EBOOK

The Rising Hard and Soft Costs of SIEM

VECTRA®

Your SIEM-based security posture can't protect your organization from modern hybrid threats–even delivering ROI is a challenge.

SIEM's legacy technology is no match against an expanding threat surface of multi-cloud environments, high volumes of attacks, and sophisticated threat actors.

Relying on SIEM alone for threat detection, investigation and response (TDIR) against hybrid attacks (i.e., network, identity, and cloud) is costly and inefficient, delaying ROI and accelerating talent burnout. Fortunately, your SIEM's capabilities can be greatly enhanced with the right AI-driven solution that goes beyond signal detection to signal clarity, so your team can quickly identify and resolve the most urgent threats.

Now is the time to innovate your SIEM-based security with AI-driven threat detection, real-time signal clarity, and automated response.

SIEM

It’s Time to Take the AI-Driven Path to Raise ROI

Avoid the rising hard and soft costs of SIEM with an AI-driven platform that lowers threat risk as it quickly raises your SIEM ROI.

Vectra AI delivers a native, integrated signal from a single source for real-time threat detection, investigation, and response (TDIR).

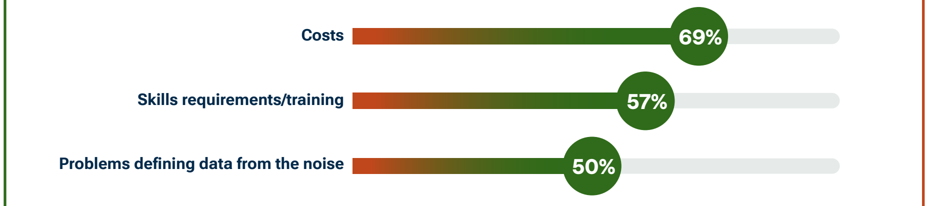
A legacy SIEM-only approach relies on delayed, third-party data, which is costly and can’t help you defend your hybrid, multi-cloud threat surface against hybrid attacks.

> “Vectra AI makes threat hunting more efficient. Automation achieves efficiencies of scale.
>
> **LIAM FU**
> Head of Information Security
> at The Very Group

Take the path from costly SIEM-based security to a cost-efficient SIEM + AI-driven TDIR security posture.

1. The Rising Hard Costs of SIEM

According to Garter, decision makers perceive



as the biggest challenges with SEIM today.

SIEM ROI is elusive.

You've invested millions into your SIEM, and yet rising hard costs make ROI a moving target. The more legacy SIEM is used for threat detection, investigation, and response (TDIR) for hybrid attacks (which all attacks now are), the more hours your team spends identifying the few real threats amongst thousands of benign alerts. It's an expensive waste of time and talent.

SIEM hasn't evolved.

SIEM relies on outdated technology from 2005. With zero innovation, it demands time investment in tedious manual processes, is awkward to work with, and relies on siloed tools that generate more signals and noise than your SOC team can possibly manage.

> “Our security operations had been decentralized, meaning each team had its own set of security tools. Most were relying on firewalls and logs to secure the perimeter of the network. Vectra AI offered excellent visibility about what attackers do inside the network.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

SIEM Setup, Licensing and Maintenance Costs

SIEM setup costs are high.

SIEM setup requires costly consultants plus someone to manage, configure, and respond to alerts. You need at least one full-time analyst to manage your SIEM solution or you'll outsource to a managed SOC service. Both are budget busters.

SIEM licensing plans can be $140,000 per year–and higher.

Whichever vendor and tier you use, you're paying through the nose *with or without data ingest costs*. SIEMs without a licensing fee have less usability and support, so you pay more on the backend.

SIEM software costs are high, too.

A software-only package from IBM or Microsoft costs about $2200/month for 1000 users, with pricing based on events per second. A SIEM also needs a threat intelligence feed, which can cost $14,000 per year.

SIEM management is labor-intensive and expensive.

You're burning time, talent and money not automating your triage processes and procedures.

SIEM-only software runs you

$26,000 or more

every year.

> The integration between Vectra AI and Splunk was so simple and easy that we were able to get up and running in the SOC very quickly.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

> Manual alert triage costs organizations approximately $3.3 billion annually in the US alone.
>
> **VECTRA AI**

The Rising Demand and Costs for Security Talent

SIEMs require a specialized SOC team, but the work is wearing them out.

Adding dedicated data experts and SIEM monitors to your SOC team means additional expenses. However, with the growing demand for security professionals in a shallow talent pool, the cost of hiring skilled analysts is rising while talent availability is falling.

> “There are 700,000 open cybersecurity positions in the U.S.
>
> **CSET**

New Use Case Rules Bust Your Budget

You may pay an additional cost for your SIEM to operationalize the data platform for the SOC.

Most SIEM solutions operate on a licensing model, which can be based on factors like data volume, number of users, or features used. A typical example of how use case development costs drive up SIEM costs:

New use-case rules costs

Splunk	**$6,000** per use case
QRadar	**$12,500** per use case
Yearly use case maintenance	**$2,500** per year

> Now we look at Vectra AI for the most critical alerts. Along with Splunk, Vectra AI has been instrumental in reducing threat investigations from several days to just a few hours.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

Remediation Costs

Staff Costs of Internal Incident Response	
Average time to containment	**2,216 hours**
Number of staff on SIRT team	**3**
Average hourly wage	**$75**
Yearly staff costs of SIRT	**$498,600**

Per IBM's 2023 Cost of a Data Breach Report, your remediation costs are about $500,000.

Expensive incident response and forensic analysis services are often required after a hybrid attack and internal incident response costs vary. IBM's 2023 Cost of a Data Breach Report studied 553 organizations that were breached between March 2022 and March 2023 and was used to set reasonable baselines.

$

The cost per record in 2022 was

$164

the highest level in seven years.

Yearly SIRT costs are about

$500,000

> Vectra AI saved the A&M System $7 million in a year and we cut threat investigation times from several days to a few minutes.
>
> **DAN BASILE**
> Executive Director of the SOC,
> Texas A&M University System

Cloud Egress Costs

Moving data between clouds and regions costs you.

