The CRITICAL**START**®
Buyer's Guide for Security Services for SIEM

Managed SIEM + Premier MDR Services for Your Organization: How to Select the Best Solution to Optimize Total Value and Uncover Hidden Threats

Table Of Contents

Executive **Summary**

Unlock the full potential of your SIEM investment and reduce the risk of a breach.

The significant challenges organizations face to protect their critical assets and data from sophisticated cyberattacks never end. The complexity of modern IT infrastructures and the increasing volume and diversity of security threats have made it difficult to effectively detect, investigate, and respond to security incidents without a holistic approach.

Critical Start simplifies the optimization of Security Information and Event Management (**SIEM**) implementations by helping organizations maximize the value of their investment. By pairing managed SIEM with our expanded MDR services, we provide 24x7x365 threat detection and response with ongoing SIEM support for optimized cost and risk reduction.

Our Security Services for SIEM are designed to help organizations go beyond log management and compliance to maximize the threat detection value of their SIEM investments and proactively manage risk. As a trusted partner of leading SIEM providers like Sumo Logic®, Microsoft® Sentinel, and Splunk®, Critical Start offers a unique blend of deep SIEM expertise, expanded MDR capabilities, (like monitoring SIEM log source health) with a transparent service delivery platform and mobile application. Our human-driven, AI-supported MDR services are backed by a 24x7x365 Security Operations Center (SOC), Cyber Research Unit, and Cyber Incident Response Team, providing unmatched threat detection and response capabilities. This human-centric approach enhances the effectiveness of our threat detection and response efforts, providing insight and adaptability that technology alone cannot achieve.

By combining the power of advanced security technologies with the knowledge and experience of our skilled security professionals, we help organizations:

- Gain full transparency and control over their security operations
- Overcome the challenges of deploying and optimizing their SIEM solutions
- Identify and take action on ensuring the most security-relevant SIEM telemetry is ingested and SIEM log health data is tracked
- Neutralize threats before they can cause significant damage with 24x7x365 MDR monitoring, threat detection, and response and around-the-clock access to our security analysts
- Reduce attacker dwell time and contain incidents on the go with our MOBILE**SOC**® mobile app
- Maximize the value of their security investments while reducing risk

Organizations focused on driving growth and opportunity and accelerating time-to-market support these goals with a cybersecurity program that includes expertly optimized and SIEM and premier MDR defense.

Use this guide to discover how a holistic Managed SIEM + MDR solution can help create a stronger foundation for your risk-resilient organization.

In addition, our unified solution is aligned with the industry-recognized **MITRE ATT&CK® Framework** and provides provable metrics, peer benchmarking, and best practices to help you demonstrate the value of your security investments to stakeholders.

With expertly guided SIEM enablement services and elevated Managed Detection and Response (**MDR**), Critical Start Security Services for SIEM provides organizations like yours with a solid foundation for continued security maturity and risk resilience.

Key **Takeaways**

What benefits to expect from a combined SIEM management and MDR services solution

1. ENHANCED THREAT DETECTION
   Proactive capabilities like prioritizing and reviewing log ingest and log health monitoring (including Zero-Log Ingest Alerts) provide **SOC signal assurance**, meaning your MDR receives the expected threats for the most effective threat detection possible.

2. RAPID INCIDENT RESPONSE
   Human-driven 24x7x365 investigation and true response mitigation, a 10-minute SLA for Critical alerts, a 60-minute Median Time to Resolution (**MTTR**), and the MobileSOC app enable swift containment of threats before they escalate.

3. RISK REDUCTION
   MITRE ATT&CK® Mitigations Recommendations and advanced threat intelligence from the Cyber Research Unit (**CRU**) help proactively identify and address potential security risks.

4. INCREASED SOC EFFICIENCY
   Offloading Tier 1 and Tier 2 support, leveraging the Unified Timeline and "Who's On Call?" features, and resolving false positives with the Trusted Behavior Registry® (**TBR®**) allows your Security Operations Center (**SOC**) team to focus on high-priority tasks.

5. ACCELERATED SIEM ROI
   Prioritizing ingest data, tuning log sources, and receiving the highest combined value between log sources and threat detections maximize your SIEM investment's operational and security potential. Our **complete signal coverage** supports various data sources, use cases, and business needs, including visibility across IT and Operational Technology (**OT**) environments, SIEM optimization, and Managed XDR for threat-centric visibility without a SIEM.

