DOI: 10.5748/20CONTECSI/PSE/SEC/7203

eLocator: e207203

VISIBILIDADE EM CIBERSEGURANÇA: UMA PESQUISA EXPLORATÓRIA

Edilene Maria Da Silva – https://orcid.org/0000-0002-4667-0216
Instituto De Pesquisas Tecnológicas Do Estado De São Paulo - Ipt

Leandro Avanço – https://orcid.org/0000-0002-7901-2797
Instituto De Pesquisas Tecnológicas Do Estado De São Paulo - Ipt

VISIBILITY IN CYBERSECURITY: AN EXPLORATORY RESEARCH

ABSTRACT

With the increasing sophistication of cyberattacks, their detection before they happen is hampered. This article presents how visibility in cybersecurity is approached by several authors, seeking to have an environment that provides proactive and mitigating actions to professionals in the IT area. The research conducted in this study highlights hidden hazard management, log collection, and insight as paramount in threat detection, leaving no doubt as to the importance of visibility in cybersecurity. In addition, ways and solutions are presented to provide visibility with various levels of complexity in a computational environment, from the use of AI, user behavioral analysis, including detection and extended response. The main contribution of this study is to show that the way to quickly identify the existence of a cyberattack is to have the highest degree of visibility possible, an important element in helping professionals in the area in identifying a cyberattack in real time or an imminent attack, as well as presenting some visibility providers that allow this to be possible.

Keywords: Cybersecurity; Cyber visibility; Cyber observability; Cyber Defense

VISIBILIDADE EM CIBERSEGURANÇA: UMA PESQUISA EXPLORATÓRIA

RESUMO

Com o crescente aumento da sofisticação dos ataques cibernéticos, sua detecção antes que aconteçam é prejudicada. Neste artigo é apresentado como a visibilidade em cibersegurança é abordada por diversos autores, buscando possuir um ambiente que proporcione ações proativas e mitigatórias aos profissionais da área de TIC. A pesquisa realizada neste estudo destaca o gerenciamento de perigos ocultos, a coleta de logs e a visão como primordial na detecção de ameaças, não deixando dúvida quanto à importância da visibilidade em cibersegurança. Além disso, são apresentadas formas e soluções para prover visibilidade com diversos níveis de complexidade em ambiente computacional, desde a utilização de IA, análise comportamental de usuários, incluindo a detecção e resposta estendida. A principal contribuição deste estudo é mostrar que a maneira de identificar de forma ágil a existência de um ataque cibernético é ter o maior grau de visibilidade possível, um elemento importante no auxílio aos profissionais da área, na identificação de um ataque cibernético em tempo real ou de um iminente ataque, bem como apresentar alguns provedores de visibilidade que permitam que isso seja possível.

Palavras-chave: Cibersegurança; Visibilidade cibernética; Observabilidade cibernética; defesa cibernética

1. INTRODUÇÃO

Os ataques estão cada vez mais sofisticados e difíceis de serem detectados antes que aconteçam. Aliado a isso, os atacantes também estão cada vez mais qualificados e buscando novas habilidades, tendências de ataques, criando ferramentas e explorando o universo vulnerável de dispositivos e sistemas disponíveis na internet. Ou seja, sempre à frente da defesa.

Em muitas empresas, os ataques são tratados em condições emergenciais, agindo apenas quando o ataque já está em andamento, o que pode representar uma situação mais grave a depender do ataque executado, ocasionando uma recuperação mais lenta do ambiente, comprometendo a disponibilidade dos recursos de Tecnologia da Informação e Comunicação (TIC).

Se não é possível adivinhar qual é a próxima estratégia do atacante, temos que ficar sempre alertas para algo que esteja acontecendo de maneira incomum em nosso ambiente.

Com uma enorme gama de informações geradas por vários dispositivos e sistemas de segurança, uma alternativa para tentar ser proativo antes que o pior aconteça, é ter visibilidade do ambiente de TIC (REPOSIFY, 2022).

O objetivo deste artigo é descrever como a visibilidade em cibersegurança é enxergada por autores diversos, que apontam a sua importância, com o propósito de ter um ambiente mais centralizado, e que proporcione ações proativas e mitigatórias aos profissionais da área de TIC.

Na seção 2 são apresentados os conceitos de visibilidade e observabilidade em cibersegurança, na seção 3 as soluções de visibilidade, na seção 4 como é possível melhorar a visibilidade em cibersegurança e, por fim, na seção 5 a conclusão deste estudo.

2. VISIBILIDADE E OBSERVABILIDADE

Segundo Reposify (2022), na última década, as organizações foram migrando para um ambiente mais digitalizado, aumentando assim a quantidade de endereços IP (*Internet Protocol*) públicos para facilitar a necessidade de conexão e interação entre seus ativos de rede internos, entre seus funcionários remotos e entre suas filiais ao redor do mundo. Esse cenário pode permitir a exposição na internet dos dados confidenciais da organização, passíveis de serem explorados ou aproveitados por um invasor.

