TECHNOLOGY PARTNER BRIEF

Symantec Technology Partner: Demisto

DEMISTO

Partner Product: Demisto Enterprise

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

Business Challenge

New, sophisticated cyber threats target enterprises across a host of entry points and attack vectors. Security teams responding to these attacks are often caught screen switching, coordinating actions across a large product stack and executing numerous manual tasks while alerts continue to rise.

In this environment, security teams need a tool that takes advantage of existing investments without adding complexity and manual coordination. The rich, actionable data that security teams provide must be aggregated, centralized, and put to use in a standardized and scalable manner.

Want to improve visibility and accelerate your attack response across an incident's lifecycle? Combine Demisto's security orchestration, automation, and response (SOAR) capabilities with a range of Symantec products, including Symantec Endpoint Protection (SEP), Advanced Threat Protection, Messaging Gateway, and Managed Security Services.

Combined Benefits

- Coordinate 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 the decision-making cycle by automating key tasks (subject to analyst review).
- Run thousands of commands (including for Symantec products) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

Integrated Solution

Harness both the Symantec product portfolio and the Demisto platform, creating a central hub that ingests data from across sources, then executes standardized playbooks of automated tasks. See the graphic on next page for a broad overview of how the joint solution works.

Use Case

Demisto ingests a suspected malware alert from Symantec Managed Security Services and executes a malware enrichment and protection playbook. This playbook automates indicator reputation lookups from integrated threat intelligence platforms and malware analysis actions from integrated sandboxes. If the malware threat is verified, the playbook uses SEP, gathering details about the affected endpoints, and then quarantines them.

Symantec™

About Demisto

Demisto is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. Our orchestration engine coordinates and automates tasks across 100s of partner products, resulting in an increased return on existing security investments. Demisto enables security teams to reduce mean time to response (MTTR), create consistent incident management processes, and increase analyst productivity.

For more information, visit www.demisto.com or email info@demisto.com.

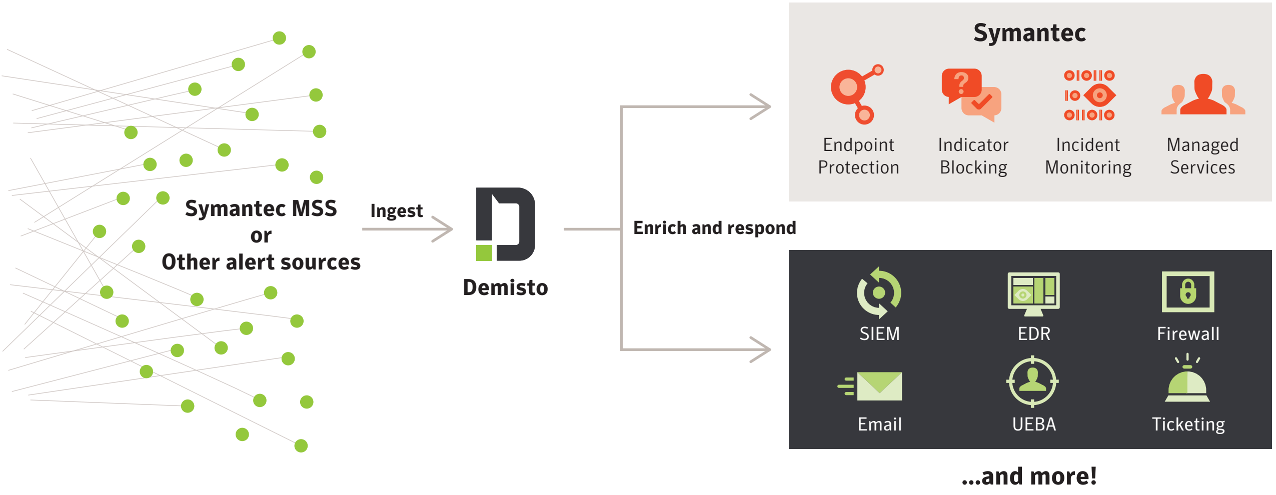
The playbook then raises the incident severity level, sends emails to affected individuals alerting them of the danger, and invites the overseeing security analyst to continue the investigation.

Benefits

Faster Response: Security teams get more investigation time with the rich data that playbooks generate, resulting in fast, critical decisions that close out incidents quickly—a result of playbooks coordinating and automating common actions across products.

Improved Investigation Quality: Security teams minimize weeding through false positives and ensure that no alert slips through the cracks—a result of playbooks raising incident severity levels, and informing analysts only when a threat actor has been verified.

Standardized Processes: Playbooks standardize enrichment and response as much as possible, enhancing security operations and incident response. Without these playbooks, rising alert volumes and staff shortages often result in uneven response processes and quality.



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.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com