6. CUSTOMIZED SOLUTION
   Tailored dashboards, reports, and log sources ensure the solution is adapted to your unique business needs, providing relevant security insights and aligning with industry standards like the **MITRE ATT&CK® Framework**.

7. COMPREHENSIVE COMPLIANCE
   Compliance dashboards and log storage and auditing make it easy for Governance, Risk, and Compliance needs.

8. REDUCED TOTAL COST OF OWNERSHIP (TCO)
   Partnering with us to help keep your SIEM optimized through log source prioritization, ingest reviews, and visibility recommendations to reduce inefficiencies.

9. REAL-TIME VISIBILITY
   Customizable dashboards and reports provide insights into your security posture, track KPIs, incident response metrics, and threat trends, and map threat and detection content to the **MITRE ATT&CK® Framework**. Our **Cyber Operations Risk & Response™** (**CORR**) platform integrates advanced security intelligence for unified visibility across your security controls.

10. CONTINUOUS IMPROVEMENT
    Quarterly service reviews, health monitoring, and ongoing analysis of log sources and detection content ensure your SIEM solution adapts to evolving threats and business needs.

What Is a **Security Information and Event Management (SIEM) Platform?**

Q: What is a SIEM platform, and how can it enhance my security posture?

A: A SIEM is a security platform that ingests event logs (records generated by various systems, applications, and devices within an organization's IT infrastructure) and offers a unified 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 acting as the centralizing layer that combines zero trust controls, vulnerability management systems, and Endpoint Detection and Response (**EDR**) tools. The result is faster detection and response, more efficient security operations, greater threat visibility, and a reduction in security breaches.

SIEM use cases include:

- **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.
- **Bring 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.
- **Gain and Maintain Certifications** — SIEMs can help you earn or maintain certain International Organization for Standardization (**ISO**) certifications.
- **Manage and Retain Logs** — Organizations may be required to collect, store, and retain certain log data for compliance, regulatory, and contractual requirements that extend beyond their security value. SIEM tools collect and aggregate log data from across your IT infrastructure into a centralized platform where it can be reviewed by security analysts.

A SIEM platform is not a "set it and forget it" technology purchase. Many organizations make the mistake of underestimating the maintenance and continual optimization a SIEM entails, quickly leading to lost business value.

While SIEMs can help secure an organization against threats, they often fail to deliver a maximized ROI. This is not because SIEMs are ineffective but because organizations need help using their SIEMs effectively. The efficacy of a SIEM investment depends upon the ongoing development and maturation of the SIEM by trained experts, tailored to the organization's specific needs.

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. However, because they are challenging to set up, add new feeds to, and tune, that promise can come with a cost that organizations can't meet alone.

> **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?**

The Business Case for **Security Services for SIEM**

Cybersecurity is not just an insurance plan against potential threats. It has evolved into a crucial driver of business growth, efficiency, and resilience amidst the ongoing digital transformation reshaping our world.

Organizations that struggle to prioritize and effectively manage their cybersecurity posture face the risk of financial losses and reputational damage. They also miss out on valuable opportunities to streamline operations, accelerate time to market, and foster innovation.

You are not alone if you find it challenging to maximize the value of your SIEM investment while managing its complexity and proving its ROI on bolstering your organization's security posture.

The complexity of SIEM deployments, the need for continuous optimization, and the lack of skilled security professionals can hinder your ability to detect, investigate, and effectively respond to security incidents.

By partnering with an MDR privider that supports SIEM telemetry readiness and detection enablement (like Critical Start's Security Services for SIEM), you can address these challenges head-on. This solution not only increases threat visibility and maximizes the value of your SIEM investment but also empowers you to enhance your overall security posture.

Your organization is empowered to:

- ✓ **Streamline security operations and reduce complexity** — Optimize your SIEM deployment, prioritize relevant data sources, and get actionable insights, enabling your teams to focus on high-value tasks and strategic initiatives.
- ✓ **Enhance threat detection and response** — Get 24x7x365 monitoring and response capabilities. When a potential issue is detected, our solution logs additional information and generates an alert while our Security Operations Center (**SOC**) analysts help ensure rapid containment and remediation of validated threats.
- ✓ **Gain a holistic view of your security posture** — Bringing together multiple data feeds provides a comprehensive view of your security posture. This centralized perspective makes it easier to spot patterns, identify anomalies, and detect potential threats that might otherwise go unnoticed.