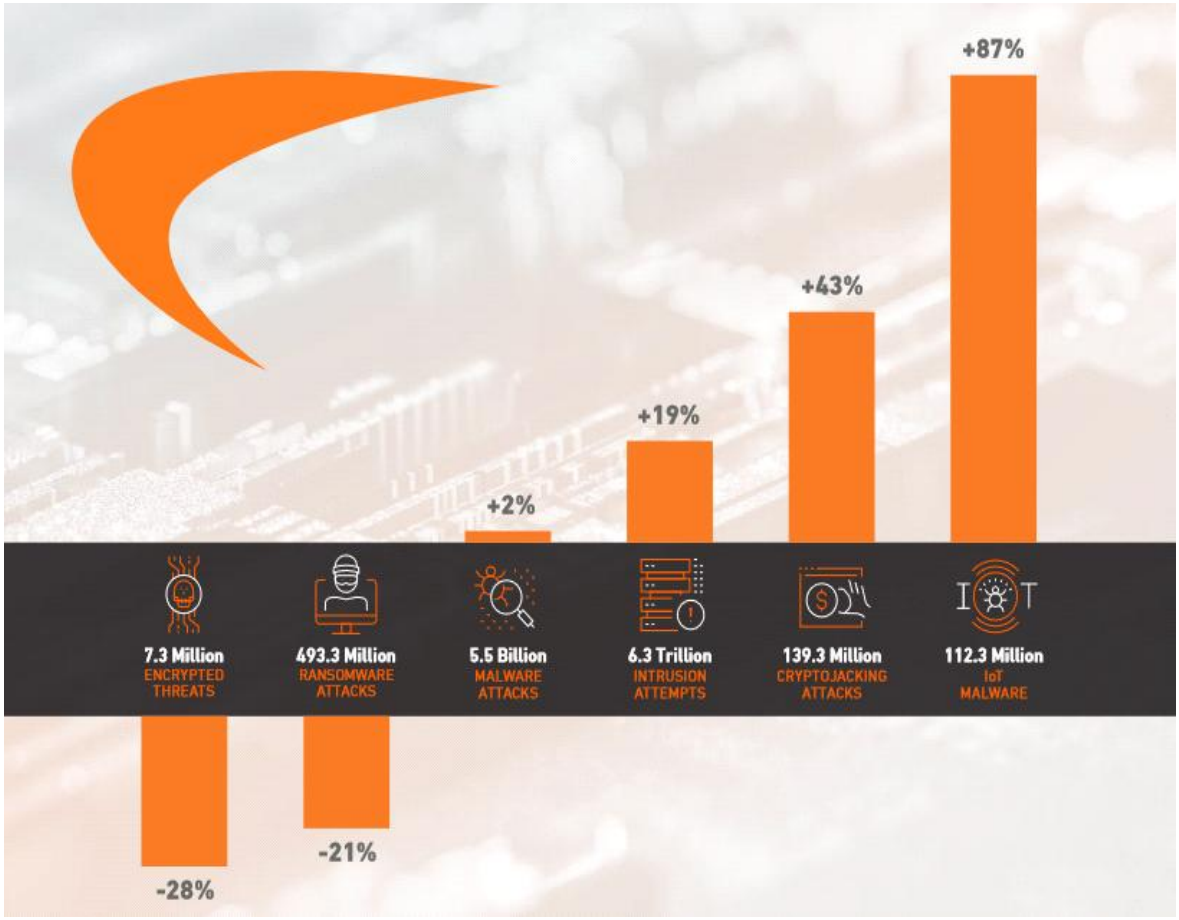
De acordo com a SonicWall (2022), o cibercrime é um fenômeno global há décadas. Para muitos, o ano de 2022 foi um alerta: não existem indústrias seguras, e não há países seguros. O cibercrime está em toda parte e está presente em nossas vidas.

SonicWall (2022) ainda afirma que é uma situação assustadora, porém, felizmente, existem profissionais de cibersegurança que se dedicam profundamente para derrotar, ou ao menos, mitigar os ataques que estão por toda parte do mundo, utilizando-se de ferramentas físicas e lógicas para enfrentar a guerra cibernética, diferente dos atores de ameaças que são motivados por dinheiro, fama, nacionalismo, entre outros.

As tendências de ciberataques estão sempre se diversificando. A Figura 1 ilustra a ameaça denominada ameaça criptografada (*encrypted threat*), aquelas que utilizam criptografia para não

serem identificadas (*ransomware*, dia zero, exfiltração de dados etc.), como a mais promissora, em uma probabilidade de 132%.

Figura 1 – Tendência Global de Ciberataques em 2022.



Fonte: Sonicwall (2023, p. 4)

Já na visão de ThoughtLab (2022), oito são as tendências que se reforçam mutuamente, tornando o cenário de segurança cibernética mais arriscado, mais complexo e mais caro de ser gerenciado, diante de uma situação de pandemia que acelerou a necessidade de trabalhos remotos, surgimento de novas tecnologias como Inteligência Artificial (IA) e dispositivos de Internet da Coisas (*Internet of Things – IoT*), guerras cibernéticas com ataques entre a Rússia e a Ucrânia etc., conforme a Figura 2

Figura 2: Cibersegurança em um ponto de inflexão crítico.