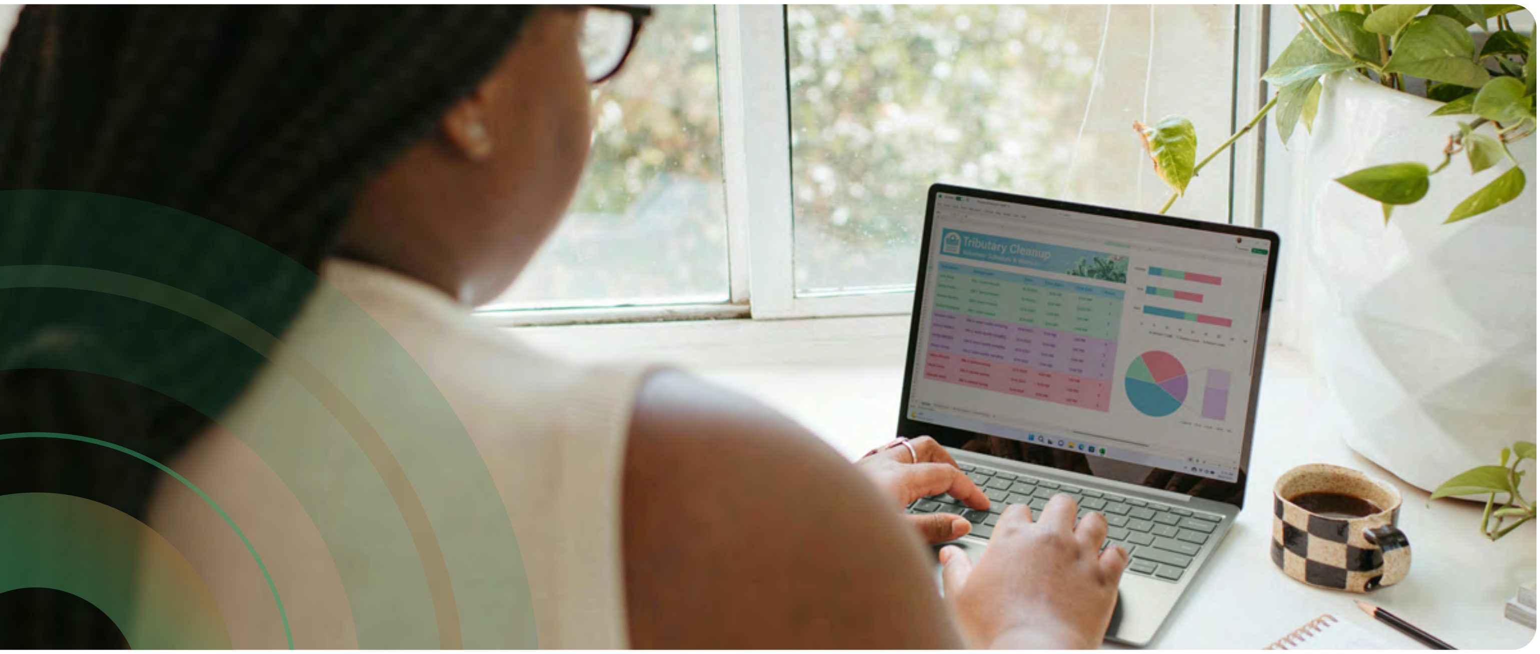
You pay fees to move data between cloud providers or regions. Costs are higher if you depend on a SIEM that's only available in one cloud, such as Chronicle in GCP, Sentinel in Azure, or Securonix in AWS.

Cloud Egress costs can be

$50,000+

If your organization has a significant footprint in a different cloud, shipping activity logs to the SIEM will increase egress charges. For example, the estimated costs of shipping 2 TB/d of CloudTrail from AWS to GCP are $50,000 a year.

> "Our security operations had been decentralized, meaning each team had its own set of security tools. Most were relying on firewalls and logs to secure the perimeter of the network. Vectra AI offered excellent visibility about what attackers do inside the network.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik



Data Processing Costs Are Steep

You're paying for too much data–often the wrong data–that doesn't improve security.

The more complex the network, the more data must be stored, normalized, and analyzed.

A 1000-person firm might ingest around 155 GB/day into their SIEM. As raw log data becomes event data, the volume will expand further. Processing this data through a cloud service like Azure will cost about $14,000/month.

A 1000-person company may spend around

$14,000

per month for data processing

Manually managing log volume is a waste of money, time, and talent, and logging the wrong or missing data can trigger compliance violations.

> “Vectra AI automated many manual tasks in our SOC. This gives us much more time to focus on critical requirements like threat hunting and incident investigations.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

Hardware Management and Configuration Costs

Adding (un)necessary hardware drives up SIEM costs.

Computational resources for logging and data analysis, whether on-premises or in the cloud, should only consume 1% to 5% of the compute capacity on any device. Most SIEMs are poorly configured and will consume much greater capacity.

The more users your SIEM serves, the higher the cost.

Your SIEM application is performance-heavy. Additional users mean more expensive hardware.

The more hardware features, the higher the cost.

Running non-essential features for your security use cases adds to your already high SIEM costs.

> “Vectra AI seamlessly integrates security insights and context about attacks into data lakes – and in the case of Fenaco, its Splunk SIEM – without the overhead and scale limitations that accompany open-source Zeek.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

Automated Analytics Costs for Threat Detection, Investigation, and Response (TDIR) are Sky High

Diverse cloud computing costs are stratospheric.

Your team relies on the cloud for use case rules to automatically detect or identify threats and analyze collected data. Compute forms and costs vary in the cloud. Some services charge by bytes scanned, some use abstract CPU cycles, and others use query time. The cost model you use for computing directly impacts the level and predictability of detection processing costs.

The quantity and frequency of detection rules in production elevate your compute costs.

Developing heuristics that account for ingest volume, data complexity, rule quantity, and analytics complexity is a significant challenge. Machine learning models that continually train on new data also play a role in driving up costs.

> “Misalignment between your environment and your SIEM’s cost model can break your security operation.
>
> **OMER ON SECURITY**
> January 18, 2024

Änderungen des Codes von 'linux' auf GitHub
Sichtbarer Überflug für Satellit 37137 COSMOS 2466 (GLONASS
Sichtbarer Überflug für Satellit 36402 COSMOS 2460 (GLONASS
Sichtbarer Überflug für Satellit 18357 COSMOS 1885 (GLONASS

The High Cost of Archive Processing

The cost of retrieving cold storage data will make you shiver.

The average organization spends $3.4 million on SIEM-related activities annually, underscoring the resource-intensive nature of these systems.

The retrieval and rehydration of old logs from cold storage back into the SIEM system is a big cost driver.

Retrieving data from cold storage costs depend on the volume of data being retrieved and the frequency of such retrievals.

Rehydration of archived logs requires re-indexing or transforming the data into a format suitable for analysis. The higher the volume, the higher the costs.

> “The average organization spends $3.4 million on such SIEM-related activities annually.
>
> THE PONEMON INSTITUTE

2. The Rising Soft Costs of SIEM

> *Manual alert triage costs organizations approximately $3.3 billion annually in the US alone.*
>
> VECTRA AI

Relying on a legacy SIEM-only approach to defend against hybrid threats is like using a Blackberry in an iPhone world.

95% of SOC teams still rely on their legacy SIEM for hybrid threat detection, investigation, and response (TDIR). This old-school, event-centric alert management approach from the early Blackberry era depends on third-party data and requires weeks and even months to identify and remediate breaches, which is why it fails to deliver effective TDIR for hybrid threats.

That's also why your team doesn't know which threats to focus on or to ignore and misses many it can't see. It's like trying to film, send, or watch a video on a Blackberry. The technical capability just isn't there.

For your SOC to keep pace with the speed and scale of hybrid attacks, you need to update your SIEM with advanced "entity-centric alert prioritization," that is, attack signal intelligence.

> Legacy SIEM is in its 'Blackberry Moment.'
>
> **MARK WOJTASIAK**
> VP of Product, Vectra AI

SIEM is a Time Thief

Hybrid attacks are the most time-consuming regarding threat detection, investigation, and response.

