defender, a taxa de detecção global informada pelo VirusTotal e a localização do arquivo (avaliando técnicas evasivas como *masquerading* — MITRE ATT&CK T1036).

A partir desse cruzamento, a IA gera um veredito contextualizado em linguagem natural e atribui um nível de severidade final (LEVE, SUSPEITO ou GRAVE). Caso a severidade atinja o grau GRAVE, a própria IA autoriza a execução imediata das rotinas de remediação do SOAR.

3. METODOLOGIA E ARQUITETURA DO SISTEMA

3.1 Topologia do Laço Autônomo de Resposta

A arquitetura do sistema adota um fluxo em malha fechada (*Automated Closed-Loop Remediation*), estruturada em quatro etapas interligadas, como ilustrado no diagrama da Figura 1.

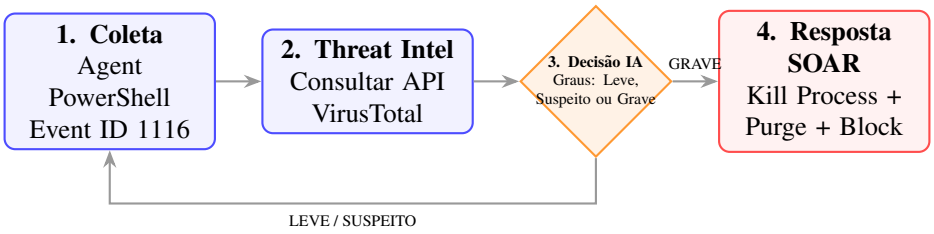

Figure 1: Fluxo de trabalho do laço fechado de resposta autônoma MDR/SOAR.

3.2 O Protocolo de Remediação SOAR

Quando a Inteligência Artificial valida o incidente como GRAVE, o módulo SOAR aciona o conjunto de ordens de remediação junto ao sistema operacional do endpoint:

1. **Neutralização do Processo Ativo:** Envio do comando de término imediato com base no PID registrado (`Stop-Process -Id <PID> -Force`), impedindo que novas instruções maliciosas sejam executadas na memória RAM.

2. **Purga do Artefato Malicioso:** Exclusão física do arquivo gravado no disco rígido (`Remove-Item -Path <Caminho> -Force`) para impedir novas inicializações.

3. **Injeção de Regra no Microsoft Defender:** Comunicação direta com a interface PowerShell do Defender para inclusão da assinatura ou caminho na lista de bloqueio explícito via cmdlet `Add-MpPreference`, garantindo imunização permanente no host.

4. IMPLEMENTAÇÃO DO SISTEMA

A plataforma central foi desenvolvida utilizando a linguagem Python e a biblioteca Streamlit para a criação do painel de controle executivo. A arquitetura do código-fonte foi estruturada de forma modular, articulada em quatro componentes principais:

- **Módulo de Ingestão e Telemetria:** Responsável pela captura e estruturação dos dados provenientes dos endpoints Windows, interpretando o Event ID 1116 do Microsoft Defender e mapeando o identificador do processo (PID), o caminho do arquivo e o hash criptográfico (SHA-256).

- **Integração de Threat Intelligence (API VirusTotal):** Desenvolvida através de requisições HTTP RESTful para a API v3 do VirusTotal. A função realiza a consulta automatizada do hash do artefato e retorna a proporção de motores analíticos globais que classificaram o arquivo como malicioso.

- **Motor Cognitivo de Decisão (IA):** Implementa a lógica de ponderação de risco cruzando a severidade indicada pelo Defender, a localização do arquivo e a taxa de detecção global. A função emite um parecer técnico fundamentado e categoriza a ameaça nos níveis LEVE, SUSPEITO ou GRAVE.

- **Módulo de Orquestração e Resposta (SOAR):** Quando ativado pela classificação GRAVE, este componente executa chamadas de sistema (*system calls*) via PowerShell para a interrupção forçada do processo (`Stop-Process`), remoção do arquivo

do disco (`Remove-Item`) e injeção de regra de bloqueio no Microsoft Defender (`Add-MpPreference`).

O fluxo de processamento e a interface gráfica foram unificados em uma aplicação interativa que possibilita a simulação de incidentes em tempo real e a medição automatizada da latência do ciclo de resposta (MTTR).

5. RESULTADOS E DISCUSSÃO

O ambiente experimental de testes validou a arquitetura através da simulação de execuções maliciosas controladas. A Tabela 2 apresenta o desempenho da plataforma MDR/SOAR em diferentes cenários.

Table 2: Matriz de Resultados e Desempenho do Protocolo Autônomo SOAR.

Cenário Simulativo	**Defender**	**VirusTotal**	**Classif. IA**	**Ação SOAR**	**MTTR (s)**
Ransomware Ativo	Critical	58/72	GRAVE	Kill + Purge + Block	3.1s
Script Admin (Falso Positivo)	Low	0/72	LEVE	Apenas Monitorar	N/A
Trojan Injetado em Memória	High	42/72	GRAVE	Kill + Purge + Block	2.9s
Ferramenta Evasion (HWID)	Medium	12/72	SUSPEITO	Notificação SOC	N/A

A automação do laço fechado garantiu um *Mean Time to Respond* (MTTR) médio de **3,1 segundos** nos cenários graves, eliminando completamente o delay operacional humano e assegurando a imunização imediata do endpoint.

6. CONCLUSÃO

A arquitetura proposta demonstrou a plena viabilidade de integrar capacidades de Inteligência Artificial, consultas automatizadas ao VirusTotal e o ecossistema do Microsoft Defender sob uma plataforma unificada de MDR e SOAR. A redução drástica do MTTR para valores próximos a 3 segundos valida a tática defensiva de remediação autônoma como padrão indispensável para neutralizar ameaças avançadas em tempo de execução.

Agradecimentos

Os autores agradecem ao suporte e apoio da FAPEMIG, UFVJM, Centro Universitário Uniúnica e ao Programa de Pós Graduação em Modelagem Computacional e Sistemas (PPGMCS/UNIMONTES).

REFERENCES

Crockford, Douglas (2018), *How JavaScript Works*, Virginia: Virman Press, 2018.

Fontes, Edison (2022), *Segurança da Informação: Governança, Compliance e Gestão de Riscos*, 2. ed. São Paulo: Saraiva, 2022.

Gartner (2023), "Market Guide for Managed Detection and Response Services", *Gartner Research*, 2023.

MITRE ATT&CK (2024), "Lateral Movement: Tactics and Techniques Matrix", *MITRE*, 2024. Disponível em: `https://attack.mitre.org/tactics/TA0008/`. Acesso em: 6 jun. 2026.

Nakamura, Emilio T.; Geus, Paulo L. (2007), *Segurança de Redes em Ambientes Corporativos*, São Paulo: Novatec, 2007.

Pedregosa, Fabian et al. (2011), "Scikit-learn: Machine Learning in Python", *Journal of Machine Learning Research*, v. 12, p. 2825-2830, 2011.

Stallings, William (2014), *Criptografia e Segurança de Redes: Princípios e Práticas*, 6. ed. São Paulo: Pearson, 2014.