Fonte: ThouhtLab (2022, p. 12, tradução dos autores)

Em se tratando das estatísticas de incidentes de segurança, Pescatore e Hicks (2022) apresentam dados coletados pela *Identity Theft Resource Center* (ITRC), durante os anos de 2020 e 2021, e primeiro quadrimestre de 2022, ilustrados no Quadro 1

Quadro 1 – Estatística de Incidentes de Segurança (comprometidos e vítimas)

Setor	Ano					
	1º Quadr. 2022		2021		2020	
	Compr.	Vítimas	Compr.	Vítimas	Compr.	Vítimas
Educação	21	106.099	125	1.681.483	42	974.054
Serviços financeiros	68	3.384.769	279	19.873.772	138	2.687.084
Governo	13	294.027	66	3.244.455	47	1.100.526
Assistência médica	73	2.560.465	330	28.216.273	306	9.700.238
Industria hoteleira	6	56.451	33	238.445	17	22.365.384
Manufatura e utilidades	52	247.852	222	49.777.158	10	2.896.627
Sem fins lucrativos / ONG	18	558.362	86	2.339.646	31	37.528
Serviços profissionais	46	1.719.850	184	22.725.185	144	73.012.145
Varejo	18	282.950	102	7.212.912	53	10.710.681
Tecnologia	16	10.832.588	79	44.679.488	67	142.134.883
Transporte	8	20.930	44	569.574	21	1.208.292
Outros	65	719.620	308	79.538.669	172	43.391.302
Desconhecidos	0	0	4	35.232.664	0	0
Totais	**404**	**20.773.963**	**1862**	**295.329.724**	**1.048**	**310.218.744**
Indivíduos afetados por violação		51.421		158.662		279.980

Fonte: Pescatore e Hicks (2022, tradução dos autores).

Assistência Médica foi o setor mais comprometido nos três períodos pesquisados, seguido do setor classificado como Outros, em 2020 e 2021, e de Serviços Financeiros em 2022. Tais setores possuem grande volume de dados que atraem atacantes para ataques com possíveis retornos financeiros consideráveis.

Os trabalhos de Reposify (2022), SonicWall (2022), ThoughtLab (2022) e Pescatore e Hicks (2022) trazem apontamentos que ilustram a necessidade de um ambiente amplamente monitorado e gerenciado para vencer tudo isso.

2.1. IMPORTÂNCIA DA VISIBILIDADE

O trabalho apresentado pela Dataprise (2022) diz que no mundo da segurança cibernética, nada é mais urgente ou importante do que a detecção de ameaças. Com perigos ocultos no ambiente, gerenciar adequadamente a segurança da informação, permite a visibilidade desses perigos, podendo assim, ter os riscos mitigados ou até mesmo, eliminados.

Segundo Reposify (2022), nos últimos anos a visibilidade tornou-se uma palavra de ordem em todo o campo de segurança cibernética pois é um componente crucial na missão de estabelecer uma rede de Tecnologia da Informação e Comunicação (TIC) completa e segura, e de manter uma postura de segurança ideal.

O registro de logs é uma fonte essencial no ambiente de TIC, mas o grande volume de logs gerados por todos os sistemas e dispositivos, torna-se difícil e trabalhoso o gerenciamento e a análise desses logs. Mais uma vez a visibilidade é o caminho para auxiliar o profissional de segurança, mostrando o que está acontecendo, porque é impossível reagir a algo que você não vê (JOHNSON, 2022).

Segundo AT&T Cybersecurity (2020), a visibilidade inclui ver e compreender o estado atual do ambiente e as anomalias na configuração e comportamento, que podem apontar para possíveis violações do sistema.

Os trabalhos de Dataprise (2022), Reposify (2022), Johnson (2022) e AT&T Cybersecurity (2020) destacam o gerenciamento de perigos ocultos, a coleta de logs, a visão e compreensão do estado atual do ambiente e as anomalias na configuração e comportamento, não deixa dúvidas quanto à importância da visibilidade na cibersegurança, para execução de ações proativas dos profissionais diante as ameaças ocultas ou mesmo expostas.

3. PROVEDORES DE VISIBILIDADE

Os principais provedores de visibilidade podem ser classificados como: Gerenciamento de Eventos e Informações de Segurança, Análise de Comportamento do Usuário e Entidades, Orquestração de Segurança, Automação e Resposta e Detecção e Resposta Estendidas.