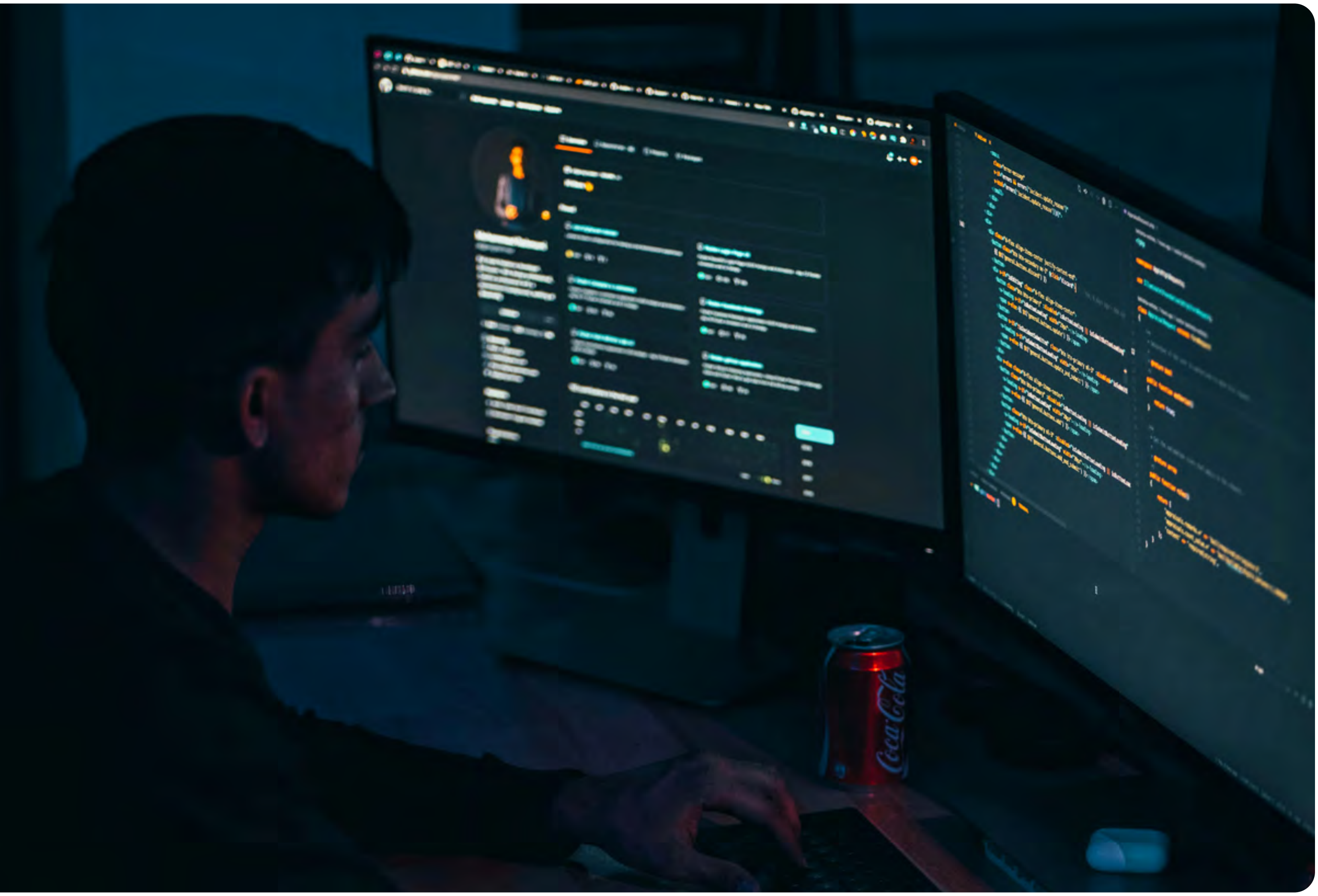
Time is the most critical factor in the detection of hidden hybrid attacks and must be detected in near real-time before key assets are stolen or damaged. SIEM robs your team of any chance of containing a hybrid breach anytime within the following nine months!

The time to containment for SIEM is a staggering

277 days

The average time to identify and contain a breach in 2022 was 277 days. Only one-third were detected by internal teams.

IBM
2023 Cost of a Data Breach report



Adding Operational Complexity

SIEM's like a perfect storm for attackers to thrive.

SIEM adds an impossible level of complexity to your team's workload while depriving them of visibility, clarity, and agility. It's the perfect storm for attackers to thrive because your SOC team is *always behind the threat curve.*

It's becoming clear — SIEM adds operational complexity and attackers thrive in operational complexity.

On average, SOC analysts receive **4,484** alerts per day

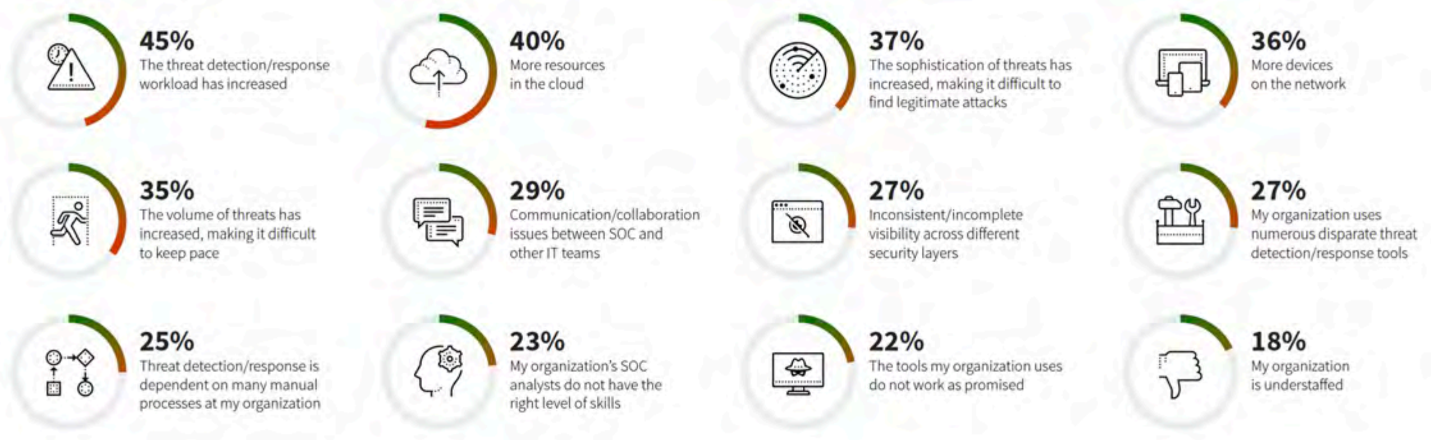
97% of SOC analyst worry they will miss an event because it's buried in a flood of security alerts.

Furthermore, **71%** of SOC analysts believe attackers have already compromised their environment.

Complexity, Threats, and SOC Workload Remain Key Issues.

Threat detection and response (TDR) continues to become more difficult for many security teams for a variety of reasons. Nearly half of organizations (45%) cited the increasing threat detection and response workload, which in many ways is the result of having to defend more distributed and dynamic environments against increasingly persistent adversaries. Environmental complexity plays a key role, with 40% of organizations citing the increase in cloud-based resources and 36% pointing to the increase in devices on the network as top challenges. The threat landscape is also top of mind, with 37% pointing to the sophistication of threats, and 35% citing the volume of threats as challenges.

Threat detection and response challenges.



