VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

Increase SOC efficiency with a balanced SIEM/NDR strategy

Cyberattacks that target intellectual property, disrupt supply chains, and impact operations with ransomware seem to have become a daily fact of life.

While midsized businesses with resource-strapped Security Operations Centers (SOCs) have historically felt the most pressure, even large organizations are feeling it. In this operating environment, it shouldn't be surprising that companies are reevaluating even the most entrenched security solutions for ROI – including aging solutions like SIEM.

Find more needles – manage fewer haystacks

Security operations teams face a growing list of imperatives. First and foremost, they must accelerate threat response as never before to protect the organization. They also face business pressure to increase operational efficiency, reduce overheads and cut ongoing maintenance costs.

SIEM is increasingly being displaced by task-optimized solutions that quickly address today's security operations challenges.

Sound familiar? If so, your organization must rethink outdated methods of managing and querying vast volumes of ever-changing data. The days of piping all your data into the SIEM and hoping for correlated threat detections to pop out the other side never materialized for most. Against the backdrop of modern AI/ML-based threat detection and response, SIEM is increasingly being displaced by task optimized solutions that quickly address today's security operations challenges. After all, why reinvent the wheel in the SIEM when it's faster, better, and cheaper with a modern and effective approach?

97% Vectra AI-driven threat detection and response scenarios cover 97% of the MITRE ATT&CK enterprise frameworks.

HIGHLIGHTS

- Vectra threat detection and response platform improves detection efficacy in ways a SIEM simply cannot.
- Vectra combines log telemetry from the cloud, threat intelligence, and other sources with the high-fidelity metadata available from packets collected from the wire to pinpoint affected assets.
- Vectra helps you extract more value from log data without paying a premium to store it in the SIEM.

"Vectra identifies anomalous behaviors. All detections are prioritized so you can quickly stop threats that pose the highest risk. This is why we chose Vectra."

Hidenori Okumura
Product Manager of Corroboration Platforms
Nissho Electronics Corp

Fill the threat detection gap

The unfortunate reality is that most SIEM deployments are little more than expensive log collection solutions that chip away at compliance mandates – not threat detection. And in the increasingly rare cases when organizations can manage all the soft costs of SIEM, the reality is that SIEM correlation alone isn't up to the task of defending the enterprise.

The Vectra threat detection and response platform improves detection efficacy in ways a SIEM simply cannot, using AI-driven behavioral models and machine learning. Vectra combines log telemetry from the cloud, threat intelligence, and other sources with the high-fidelity metadata available from packets collected from the wire to pinpoint affected assets. Unlike SIEM-based solutions, it moves across environments with the attack, feeding analysts actionable security intelligence based on real-time cloud and network behaviors. These capabilities make Vectra perfectly suited to achieve many of the same use cases (plus a significant number of new ones) previously envisioned for the SIEM, with greater efficacy and at lower costs.

*CWPP has wide coverage, but only where agents can be deployed, which is lacking in cloud

Add value to your SIEM deployment

Whether you currently have SIEM, are still determining SIEM use cases, are in the process of planning a SIEM rollout, or looking to retire your SIEM, Vectra can help you:

- **Improve threat detection and response**. Vectra provides rapid, highly actionable insights into attacker behavior using AI and machine learning in the cloud and through the network. Its AI-assisted intelligence provides broader coverage, more actionable detections, and reduces noise and false positives compared to detections found in SIEMs.
- **Simplify your number of SIEM use cases to reduce development costs and lower management overhead**. Planning and deploying mature SIEM use cases requires months or years, and managing each use case is an ongoing expense. Instead, use Vectra for AI-driven threat detection and response scenarios covering 97% of the MITRE ATT&CK enterprise frameworks, while you focus on refining select SIEM-based use cases unique to your organization.
- **Maximize your budget by sending enriched data to your SIEM**. Vectra helps you extract more value from log data without paying a premium to store it in the SIEM. This approach follows Gartner's guidance of adopting an "output-driven SIEM model where nothing enters the SIEM tool unless there is clear knowledge of how it would be used."[1] It also can lower annual maintenance and log-retention costs by up to 50 percent.
- **Accelerate time to value while integrating SIEM uses cases at your own pace**. As a detection and response optimized solution, Vectra provides immediate value and helps you to refine SIEM/SOAR/EDR operational flows using pre-built integration modules.

Typical SIEM cost savings[2]

	Before Vectra	After Vectra
SIEM use case development costs	• Splunk $6,000/use case • QRadar $12,500/use case	• 50-68% of SIEM use cases covered by Vectra • Reduction of use case development cost
Yearly use case maintenance cost	• $2,500/use case/year	• Reduced costs with fewer use cases
Log volume		• Up to 50% log volume reduction in SIEM • 37.5% on average
SIEM use case reduction		• 50-63% reduction of # of use cases in SIEM
SOC Level-1 work		• 34x workload reduction in SOC Level-1
IDPS consolidation		• Reduced need of classic IDPS • Includes cloud apps & environments
IR response time		• Accelerated IR response • Increased investigation confidence

Optimize limited SOC time and resources

Remote workers, IoT devices, and cloud computing place new demands on security operations teams. Vectra can help you evolve your SOC with better threat detection coverage, better alert efficacy and actionable threat intelligence to reduce analyst workloads.

Accelerate your SOC transformation

SOC 1.0	SOC 2.0
Data source = Logs Coverage depends on log coverage	Data source = Logs + endpoints + network Cover all attack surfaces (on-prem, cloud & SaaS
Detect the “known bad” (threat intel)	Detect unknown & lateral movement attacks
Detection based on rules and thresholds	ML automates attacker behavior detection
Centered on the smart SOC analysts	AI automates Tier-1 analyst workflow
Slow to deploy – custom use cases, log ingestion, alert fatigue, false positives	Works out-of-the box, self-learning
SLA focused on processing events	SLA focused on stopping breaches

BOOST OPERATIONAL PRODUCTIVITY

Give SecOps staff and analysts triaged, AI-driven insights to:

- Improve alert accuracy and reduce false positives
- Optimize analysis-lead investigations using predictive analysis
- Expose hidden attackers in workloads and user/IoT devices
- Automate tedious, labor-intensive threat hunting
- Detect, score and prioritize high-risk threats

Learn more

The Vectra detection and response platform can be up and running in days. It's clientless, device agnostic and doesn't require in-line deployment. Vectra also delivers rapid ROI and can be a self-funding solution that's easily justified through lower SIEM costs and higher SOC efficiency. Ask your service representative for a demo.

[1] A Guidance Framework for How to Architect and Deploy a SIEM Solution, Gartner, April 1, 2021
[2] Based on Vectra AI average customer deployment

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai

Tearing down the firewall log-jam

Nissho Electronics' SOC team was overwhelmed with firewall log data as it struggled to address insider misuse, outsider attacks and regulatory compliance issues. The company moved beyond time-consuming log analysis to rapid detection and response with Vectra. As a result, the company has dramatically reduced the time to detect and respond to alerts, enhanced the threat-hunting accuracy of its SOC team, and improved compliance reporting to its board members.

"With Vectra we can disclose information to members of our board as soon as possible. We have also dramatically reduced the time to detect and respond to alerts and improved the threat-hunting accuracy of our SOC team."

Hidenori Okumura
Product Manager of Corroboration Platforms
Nissho Electronics Corp

Read the case study