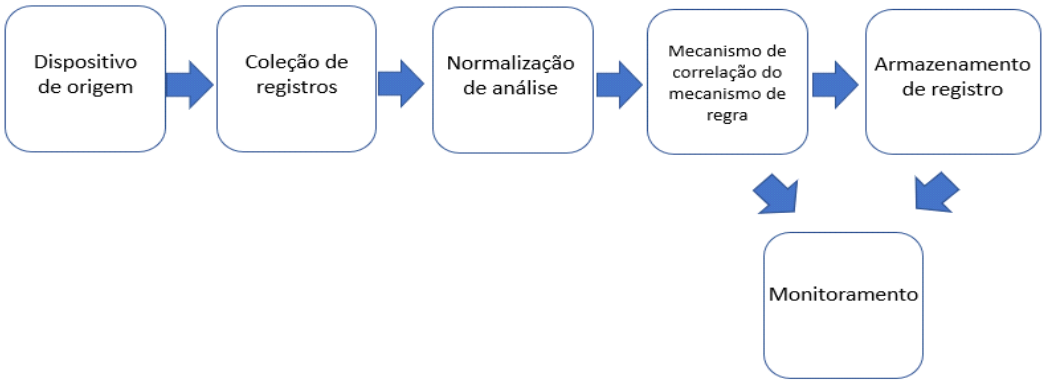
3.1. GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA

González-Granadillo, González-Zarzosa e Diaz (2021) dizem que sistemas de Gerenciamento de Eventos e Informações de Segurança (*Security Information and Event Management* – SIEM) têm sido uma ferramenta amplamente poderosa para prevenir, detectar e reagir contra os ataques cibernéticos. As soluções SIEM evoluíram para se tornarem sistemas abrangentes que fornecem uma ampla visibilidade para identificar áreas de alto risco e focar proativamente em estratégias de mitigação visando reduzir custos e tempo para resposta a incidentes.

Em geral, o SIEM têm a capacidade de coletar, agregar, armazenar e correlacionar eventos gerados por uma infraestrutura gerenciada, constituindo a plataforma central de centros de operações de segurança modernos à medida em que reúnem eventos de vários sensores (detecção de intrusão, sistemas, antivírus, firewalls, etc.), correlacionam esses eventos e fornecem visualizações sintéticas dos alertas para tratamento de ameaças e relatórios de segurança (GONZÁLEZ-GRANADILLO; GONZÁLEZ-ZARZOSA; DIAZ, 2021).

Os componentes básicos de um SIEM são ilustrados na Figura 3

Figura 3 – Componentes básicos do SIEM.



Fonte: González-Granadillo, González-Zarzosa e Diaz (2021, p. 2, tradução dos autores).

Segundo IBM (2022), independentemente do tamanho da sua organização, é essencial tomar medidas proativas para monitorar e mitigar os riscos de segurança de TI. As soluções SIEM beneficiam as empresas de várias maneiras e se tornaram um componente significativo na simplificação dos fluxos de trabalho de segurança. Alguns dos benefícios incluem:

- As soluções de monitoramento ativo SIEM de reconhecimento avançado de ameaças em tempo real em toda a sua infraestrutura reduzem significativamente o tempo necessário para identificar e reagir a possíveis ameaças e vulnerabilidades de rede, ajudando a fortalecer a postura de segurança à medida que a organização cresce;
- As soluções SIEM de auditoria de conformidade regulamentar, permitem auditoria e relatórios de conformidade centralizados em toda a infraestrutura de negócios. A automação avançada agiliza a coleta e a análise de logs do sistema, e eventos de segurança para reduzir a utilização de recursos internos e, ao mesmo tempo, atender aos rígidos padrões de relatórios de conformidade.

3.1.1. Automação Orientada por IA

As soluções SIEM de última geração integram-se com recursos poderosos de Automação e Resposta de Orquestração de Segurança, economizando tempo e recursos para as equipes de TI enquanto gerenciam a segurança dos negócios. Usando aprendizado de máquina profundo que se adapta automaticamente ao comportamento da rede, essas soluções podem lidar com

identificação de ameaças complexas e protocolos de resposta a incidentes em muito menos tempo do que equipes físicas (IBM, 2022).

3.1.2. Eficiência organizacional aprimorada

Devido à visibilidade aprimorada dos ambientes de TIC que ele fornece, o SIEM pode ser um fator essencial para melhorar as eficiências interdepartamentais. Com uma visão única e unificada dos dados do sistema e Orquestração de Segurança, Automação e Resposta integrado, as equipes podem se comunicar e colaborar com eficiência ao responder a eventos percebidos, e a incidentes de segurança (IBM, 2022).

3.1.3. Detectando ameaças avançadas e desconhecidas

Considerando a rapidez com que o cenário de segurança cibernética muda, as organizações precisam poder contar com soluções que possam detectar e responder a ameaças de segurança conhecidas e desconhecidas. Usando feeds integrados de inteligência de ameaças e tecnologia de IA, as soluções SIEM podem atenuar com sucesso, as violações de segurança modernas, como (IBM, 2022):

- Ameaças internas – Vulnerabilidades de segurança ou ataques originados de indivíduos com acesso autorizado a redes e ativos digitais da empresa. Esses ataques podem ser o resultado de credenciais comprometidas;
- Ataques de *phishing* – ataques de engenharia social disfarçados de entidades confiáveis, geralmente usados para roubar dados de usuários, credenciais de login, informações financeiras ou outras informações comerciais confidenciais;
- Injeção de SQL (*SQL Injections*) – Código malicioso executado por meio de uma página da web comprometida ou aplicativo projetado para contornar medidas de segurança e adicionar, modificar ou excluir registros em um banco de dados SQL;
- Ataques DDoS – Um ataque distribuído de negação de serviço (*Distributed Denial of Service* – DDoS) projetado para bombardear redes e sistemas com níveis de tráfego incontroláveis, degradando o desempenho de sites e servidores até que fiquem inutilizáveis;
- Exfiltração de dados – O roubo ou extrusão de dados geralmente é obtido aproveitando-se de senhas comuns ou fáceis de decifrar em ativos de rede ou por meio do uso de uma *Advanced Persistent Threat* (APT).

