REVERSINGLABS

Empowering the SOC: Exposing Hidden Software Supply Chain Threats

Why Software Supply Chain Security Matters to SOC Teams

88%

said software supply chain security presented an enterprise-wide risk[1]

59%

of businesses that suffered a supply chain attack did not have a response strategy in place[2]

Only

24%

of organizations say they can resolve security incidents within hours or days[3]

Threat actors are constantly exploring new techniques to exploit enterprise systems, and the rise in successful supply chain attacks is a clear indicator of a largely unaddressed attack surface. SOC teams often lack the critical tools enabling them to properly address threats. Unknown and unmitigated risks, such as software tampering and malware, introduce unprecedented security and privacy risks to enterprises. And these security implications continue to rise as software systems become more interconnected and dependent on each other.

According to Ponemon's and Exabeam's studies, 24% of organizations can resolve security incidents in hours or days with only 22% of SOC operators measuring their mean time to detect (MTTD)[3]. Additionally, third party software components are large and complex, typically containing files that are several gigabytes with hundreds of thousands of executables, causing slower scanning and detection.

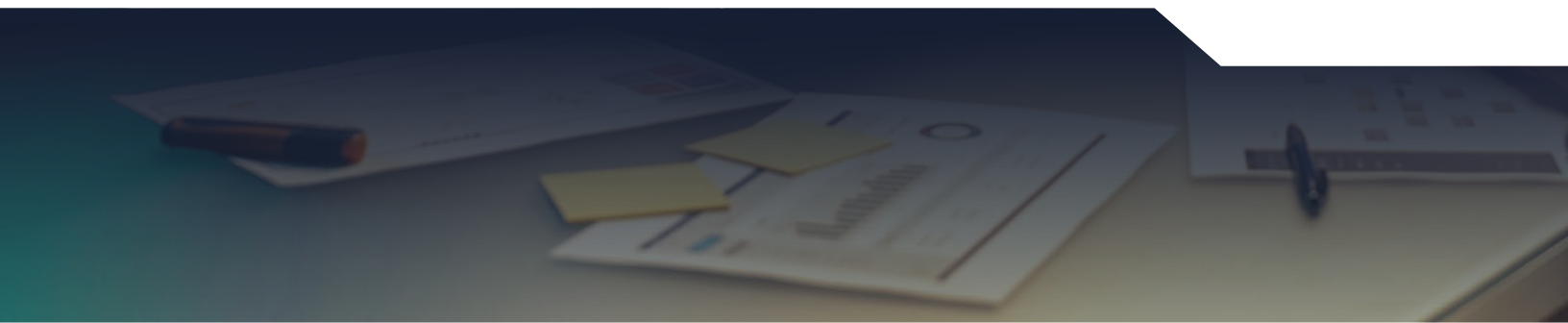
SOC teams often lack in-depth malware coverage and are commonly inefficient when identifying and remediating threats, making them unaware of supply chain threats. And with attacks becoming increasingly sophisticated, primitive or insecure security processes will likely be exploited, putting enterprises and their data, customers, and brand at risk. As a result, it is important to understand how to efficiently locate and respond to issues, improve operational practices, and resolve common security challenges.

Sources:

[1] https://www.reversinglabs.com/resources/infographic-companies-scramble-to-cover-software-supply-chain-security-gaps

[2] https://www.businessnewsdaily.com/supply-chain/smb-cyberattacks

[3] https://securityboulevard.com/2020/07/10-stats-about-soc-performance-practices-and-analyst-attitudes-in-2020/



Common Challenges in SOC Efficiency

While SOC teams commonly lack in-depth coverage and intelligence to identify and appropriately respond to supply chain threats, they also struggle to operate efficiently and remediate issues promptly.

This is because of alert fatigue, manual workflows, and portal fatigue, which causes slow response times, inefficiencies, and skill and coverage gaps.

CHALLENGE	WHY IT'S A CHALLENGE	HOW IT AFFECTS SECURITY TEAMS
Alert fatigue	• Security tools generate 1,000 of daily alerts • 20% of alerts are false positives	• SOC teams cannot respond to each alert and miss critical threats
Manual workflows	• Security architects must integrate multiple tools into a single workflow • Multiple tools' data must be reviewed to investigate and respond to threats	• Inefficient security practices lead to longer response times to vulnerabilities, threats, and alerts
Portal fatigue	• Working with several tools is overwhelming to manage • There's a greater learning curve for inexperienced analysts	• Large skill gaps between experienced and inexperienced analysts leads to inconsistent security practices and more mistakes

These challenges limit enterprises' ability to quickly identify, understand, and react to threats, causing them to remain hidden and potentially damage their systems.