45% The threat detection/response workload has increased

40% More resources in the cloud

37% The sophistication of threats has increased, making it difficult to find legitimate attacks

36% More devices on the network

35% The volume of threats has increased, making it difficult to keep pace

29% Communication/collaboration issues between SOC and other IT teams

27% Inconsistent/incomplete visibility across different security layers

27% My organization uses numerous disparate threat detection/response tools

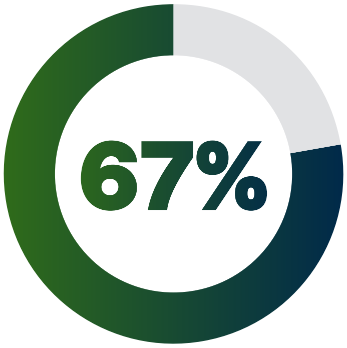
25% Threat detection/response is dependent on many manual processes at my organization

23% My organization's SOC analysts do not have the right level of skills

22% The tools my organization uses do not work as promised

18% My organization is understaffed

"SIEM Angst": A Decline in Your Team's Confidence and Competence

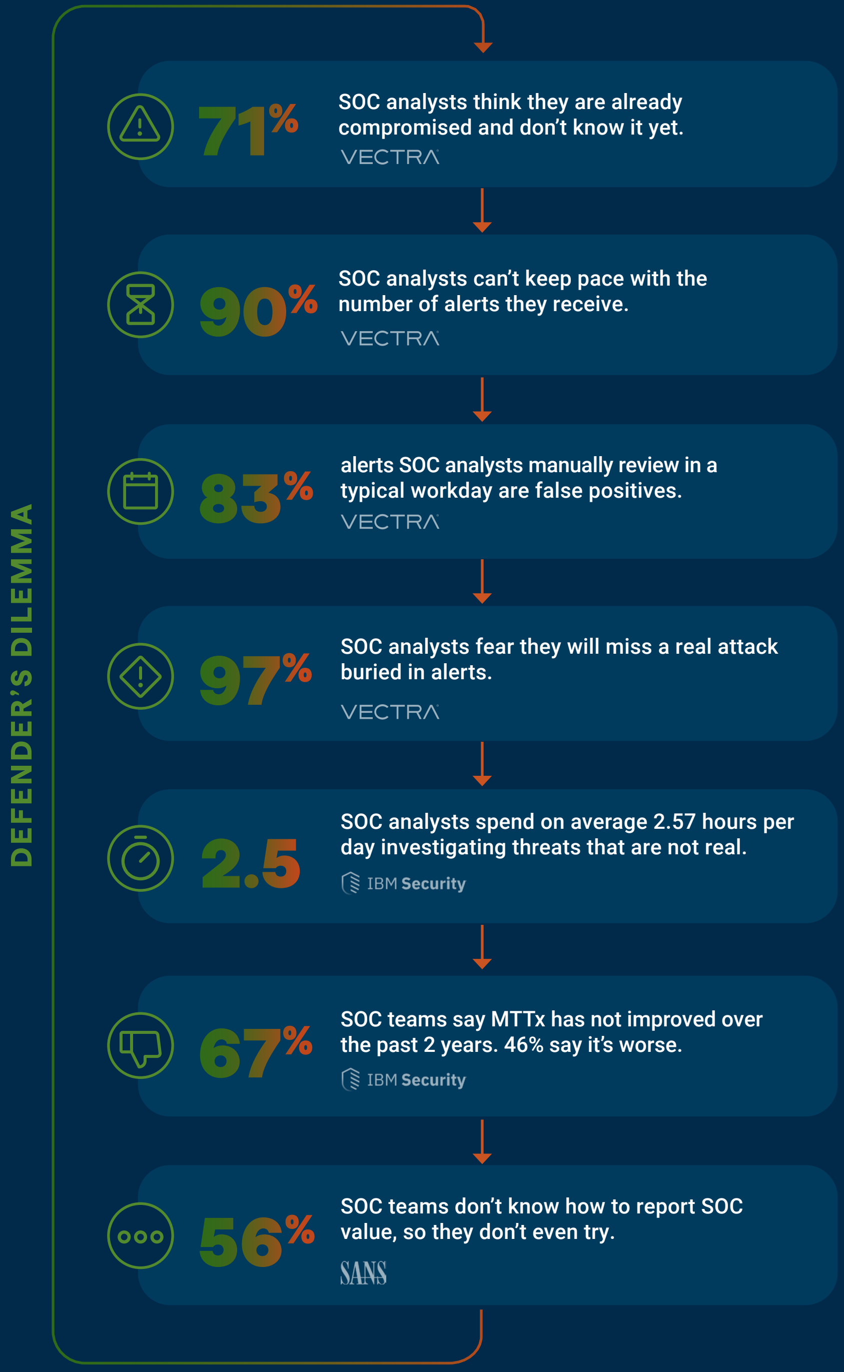


67% are considering leaving or are actively leaving their job.

SIEM hates your team. The feeling is mutual.

There aren't enough hours in the day nor enough team members to make legacy SIEM work the way you need it to.

The "Value" Outputs of Your SIEM



71% SOC analysts think they are already compromised and don't know it yet.
VECTRA

90% SOC analysts can't keep pace with the number of alerts they receive.
VECTRA

83% alerts SOC analysts manually review in a typical workday are false positives.
VECTRA

97% SOC analysts fear they will miss a real attack buried in alerts.
VECTRA

2.5 SOC analysts spend on average 2.57 hours per day investigating threats that are not real.
IBM Security

67% SOC teams say MTTx has not improved over the past 2 years. 46% say it's worse.
IBM Security

56% SOC teams don't know how to report SOC value, so they don't even try.
SANS

Your SIEM should be supporting your team, not the other way around.

3. The Path From Detection to Signal Clarity & Prioritization

Vectra AI Expands SIEM Capabilities and Attack Surface Coverage

Optimize Your SIEM Strategy

- Increase efficacy using analytics-led detection vs. analysis led SIEM approach in our hybrid environment?
- Pinpoint affected assets correlating telemetry from the cloud, threat intelligence, and other sources combined with the high-fidelity metadata collected from the network.
- Extract more value from log data without shifting work to the humans and paying premium to store it in the SIEM.

Only Vectra AI Attack Signal Intelligence can deliver signal clarity for real-time threat detection, investigation, and response (TDIR).

The asymmetry of your limited resources v. an unlimited set of threats means your tools must increase your team's productivity and agility, not drain it.