3.1.4. Conduzindo investigações forenses

Soluções SIEM são ideais para conduzir investigações forenses digitais quando ocorre um incidente de segurança. As soluções SIEM permitem que as organizações coletem e analisem com eficiência, dados de log de todos os seus ativos digitais em um só lugar. Isso lhes dá a capacidade de recriar incidentes anteriores ou analisar novos para investigar atividades suspeitas e implementar processos de segurança mais eficazes (IBM, 2022).

3.1.5. Avaliação e relatórios sobre conformidade

Auditoria e relatórios de conformidade são tarefas necessárias e desafiadoras para muitas organizações. As soluções SIEM reduzem drasticamente os gastos com recursos necessários para gerenciar esse processo, fornecendo auditorias em tempo real e relatórios sob demanda de conformidade regulatória sempre que necessário (IBM, 2022).

3.1.6. Monitoramento de usuários e aplicativos

Com o aumento da popularidade de forças de trabalho remotas, aplicativos SaaS (*System as a Service*) e políticas do tipo "Traga seu próprio dispositivo" (*Bring Your Own Device - BYOD),* as organizações precisam do nível de visibilidade necessário para mitigar os riscos de rede fora do perímetro de rede tradicional. As soluções SIEM rastreiam toda a atividade de rede em todos os usuários, dispositivos e aplicativos, melhorando significativamente a transparência em toda a infraestrutura e detectando ameaças, independentemente de onde os ativos e serviços digitais estão sendo acessados (IBM, 2022).

3.1.7. Ferramentas e recursos envolvidos em uma solução SIEM

Esta seção destaca as tecnologias e elementos que compõem um SIEM, abordando os recursos cruciais para a coleta e análise de dados de segurança, visando à detecção e resposta a ameaças cibernéticas em tempo real.

- Gerenciamento de dados de registro: A coleta de dados de log é a base do gerenciamento de eventos e informações de segurança. Coleta, análise e correlação de dados em tempo real maximizam a produtividade e a eficiência;
- Visibilidade da rede: Ao inspecionar as capturas de pacotes para visibilidade dos fluxos de rede, o mecanismo de análise SIEM pode obter informações adicionais sobre ativos, endereços IP e protocolos para revelar arquivos maliciosos ou a exfiltração de dados de Informações de Identificação Pessoal (*Personally Identifiable Information – PII*) que se movem pela rede;
- Inteligência de Ameaças: Ser capaz de incorporar feeds de inteligência proprietários ou de código aberto em sua solução SIEM é essencial para reconhecer e combater as vulnerabilidades modernas e assinaturas de ataque;
- Análise: Nem todas as soluções SIEM oferecem o mesmo nível de análise de dados. Soluções que incorporam tecnologia de última geração, como aprendizado de máquina e inteligência artificial, ajudam a investigar ataques mais sofisticados e complexos à medida que surgem;
- Alerta em tempo real: As soluções SIEM podem ser personalizadas de acordo com as necessidades de negócios, fazendo uso de alertas e notificações pré-definidos e em camadas em várias equipes;
- Painéis e relatórios: Em algumas organizações, centenas ou até milhares de eventos de rede podem ocorrer diariamente. Compreender e relatar incidentes em uma visão personalizável, sem atrasos, é essencial;

- Conformidade de TI: Os requisitos de conformidade regulatória variam consideravelmente de uma organização para outra. Embora nem todas as ferramentas SIEM ofereçam toda a gama de cobertura de conformidade, as organizações em setores altamente regulamentados priorizam a auditoria e os relatórios sob demanda em detrimento de outros recursos;
- Integrações de segurança e de TIC: A visibilidade organizacional começa com a integração do SIEM com uma variedade de fontes de log de segurança e não segurança; as organizações estabelecidas se beneficiarão de um SIEM que se integra aos investimentos existentes em segurança e ferramentas de TIC (IBM, 2022).

3.2. ANÁLISE DE COMPORTAMENTO DO USUÁRIO E ENTIDADES

Segundo Netsurion (2022), além de perceber comportamentos suspeitos na rede, os SIEMs evoluíram para incluir Análise de Comportamento do Usuário(*User Behavior Analytics - UBA*) ou Análise de Comportamento do Usuário e Entidades(*User and Entity Behavior Analytics - UEBA*). O UBA/UEBA aciona um alerta quando ocorre um comportamento incomum do usuário ou da entidade. Esse é um recurso importante agora que as credenciais comprometidas representam 76% de todas as invasões de rede.

Quando as credenciais são roubadas, elas tendem a ser usadas de maneiras, lugares e horários incomuns. Por exemplo, se ocorrer um login fora do padrão normal, isso será imediatamente sinalizado para investigação (NETSURION, 2022).

