TECHNOLOGY PARTNER BRIEF

Symantec Technology Partner: CyberSponse

CYBERSPONSE
ADAPTIVE SECURITY

Partner Product:	CyberSponse
Product:	CyOPs 4.11
Symantec Products:	Multiple Products

Business Challenge

Organizations using multiple security solutions to defend against cyber attack soon learn that, unless these tools are properly orchestrated, they yield disjointed alert information that is difficult and time-consuming to use effectively.

Cyber security analysts in these organizations spend much of their time and energy collecting and manually processing data, managing disparate tools, and performing repetitive tasks. With orchestration, however, these security solutions automate repetitive tasks, empower you to engage in dynamic investigations, and tap into relevant threat intelligence data so you stay on top of your adversaries' ever-evolving tactics, techniques, and procedures (TTPs).

Combined Benefits

CyberSponse CyOps integrates with a range of Symantec products, enabling you to:

- Orchestrate dynamic investigation workflows.
- Automate repetitive tasks, such as alert enrichment and initial triaging, by tapping into Symantec DeepSight Intelligence, Symantec Endpoint Protection (SEP), Symantec CloudSOC, VirusTotal, Anomali ThreatStream, and other solutions.
- Ingest alerts from multiple sources—such as Symantec Advanced Threat Protection (ATP), SEP, Email Security.cloud—into a single CyberSponse console for automatic and orchestrated investigations.
- Move data bidirectionally between solutions.
- Take advantage of highly configurable case management capabilities and the contextual data visualization engine.
- Create dynamic investigation workflows with 250+ integrations (using the CyOPs Visual Playbook Builder).

Integrated Solution

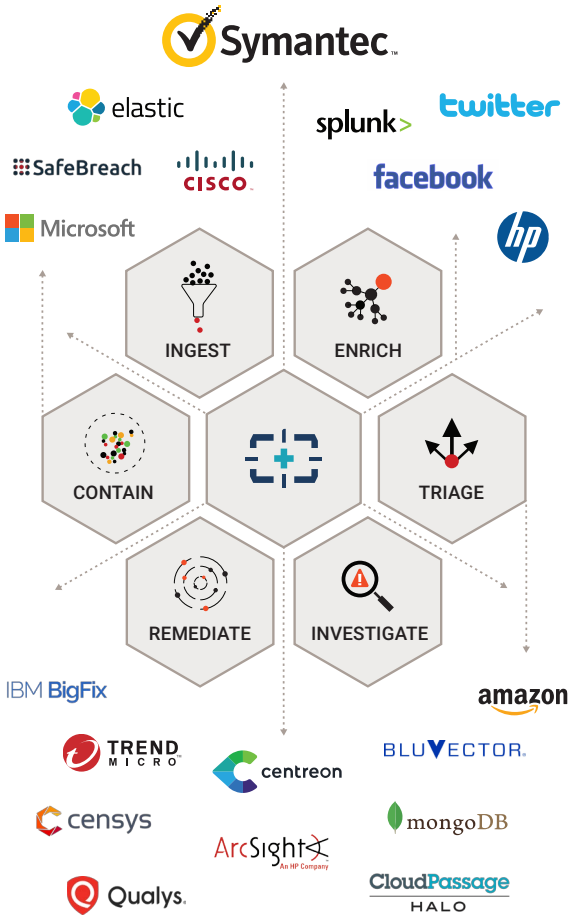
CyberSponse integrates with the following Symantec products:

- ATP
- ProxySG
- Content Analysis
- Control Compliance Suite Vulnerability Manager
- CloudSOC
- DeepSight Intelligence
- Data Loss Prevention
- Endpoint Detection and Response—Cloud
- Email Security.cloud
- SEP
- Web Security Services

CyberSponse provides reference playbooks and use case examples for these integrations to get you started producing investigation workflows.

Symantec™

250+ Product Integrations



Use Cases

CyberSponse/Symantec security integrations create a plethora of automated and dynamic investigation workflows such as:

Automatic Remediation of Symantec ATP incidents

A Symantec ATP incident is pulled for investigation; remediation actions are taken after gaining necessary approvals.

1. Enrich asset information (based on owner email and validation and ID tag).
2. Obtain reputation of involved file-hash from **Symantec DeepSight Intelligence** and **Anomali ThreatStream**.
3. If the file is found to be malicious, use **Symantec ATP** to isolate the machine and backlist the files.

Other use case scenarios include:

- Automatic Enrichment of Indicators (IP, URL, domain, file, etc.)
- Automatic Investigation of Brute Force Attacks, Command and Control Attacks, DNS Tunneling, and other common threat scenarios
- Automatic Remediation of Email Security.cloud Alerts
- Automatic Remediation of Phishing Alerts

Conclusion

The CyberSponse and Symantec integration enables analysts to focus on real threat scenarios by automating the repetitive tasks that cause distraction. Create a comprehensive threat investigation pipeline across multiple scenarios with Cybersponse's other 250+ integrations. With role-based dashboards, reporting, and audit logging, it's easy to view the threat story at each investigation checkpoint.

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

19C209912_SB_TIPP_CYBERSPONSE_EN