#1

Most-referenced
in MITRE D3FEND

35

AI threat detection patents

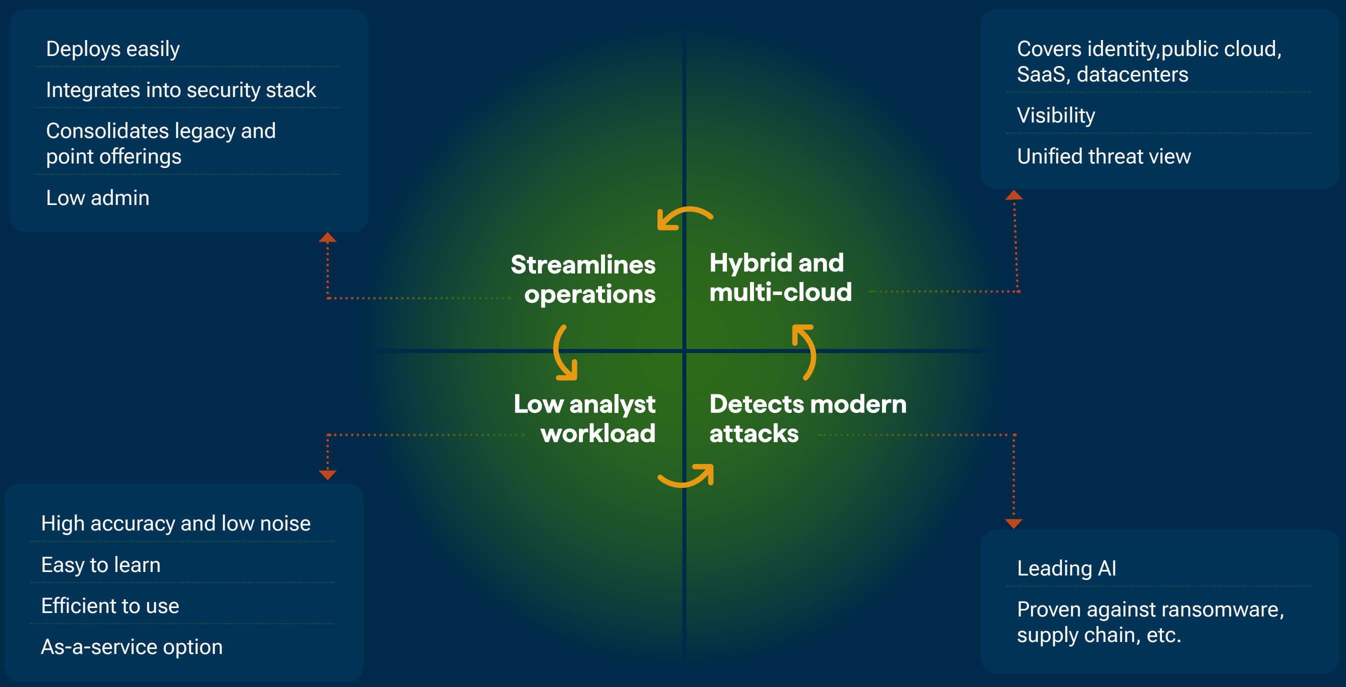
>90%

MITRE ATT&CK coverage

Optimize your team’s workflow with the most comprehensive integrated signal to identify urgent attacks across the hybrid surface.

Key elements of a detection and response solution

Delivering fast time-to-value and ongoing operational efficiency



Streamlines operations

- Deploys easily
- Integrates into security stack
- Consolidates legacy and point offerings
- Low admin

Hybrid and multi-cloud

- Covers identity,public cloud, SaaS, datacenters
- Visibility
- Unified threat view

Low analyst workload

- High accuracy and low noise
- Easy to learn
- Efficient to use
- As-a-service option

Detects modern attacks

- Leading AI
- Proven against ransomware, supply chain, etc.

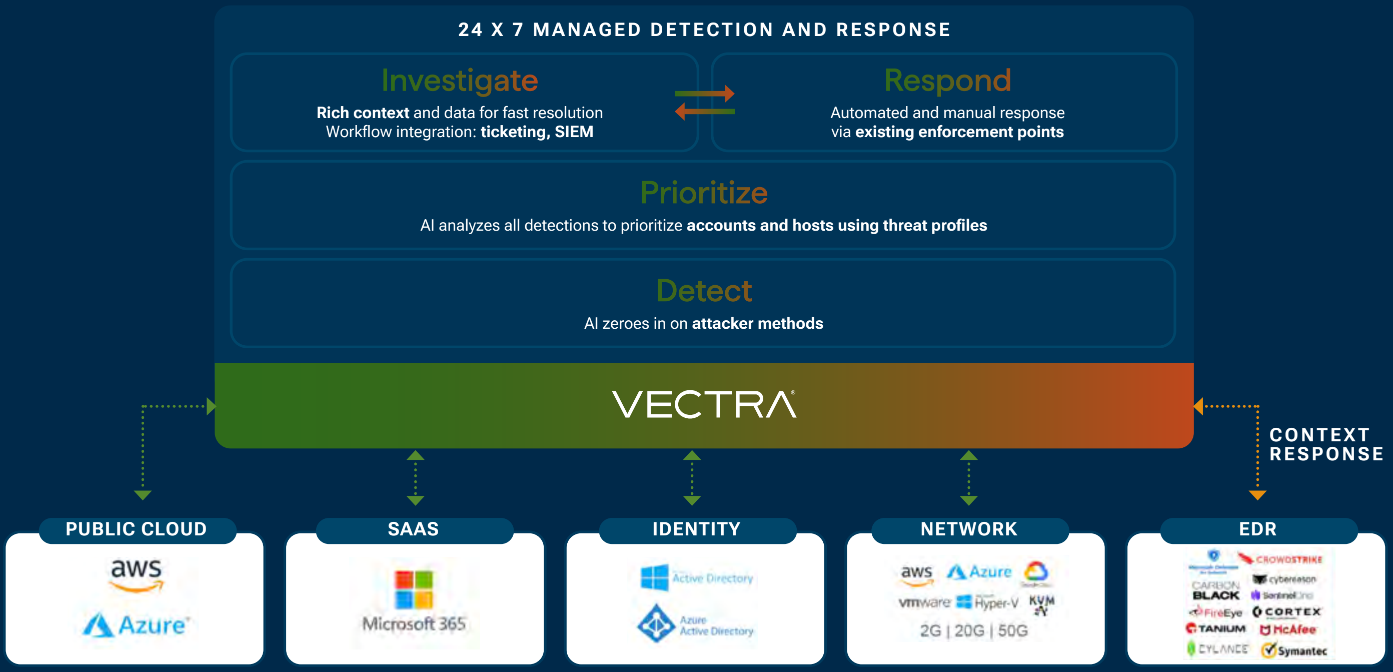
The Vectra AI XDR Platform does the heavy lifting around data quality and the number of data logs ingested off the SIEM.

> “The Vectra AI solution was up and running quickly in the POC test and showed speedy time-to-value.
>
> **DANIEL LUTTERMANN**
> Security Team Lead Rossmann IT

See & Eliminate Unknown Cloud Attacks

Vectra AI: threat detection and response for hybrid & multi-cloud

Sees in places EDR can't go. Looks in ways legacy IDS and SIEM don't.



24 X 7 MANAGED DETECTION AND RESPONSE

Investigate
Rich context and data for fast resolution
Workflow integration: **ticketing, SIEM**

Respond
Automated and manual response
via **existing enforcement points**

Prioritize
AI analyzes all detections to prioritize **accounts and hosts using threat profiles**