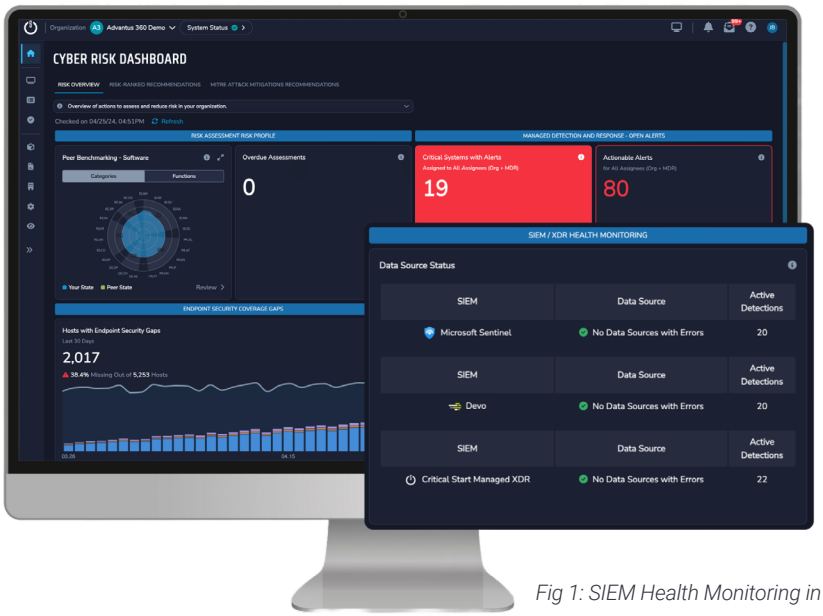

Fig 1: SIEM Health Monitoring in the Cyber Risk Dashboard

The Business Case for **Security Services for SIEM** *(cont.)*

- ✓ **Proactively identify and resolve coverage gaps** — Reduce the risk of missed threats by identifying and resolving inconsisent SIEMtelemetry, ensuring that security-relevant logs are properly ingested (***Fig 2***) and that you have comprehensive threat detection coverage.
- ✓ **Leverage advanced analytics and threat intelligence** — Only true-positive alerts are escalated to your team, enabling them to focus on genuine threats and priority incidents. Curated threat intelligence feeds and operationalized threat intelligence enhance your SIEM's detection capabilities and protect you against the latest attacker techniques, tactics, and procedures (**TTPs**).
- ✓ **Improve team productivity and scale security operations** — Offloading Tier 1 and Tier 2 SOC support and leveraging guided remediation frees up your team to focus on higher-priority tasks and strategic initiatives. Scale your security operations efficiently to do more with less and adapt as your organization's needs evolve.
- ✓ **Achieve and maintain compliance** — Meet and maintain various compliance requirements, such as International Organization for Standardization (**ISO**) certifications. Manage and retain logs and ensure that your SIEM collects and aggregates log data from across your IT infrastructure into a centralized platform for review and storage.
- ✓ **Optimize costs and maximize ROI** — Help guide SIEM optimization efforts to reduce the Total Cost of Ownership (**TCO**) and increase the return on your security investment. Log prioritization, health monitoring (***Fig 1***), and ingest cost analysis ensure you get the most value from your SIEM without overextending your budget.

