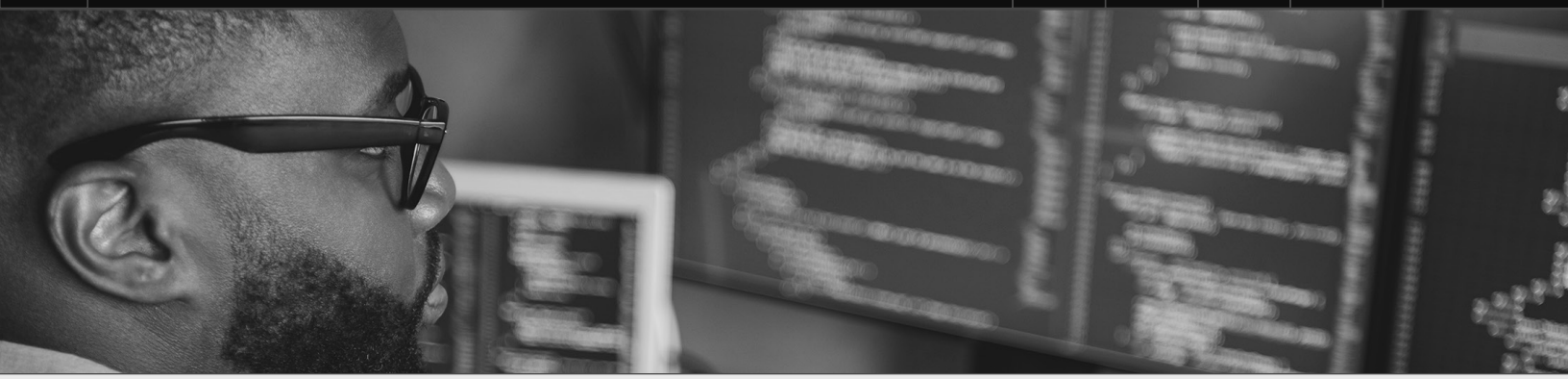
BINARY DEFENSE

WHITEPAPER

Security Use Cases for Your SIEM

Table of Contents



Identifying Critical Log Sources is Paramount for Cyber Resilience

SIEM technology provides the ability to generate and monitor alerts of potential security threats in real time. Identifying critical log sources to be ingested into the SIEM is paramount to ensure specific threat management use cases align with your business and cyber security goals for detecting and preventing a cyberattack.

Understanding Your Risk

Cyberattacks are becoming more frequent, targeted, and complex. A cyberattack can have a crippling effect on your organization — not only could it disrupt normal operations, but it may damage your brand's reputation, cause revenue losses from system downtime, and damage important IT assets and infrastructure that can be impossible to recover. The expanding attack surface caused by remote working, digital transformation, and cloud migration are well-known concerns for IT security leaders. Ransomware attacks are at an all-time high, and cybercrime is up 600% as a result of the COVID-19 pandemic. As ransomware and destructive malware attacks have grown more common, executives understand that it's not a question of will my organization be breached, but rather, when a breach occurs are we prepared to respond? By understanding the types of attacks and consequences, IT leaders, cybersecurity strategists, and risk management officers can minimize potential risk, gain value in cybersecurity efforts, and even prevent future attacks.

24/7 Security Operations Center

Stop an Attack in its Tracks

Whether you are a small business, or a global enterprise, attackers are relentless using a variety of breach methods to get past network defenses. Most attackers only need a matter of minutes between the initial attack and the successful compromise of sensitive information — and the more time an attacker spends undetected within corporate systems, the more damage can be done. The problem is that for most businesses, the gap between the time when a breach occurs — and the time when the breach is discovered and action is taken to stop it — is not hours or days, but months. The best defense against sophisticated attacks requires a team of cybersecurity experts working 24/7 to protect your business. By identifying and responding to a potential cybersecurity threat immediately, cybersecurity experts can stop an attack in its tracks and keep damages to a minimum.

24/7 Security Operations Center

Cyber resilience requires speed, accuracy and agility to detect and respond to attacks as they occur. Outsourcing the deployment of SIEM technology and 24/7 Security Operations Center (SOC) monitoring and response to cyber threats can reduce risk, simplify security operations, and help organizations utilize a team of experts that the organization may not have in place, or augment an existing cybersecurity team and allow the in-house team to focus on tasks other than monitoring. A SIEM is a centralized security platform that brings together threat intelligence, log search, user activity and endpoint data into a single visual timeline to speed up investigations. From antivirus events to firewall logs, the SIEM platform collects data in real-time and sorts it into categories, such as malware activity, failed and successful logins and other potentially malicious activity. SIEMs also have long-term log storage for historical analysis of security events and generating compliance reports.

SIEM Technology

SIEM technology and continuous SOC monitoring are critical for detecting and quickly responding to security incidents to ensure minimal impact and continued business operations. The SOC is staffed by highly-trained security analysts that detect and analyze advanced attack patterns and alert you of malicious threats within minutes — to help minimize threat actor dwell time, stop the spread of malware or malicious activity on internal systems, and work proactively to prevent a full-blown attack.

When implementing a SIEM, it's critical to identify the log sources that should be monitored to help you better protect the data that your organizations success depends upon — this requires a deep understanding of your data sources that are coveted targets for threat actors, as well as the various tactics, techniques and procedures that are likely to be used to compromise your critical assets.

Threat Intelligence

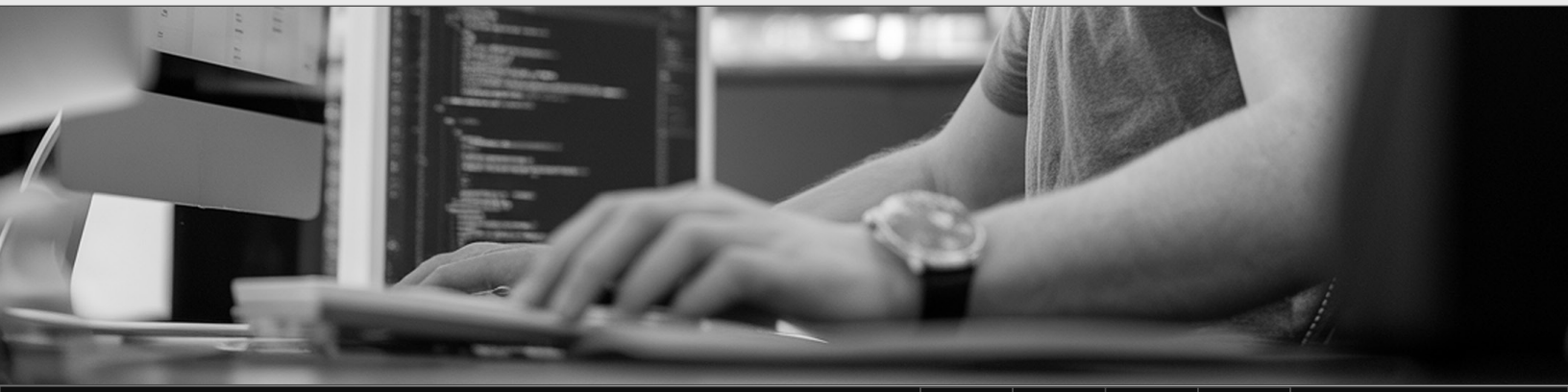
Centralized log management with integrated Threat Intelligence is vital in the fight against cyber threats. Threat intelligence identifies pieces of data that have previously been detected during a compromise attempt. These "indicators of compromise" (IOCs) are collected into both open source and proprietary databases known as threat intelligence feeds and include all the necessary information about known threats — such as zero-day attacks, malware, botnets, and other security threats. Threat intelligence can be compared in real-time with data coming from your log entries to identify a potential breach.

Preventing a Catastrophic Loss

We've highlighted the most common cyberattack methods and stages of an attack as well as the recommended network and data sources that should be monitored to prevent a catastrophic loss.

Attack Methods

- Account compromise
- Credential sharing
- Data exfiltration
- Denial of service attack
- Insider threats
- Password attacks
- Persistent and advanced threats
- Phishing
- Privileged access abuse
- Ransomware and malware
- Suspicious file sharing, permission changes, and downloads
- Suspicious login events
- Unauthorized email permission changes
- Unpatched operating systems and networking devices



Important Log Sources

Network Data Sources

- Unified Threat Management (UTM)
- Firewalls (RADIUS)
- Intrusion Prevention System and Intrusion Detection System (IPS/IDS)
- Web Filter/Proxy
- Load Balancers (Elastic, F5)
- Network Access Control (NAC)
- Network Traffic Analysis (NTA)

Data Sources

- VPN and External Access — RDP Gateways, Citrix
- Azure, AWS, Google Cloud Platform (GCP)
- Switches and Routers n Multi-factor Authentication (MFA) — Okta, Duo, or others
- Endpoint Detection and Response (EDR) and Antivirus
- Web Application Firewalls (WAF) n FTP Server
- Data Loss Prevention (DLP)
- Applications — Microsoft 365 (M365), G Suite, and others
- Database
- Email Gateway
- DNS/DHCP

Windows/Linux/Mac

- Active Directory (AD)
- Servers (Standard windows logs, Sysmon, advanced file sharing, PowerShell command log)
- Workstations

Cyberattack Methods

Discovery

Today's cyber adversaries are savvy at infiltrating systems with automated tools or using a variety of constantly evolving tactics. Once adversaries gain access to an organizations network, they silently watch and learn how to exploit security weaknesses to achieve their objectives by surprise. Smart organizations can avert the impact of a breach by denying intruders the opportunity to get oriented with their environment in the first place.

During the discovery phase of a cyberattack, an adversary explores what they can control at the initial point of entry and how it could benefit their objectives. Understanding the discovery phase can prepare you to counter nefarious activities and any potential downstream consequences. Attackers often target Active Directory as it houses a great deal of information tied to user accounts, key systems, and sensitive data repositories. Targeting Active Directory first can enable adversaries to gather intelligence about key systems without even leaving the initial point of compromise. Clever reconnaissance often exploits default settings and misconfigurations — a simple query of group membership may give threat actors access to authenticated domain user information for other systems and accounts. Adversaries then use the extracted information to identify systems or accounts with elevated privileges.

Privilege Access Abuse

Outside threat actors use various privilege escalation techniques to access unauthorized resources. Web intrusions are usually only the first stage of a complex attack. Malicious parties gain basic access to certain resources and then continue with privilege escalation attacks to gain more control. Threat actor goals may include accessing sensitive data, installing malware, introducing malicious code, or even hijacking a single computer system or multiple systems. Privilege elevation is typically the second step of an attack where a threat actor tries to get file system and/or console access. After they gain shell access to the web server, they often rely on misconfigurations or unpatched operating systems to gain access to the system administrator or another privileged account.

Ransomware and Malware

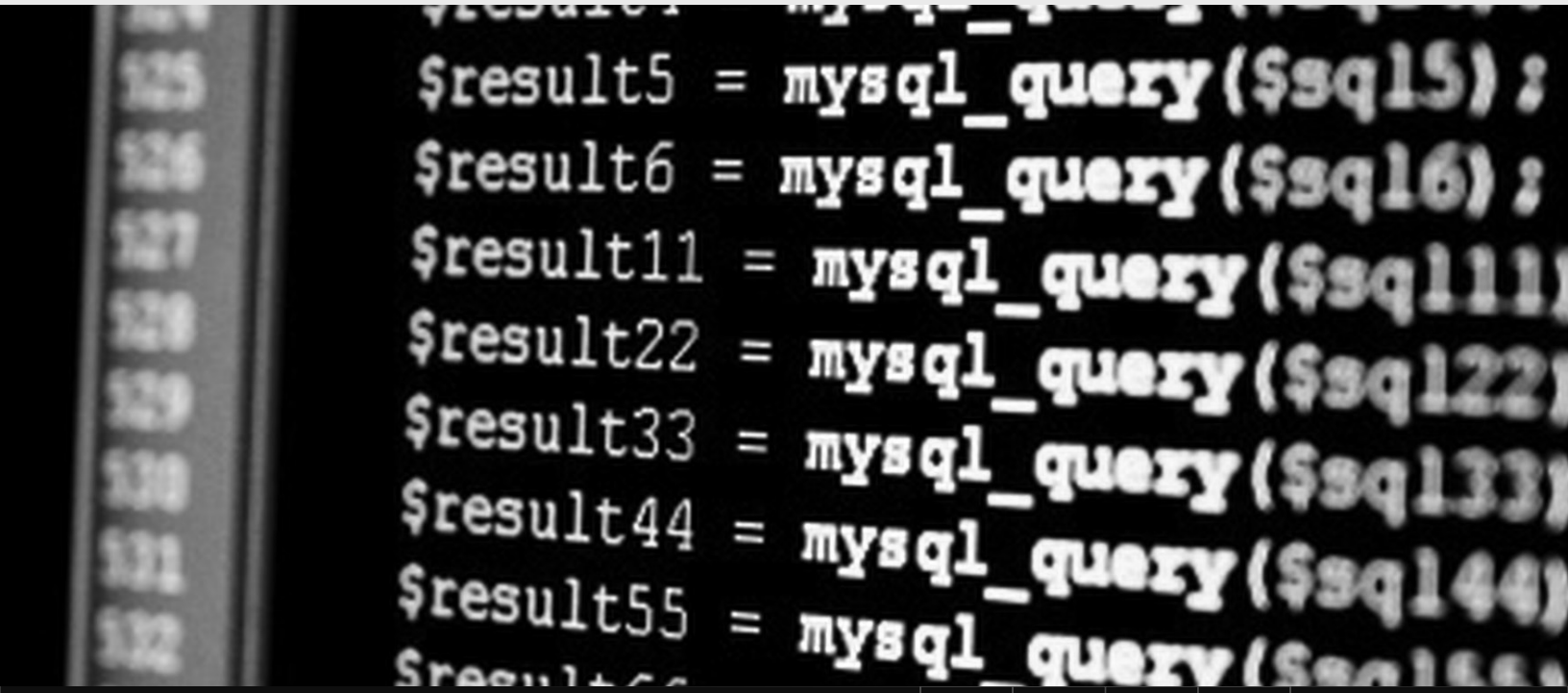
As ransomware attacks continue to intensify, organizations must prioritize their cybersecurity to prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Malware impacts the productivity of organizations by completely blocking access to business-critical systems. Ransomware actors often target critical infrastructure, small businesses, hospitals, schools, and local government and then threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. The economic and reputational impacts of ransomware incidents is exponential and malicious actors continue to adjust and evolve their tactics over time making ransomware incidents more destructive and impactful in nature and scope.

System Availability

Attackers use automated tools to orchestrate denial of service attacks that execute simultaneous requests to overload systems and make them inoperable. Downtime on systems can have signifi cant impacts to critical services for customers, workforce productivity, or life-supporting medical devices. SIEM monitoring can provide a warning so that incident responders can quickly react to an influx of connections from availability attacks.

SQL Injection

SQL injection allows an attacker to interfere with the queries that an application makes to its database and allows the attacker to view data that they are not normally able to retrieve, such as data belonging to other users, or any other sensitive data that the application is able to access such as passwords, credit card details, or personal information. In most cases an attacker can modify or delete the data, causing persistent changes to the application's content or behavior. An attacker can also escalate an SQL injection attack to compromise the underlying server, other back-end infrastructure, or to perform a denial-of-service attack. Many high-profile data breaches in recent years have been the result of SQL injection attacks — leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for months.



Advanced Persistent Threat (APT)

Motivated by financial or political goals, advanced persistent attackers are well-funded and laser-focused adversaries that use zero-day or lesser-known vulnerabilities to breach a network to extract or damage highly sensitive or valuable information. Organizations that should be concerned about advanced persistent threats (APTs) are those that deal with critical infrastructure, sensitive personal information such as medical records or financial data, or sensitive information that may provide a significant competitive advantage should it be extracted or manipulated.

In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. Once that is accomplished, they use persistent techniques to maintain their foothold on the compromised account. Techniques used for persistence include any access, action, or configuration changes that let threat actors preserve access to compromised systems, such as replacing or hijacking legitimate code or adding startup code. Many threat actors modifying credentials or permission groups, or they subvert security policies with iterative password updates to bypass password duration policies. High fidelity threat intelligence and skilled cybersecurity experts that specialize in identifying irregular behavior or suspicious activities are critical for combating APTs.

Data Integrity

Adversaries ultimate goal is to exploit data associated with key integrity-driven systems to damage the trust in an organization's reputation or brand. Data integrity breaches affect critical databases and file systems and can be targeted by external adversaries or by internal personnel, either maliciously or in error. When network users have more access rights than they need to do their jobs, it puts IT systems at risk of users deleting information, accessing sensitive information or stealing intellectual property.

Organizations that regularly interact with information that is used for business-critical decision making, such as healthcare, financial trading, government organizations, or defense suppliers should have critical databases, files systems, and specific files and/or folders of interest monitored. Other examples include organizations with highly automated operations that depend on the accuracy of information — and a compromise of the information could lead to significant financial losses.

Data Theft

Data exfiltration occurs when a malicious actor carries out an unauthorized data transfer from a computer with the goal of damaging consumer confidence, corporate valuation, or national security. Most adversaries aim to exploit large volumes of data to gain a competitive advantage by stealing proprietary business secrets and intellectual property or for financial gain by stealing mailing addresses, social security numbers, usernames and passwords, or personal financial information such as credit card numbers.

If an attacker can gain privileged remote access to the server containing data that they wish to exfiltrate, their chances of success are significantly higher. For example, a system administrator could plant and execute malware that transmits data to an external command and control server, or a malicious actor could compromise user accounts with weak passwords on remote access applications to transfer targeted data elsewhere. More sophisticated forms of data exfiltration conceal detection by network defenses. For example, Cross Site Scripting (XSS) can be used to exploit vulnerabilities in web applications to provide a malicious actor with sensitive data, or a timing channel can send data — a few packets at a time at specified intervals, so that it is even more difficult for network defenses to detect and prevent.

Real-time monitoring reduces the likelihood that a data breach will go unnoticed and helps to proactively remediate a breach before data exfiltration is completed. Most data is extracted in small amounts over long periods of time, but monitoring helps to proactively identify a breach and remediate it quickly.

Phishing and Man-in-the Middle Attacks

Threat actors can run attacks using automated software, while other attacks require a more active role from threat actors. A man-in-the-middle (MITM) attack is a type of eavesdropping attack, where threat actors interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants. This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late.

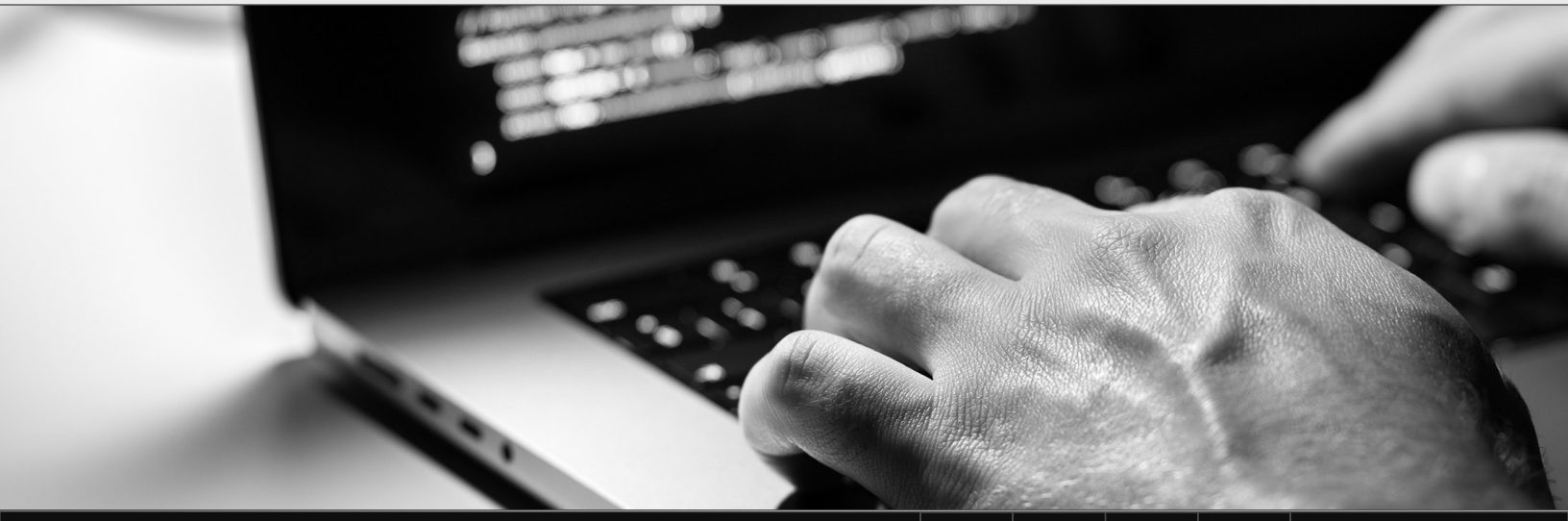
With a traditional MITM attack, the cybercriminal usually gains access to an unprotected or poorly secured Wi-Fi access point. These types of connections are generally found in public areas with free Wi-Fi hotspots, or the homes of remote workers that haven't protected their network. Attackers can scan the access point looking for specific vulnerabilities such as a weak password. Once attackers find a vulnerable access point, they can deploy tools to intercept and read the victim's transmitted data. The attacker can then also insert their tools between the victim's computer and the websites the user visits to capture login credentials, banking information, and other personal information.

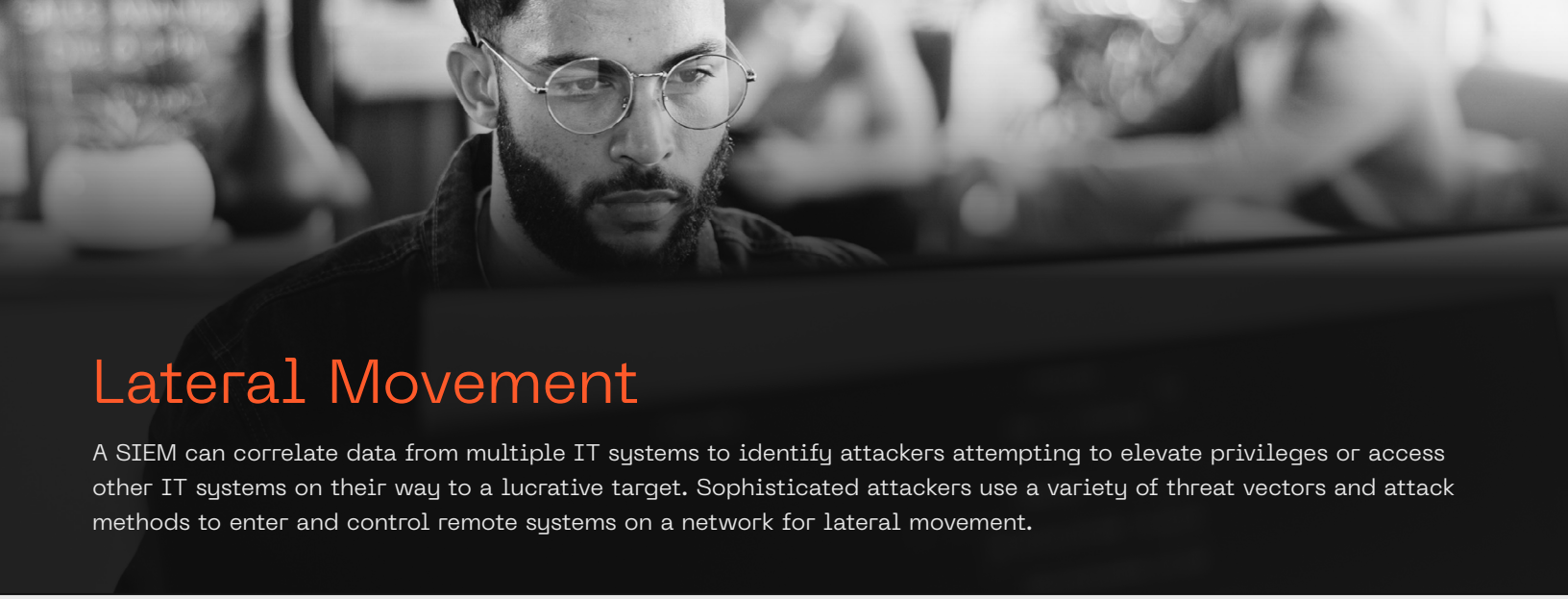
Another example is a Phishing attack where a threat actor sends an email or text message to a user that appears to come from a trusted source, such as a bank. By clicking on a link or opening an attachment in the Phishing message, the user inadvertently loads malware onto their computer or mobile device. The malware records the data sent between the victim and the targeted banks website and transmits it to the attacker.

The top attacks, phishing and ransomware, are exacerbated by the remote workforce. Phishing scams typically involve social engineering in traditional email and cloud services attacks. Phishing can result in ransomware, credential theft, Business Email Compromise (BEC), Account Takeover (ATO), and other security breaches. Emails are typically disguised as messages from trusted individuals like a manager, coworker, or business associate that trick users to click a link or open an attachment to activate the enclosed malware, or trick victims into divulging confidential information or granting unauthorized access to systems. The COVID-19 pandemic and remote work have resulted in an explosion of Phishing attacks that have become increasingly sophisticated and often transparently mirror the targeted website, allowing the attacker to observe everything while the victim is navigating the site with the goal of stealing sensitive data like login credentials or personal identifiable information such as social security numbers or credit card information.

Cloud Threats

With the rapid and widespread adoption of remote work following COVID-19, the necessity for cloud-based services and infrastructure increased drastically. While cloud services offer a wealth of benefits such as scalability, efficiency and lower costs, they're still a prime target for attackers. Misconfigured cloud settings are a leading cause of data breaches.





Lateral Movement

A SIEM can correlate data from multiple IT systems to identify attackers attempting to elevate privileges or access other IT systems on their way to a lucrative target. Sophisticated attackers use a variety of threat vectors and attack methods to enter and control remote systems on a network for lateral movement.

Detecting Lateral Movement

Sophisticated attackers use a variety of threat vectors and attack methods to enter and control remote systems on a network for lateral movement. Once they get in, they pivot through multiple systems gaining access to accounts. Adversaries might install their own remote access tools or use legitimate credentials with native network and operating system tools, which are more difficult to detect. Examples of lateral movement include:

Spearphishing — Attachment employs the use of malware attached to an email that are electronically delivered social engineering targets at a specific individual company or industry.

Fileless Attacks and Living Off the Land — A fileless attack usually starts with an email that links to a malicious website. By employing social engineering tactics on the malicious website, the attacker can use system tools, such as PowerShell, to retrieve and implement payloads in the system memory.

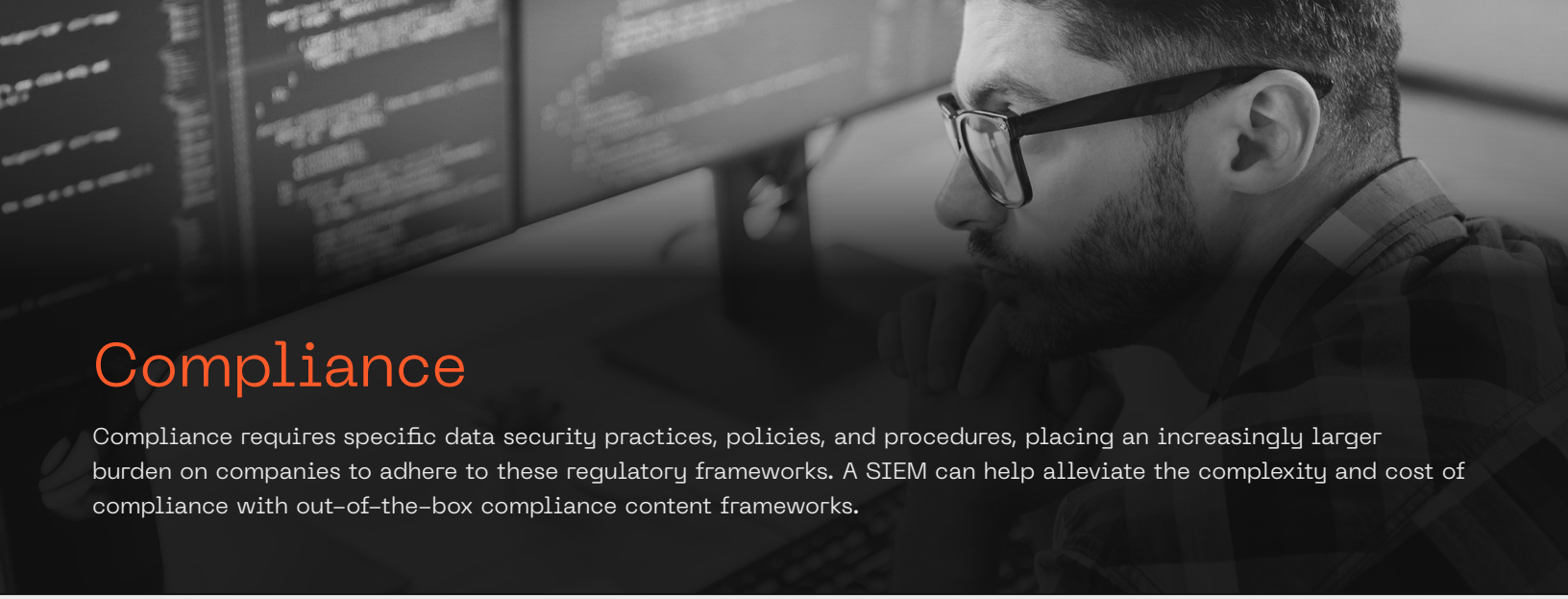
Trusted Host and Entity Compromise — Attackers take control of user credentials or hosts within an organizations network and stealthily carry out attacks for months or years. Unauthorized network connections or anomalous activity across servers, user accounts, network devices and antivirus help identify attackers.

Credential Dumping — Adversaries attempt to dump credentials to obtain account login and credential material, in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform lateral movement and access restricted information.

Brute Force — A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly and 'force' their way into your private account to steal personal data and valuables or spread malware to cause disruptions

Web Applications — Monitoring usage of organizational web applications by outsiders, or inside usage of external web applications, which might involve downloads or browser access to sensitive data.

Backdoors, Rootkits and Botnets for Command-and-Control Communication — Anomalous user behavior such as logins at unusual hours or frequency, or accessing unusual data or systems, or malware communicating with external attackers can be detected by a SIEM when network traffic is correlated with threat intelligence to identifying infected systems transmitting data to unauthorized parties. SOC analysts monitor the alerts and more importantly are trained to identify anomalous patterns during investigations.



Compliance

Compliance requires specific data security practices, policies, and procedures, placing an increasingly larger burden on companies to adhere to these regulatory frameworks. A SIEM can help alleviate the complexity and cost of compliance with out-of-the-box compliance content frameworks.

PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) ensures credit cardholder data is secure from theft and misuse. This retail standard is required for organizations involved in credit card processing, including merchants, processors, and 3rd party service providers. PCI Compliance requires the following protection:

Perimeter Security — Detecting unauthorized network connections, searching for insecure protocols and services, and traffic flow.

User Identity — Monitoring any event that results in changes to user credentials as well as any activity by terminated users.

Real-time Threat Detection — Monitoring all network activity to rapidly detect, analyze, investigate and respond to threats.

Production and Data Systems — Searching production systems for development testing credentials, default credentials, or replicas of credentials.

Auditing and Reporting — Collecting system and security logs, auditing and reporting data for regulatory and compliance requirements.

Personal Identifiable Information (PII) — Protection for sensitive personal data such as an IP address, username, social security number, or medical records.

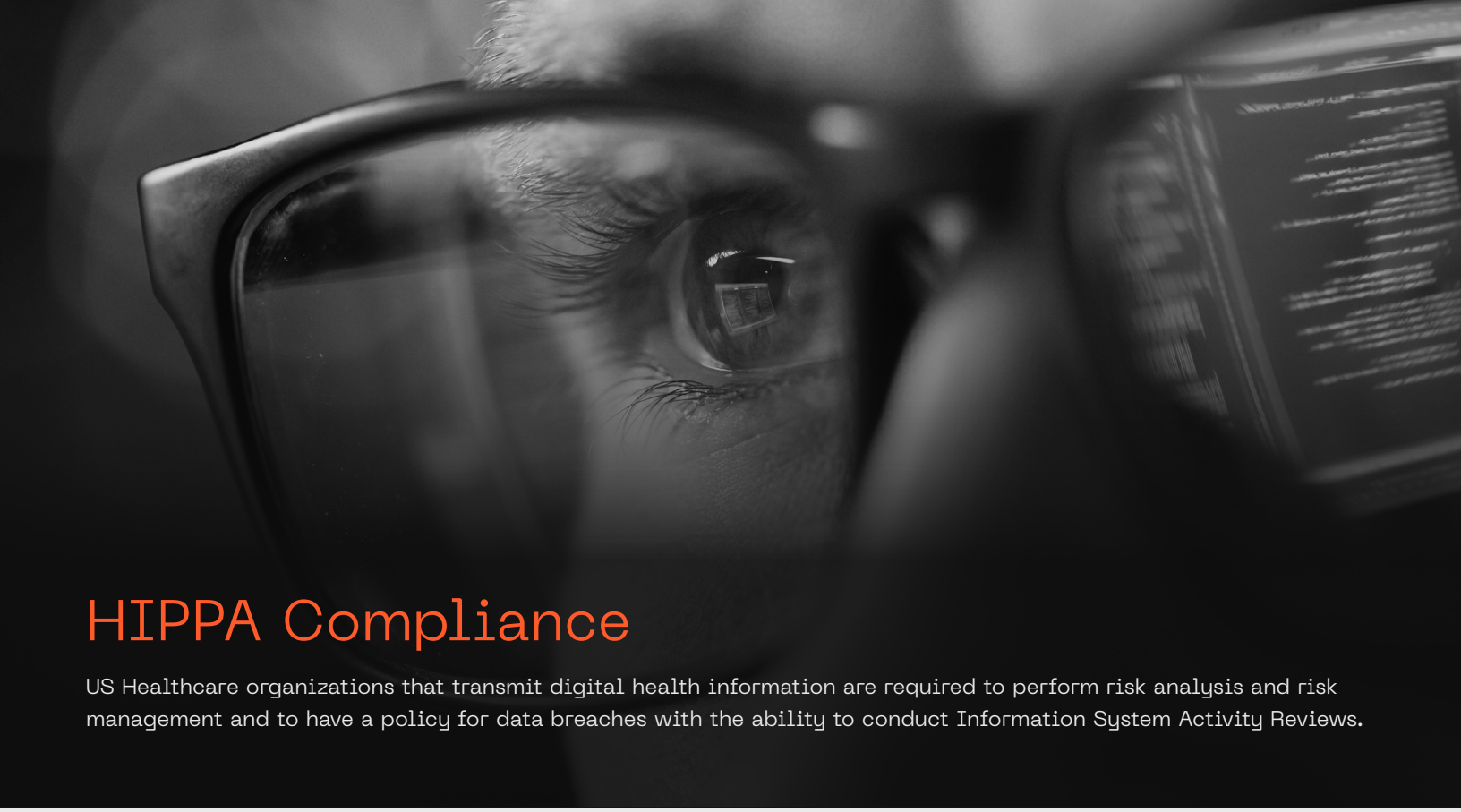
Data Protection — Auditing and verifying that security controls and user data follow appropriate data protection procedures.

Visibility into Log Data — Providing structured access to log information to enable reporting to individual data owners.

Logging and Auditing — Monitoring critical changes to credentials and security groups as well as tracking assets that store sensitive data and auditing databases and servers storing PII.

Breach Notification — Detecting data breaches, alerting security staff, analyzing incidents to uncover the full impact of a breach, and quickly generating detailed reports.

Data Processing Record — Identifying events related to personal data, auditing any changes to the data and generating reports.



HIPPA Compliance

US Healthcare organizations that transmit digital health information are required to perform risk analysis and risk management and to have a policy for data breaches with the ability to conduct Information System Activity Reviews.

Security Management Process — Discovering new IT assets, identifying systems at risk, monitoring access to system files, and monitoring user activity and privileges in critical systems.

Employee Access — Monitoring access to critical files and data, and capturing login attempts from viable and terminated users.

Information Access Management — Identifying logon success and failures, privilege escalation and modification of user accounts.

Security Awareness — Detecting vulnerabilities, malware, and systems without antivirus as well as monitoring logon to critical systems and security devices.

Security Incidents — Automatically detecting threats, generating and prioritizing alerts, enabling threat investigation, and orchestrating automated response to incidents.

Access Control — Monitoring changes to credentials and permissions, session timeouts, and changes to encryption settings.

Audit Controls — Monitoring changes to policies, Data Leakage Protection (DLP) events, file integrity and log analysis for protected data.

Data Integrity — Monitoring modification of health information and changes to data policies.

Transmission Security — Identifying unauthorized communications and attempts to modify applications or storage containing health information.

Attack	Method	Log Sources
Malware	Malware infects a computer and changes how it functions, destroysdata, or spies on the user or network traffic	EDR, IPS/IDS, Proxy
Ransomware	Ransomware is a type of Malware that threatens to publish a victim's data or block access to their data unless a ransom is paid	EDR, IPS/IDS, Proxy
Brute Force	Attackers use automated bots to guess the login credentials of targeted systems to steal data or spread Malware to cause disruptions	AD, RADIUS, VPN, Azure AD, M365, MFA
Phishing	A malicious actor sends emails that seem to be coming from trusted legitimate sources in an attempt to steal sensitive information	M365, Web Filter/ Proxy Email Gateway
Command and Control Communication	SIEMs correlate network traffic with threat intelligence to identify Malware communicating with external attackers such as suspicious file sharing and downloads	DNS, Firewall, Web Filter/Proxy, IPS/IDS, EDR
Compromised User Credentials	SIEMs detect anomalous behavior such as logins at unusual hours or irregular frequency or attempts to access rare data sources and systems	RADIUS, MFA, UNIX or Windows Local Logs, VPN, Linux Auth, AD
Insider Threat Data Exfiltration	SIEMs use behavioral analysis to combine and analyze seeminglyunrelated events, such as insertion of USB thumb drives, use ofpersonal email services, unauthorized cloud storage or excessive printing	EDR, DLP, Proxy, Application Monitoring, NTA
Lateral Movement	SIEMs have a broad view of multiple IT systems and can detect unusual behavior such as attempts to switch accounts, machines and/or IP addresses	PIM/PAM, IAM, Authentication Applications, UNIX or Windows, VPN
Advanced Persistent Threats	Attackers use zero-day or lesser-known vulnerabilities to breach a network then use persistent techniques to maintain access by hijacking legitimate code and replacing it with startup code or modify credentials or permission groups	EDR, UNIX or Windows local logs, AD
Insider Threat Privileged Access Abuse	When users have more access rights than they need to do their jobs it puts IT systems at risk that users may delete information, access sensitive information or steal intellectual property	UNIX or Windows Local Logs, AD
SQL	SQL injection allows an attacker to interfere with the queries that an application makes to its database and allows the attacker to view data that they are not normally able to retrieve, such as passwords, credit card details, or personal information	WAF

BINARY DEFENSE

Preventing network intrusion attempts and cyber attacks

Real-time threat detection and historical analysis of security events and data sources are critical for identifying and responding to intruders earlier in the attack chain. Besides tracking threats, a key benefit of a SIEM is the detailed visibility into every aspect of enterprise security. While SIEM technology can process contextual information about users, assets, threats, and vulnerabilities — it requires skilled analysts to conduct real-time and historical analysis of events and user and entity behaviors for successful security incident investigation and threat response. By understanding the types of attacks and identifying key sources of data for monitoring you can take a proactive approach to protecting your organization from increasingly sophisticated and potentially devastating cyberattacks.

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com