Detect
AI zeroes in on **attacker methods**

VECTRA

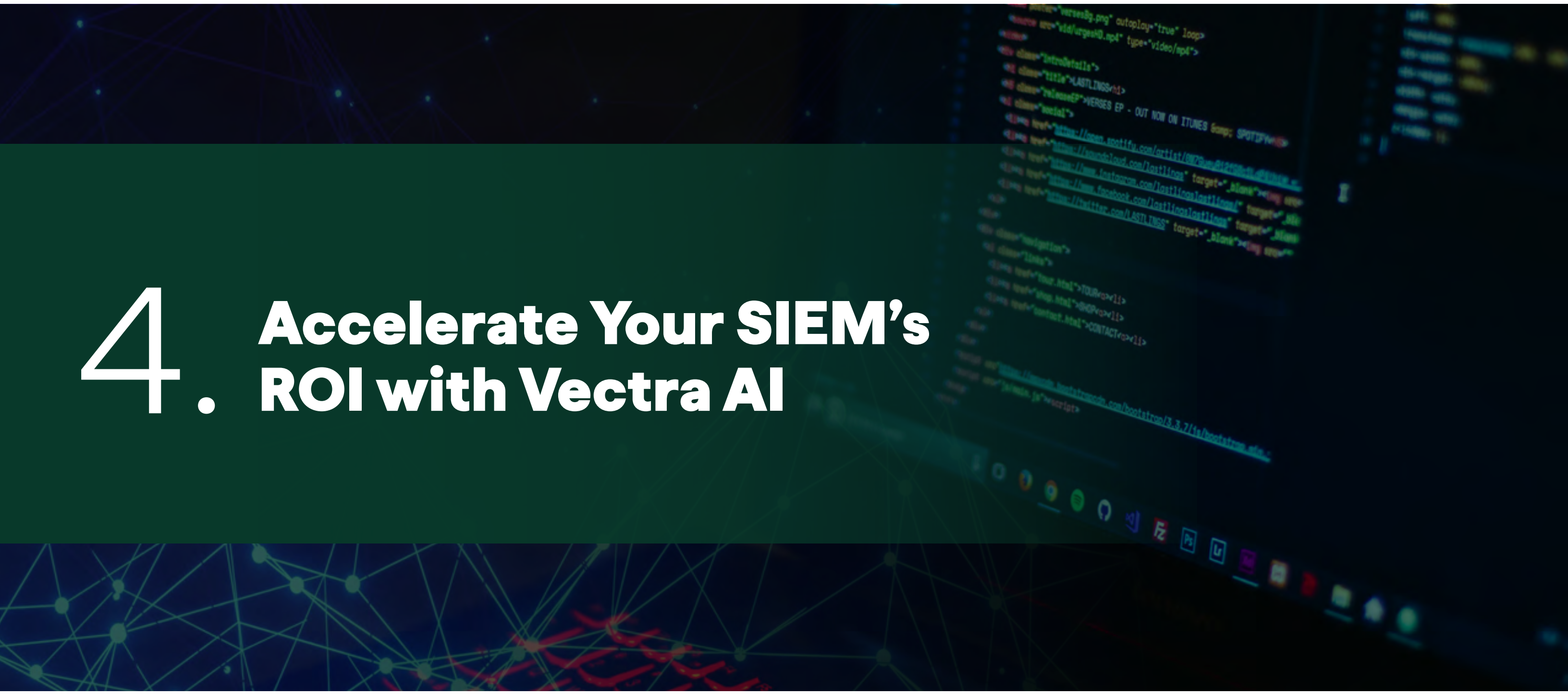
CONTEXT RESPONSE

PUBLIC CLOUD · SAAS · IDENTITY · NETWORK · EDR

Only Vectra AI provides Cloud Detection and Response (CDR) powerful enough to reveal the earliest signs of hybrid cloud attacks.

With 11 references in the MITRE D3FEND framework–more than any other vendor–you get more than 90% MITRE ATT&CK coverage. No wonder 44% of organizations are looking to augment their SIEM solutions.

> “Now, we focus on investigations and proactive threat hunting instead of chasing down logs.
>
> **JOHN SHAFFER**
> CIO, Greenhill



4. Accelerate Your SIEM's ROI with Vectra AI

When added to your SIEM, Vectra AI-driven XDR will:

- Accelerate the ROI time-to-value of your SIEM investment
- Accelerate and simplify the number of use cases in a SIEM
- Reduce development and maintenance costs
- Retain talent and add value to your SOC

> “The Vectra AI platform doesn't require much labor to be an effective weapon against cyberattacks.
>
> **DANIEL LUTTERMAN**
> Security Team Lead
> Rossmann IT

Accelerate SIEM ROI with Vectra AI

Staff Costs of Daily Analysis with Vectra AI	
Percentage of events per year	34
Average time to containment in hours	3
Number of staff on SIRT team	3
Average hourly wage	$75
Yearly staff costs of SIRT	$22,950
Yearly savings	$87,975

The average savings for organizations using security AI and automation extensively is

$1.76 million

> “Vectra AI sends a strong, high-fidelity threat signal, there's no noise, and no alert fatigue. If a critical detection appears in the dashboard... we know it's worthy of our attention.
>
> **DANIEL LUTTERMAN**
> Security Team Lead
> Rossmann IT

Accelerate Detection and Lower the Number of Use Cases in SIEM

The Vectra AI Platform uniquely automates security event detection, triage, and prioritization.

This would normally require multiple hours of manual effort daily from highly trained security analysts and data scientists. Additionally, Vectra AI provides over a decade of research included in the product, and over 100 models that would cost between $1- 3M to build.

Improved Analyst Efficiency and Time to Detection Are Common Benefits

Security teams reported a variety of benefits. In fact, respondents claimed at least three benefits on average. Improved SOC analyst efficiency was reported by 60% of organizations. Similarly, 59% cited reduced mean time to detection, and nearly half (49%) indicated they had fewer data breaches. In addition to positive security outcomes, 49% claimed reduced operational costs, and 47% noted reduced operational complexity. While cited least often, nearly a quarter (24%) said cloud migrations have accelerated. So, while threat detection and response strategies can vary widely, organizations achieved both better security and business outcomes.

60% **Improved SOC analyst efficiency**

59% **Reduced mean time to detection**

49% **Reduced operational costs**

49% **Fewer data breaches**

47% **Reduced operational complexity**

44% **Reduced mean time to response**

24% **Accelerated cloud migrations**

> “Vectra AI's ease of use and automation – combined with low noise and a strong threat signal – save(s) us time and give us a greater understanding about the context of every threat.
>
> **DANIEL LUTTERMAN**
> Security Team Lead
> Rossmann IT

Most network intrusions remain undetected for an average of

16 days

2023 MANDIANT M-TRENDS REPORT

Once a threat is detected, the time to contain the attack can take months.

The Vectra AI Platform dramatically reduces both of these figures

IBM

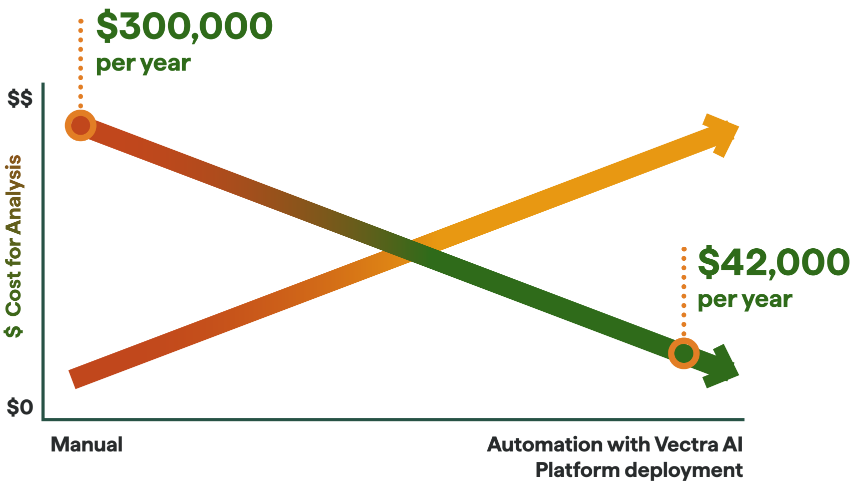
Reduce Your Development and Maintenance Costs by 50%

The Vectra AI Platform for XDR reduces use case maintenance costs and log volume by up to 50% in SIEM.

Optimize workflow with the integrated signal that delivers data quality and handles ingested data logs instead of waiting for your legacy SIEM.