QUALITY THREAT DETECTION OUTPUT IS DETERMINED QUALITY LOG INPUT

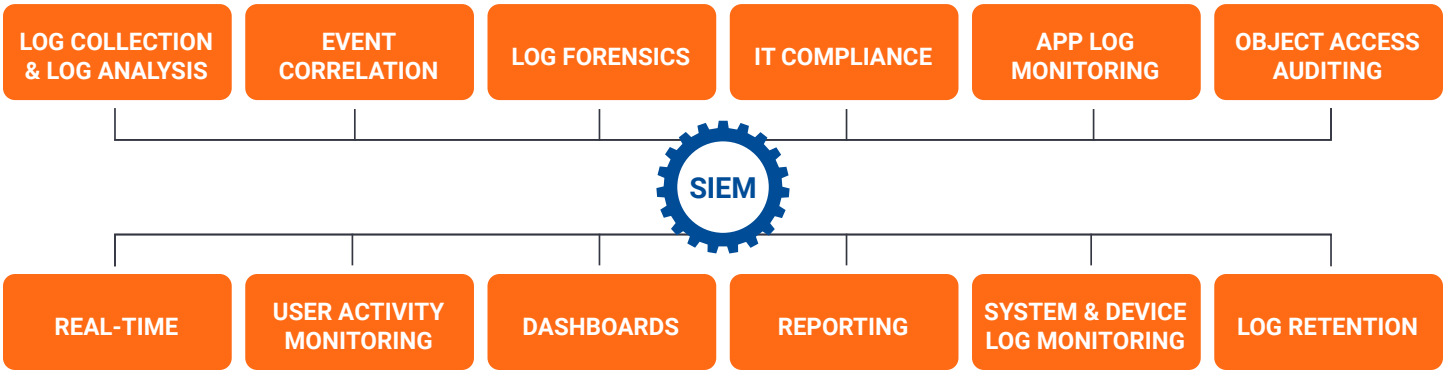

Fig 2: Log ingestion reviews and prioritization means only relevant information across various security devices is prioritized and guided for collection and analysis, resulting in valuable outputs that matter to your organization.

Addressing the Common Challenges of **Reaching the Full Operating Potential of Your SIEM**

Q: How can my organization keep up with the ongoing maintenance, tuning, and optimization necessary to maximize the value of our SIEM investment?

A: Critical Start begins with detailed scoping and architecting of your SIEM environment, including evaluating which log sources you have and how to prioritize what log sources are ingested.

1. LOG SOURCE PRIORITIZATION AND CONFIGURATION

One of the biggest challenges in managing a SIEM is deciding which log sources to ingest and ensuring that the data being collected is relevant and actionable.

Deciding what log sources to bring into the SIEM isn't always as clear-cut as limiting sources to "security-relevant" data. Instead, it depends on your operating environment and specific security needs and requirements.

Critical Start's experts help you configure your SIEM to prioritize log sources based on your needs, their security relevance, and their potential for driving effective threat detection. (***Fig 3***) We ensure they are working correctly, closing any visibility gaps that could leave your organization vulnerable.

Common SIEM challenges include:

- **Log Source Prioritization and Configuration**
- **Customization and Alignment with Business Needs**
- **SIEM Health Monitoring and Risk Reduction**
- **Optimization and Cost Management**
- **Compliance, Auditing, and Log Storage**
- **Security Staffing Shortages**
- **SIEM Telemetry**

