The CRITICALSTART® Buyer's Guide for MDR Services for SIEM

Overcome Complexity and Achieve the Full Potential of Your SIEM Investment

CRITICALSTART®

Executive **Summary**

Market turmoil and an ever-evolving threat landscape are why companies turn to a solution that provides increased security without compromising value. In a world where any alert can be a threat, businesses need end-to-end visibility across their security ecosystem, confidence that their SIEM is ingesting the most relevant data and the reassurance that every alert (regardless of criticality) is resolved.

A Security Information and Event Management (SIEM) system seamlessly combines multiple functions, data handling and event management. Yet with more detections from more sources, SIEM systems are growing in complexity, creating more noise for your team and often higher costs for your business.

You are not alone if you are wondering how to choose the right data to:

- Ingest while staying on budget
- Keep your team from drowning in meaningless security alerts
- Keep up to date with new attacker techniques as they come out.

2023 predictions reveal CISOs will be carefully assessing their existing security programs, concentrating their efforts on hygiene and posture management and improving existing processes and controls.

In a year of economic uncertainty, partnering with the right MDR provider with experience combining SIEM with MDR Services is a practical way to focus on priorities, existing resources and getting the most significant ROI on your security spend.

> **Use this guide to navigate the intricacies of implementing MDR Services for SIEM, learn how to accelerate the return on your SIEM investment and ensure you have the most effective end-to-end security coverage to prevent breaches.**

Key **Takeaways**

1

Yes, your SIEM platform can meet the growing needs of your security practitioners as they face emerging threats. Managed effectively, it can go beyond compliance monitoring and log management to enhance your detection coverage and cybersecurity posture.

2

From implementation to optimization, SIEMs require constant "feed and caring."

3

Consider your needs when deciding on an MDR for SIEM vendor, including capabilities such as platform health and configuration, security and monitoring, investigation and escalations, custom dashboards, reports, log sources and alerts.

4

You have the power to control costs with spend-related support.

5

This buyer's guide can be forwarded to other critical decision-makers and SMEs within your organization to ensure everyone aligns across business priorities regarding cybersecurity.

The Business Case For **MDR For SIEM**

What is SIEM and how can it enhance your security posture?

SIEM is a security platform that ingests event logs and offers a single view of this data with additional insights. SIEMs can help you resolve misconfigurations and compensate for operational flaws and other engineering errors—benefits you cannot get from an MDR solution alone.

SIEMs can also help create a comprehensive security ecosystem by combining zero trust, vulnerability management and Endpoint Detection and Response (EDR). The result is faster detection and response, more efficient security operations, greater threat visibility and a reduction in security breaches.

Additional reasons SIEMs continue to grow in popularity include:

- ✓ **The need for continuous monitoring and incident response** — When a potential issue is detected, a SIEM can log additional information, generate an alert and instruct other security controls to stop an attacker's progress.
- ✓ **Bringing together multiple feeds** — Looking at all security-related data from a single point of view makes it easier to spot patterns that are out of the ordinary.
- ✓ **Gaining and maintaining certifications** — SIEMs can help you earn or maintain certain International Organization for Standardization (ISO) certifications.
- ✓ **Managing and retaining logs** — SIEM tools collect and aggregate log data from across your IT infrastructure into a centralized platform where it can be reviewed by security analysts and stored to meet regulatory requirements.