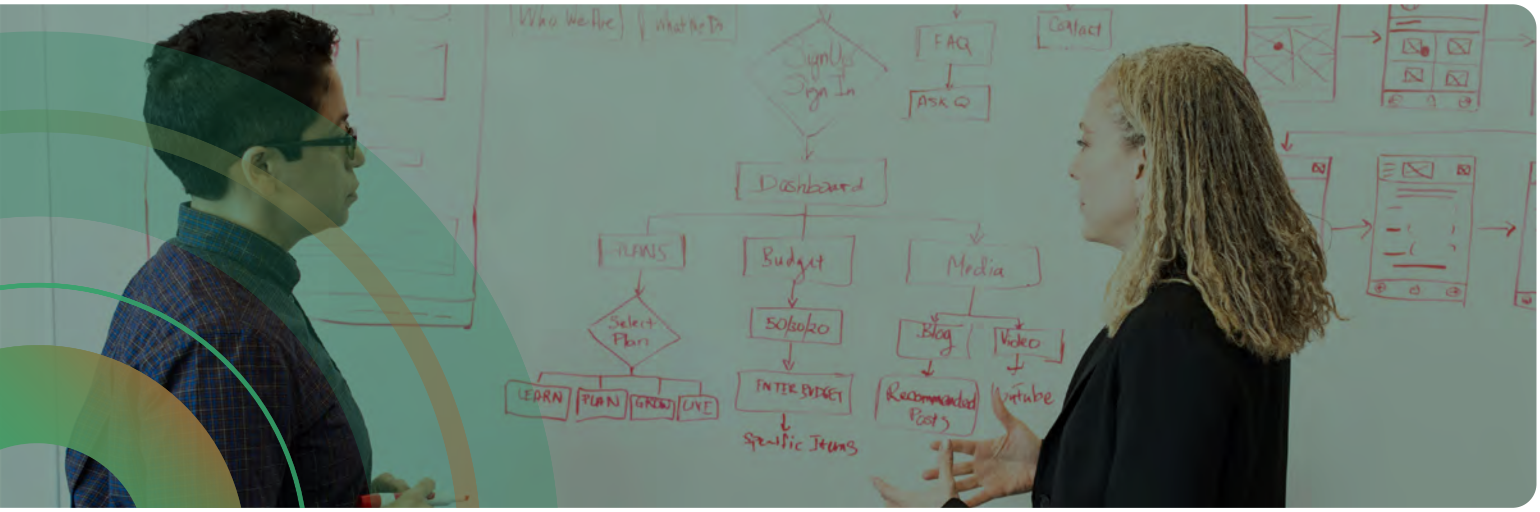
> Every organization at some point is subject to a breach, incident, or cyber event. The ability to quickly and accurately detect and respond to threats is paramount, and Vectra is helping us reduce business risk.
>
> **LIAM FU**
> Head of Information Security at The Very Group

Transform your SIEM's efficiency–and your SOC's value.



> Vectra AI has been instrumental in reducing threat investigations from several days to just a few hours.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

Unlike manual approaches that focus on small amounts of suspicious traffic, the Vectra AI Platform analyzes all traffic – across the entire hybrid attack surface– network, public cloud, identity, SaaS, and endpoints.



Our industry-leading AI-driven XDR transforms your SIEM's performance.

But don't take our word for it, see why a top global healthcare company chose Vectra AI when their SIEM alone wasn't cutting it:

While monitoring over 1 million identities, users and services — SIEM failed to detect malicious hybrid cloud attack behavior in public cloud environment (AWS).

SIEM missed events attempting to disable security tools within the environment to disrupt overall operations.

SIEM's lack of integrated signal caused significant gaps in post-exploitation coverage.

SIEM Savings with the Vectra AI Platform

50–60%
SIEM use cases covered by Vectra AI

Up to
50%
log volume reduction in SIEM

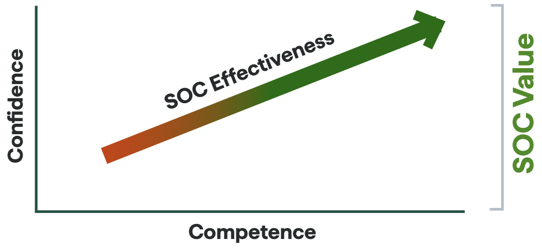
34x
workload reduction in SOC Level-1

The Vectra AI Platform for XDR reduces noise, enhances compliance, is a force multiplier, accelerates operational flow for SOC security analysts, and avoids third-party incident response and investigation costs while lowering dependence on manual log analysis.

Retain Talent, Enhance Team Performance

SOC Value is Rooted in SOC Effectiveness

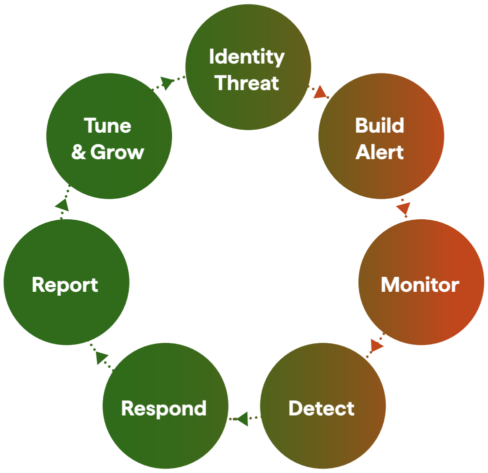
Increase talent confidence & competence, increase SOC effectiveness, prove **SOC Value**.



AI-driven integrated XDR improves team performance.

It will also *help you retain your talent* and address your most pressing skills shortages in IT security – cybersecurity analysis, incident response, and data science.

3 Keys to Maximize Talent Effectiveness & Value



Reduce exposure post compromise
From unknown to known

Remove SOC latency and workload
From manual to automated

Know what is real, critical, urgent
From detection to signal

> Without the detection activities that come from Vectra AI, we wouldn't have been able to identify the true cause of an event's severity by relying on other tools. Vectra AI can aggregate the risk of multiple detections, and we are able to identify and find them within a couple of hours.
>
> **VECTRA AI MANUFACTURING CUSTOMER**

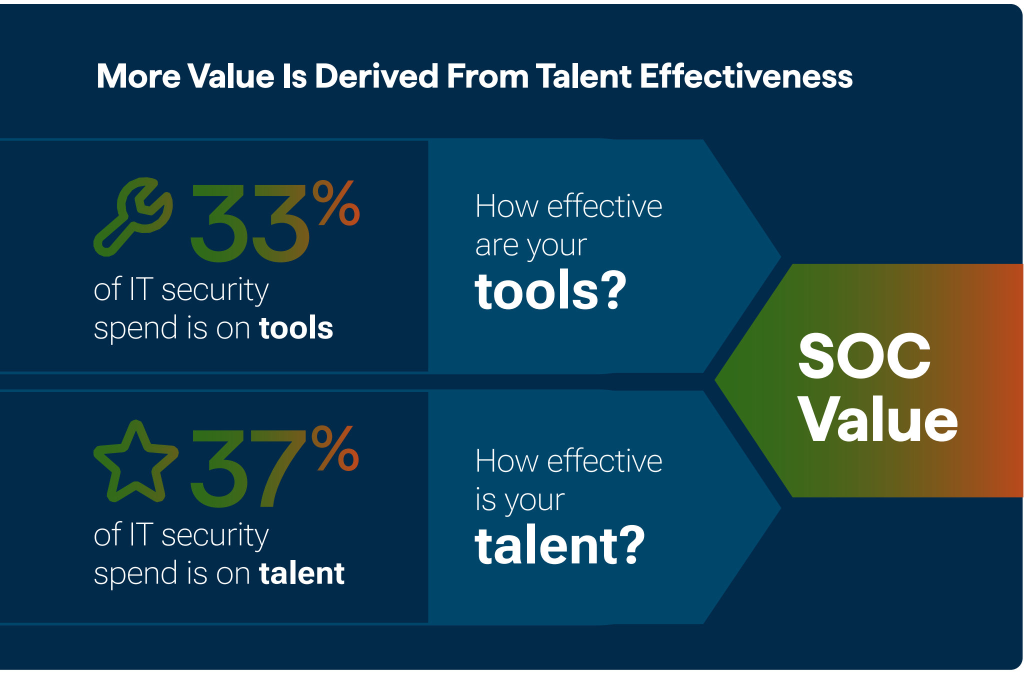
5. The Vectra AI-Driven SIEM Value Proposition