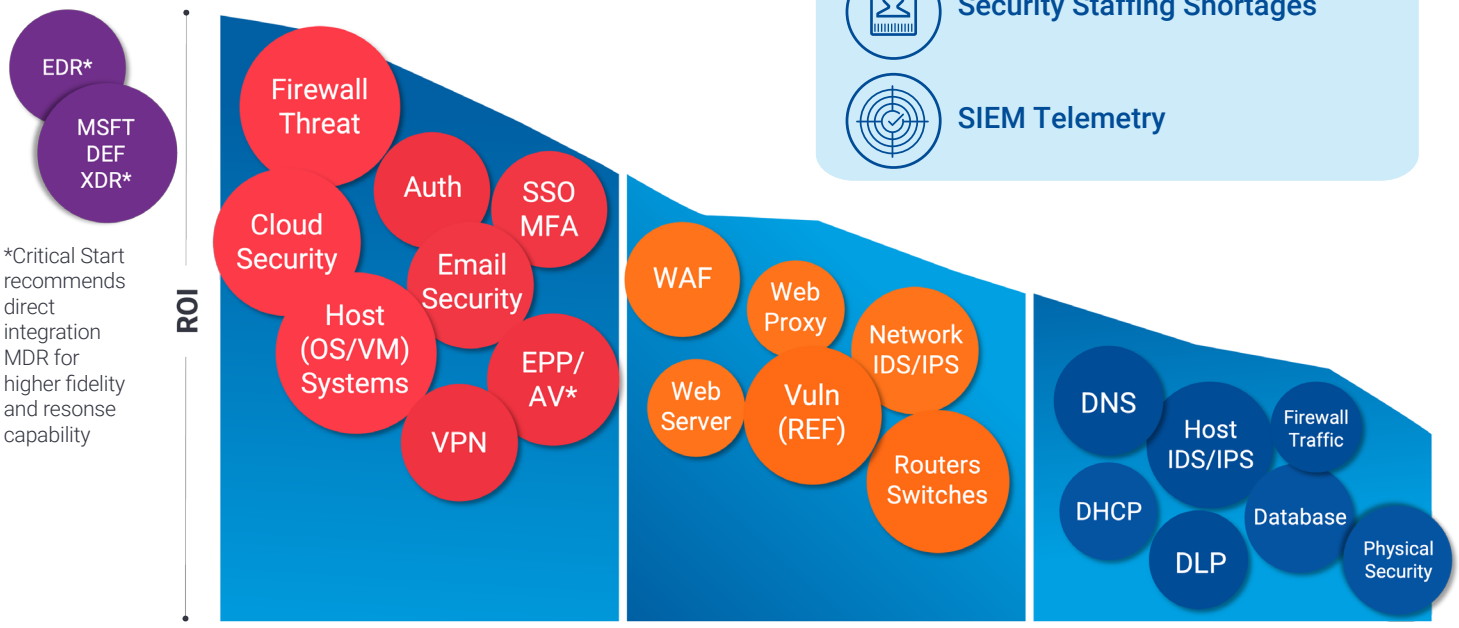

Fig 3: Log source prioritization for better security value

Addressing the Common Challenges of **Reaching the Full Operating Potential of Your SIEM** (*cont.*)

2. CUSTOMIZATION AND ALIGNMENT WITH ORGANIZATIONAL NEEDS

If ingest and storage cost management are not a driving concern, it's essential to log as much raw data and telemetry as possible for use cases beyond alerts, including audit, forensics, investigation, analytics, threat hunting, and machine learning. In reality, that may not be possible due to your organization's unique budgetary, security, risk, compliance, and audit requirements.

For effective threat detection and investigation, knowing what to ingest into your SIEM platform and managing that against the value those data sources provide to your security program is paramount. So, if your organization needs to pare down or remove certain logs from the log sources ingested, we will work with you to understand your goals and make appropriate recommendations.

For example, if reducing SIEM cost is a concern, we suggest reducing log volume, primarily by filtering/dropping events at the source itself or the forwarder level (Syslog server, heavy forwarder, etc.).

If the concern is a lack of space or storage costs, we may recommend keeping the same log volume but allocating non- or low-security-value logs to low-cost log storage (like Basic Log Tiers vs. Analytic Rules Tier in Sentinel).

To increase security effectiveness, get the highest combined value between log sources and threat detections, reduce non-actionable events, and drive better context for investigations, we recommend customers evaluate logs on a source-by-source basis, focusing on the "known good" like benign traffic and non-security-relevant logs.

Address potential blind spots in your security infrastructure and have confidence that your organization is receiving all expected telemetry with visibility and validation that all log sources are ingested.

2. CUSTOMIZATION AND ALIGNMENT WITH ORGANIZATIONAL NEEDS *(cont.)*

Preventing Data Overload

Customize and align with your organizational needs while preventing data overload by prioritizing log sources based on the security value you are getting. Focus first on security-relevant (**Primary**) log sources with the highest fidelity telemetry, including:

- Email Security
- Firewall Threat
- Authentication
- Cloud Security Host Systems OS/VM (Operating Systems/Virtual Machines)
- Single Sign On (**SSO**) and Multifactor Authentication (**MFA**)
- Virtual Private Network (**VPN**)
- Endpoint Protection/Antivirus (**EPP/AV**)

Secondary log sources may include:

- Web Application Firewall (**WAF**)
- Web Proxy
- Network IDS/IPS logs (Intrusion Detection/ Prevention System)
- Web Server
- Router Switches
- Vulnerability

Followed by **Tertiary log sources** that you can leverage for specific detections or enrichment purposes:

- Domain name system (**DNS**)
- Data loss prevention (**DLP**)
- Host IDS/IPS (Intrusion Detection/Prevention System)
- Dynamic Host Configuration Protocol (**DHCP**)
- Firewall Traffic
- Database
- Physical Security

Once this log data is collected and aggregated from across your IT infrastructure into a centralized platform, it can be reviewed by security analysts and stored to meet regulatory requirements. (***Fig 4***)