SIEM: QUALITY OF OUTPUT DETERMINED BY QUALITY OF INPUT

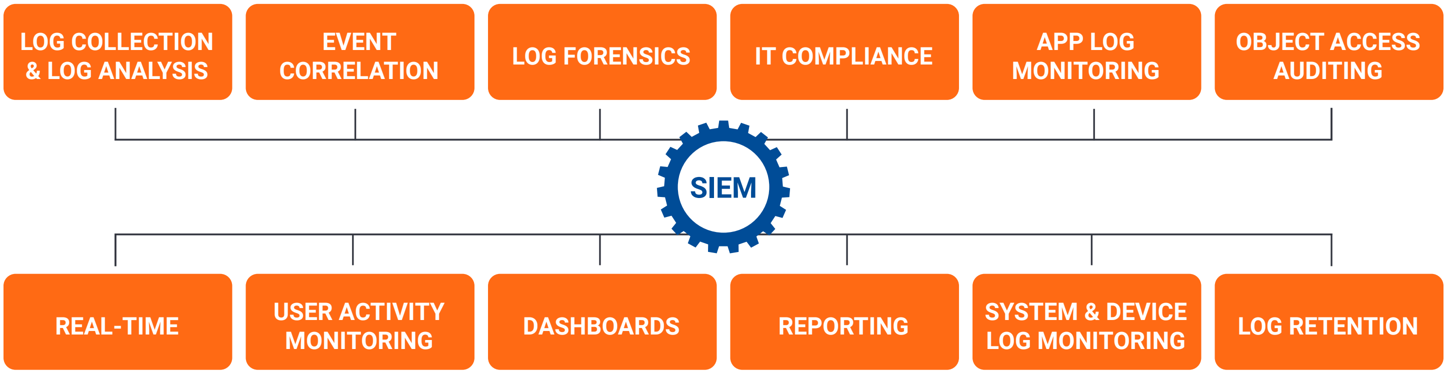


Figure 1: Quality management of your SIEM solution means only relevant information across various security devices is collected, monitored and analyzed, resulting in valuable outputs that matter to your enterprise.

Addressing the Common Challenges of **SIEM Implementations**

What are the pitfalls of SIEM and how can you avoid them?

While SIEMs can help secure your organization against threats from the ever-expanding attack surface, in practice, they often fail to deliver business value. Not because SIEMs are ineffective but because companies need help to use their SIEMs effectively.

A SIEM platform is not a “set it and forget it” technology purchase.

The efficacy of a SIEM investment depends upon the ongoing development and maturation of the SIEM from trained experts, tailored to the business’s specific needs.

Still, many companies make the mistake of underestimating the maintenance and continual optimization a SIEM entails, quickly leading to lost business value.

SIEMs hold a lot of promise as a centralized solution for unlocking the secrets contained in enterprise system logs and combining them with threat intelligence, but that promise comes at a cost. SIEMs are challenging to set up, add new feeds to and tune.

Integrating your SIEM platform with an MDR solution can help. Use this guide to help you address these common challenges inherent in using SIEM tools:

- Log Source Selection
- Rule Creation, Validation and Ongoing Enhancement
- Alert Saturation
- Lack of Response Guidance
- Security Staffing Shortages

> **Are your security analysts prepared to handle the heavy lifting—from creating new detection rules to analyzing false positives, tuning existing rules and ensuring that data sources are as comprehensive as possible?**

Log Source Selection

While most SIEM platforms let you ingest whatever log sources you want, being able to do something with that data is a different story.

To effectively drive threat detection and provide only the pertinent content needed for investigations, **you must decide what you want to ingest into the SIEM platform and manage that against the value those data sources provide to your security mission.**

Look for a vendor that can help you prioritize your data based on security value by separating it into tiers, such as:

- ✓ **The need for continuous monitoring and incident response** — When a potential issue is detected, a SIEM can log additional information, generate an alert and instruct other security controls to stop an attacker's progress.
- ✓ **Bringing together multiple feeds** — Looking at all security-related data from a single point of view makes it easier to spot patterns that are out of the ordinary.
- ✓ **Gaining and maintaining certifications** — SIEMs can help you earn or maintain certain International Organization for Standardization (ISO) certifications.
- ✓ **Managing and retaining logs** — SIEM tools collect and aggregate log data from across your IT infrastructure into a centralized platform where it can be reviewed by security analysts and stored to meet regulatory requirements.

What this means:

- ✓ Increased effectiveness with the highest combined value between log sources and threat detections
- ✓ Reduction in non-actionable events
- ✓ Better context for investigations

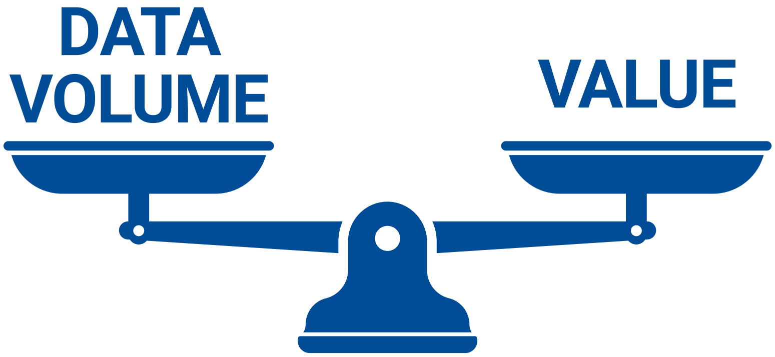


Figure 2: Never compromise: Always get the highest combined value between log sources and threat detections to continuously balance volume and value.