3.3. ORQUESTRAÇÃO DE SEGURANÇA, AUTOMAÇÃO E RESPOSTA

Embora os alertas para comportamentos suspeitos sejam necessários, o objetivo real é agir sobre o comportamento suspeito da forma mais rápida e eficaz possível. Essa é a próxima evolução do SIEM: Orquestração de Segurança, Automação e Resposta (*Security Orchestration Automation and Response – SOAR*). Enquanto os SIEMs tradicionais podem “dizer” algo, aqueles que incorporam o SOAR podem “fazer” algo.

O SOAR consolida fontes de dados, usa informação fornecida por feeds de inteligência de ameaças e automatizam respostas para melhorar a eficiência e a eficácia (IBM, 2022).

3.4. DETECÇÃO E RESPOSTA ESTENDIDAS

Segundo Williams (2022), a Detecção e Resposta Estendidas (*Extended Detection and Response – XDR*), é uma nova abordagem para a detecção de ameaças. Ele fornece proteção mais completa contra os ataques cibernéticos, bem como acesso não autorizado e uso indevido de dados. O XDR permite que as equipes de segurança descubram ameaças ocultas e avançadas e fornece a elas as ferramentas para automatizar respostas complexas em várias etapas.

4. COMO MELHORAR A VISIBILIDADE

Ollmann (2022) defende que é importante saber o que está acontecendo em seu ambiente antes que seja tarde demais. Os maus atores dependem de permanecerem ocultos no ruído de logs, sistemas, ferramentas, equipes, processos e silos organizacionais.

A pesquisa realizada por Filkins e Pescatore (2021) registra que 80% das organizações que não têm visibilidade de seus ativos relatam aproximadamente três vezes mais incidentes de segurança cibernética. E quando solicitados a identificar a maior causa da ineficácia do Centro de Operações de Segurança (*Security Operation Center* - SOC), 65% dos líderes citaram a Visibilidade na Superfície de Ataque, conforme Quadro 2:

Quadro 2 – Resultado da Pesquisa de Lacuna de Visibilidade.

Classificação	Lacuna de visibilidade
1.	Falta de visibilidade sobre quais dados estão sendo processados na infraestrutura
2.	Acesso a informações confidenciais por dispositivos não gerenciados inseguros
3.	Uso indevido por membros da organização
4.	Não saber com certeza onde os dados confidenciais estão geograficamente localizados ou armazenados
5.	Acesso não autorizado por indivíduos a dados confidenciais
6.	Incapacidade de auditar o acesso do usuário
7.	Incapacidade de responder a incidentes que atravessam a infraestrutura
8.	Interfaces mal configuradas ou seguras (por exemplo, APIs)
9.	Má configuração e segurança de componentes de aplicativos rapidamente desenvolvidos (por exemplo, contêineres)
10.	Invasão de malware
11.	Acesso não autorizado por aplicativos a dados confidenciais
12.	Acesso não autorizado por estranhos à infraestrutura
13.	Configuração incorreta ou vulnerabilidade ou hypervisors e outros gerenciadores de virtualização
14.	Reconhecendo o tempo de inatividade ou indisponibilidade de aplicativos quando necessário

Fonte: Filkins e Pescatore (2021, p. 6, tradução dos autores).

Filkins e Pescatore (2021) dá três dicas para melhorar a visibilidade da segurança de uma organização, como:

- Ser capaz de visualizar todos os dados em toda a organização e protegê-los adequadamente;
- Adotar análises de segurança que aproveitam a automação baseada em aprendizado de máquina e em Inteligência Artificial (IA), e que permitam investigações confiáveis e repetíveis de ameaças em todos os seus dados, o tempo todo;
- Adotar uma abordagem científica onde a Inteligência Artificial aprende com o humano pois não tem informações ou confiança suficientes para fornecer uma resposta autônoma, e o humano expande seu conhecimento à cerca do tema e de tecnologias em evolução.

Na visão de Jefferies (2022), existem cinco dicas importantes para melhorar a visibilidade e o controle de segurança cibernética:

- Ter os funcionários como sua primeira linha de defesa, mantendo a segurança em mente enquanto os funcionários estão fora do escritório, com realização de treinamento de conscientização sobre segurança cibernética;

- Proteger os dispositivos utilizados pelos usuários, como desktop, notebook, tablet, smartphone etc, limitando quais atividades podem ser realizadas no dispositivo;
- Usar os melhores serviços de detecção e resposta para ter monitoramento, detecção de ameaças e resposta a incidentes oriundos de variados dispositivos de segurança;
- Proteger a organização na nuvem, como por exemplo, implementando a autenticação multifator (*Multifactor Authentication – MFA*) e gerenciando acesso do usuário;
- Prevenir reavaliando a estratégia de segurança cibernética, tendo ferramentas e serviços, e aplicando treinamentos e testes eficazes aos funcionários.

AT&T Cybersecurity (2020) defende a estrutura de segurança cibernética desenvolvida pelo National Institute of Standards and Technology (NIST). Essa estrutura orienta como fornecer visibilidade completa em todo ambiente, do pré-ataque ao pós-ataque, e tem como funções: Identificar, Proteger, Detectar, Responder e Recuperar (Quadro 3).