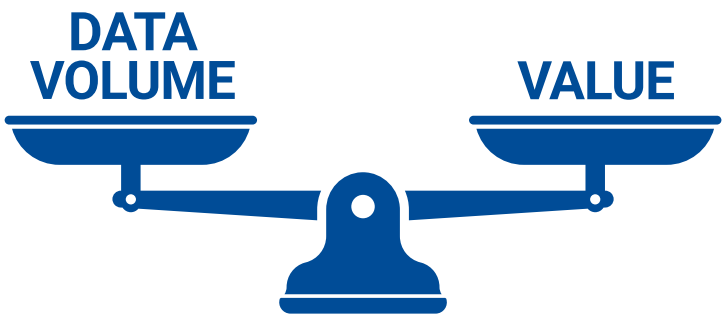

Fig 4: Customization helps your organization balance volume and value

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

Addressing the Common Challenges of **Reaching the Full Operating Potential of Your SIEM** (*cont.*)

3. SIEM HEALTH MONITORING AND RISK REDUCTION

To ensure continuous visibility and effective threat detection, Critical Start provides proactive SIEM features like log and health monitoring, including:

- **Zero-Log Ingest Alerts**
- Log source performance, availability, and capacity monitoring to identify potential issues with log ingestion and
- **Quarterly Review of Telemetry Coverage Gaps** to help you stay ahead of evolving threats

4. OPTIMIZATION AND COST MANAGEMENT

Optimization across teams, technologies, and processes is the only way to "future-proof" your SIEM and ensure costs are managed in the long term. This includes shifting from a "set it and forget it" mentality to one of constant care and feeding.

While all that attention given to the SIEM seems counter-intuitive when looking to cut costs, it is the only way to continue scale and mature your security posture and get the highest ROI from a SIEM solution.

Security teams can achieve this by:

- Prioritizing and ingesting the highest-fidelity log sources
- Retaining only the most relevant data (or move non-critical data to a more cost-effective storage solution)
- Monitoring log source performance, availability, and capacity to identify potential issues with log ingestion
- Conducting regular audits
- Utilizing customized dashboards, reports, and log sources to support specific security, risk, compliance, and audit use cases to gain more control over SIEM data and costs

5. COMPLIANCE, AUDITING, AND LOG STORAGE

Storage costs and legal rules and regulations are two areas that influence data storage and archiving.

We work with you to understand if your organization is required to collect, store, and retain specific log data for compliance, regulatory, and contractual requirements that extend beyond their security value (e.g., **HIPPA**, **GDPR**, **PCI DSS**, etc.), or for any additional needs and end goals you may have (like earning or maintaining certifications including certain International Organization for Standardization (**ISO**) certifications).

With that in mind, we may recommend beginning with ingesting the following logs:

- Firewall Threat
- Authentication
- Endpoint Protection/Antivirus (**EPP/AV**)
- Web Server
- Network Intrusion Detection/Prevention System **(IDS/IPS**) logs
- Host Systems Operating Systems/Virtual Machines (**OS/VM**)
- Security Logs (i.e., Domain Controllers)

Addressing the Common Challenges of **Reaching the Full Operating Potential of Your SIEM** (*cont.*)

6. SECURITY STAFFING SHORTAGES

Ensuring that SIEM telemetry sources remain connected and properly ingested allows your analysts to remain focused on real and emerging threats and helps you avoid costly downtime.

Help your team work more efficiently by optimizing processes, including automating everyday tasks, having an expert available for guidance on how to quickly and effectively respond to incidents using your SIEM data, and using customized detection and reporting content that translates alerts into information you can do something with.

Automation and pre-determined workflows give you more control over your SIEM data, the use cases it supports, and escalation processes and operations, resulting in increased efficiency and cost optimization.

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

How We Bring Value to Your Team

Onboarding and Planning

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

Personalization and Deployment

- 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 our **Trusted Behavior Registry**® (**TBR**®) to reduce false positives
- Ensure SIEM is working effectively

Investigation and Resolution

- Resolve every threat alert, regardless of criticality
- Contractual Service Level Agreements (**SLAs**) of 10-minute notifications for Critical alerts and 60-minute or less Median Time to Resolution (**MTTR**)
- 24x7x365 alert triage, analysis, and response
- Playbook orchestration and alert routing
- MobileSOC mobile app to mitigate risk and respond to threats

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 (monthly with Customer Success)

Optimization of Detection Coverage and SIEM Performance

- Log Health monitoring (offering log source performance, availability, and capacity monitoring to identify potential issues with log ingestion)
- Ingest Cost Analysis for a more efficient allocation of your resources
- Quarterly Service Reviews for full visibility into what logs you are ingesting and how your SIEM is performing
- Customization
- Configuration

The power of **Managed SIEM + Elevated MDR Services**

Q: How do I know my MDR is recieving all of the expected threat signals so I can measurably reduce cyber risk, prevent breaches, and stop business disruption?