Rule Creation, Validation and Ongoing Enhancement

The value of your SIEM directly correlates with the relevancy of the information it provides. **Therefore, you must configure your SIEM tool to only ingest security-relevant data.** After you have fed your log sources into the SIEM, your MDR solution must add all the threat detection content it needs to turn this data into meaningful alerts. It can do this by creating rules to generate alerts, validating that those rules are effective and continuing to validate and tweak those rules to eliminate any that are not working correctly.

Critical Start adds threat detection content in two ways:

1 Vendor-supplied:

SIEM vendors provide rules, but they are often limited, vague and prone to false positives. Most SIEM vendors do not have teams dedicated to updating these rules when log source changes occur.

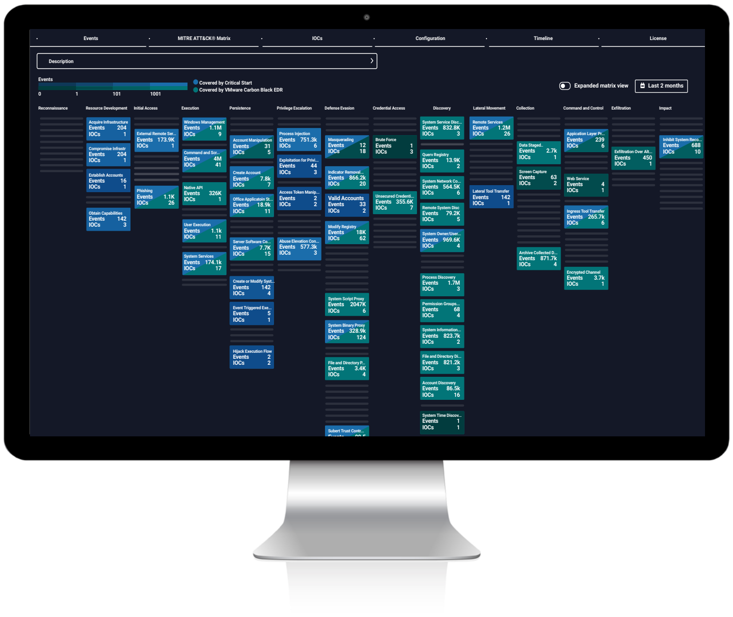
For example, if your network firewall is updated, data may be presented to the SIEM in an entirely new way that renders your existing rules useless. A best-of-breed MDR solution like Critical Start will update rules to account for user history and context when such changes occur.

2 High-value Content for Full Visibility:

Expanded, high-value content can help you manage, maintain and curate out-of-the-box detections and indicators of compromise (IOCs).

At Critical Start, our Threat Detection Engineering team:

- Continuously maps your detection content to the **MITRE ATT&CK® Framework** to identify any coverage gaps based on current log source feeds, and
- Adds new detections based on the latest threat intelligence curated by our Cyber Threat Intelligence team and other sources to fill any gaps.


Events
MITRE ATT&CK® Matrix
IOCs
Configuration
Timeline
License
Description
Events
0
1
101
1001
Covered by Critical Start
Covered by VMware Carbon Black EDR
Expanded matrix view
Last 2 months
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Acquire Infrastructure Events 204 IOCs 1
Compromise Infrastr Events 204 IOCs 1
Establish Accounts Events 16 IOCs 1
Obtain Capabilities Events 142 IOCs 3
External Remote Ser... Events 173.9K IOCs 1
Phishing Events 1.1K IOCs 26
Windows Management Events 1.1M IOCs 9
Command and Scr... Events 4M IOCs 41
Native API Events 326K IOCs 1
User Execution Events 1.1k IOCs 11
System Services Events 174.1k IOCs 17
Account Manipulation Events 31 IOCs 5
Create Account Events 7.8k IOCs 7
Office Applicatoin St... Events 18.9k IOCs 11
Server Software Co... Events 7.7K IOCs 15
Create or Modify Syst... Events 142 IOCs 4
Event Triggered Exe... Events 5 IOCs 1
Hijack Execution Flow Events 2 IOCs 2
Process Injection Events 751.3k IOCs 6
Exploitation for Privi... Events 44 IOCs 3
Access Token Manip... Events 2 IOCs 2
Abuse Elevation Con... Events 577.3k IOCs 3
Masquerading Events 12 IOCs 18
Indicator Removal... Events 866.2k IOCs 20
Valid Accounts Events 33 IOCs 2
Modify Registry Events 18K IOCs 62
System Script Proxy Events 2047K IOCs 6
System Binary Proxy Events 328.9k IOCs 124
File and Directory P... Events 3.4K IOCs 4
Subert Trust Contr...
Brute Force Events 1 IOCs 3
Unsecured Credenti... Events 355.6K IOCs 7
System Service Disc... Events 832.8K IOCs 3
Querv Registry Events 13.9K IOCs 2
System Network Co... Events 564.5K IOCs 6
Remote System Disc Events 79.2K IOCs 5
System Owner/User... Events 969.6K IOCs 4
Process Discovery Events 1.7M IOCs 3
Permission Groups... Events 68 IOCs 4
System Information... Events 823.7k IOCs 2
File and Directory Di... Events 821.2k IOCs 3
Account Discovery Events 86.5k IOCs 16
System Time Discov... Events 1 IOCs 1
Remote Services Events 1.2M IOCs 26
Lateral Tool Transfer Events 142 IOCs 1
Data Staged.. Events 2.7k IOCs 1
Screen Capture Events 63 IOCs 2
Archive Collected D... Events 871.7k IOCs 4
Appication Layer Pr... Events 239 IOCs 6
Web Service Events 4 IOCs 1
Ingress Tool Transfer Events 265.7k IOCs 6
Encrypted Channel Events 3.7k IOCs 1
Exfiltration Over Alt... Events 450 IOCs 1
Inhibit System Reco... Events 688 IOCs 10

