DEMISTO | Symantec

Automated Endpoint Protection, Email Security, and Incident Response

Benefits

- Coordinate Symantec endpoint protection, threat protection, and incident monitoring actions through automatable Demisto playbooks.
- Further enrich Symantec data with intelligence from other security tools via Demisto's orchestration.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review

Compatibility

- Products: Demisto Enterprise, Symantec Advanced Threat Protection, Symantec Endpoint Protection, Symantec Messaging Gateway, Symantec Managed Security Services

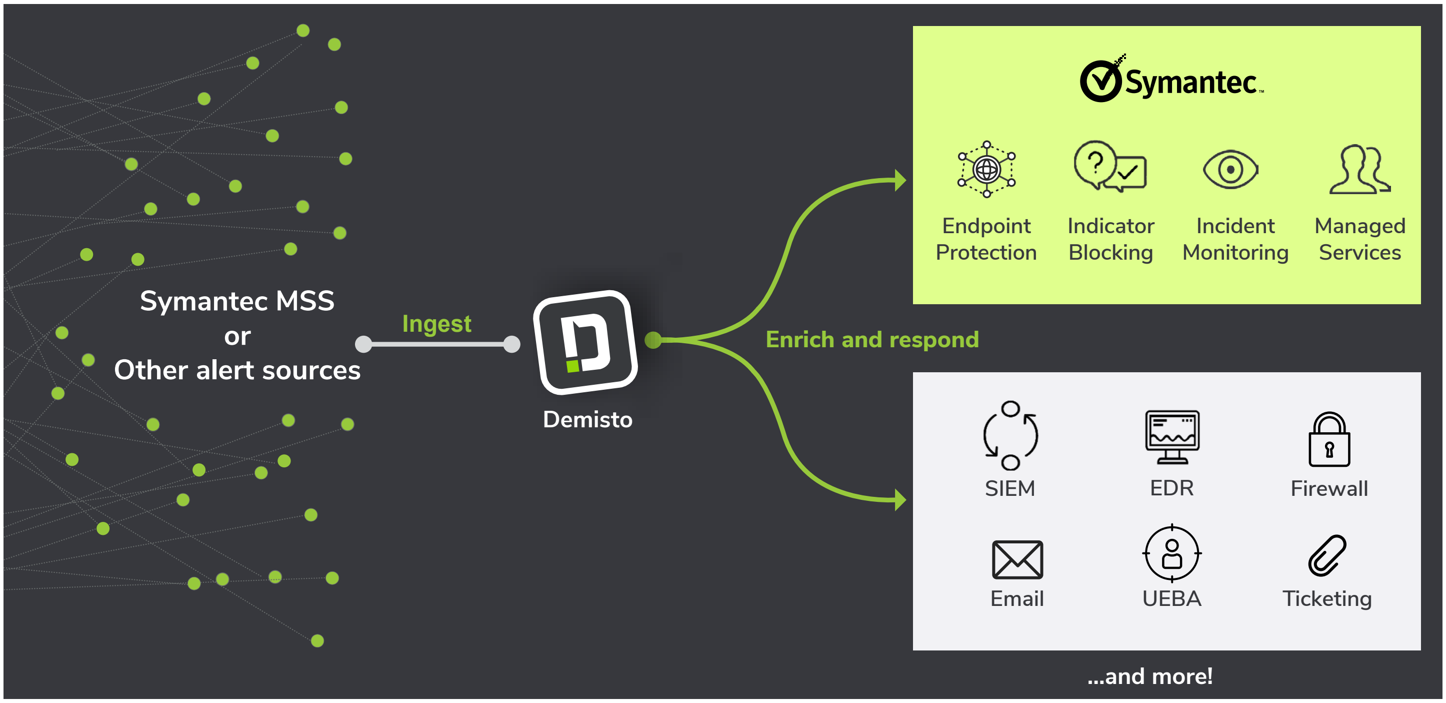
Today's security landscape is ever-changing. New forms of sophisticated cyberthreats continue to emerge and target enterprises by using different entry points and attack vectors. While responding to these attacks, security teams are often caught in a screen-switching cycle, coordinating actions across a large product stack and executing a high volume of manual tasks while alerts continue to rise.

In this environment, security teams need a tool stack that can leverage existing investments without the need for complex and manual coordination. The rich, actionable data that security tools provide must be aggregated, centralized, and executed upon in a standardized and scalable manner.

Users can now leverage Demisto's security orchestration and automation capabilities with a range of Symantec products (SEP, ATP, Messaging Gateway, MSS) to improve visibility and accelerate response across the incident lifecycle.

Integration Features

- Execute endpoint protection actions from the Symantec Advanced Threat Protection and Endpoint Protection tools as automatable playbook tasks within Demisto.
- Ingest alerts from Symantec Managed Security Services into Demisto to kick off playbooks tied to those incidents that coordinate actions across the security product stack
- Manage Symantec Messaging Gateway indicator blocklists (add, access, delete) from within Demisto, either as automated playbook tasks or as real-time actions.
- Leverage hundreds of Demisto product integrations to further enrich Symantec data and vice versa while coordinating response across security functions.
- Run thousands of commands (including for Symantec products) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED MALWARE ENRICHMENT AND RESPONSE

Challenge: When responding to alerts, time is of the essence. This time constraint is often at odds with the vast array of security products analysts must navigate while extracting context and driving incidents to response. Many of these product-specific tasks, while essential to incident response, are repetitive and time-consuming, miring analysts in fatigue and preventing them from actual problem-solving.

Solution: SOCs can integrate usage of Demisto Enterprise with multiple Symantec products – MSS, Messaging Gateway, SEP, and ATP – to orchestrate and automate a variety of critical but repeatable actions during incident response.

For instance, if a suspected malware alert is ingested into Demisto from Symantec MSS, a malware enrichment and protection playbook gets executed. This playbook looks up indicator risk scores from integrated threat intelligence platforms and malware analysis actions from integrated sandboxes. If the malware threat is verified, the playbook uses SEP to get details of affected endpoints and quarantine those endpoints. The playbook then raises the severity of the incident, sends automated emails to affected individuals apprising them of the danger, and sends an email to the overseeing security analyst to come in and continue the investigation.

Benefit: Demisto acts as a bridge between Symantec products and other security products that a SOC may use to both quicken incident resolution and orchestrate any allied tasks that fall outside the direct purview of incident response. This ensures standardized response and updates, reduced effort and time through automation, and archived documentation for future learning.

USE CASE #2 INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: Apart from running automated actions, attack investigations usually require additional real-time tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, grabbing and archiving evidence, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can gain greater visibility and new actionable information about the attack by running Symantec commands in the Demisto War Room. For example, if playbook results throw up a set of indiactors, analysts can run the **smg-block-domain** and **smg-block-ip** commands to block any malicious indicators in real-time without having to switch consoles.

Analysts can also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation that coordinates across the product stack. The War Room will document all analyst actions and suggest the most effective analysts and command-sets with time.

Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their environment from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from a unified console. They will also prevent the need for collating information from multiple sources for documentation.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from the real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. The platform (and you) get smarter with every analyst action. Demisto is backed by Accel with offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.