Quadro 3 – Detalhamento da Estrutura de Segurança Cibernética do NIST.

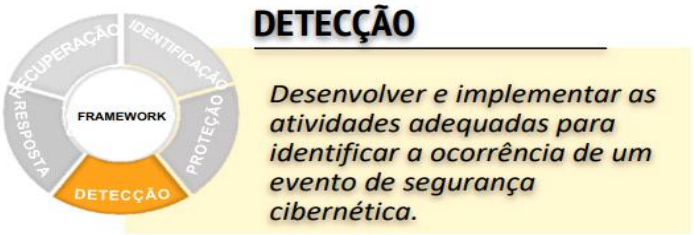
Componentes da estrutura	O que é isso
Funções	Cinco componentes que compõem a visão estratégica de alto nível da estrutura: identificar (ID), proteger (PR), detectar (DE), responder (RS) e recuperar (RC).
Categorias	Cada função tem várias categorias que definem os resultados desejados. Exemplo: O resultado desejado de uma categoria de gerenciamento de ativos é obter um forte entendimento de todos os ativos do ambiente.
Subcategorias	Definições mais granulares dos resultados desejados, por categoria.
Padrões	Referências informativas aos padrões aplicáveis do setor para ajudar a definir a estratégia.

Fonte: AT&T Cybersecurity (2020, tradução dos autores).

Fazer uma avaliação para identificar em qual status a organização está, é importante desenvolver um roteiro de onde ela quer estar. Ajudará o negócio a entender os passos certos de como chegar lá.

Cinco componentes compõem o framework do NIST. O Quadro 4 apresenta detalhadamente as funções e categorias, e é uma forma de medir a maturidade e a completude do ambiente, porém isso requer ser honesto consigo mesmo, tendo um olhar rigoroso.

Figura 3 – Detecção: uma das cinco funções do Framework do NIST.



Fonte: Amahn et al. (2021, p. 2).

Quadro 4 – Estrutura do NIST detalhada

Identificador único das funções	Funções	Identificador único das categorias	Categorias
ID	Identificar	ID AM	Gestão de ativos
		ID BE	Ambiente de negócios
		ID GV	Governança
		ID RA	Avaliação de risco
		ID RM	Estratégia de gerenciamento de risco
		ID SC	Gerenciamento de risco da cadeia de suprimentos
PR	Proteger	PR AC	Controle de Acesso
		PR AT	Conscientização e Treinamento
		PR DS	Segurança de Dados
		PR IP	Processos e procedimentos de proteção da informação
		PR MA	Manutenção
		PR PT	Tecnologia de proteção
DE	Detectar	DE AE	Anomalias e eventos
		DE CM	Monitoramento contínuo de segurança
		DE DP	Processos de detecção
RS	Responder	RS RP	Planejamento de resposta
		RS CO	Comunicações
		RS NA	Análises
		RS MI	Mitigações
		RS IM	Melhorias
RC	Recuperar	RC RP	Planejamento de recuperação
		RC IM	Melhorias
		RC CO	Comunicações

Fonte: Amahn et al. (2021, tradução dos autores).

Como o foco deste trabalho é visibilidade, será abordada apenas a Função Detecção (Figura 3).

A Função Detecção permite a descoberta oportuna de ocorrências de segurança cibernética, tendo como categorias: Anomalias e Ocorrências, Monitoramento Contínuo de Segurança e Processos de Detecção.

Atividades para a função Detecção, descritas pela Publicação Especial NIST 1271 (AMAHN et al., 2021) são apresentadas a seguir:

- Testar e atualizar os processos de detecção: É preciso desenvolver e testar processos e procedimentos para detectar entidades e ações não autorizadas nas redes e no ambiente físico, incluindo atividades de pessoal. A equipe deve estar ciente de suas funções e responsabilidades quanto à detecção e às denúncias desse tipo de ação, seja dentro da sua organização ou perante o controle externo e autoridades jurídicas;
- Conhecer os fluxos de dados esperados na sua empresa: Se você souber como e quais são os dados esperados pela sua empresa, você terá uma probabilidade muito maior de perceber algo inesperado; e o inesperado nunca é bom quando se trata de segurança cibernética. Fluxos de dados inesperados podem incluir a exportação de informações de clientes de um banco de dados interno para a rede. Caso você tenha contratado um provedor de serviços gerenciado ou em nuvem, discuta com ele como

será feita a monitoração de fluxos e relatórios de dados, incluindo os eventos inesperados;

- Manter e monitorar registros: Os registros são cruciais para identificar anomalias nos computadores e aplicativos de sua empresa. Esses registros documentam eventos como alterações de sistemas ou contas, assim como a iniciação de canais de comunicação. Considere o uso de ferramentas de software que possam agregar esses registros e buscar padrões ou anomalias em comportamentos esperados da rede;
- Entender o impacto de eventos de segurança cibernética: Se um evento de segurança for detectado, sua empresa deve agir de forma rápida e cuidadosa para entender a amplitude e gravidade do impacto. Busque ajuda. Comunicar as informações sobre o evento com as respectivas partes interessadas vai deixá-lo em uma boa posição em termos de parceiros, órgãos de fiscalização e outros (incluindo, potencialmente, investidores), além de ajudá-lo a aprimorar políticas e processos.