What this means:

- ✓ Validation of security coverage across data sources
- ✓ Transparent threat detection coverage
- ✓ Relentlessly transparent reporting on security posture

Figure 3: Critical Start Threat Navigator provides a real-time view of your security posture, mapped to the MITRE ATT&CK® Framework.

Alert Saturation

The number of alerts generated for security teams is a problem. According to a 2021 report conducted by IDC and Critical Start, firms of all sizes struggle with investigating alerts, with **an average of 27% of overall alerts going ignored or uninvestigated due to the sheer volume received daily.** Organizations need a way to navigate this alert saturation and still have the flexibility to add more sources and monitor every alert generated while wasting less time with false positives.

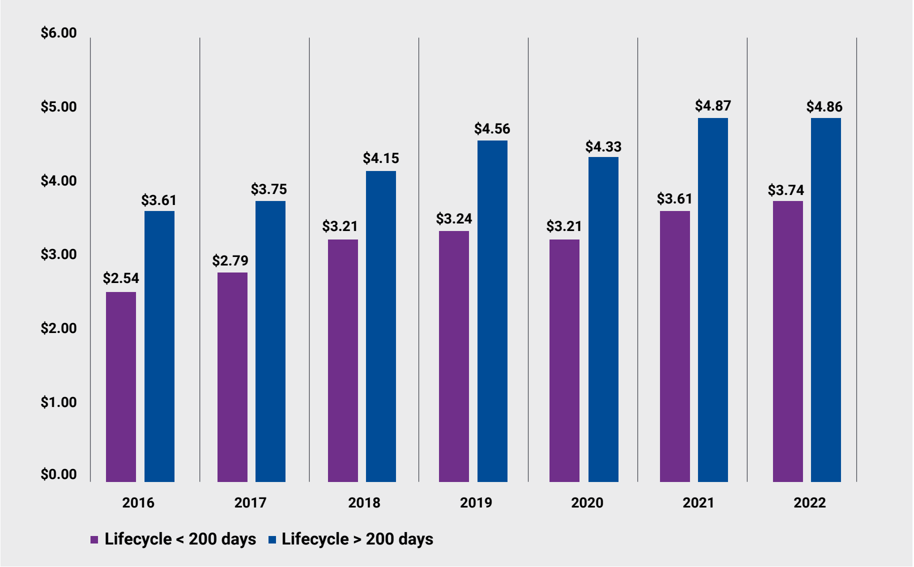
MDR providers take different approaches to the alert saturation issue:

- Some vendors disable inputs or alter the correlation logic that generates alerts. The downside of this approach is that it forces you to accept risk without understanding the implications and robs you of your ability to see if your business is secure.
- Other vendors focus on only critical alerts, leaving medium and low-priority alerts untouched. Unfortunately, threat actors know most organizations ignore the mediums and lows and can hide in their environments for months.

What this means:

- ✓ Fewer false positives, while still being able to add more log source feeds
- ✓ Threats detected earlier in the attack cycle, resulting in a shorter data breach lifecycle and therefore lower costs *(Fig 4)*
- ✓ Relief from alert fatigue

Average cost of a data breach based on a data breach lifecycle



(IBM Security. Cost of a Data Breach Report 2022)

Figure 4: Average cost of a data breach based on data breach lifecycle. Measured in USD millions. Sum of days to identify and days to contain equals the breach lifecycle.

Alert Saturation (continued)

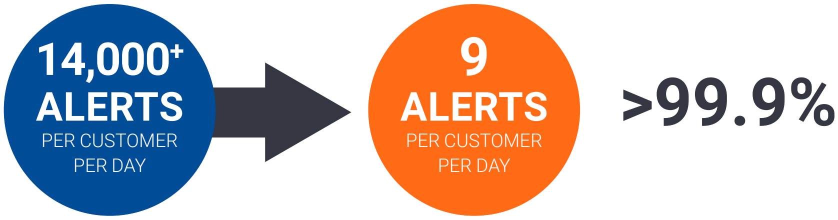
Critical Start's Trusted Behavior Registry™ (TBR), a proprietary technology within our **Zero Trust Analytics Platform™ (ZTAP®),** eliminates false positives at scale and brings in critical thought processes by engaging humans to investigate and resolve all remaining alerts, regardless of priority. *(Fig 5)*

Critical Start Delivers the Scalability to

RESOLVE EVERY ALERT

FOR EVERY PRIORITY

Zero Trust Analytics Platform (ZTAP) automatically resolves >99.9% of all alerts

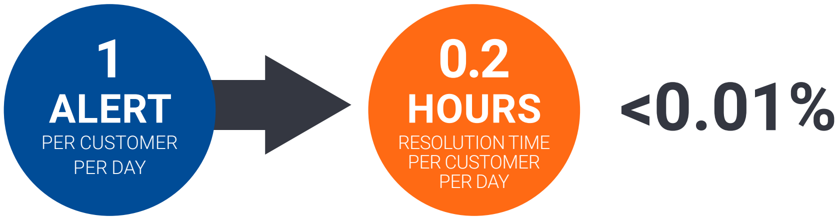


14,000+ ALERTS PER CUSTOMER PER DAY

9 ALERTS PER CUSTOMER PER DAY

>99.9%

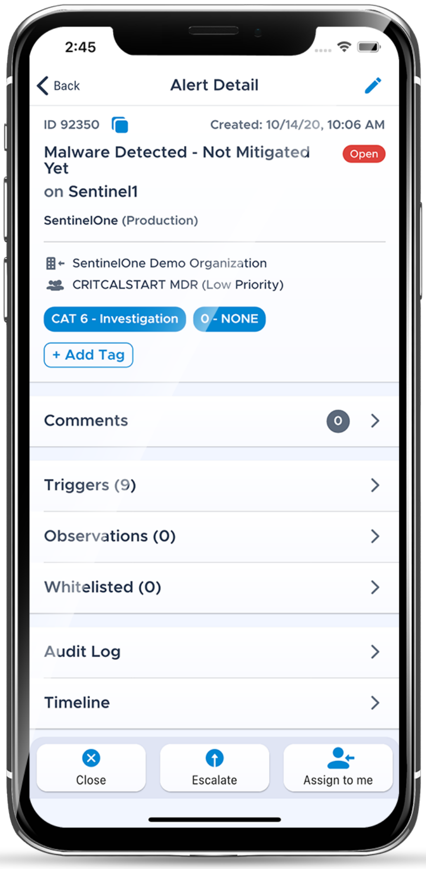
Critical Start SOC escalates only <0.01% of all alerts to our customer



1 ALERT PER CUSTOMER PER DAY

0.2 HOURS RESOLUTION TIME PER CUSTOMER PER DAY

<0.01%



2:45

< Back — Alert Detail

ID 92350 — Created: 10/14/20, 10:06 AM

Malware Detected - Not Mitigated Yet — Open

on Sentinel1

SentinelOne (Production)

SentinelOne Demo Organization

CRITCALSTART MDR (Low Priority)

CAT 6 - Investigation — 0 - NONE

+ Add Tag

Comments 0

Triggers (9)

Observations (0)

Whitelisted (0)

Audit Log

Timeline

Close — Escalate — Assign to me

Figure 5: All statistics are averages based on six months of data recorded by the Critical Start SOC.

Lack of Response Guidance

What do you do when an alert turns out to be an actual attack?

Different attacks require different expertise.

Few security teams have the breadth of experience necessary to respond effectively to every attack–even if they discover it early.

SIEM alerts can compound this issue. While SIEM opens the door to cross-correlation across security events and data streams, investigating the alerts created by SIEM often requires pivoting into one or more security consoles before understanding the full scope of an attack.