Vectra AI solves SIEM challenges:

- Attack Signal Intelligence™ powers the Vectra AI Platform with precisely the right data SOC analysts need to move at the speed and scale of hybrid attackers.
- The Vectra AI Platform removes the operational headaches from SIEM by optimizing the workflow around threat prioritization, triage and response activities with our AI-driven detections.
- Coverage of 90% of MITRE ATT&CK techniques, surfacing threats immediately without tuning or customer configurations, while reducing alert noise by 85% or more.

> “The Vectra AI solution was up and running quickly in the POC test and showed speedy time-to-value.
>
> **DANIEL LUTTERMANN**
> Security Team Lead Rossmann IT

Cybersecurity is a People-Driven Effort



More Value Is Derived From Talent Effectiveness

33% of IT security spend is on **tools**

How effective are your **tools?**

37% of IT security spend is on **talent**

How effective is your **talent?**

SOC Value

> Vectra AI automated many manual tasks in our SOC. This gives us much more time to focus on critical requirements like threat hunting and incident investigations.
>
> **GUSTAVO RICCO**
> Security Operations Manager,
> Fenaco Informatik

Behind even the most sophisticated hybrid and multi-cloud attacks are people.

Your team is more valuable than your SIEM. Give them the solution so they can do what they do best – find, focus on, and defend against the real threats across your hybrid threat surface.

Use Case–Accelerate Time-to-Value and Efficacy of Your SIEM

Case Study: Large Retail Customer

Scope.

The original scope Managed SIEM including licensing for 3TB of Splunk cloud

Game Changer.

Instead of offering 3TB log ingest for Splunk at $10,9M, customer acquired Vectra NDR + 200GB log ingest for Splunk for $4.7M

SIEM (Splunk) license reduction by

↓93%

(3TB→200GB)

↓50%

tooling cost reduction AFTER factoring in the Vectra investment

Case Study: Mapping Vectra AI Detections to SIEM Use Cases

Vectra AI simplifies from technology approach to attacker behavior detection.

- Originally 89 use cases
- Reduce use cases to 52 by mapping 37 of them to 22 Vectra AI detections
- 37 less use cases to maintain = $92,500 yearly maintenance saving
- Example AD log on/log off 22gb/day in Splunk vs 17mb based on Vectra AI Detections = same outcome/result!

DETECTION NAMES	USE CASE
Brute Force	Brute force attach against Azure Portal
	Successful logon customer from IP and failure from a different IP
	AD - Multiple authentication failures followed by a success
Brute Force Attempt	Distributed Password cracking attempts in Azure AD
	AD - Failed logins to one account from multiple sources
	AD - Failed logins to one account from single source
	AD - Password spray attack against Azure AD
Change to Trusted IP Configuration	Attempt to bypass conditional access rule in Azure AD
Cryptocurrency Mining	Crypto Mining by resource hijacking
	DNS events related to mining pools
Disabled Account Attempt	Attempt to sign in to disabled accounts
HTTP/HTTPS Hidden Tunnel	Palo Alto - potential beaconing detected
MFA Disabled	MFA disabled for a user
Newly Created Admin Account / Admin Account Creation	AD - New user created and added to the built-in administrators group
Newly Created Admin Account / Admin Account Creation / Redundant Access Creation	AD - High Privilege Role was assigned
0365 Disabling of Security Tools / 0365 Log Disabling Attempt	Security Event log cleared
Outbound DoS	Network DDOS Detected
Port Scan	Firewall - Potential Local Port Scan Detected
	Palo Alto - possible internal to external port scanning
Redundant Access Creation	Azure - User was granted subscription admin access rights
Smash and Grab	Data Transfer to untrusted VPCs
	Time series anomaly for data size transferred to public internet
Suspect Domain	DNS - Rare high NXDomain count
Suspicious Application Permissions	Rare application consent
	Azure - Granting consent to Third-Party Application with suspicious permissions
	Azure - Suspicious application consent for offline access
Suspicious Azure AD Operation	AD - User added to a privileged group
	AD - Account added and removed from privileged groups
	AD - User account added to built in domain local or global group
Suspicious Azure AD Operation / Admin Account Creation / Newly Created Admin Account	Suspicious granting of permissions to an account
Suspicious Remote Execution	Suspicious Powershell Invocation
Suspicious Sharing Activity	Suspicious Bulk Download Activity
Suspicious Sign-on	Anomalous sign-in location by user account and authenticating application
Suspicious HTTP	Malformed user agent
Tor Activity	DNS - tor proxies

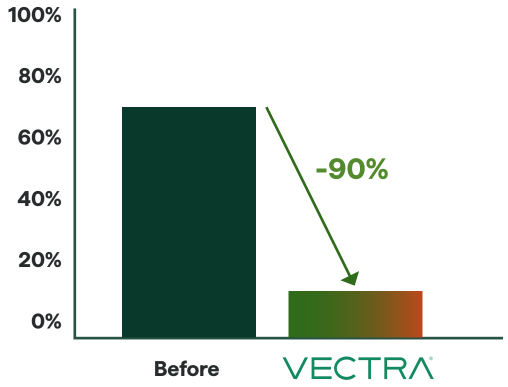
Use Case–Accelerate Time to Value and Efficacy of Your SIEM–Cont.

Vectra AI Changes the Game for Security Teams

Find more threats with less work...while reducing overall tool spend.

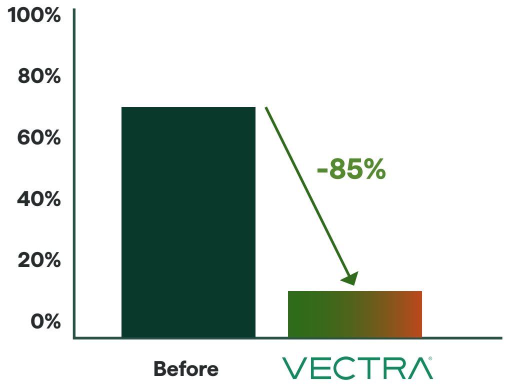
90% fewer undetected threats

% of threats bypassing prevention that were not detected before impact



85% less alert noise

Alerts investigated per impactful threat



30%+ savings through tool consolidation

SEIM: use case development, maintenance, licenses, infrastructure, log transfer and storage

EDR: Can be bypassed

IDS, Netflow tools: replacement

VECTRA®

About Vectra AI

Vectra AI is the leader in hybrid attack detection, investigation and response. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai