BINARY DEFENSE™

CYBER PROTECTION – UNDERSTANDING CRITICAL ASSETS TO MONITOR

Understanding Your Risk

Ransomware attacks are at an all-time high, and cybercrime is up 600% as a result of the COVID-19 pandemic. 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?

24/7 Security Operations Center

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 best defense against sophisticated attacks requires a team of experts working 24/7 to protect your business.

SIEM Technology

By identifying and responding to a potential threat immediately, cybersecurity experts can stop an attack and keep damages to a minimum. SIEM technology and 24/7 Security Operations Center (SOC) monitoring are critical for detecting and quickly responding to security incidents to ensure minimal impact and continued business operations.

A SIEM is a centralized security platform that requires a combination of technology, processes and people for successful threat detection and response. The SIEM brings together log search, user activity and endpoint data into a single visual timeline — from antivirus events to firewall logs, the SIEM identifies data and sorts it into categories such as malware activity, failed and successful logins and other potentially malicious activity providing complete visibility for SOC analysts to detect and respond to potential threats.

Threat Intelligence

Threat intelligence is the information gathered by expert researchers about current threats. Centralized log management with integrated threat intelligence is vital in the fight against cyberattacks. Threat intelligence identifies pieces of data that have previously been detected during a compromise attempt. These "indicators of compromise" (IOCs) are collected into open source and proprietary databases known as threat intelligence feeds and include 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.

Security Experts

The Binary Defense Security Operations Task Force analysts are highly-trained security experts that detect and analyze advanced attack patterns and alert you of threats as soon as they are identified. Their main objectives are to minimize threat actor dwell time and stop the spread of malware or malicious activity on internal systems to prevent a full-blown attack.

When implementing a SIEM it's critical to identify the log sources that should be monitored to protect the data that your organizations success depends upon. This requires a deep understanding of the 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 critical assets. Ensuring that your SOC team is monitoring all the necessary log sources can minimize risk, add value to your cybersecurity efforts, and prevent future attacks.

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.

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
- Multi Factor Authentication (MFA) – Okta, Duo, or others
- Endpoint Detection and Response (EDR) and Antivirus
- Web Application Firewalls (WAF)
- 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

Attack	Method	Log Sources
Malware	Malware infects a computer and changes how it functions, destroys data, 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 seemingly unrelated events, such as insertion of USB thumb drives, use of personal 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

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. Besides tracking threats, a key benefit of a SIEM is improved security operations because it provides detailed visibility into every aspect of your endpoint, network, and cloud environments. 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 behaviors for successful 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.

FIND THE BEST CYBERSECURITY SOLUTION FOR YOUR BUSINESS

Discover how Binary Defense can shield your business from cyber threats.

600 Alpha Pkwy Stow, OH

Phone: 1-800-BINARY2 (246-2792)

Phone: 330-777-4300

Email: sales@binarydefense.com

Website: www.binarydefense.com

FOLLOW US

binarydefensesystems

Binary_Defense

binarydefense