Common challenges - New software supply chain tactics, techniques, and procedures

When threat actors access enterprises' systems through software supply chain attacks, they scrape credentials and escalate privileges to override domain controllers and access resources stored on the network.

This allows attackers to understand the devices on the network and use the scraped credentials to install malicious packages, facilitating highly destructive ransomware and disk-wiping attacks.

To combat software supply chain threats, security leaders need to study new tactics, techniques, and procedures (TTPs) alongside advanced technologies to respond quickly and remediate attacks.

ReversingLabs provides an advanced malware analysis solution protecting enterprises from new attack vectors by:

- Delivering deep visibility to accurately identify malicious code hiding in large and complex software
- Working with other security tools to effectively contain and remediate the attack
- Providing early warnings into emerging threat to proactively prepare response strategies
- Seamlessly integrating with existing SOC workflows

How ReversingLabs Enables SOC Operators to Address the Gap

ReversingLabs reduces false positives, automates workflows, and displays data from multiple tools while providing an expansive good ware and malware library, helping teams quickly respond to alerts, simplify their operations, and protect themselves from software supply chain, ransomware, and other file-based attacks.

RECURSIVE BINARY ANALYSIS

Delivers unmatched visibility into malware and their behaviors. Superior file decomposition:

- Exposes malicious code hiding in deep layers of complex software.
- Indicator and metadata extraction reveals the full life cycle of an attack.
- Enriches the detection and response capabilities of other tools.

CURATED FILE-THREAT INTELLIGENCE

Largest commercial repository of goodware and malware.

- Pre-processed by RL Recursive Binary analysis.
- Reduces false positives by correlating alerts to known goodware
- Delivers detailed intelligence to proactively identify and prevent emerging threats.

SOAR INTEGRATION

Integration Team chartered with integrating with popular SOAR platforms Including: Microsoft Sentinel, Palo Alto Cortex XCSOAR, and Splunk

- Integration via out of the box connectors and APIs.
- Out-of-box playbooks that
  - Enrich malware analysis
  - Auto-resolve false positives
  - Automate and enrich triage, investigation and response
  - Automate proactive threat hunting

ReversingLabs malware and threat hunting solutions provide software supply chain protection that helps users:

- Reduce business risk from Ransomware, and other malicious packages
- Reduce reliance on hard-to-find and retain malware analysis expertise
- Enrich SOC operations to improve detection and response efficacy
- Proactively prevent new and emerging threats
- Increase detection capabilities and value of other security tools

ReversingLabs Features

ReversingLabs malware and threat hunting products integrate advanced malware analysis into automated SOC workflows to provide deep insights and create efficient security measures.

AUTOMATICALLY RESOLVING FALSE POSITIVES

Continuously identify and remove false positives and focus on actual security threats

SEAMLESSLY COLLECT DATA FROM MULTIPLE SOURCES

Use an interface collects and displays information from several tools, reducing investigation and response times

PROACTIVE PROTECTION AGAINST MALWARE

Add malware packages into our file repository and scan your environment to determine whether you are comprised by similar packages

SECURE LARGE AND COMPLEX FILES

Efficiently scan large file types with thousands of executables to quickly locate threats

IN-DEPTH SCANNING AND VISIBILITY

Identify threats that would otherwise remain hidden by scanning files with the world's largest repository of malware and goodware

DELIVERING WHAT MATTERS MOST

Reduced business risk from software supply chain, ransomware, and other malicious packages by promoting efficient SOC operations with faster response times and remediation and in-depth coverage with a large repository of malware and goodware

RICH CONTEXT AND INTELLIGENCE

Receive alerts that are ranked by severity with recommended steps for remediation for fast response times

Get Started!

REQUEST A DEMO

www.reversinglabs.com

About ReversingLabs

ReversingLabs, the leader in software supply chain security, offers the only holistic software supply chain solution that secures 3rd party software and open source components and identifies active threats. ReversingLabs provides protection against malware and tampering in pre and active production. For more information or to schedule a demo, contact us today.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com