Malwarebytes

SOLUTION BRIEF

SIEM integrations to streamline active threat response

Malwarebytes business products provide integration opportunities with multiple industry-leading partners to drive further automation of your active threat response processes. This delivers enterprise cyber resilience that is nimble with faster actions that protect and respond to attacks as they occur.

When it comes to detecting and responding to threats, time is of the essence. If a bad actor executes an attack that slips past network defenses, the more time they spend undetected within corporate systems, the more damage can be done. Active threat response requires teams to use tools that help minimize dwell time, stop the spread of malware on internal systems, and prevent a negative outcome from a breach.

Use case: Automated remediation and enriched security investigations

When an attack occurs, security analysts need enriched intelligence to quickly understand the extent of the threat, as well as automated response actions that accelerate eradication of the event and compress dwell time.

Integrations between Malwarebytes business products and your security information and event management (SIEM) platform will help advance your security response processes, so your team can respond with efficiency and focus to address the extent of the issue.

Example of integration with Malwarebytes that accelerates incident response processes:

- Via the SIEM platform, Malwarebytes scan of a user machine is initiated
- The scan returns positive identification of a high-severity threat on the user machine
- Malwarebytes performs complete remediation to automatically disinfect the machine
- Malwarebytes sends Suspicious Activity alerts back to your SIEM. This will enrich the SIEM's analytics and can be used by your security team to efficiently investigate the event.

Security operations benefits:
Automating response mitigates the potential for damage, reduces malware spread, and minimizes the impact of a possible infection or breach. In addition, when your SIEM intelligence is enriched with a Malwarebytes detected threat, your analysts can increase their efficiency of focusing on high-priority security issues.

Malwarebytes partner integrations that support this use case:
Azure Sentinel, Rapid7, Splunk, IBM QRadar

Use case: Automate support ticket workflows

Security teams are inundated daily with alerts on possible infections. While it would be ideal if teams could respond to tickets as soon as an alert is created, this kind of speed is impossible. It can often take days for teams to give an alert the attention it needs, and that gives malware days to spread.

Integrations between Malwarebytes business products, your SOAR, and your service management solution enables an automated response to support tickets that accelerates your threat response.

Workflow example of an automated support ticket through integration with Malwarebytes:

- A scheduled Malwarebytes scan of the user machine is initiated
- The scan returns positive identification of a high-severity threat on the user machine
- Malwarebytes sends a request to a security orchestration, automation and response (SOAR) platform to kick off the workflow and generate a support ticket. It provides all relevant information on the scan and threat discovery.
- A support ticket is created and routed immediately to the assigned security staff for review
- Security staff receives the support ticket and initiates rapid response to the discovered threat

Security operations benefits:
With automated support for tickets, mean time to respond (MTTR) rates are reduced significantly. Instead of a near-constant need to respond to alerts, automation allows teams to focus on more mission-critical tasks and/or higher-level work.

Malwarebytes partner integrations that support this use case:
ServiceNow, Cortex XSOAR, Splunk Phantom

Use case: Proactive threat hunting

Proactive threat hunting is just as it sounds—finding a problem before it becomes a bigger problem. Your organization's anomalous behavior can be investigated and remediated before damage occurs. As part of this process, having a holistic view of security data is essential. Data in siloes will not provide a complete picture of potential problems on disparate parts of a network.

How integration with Malwarebytes works for actively uncovering hidden malware:

- Data from multiple security-related tools are integrated onto a SIEM platform
- A security analyst identifies an indicator of compromise (IOC) as a malicious file (MD5/SHA256)
- The SIEM correlates file usage with anomalous behavior data provided by Malwarebytes Suspicious Activity running on user machines
- The analyst investigates anomalous behavior on select endpoints by initiating Malwarebytes Scan and Remediation to discover hidden malware. This initiates endpoint remediation.
- Via the SIEM platform, an analyst continues the threat hunt by initiating scans on all endpoints touched by the nefarious IP address, enacting remediation events when hidden malware is discovered

Benefit to your security process:
Through security data correlation and proactive threat hunting within your SIEM, unknown threats are discovered before they infect endpoints, and MTTR is reduced. This integration also helps prevent lateral spread and stop or significantly minimize impact.

Malwarebytes partner integrations that support this use case:
Azure Sentinel, Rapid7, Splunk, IBM QRadar

LEARN MORE

Want to learn more about how Malwarebytes' partner integrations can help you streamline your security program?

Visit malwarebytes.com/integrations

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediation, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. For more information, visit https://www.malwarebytes.com.