For example:

A network alert correlated with threat intelligence in a SIEM will generate an alert about malicious traffic on the network heading toward critical infrastructure. But this alert will not tell you if the malware reached the target, if the antivirus blocked it, or if someone used stolen credentials to send the file across the network. You're still forced to rely on multiple other security tools to decide what actions to take.

> **Hiring and training security professionals who can turn contextual alerts into definite answers requires a high level of expertise. In addition, these expensive resources often find themselves torn between the critical work of securing the organization and the urgent work of investigating security alerts, most of which end up being false positives.**

Lack of Response Guidance (continued)

Critical Start has a guaranteed one-hour SLA with all our customers, including:

Time to Detect (TTD) and Median Time to Resolve (MTTR).

TTD is measured as one hour from the time the alert is created until the alert is assigned to an analyst. This means that if the alert sits in the queue for more than an hour without someone assigning it to themselves, we owe the customer money.

Our **MTTR** is one hour from the time an alert is generated until a resolution action is taken on that alert. Resolution actions include:

- Escalation to the customer
- Orchestration creation and category change to tuning
- Alert closure

What this means:

- ✓ Finding and stopping threats early in the attack cycle
- ✓ Guaranteed active response to all events in your security environment within minutes
- ✓ Extending incident response beyond the SIEM
- ✓ Adding just-in-time expertise to your team

> **When considering MDR for SIEM, look for vendors with experience responding to events using your full security toolset. These vendors can turn broad, contextual SIEM alerts into definitive write-ups for executive and technical resources and provide clear guidance and active remediation support throughout incidents.**

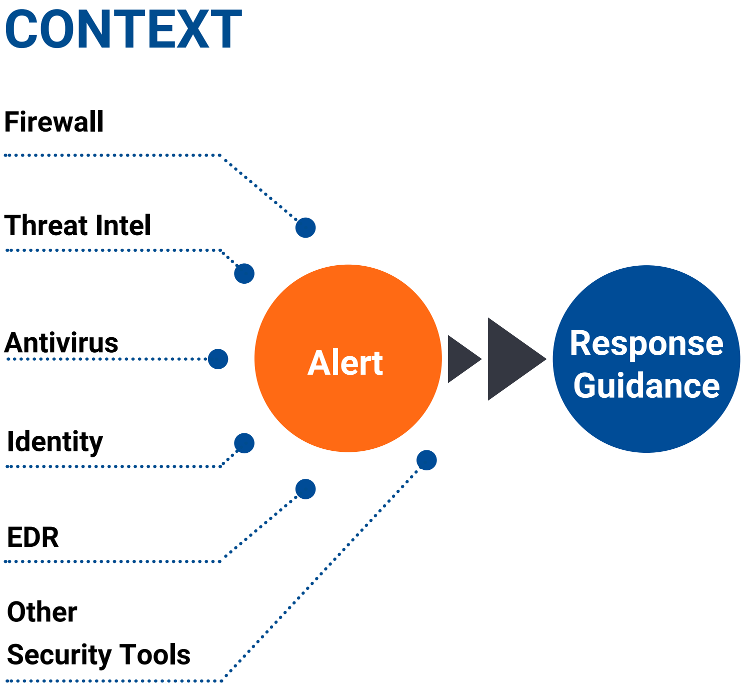


Figure 6: A SIEM is contextual, so effective response guidance requires investigation and correlation across multiple security tools.

Security Staffing Shortages

There are a limited number of cybersecurity experts, and the problem is getting worse. Organizations need people who can focus their time on building security into their core functions.

For example, the skills required to secure a bank, protect Continuous Integration/Continuous Delivery (CI/CD) pipelines, or defend a manufacturing site have little to nothing to do with maintaining SIEM infrastructure and use cases.

Organizations face the impossible choice of either hiring generalists to help take care of the day-to-day flood of cyber security tasks, or focused experts who can facilitate the secure execution of the company's goals.

What this means:

- ✓ Give your internal staff the freedom to focus on other strategic tasks
- ✓ Accelerate the return on your SIEM investment
- ✓ Improve team efficacy, retain talent
- ✓ Offload tedious tasks
- ✓ Elevate the stature of your security team

> **MDR for SIEM gives you the best of both worlds—the ability to focus your limited internal resources on projects that achieve your goals while adding an MDR vendor to handle the urgent day-to-day tasks triggered by security alerts. Best of all, you are no longer forced to waste resources on tasks unrelated to your company's vision and purpose. Without increasing headcount, MDR for SIEM provides you with the resources required to mature your SOC.**

Security Staffing Shortages (continued)

Onboard and Plan

- ✓ Review existing SIEM configuration
- ✓ Recommend initial data sources
- ✓ Advise on data source configuration

Personalize and Deploy

- ✓ Data source onboarding
- ✓ Install standard data source apps and visualizations
- ✓ Deploy initial threat detection content
- ✓ Alert baselining and content tuning
- ✓ Set up and deploy initial playbooks and alert routing lists/groups
- ✓ Connect your SIEM to **ZTAP** to reduce false positives
- ✓ Ensure SIEM is working effectively

Investigate and Resolve

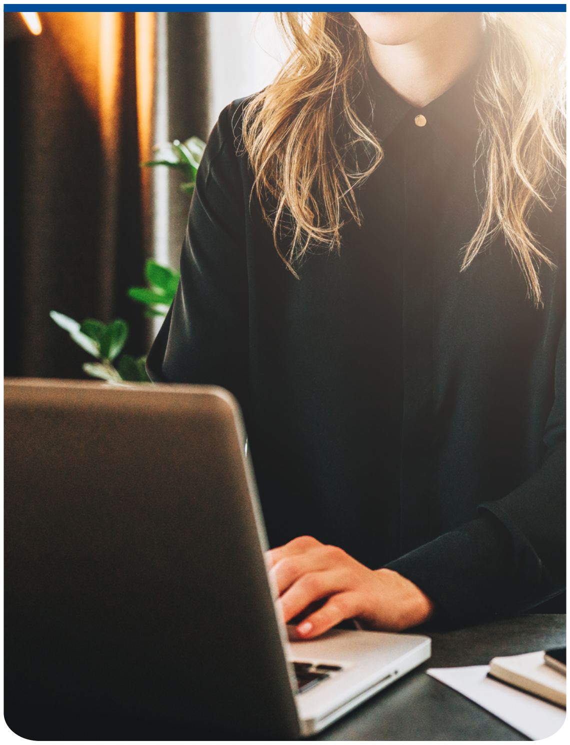
- ✓ Resolve every SIEM alert
- ✓ One hour SLA for **Time to Detect (TTD)** & **Median Time to Resolution (MTTR)**
- ✓ **24x7x365** alert triage, analysis and response
- ✓ Playbook orchestration and alert routing
- ✓ Data source health monitoring
- ✓ MOBILE**SOC**® mobile app to review metrics and respond to alerts

Scale and Mature

- ✓ Ongoing development and deployment of new threat-detection content
- ✓ Playbook refinement according to evolving business needs
- ✓ Recommend new data sources
- ✓ Operational Reviews

Optimize

- ✓ Health and ingest cost analyses
- ✓ Customization
- ✓ Configuration
- ✓ Risk reduction review
- ✓ More efficient allocation of your resources



MDR for SIEM Vendor Checklist

Use This Checklist To Compare Key Capabilities & Features of MDR Vendors Who Integrate With Leading SIEM Tools:

CAPABILITY/FEATURE	Critical Start	Vendor #2	Vendor #3	Vendor #4
Platform Health & Configuration				
Architecture review of your existing configuration	✓			
Health reporting for Supported Data Sources	✓			
Spend-related support to optimize or reduce spend	✓			
Security Alert Monitoring, Investigation & Escalations				
Monitoring and support for Supported Log Collectors	✓			
Detection personalization specific to your business, network appliances and users	✓			
Review of every security alert generated by SIEM tool	✓			
Playbook orchestration & alert routing to appropriate groups or users	✓			
One-hour SLA for Time to Detect (TTD) and Median Time to Resolution (MTTR) with security alerts	✓			
Investigation	✓			
Ability to take response actions on your behalf with supported endpoint security solutions	✓			
Complete transparency (full access to the platform, investigation tools and audit activity)	✓			
Dashboards, Reports & Extras				
Alert enrichment with details about IPs, hashes and domains to provide additional context	✓			
Data onboarding and dashboards/app implementation for Supported Data Sources	✓			
Installation of vendor-supported apps for common security vendors' dashboards and reports	✓			
Customized log sources & content	✓			
Customized dashboards	✓			

Critical Start SIEM Solutions

Every log is different, and so are the MDR services that manage them.

Critical Start offers comprehensive Managed SIEM and MDR for SIEM services that include:

- ✓ Access to security experts who understand your environment
- ✓ Finding and stopping attacks at the earliest stage of compromise
- ✓ Resolving every alert, of every priority, from every security source, within one hour
- ✓ Defining and eliminating the noise so that legitimate attacks rise to the top
- ✓ Active remediation against attacks
- ✓ Configuration and customization tailored to your unique business needs
- ✓ Health monitoring and risk reduction reviews
- ✓ Access to the SOC at any time and any place with our iOS/Android mobile application (MobileSOC)
- ✓ Spend-related support to optimize or reduce spend

Simplify breach prevention and get direct access to security experts and mobile tools to respond to and remediate incidents. With Critical Start, you can achieve full operational security potential of your SIEM investment, control your total cost of ownership and free up your resources to focus on security projects that matter most.

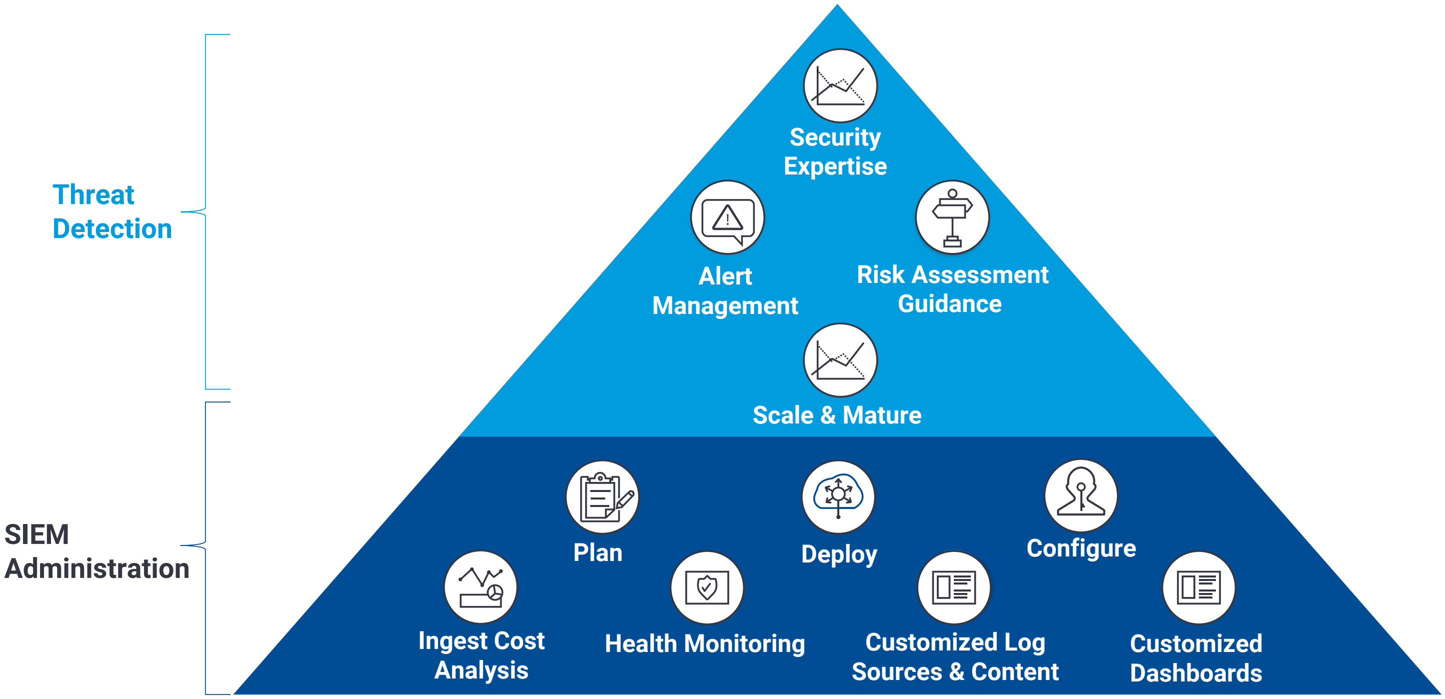


Figure 7: Simplifying breach prevention

Eliminate False Positives and Focus on Known and Emerging Threats

Respond Quickly with the Right Actions

Increase your Security Posture with MDR for SIEM Adapted to Your Business

Reduce Operating Costs and Improve Team Productivity with Better Resource Allocation

CRITICALSTART®

They're good. We're better.

Contact us for more information about Critical Start Managed SIEM and other SIEM solutions and services, or schedule a demo at:

www.criticalstart.com/contact/request-a-demo/