5. CONCLUSÃO

Considerando todos os aspectos abordados neste estudo, é evidente que as corporações, os profissionais de cibersegurança e os órgãos regulamentadores voltados para a cibersegurança estão profundamente preocupados com a questão da visibilidade do ambiente de Tecnologia da Informação e Comunicação (TIC).

Embora seja claro que a visibilidade por si só não possa eliminar completamente a ocorrência de ataques cibernéticos ou potenciais ameaças, ela desempenha um papel crucial ao fornecer um alerta antecipado que os profissionais de cibersegurança necessitam para iniciar uma investigação no ambiente. Essa ação pode, em muitos casos, prevenir que uma tentativa de ataque seja bem-sucedida.

É importante ressaltar que a eficácia da visibilidade cibernética está diretamente relacionada à existência de um ambiente bem estruturado, com a implementação de um conjunto de provedores capazes de oferecer essa visibilidade. Além disso, é essencial que haja recursos adequados para alimentar esses provedores com uma ampla gama de dados que possam ser rastreados, analisados e tratados de maneira eficiente.

Embora diferentes autores possam abordar as ameaças cibernéticas sob diferentes perspectivas, todos convergem para a mesma solução: aumentar a visibilidade cibernética no ambiente de TIC das organizações. Essa abordagem proativa, reativa e preditiva é fundamental para mitigar os riscos e fortalecer a postura de segurança cibernética das organizações em um cenário cada vez mais complexo e perigoso.

6. REFERÊNCIAS

AMAHN, A. M. *et al.***Introdução ao Framework de Segurança Cibernética do NIST: Um guia de iniciação rápida**. [*S.l.*]: NIST, 2021. 3 p. (Publicação Especial NIST 1271).

AT&T CYBERSECURITY. **How the NIST Cybersecurity Framework Transforms Security Visibility**. [*S.l.*]: AT&T, 2020. 5 p. Disponível em: nist-cybersecurity-framework-transforms-security-visibility.pdf. Acesso em: 3 dez. 2022.

DATAPRISE. **Three Critical Types of Cybersecurity Visibility**. Disponível em: https://www.dataprise.com/resources/blog/better-cybersecurity-visibility. Acesso em: 3 dez. 2022.

FILKINS, B.; PESCATORE, J. A **SANS 2021 Report:** Making Visibility Definable and Measurable. [*S.l.*]: Sans, 2021. 15 p. (White paper). Disponível em: https://assets.extrahop.com/whitepapers/sans-making-visibility-definable.pdf. Acesso em: 3 dez. 2022.

GONZÁLEZ-GRANADILLO, G.; GONZÁLEZ-ZARZOSA, S.; DIAZ, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. **Sensors**, v. 21, art. 4759, p. 1-28, 2021.

IBM. **What is SIEM?** Disponível em: https://www.ibm.com/topics/siem. Acesso em: 3 dez. 2022.

JEFFERIES, L. Five top tips for improving your cyber security visibility and control. **The AI Journal,** 9 May 2022. Disponível em: https://aijourn.com/five-top-tips-for-improving-your-cyber-security-visibility-and-control/. Acesso em: 3 dez. 2022.

JOHNSON, D. **The importance of network visibility for your business**. Disponível em: https://www.verizon.com/business/resources/articles/why-network-visibility-is-important-for-your-business/. Acesso em: 3 dez. 2022.

NETSURION. **SIEM, UEBA, SOAR and Your Cybersecurity Arsenal**. Disponível em: https://www.netsurion.com/articles/siem-ueba-soar-and-your-cybersecurity-arsenal. Acesso em: 3 dez. 2022.

OLLMANN, G. **Tips for Improving Security Visibility - Focus on the threats that matter most with data and automation technologies to keep your organization safe**. Disponível em: https://www.csoonline.com/article/3674129/tips-for-improving-security-visibility.html. Acesso em: 3 dez. 2022.

PESCATORE, J.; HICKS, T. **SANS 2022 Top New Attacks and Threat Report**. [*S.l.*]: Sans, 2022. 15 p. (White paper).

REPOSIFY. **The Spectrum of Cyber Risk Visibility**. Disponível em: https://web.archive.org/web/20220702163934/https://reposify.com/blog/the-spectrum-of-cyber-risk-visibility/. Acesso em: 2 jul. 2022.

SONICWALL. **2023 SonicWall Cyber Threat Report**. Milpitas, CA: SonicWall, 2022. 69 p.

THOUGHTLAB. **Cybersecurity Solutions for a Riskier World How business and government can protect themselves in the emerging risk landscape**. SaltLake City: Thoughtlab, 2022. 85 p.

WILLIAMS, A. **SIEM vs. SOAR vs. XDR vs. UEBA:** How Are They Different? Each covering different cybersecurity areas, often with one requiring functions of another, using these tools in combination may be the best solution. Disponível em: https://www.mimecast.com/blog/siem-vs-soar-vs-xdr-vs-ueba-how-are-they-different/. Acesso em: 3 dez. 2022.