TECHNOLOGY PARTNER BRIEF

Symantec Technology Partner: D3 Security

Partner Product: D3 SOAR

Symantec Products: Multiple products

Business challenges

Security tools generate thousands of daily alerts, overwhelming already overburdened and under-resourced security teams. It's a formula for analyst burnout and missed cyber threats.

You need a way to aggregate alerts from numerous sources, identify which alerts point to real threats, and then quickly respond. But most available solutions lack the deep functionality you require—features such as investigative case management, robust reporting, and evidentiary-quality audit logs.

Integrated solution

Think of D3 SOAR—D3 Security's award-winning security orchestration, automated investigation, and incident response platform—as connective tissue for the security operations center (SOC). It ingests events across your security infrastructure, assesses their criticality, and triggers incident-specific response plans.

D3 SOAR centralizes, enriches, and correlates data, making that data more actionable. Working with Symantec tools, D3 SOAR streamlines SecOps and IR workflows, reduces manual coordination, automates SOC tasks, and makes the most of your existing security infrastructure.

D3 SOAR integrates with these Symantec products:

- Symantec Endpoint Protection
- Symantec Endpoint Detection and Response
- Symantec Data Loss Prevention
- Symantec Email Security

Use this joint solution to:

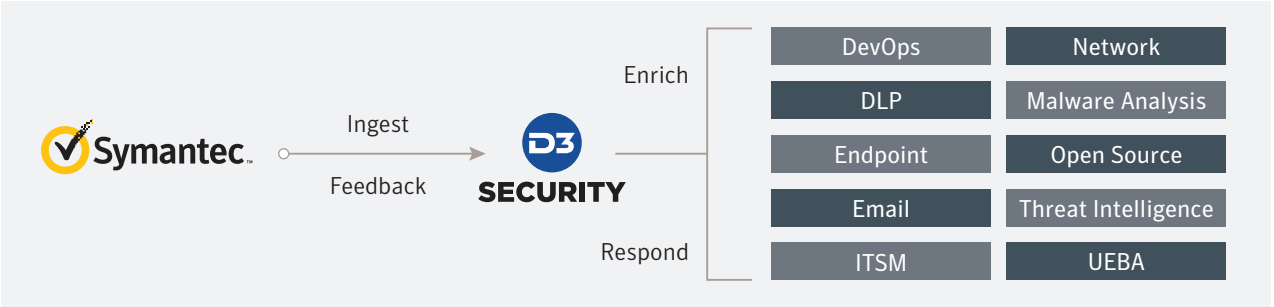
- Trigger endpoint protection actions and IR workflows from within Symantec tools.
- Ingest Symantec alerts that trigger D3 SOAR playbooks, automating and orchestrating tasks across your security infrastructure.
- Add, access, and delete whitelists and blacklists via D3 SOAR.
- Execute commands in real time across Symantec (and other) tools.
- Import Symantec data into custom D3 SOAR dashboards.

Combined benefits

- Stronger endpoint protection, broader compliance, and faster incident response
- Faster, higher quality investigations
- Coordinated security processes including endpoint protection, threat hunting, and incident response
- Enriched Symantec data available via D3 SOAR
- Greater SOC and analyst efficiency due to centralized alerts and reduced context /tool switching during investigations

About D3 Security

D3 Security's orchestration, automation, response, and case management solutions are the foundation of the world's most advanced security operations, including over 20 percent of the Fortune 500. D3 seamlessly facilitates collaboration within the security operations center and across departments through a flexible platform that streamlines incident management, orchestrates human and machine processes, and documents all actions taken to assure that organizations meet industry requirements and compliance reporting standards. Learn more at www.d3security.com



Sample use cases

Enriched malware alerts and incident response

Challenge: Screen switching, data silos, and outdated or too little information—each especially hampers your analysts during a cyber attack, when they must quickly gather contextual data and neutralize the threat. The result: Extended dwell and remediation times plus increased frustration and greater likelihood of error.

Solution: Orchestrate actions across your security infrastructure, minimizing and automating repetitive tasks. Trigger malware-specific playbooks, automatically enriching alerts (from Symantec Endpoint Detection and Response, for example) with threat intelligence and historical data that highlights correlations and quantifies risk. Use playbooks to trigger automated remediation actions—such as quarantining an affected endpoint—or to notify analysts and guide them through the necessary steps.

Investigative case management

Challenge: Investigators get stuck switching between screens as they make correlations, gather evidence, and collaborate with colleagues. Context-switching doesn't just slow down investigations—it makes it difficult to properly document processes.

Solution: Easily orchestrate investigations across Symantec products and other tools without leaving your D3 SOAR screen. The D3 SOAR visual link analysis tool identifies connections to other incidents, indicators, and persons that you should investigate further—or, in the case of malicious indicators, that you should block (with Symantec Endpoint Detection and Response). Use its digital forensics tool to collect and preserve Symantec-gathered evidence.

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, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

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

20A233086_SB_TIPP_D3_SECURITY_EN