A: The strength of your security posture depends on a well-managed SIEM solution. We start by operationalizing your SIEM, then ensuring all expected threat signals are recieved with proactive functionality like SIEM Log Health and then resolve every MDR threat alert, including those sourced from SIEM telemetry, regardless of criticality.

1. HOW DOES SIEM LOG DATA GET TURNED INTO MEANINGFUL SECURITY ALERTS?

The value of your SIEM directly correlates with the relevancy of the information it provides. 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 simplifies rule management by adding all the threat detection content needed to turn your SIEM log data into meaningful alerts in two ways:

1. Updating Vendor-Supplied Rules

Without a dedicated team, vendor-supplied rules may not get updated 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.)

To avoid rules that are outdated, limited, vague, and prone to false positives, Critical Start will update rules to account for user history and context when such changes occur.

2. Providing High-Value Content for Full Visibility:

Critical Start provides custom threat detections based on what we have observed with other customers and Indicators of Compromise (**IOCs**).
Our Cyber Threat Intelligence (**CTI**) team:

- Maps your detection content to the industry-recognized **MITRE ATT&CK® Framework** (***Fig 5***) to identify any coverage gaps based on current log source feeds and
- Adds new detections based on the latest threat intelligence and other sources to fill any gaps.

This expanded, high-value content helps you manage, maintain and curate out-of-the-box detections and IOCs.

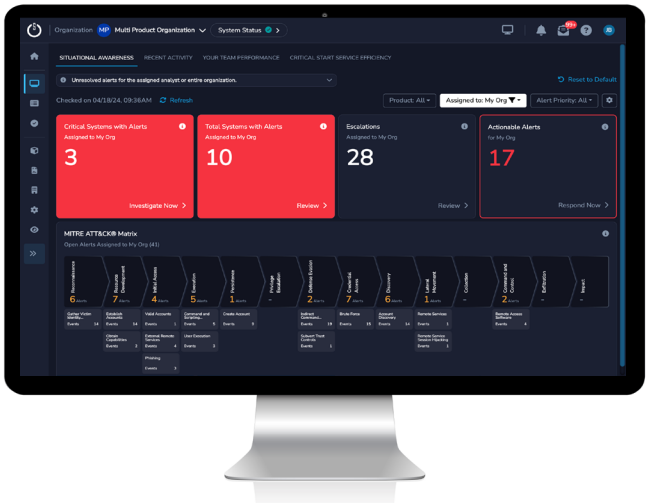

Fig 5: Critical Start provides a real-time view of your security posture mapped to the MITRE ATT&CK® Framework.

What this means:

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

2. HOW CAN I PREVENT MY SECURITY TEAM FROM BEING OVERWHELMED BY ALERTS?

Alert fatigue is a common problem for security teams, with many struggling to investigate the sheer volume of alerts generated daily.

According to IBM's 2024 Cost of a Data Breach report, security teams are doing much better at detecting and containing breaches "despite a stubborn skills shortage."

However, the average data breach cost had the most significant jump since the pandemic, reaching **USD 4.88 million** (an increase of **10%** in one year). Organizations still need support staying ahead of alert saturation to avoid costly data breaches while maintaining the flexibility to add more sources and monitor every alert generated without wasting time with false positives.

To enable your team to focus only on genuine threats and ensure nothing falls through the cracks, Critical Start leverages our trust-oriented approach to MDR by using our **Trusted Behavior Registry**® (**TBR**®) and our **Cyber Operations Risk & Response**™ (**CORR**) platform to auto-resolve false positives at scale, while our human-driven approach ensures every remaining alert is investigated, regardless of priority.

Our CTI team provides us with the latest threat intelligence to streamline investigation and response processes, and our security analysts implement a two-person integrity review before any action is taken.

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
- ✓ Relief from alert fatigue

How Much Risk Are You Willing to Accept?

MDR providers take different approaches to the alert saturation issue:

- Disabling inputs or altering 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.
- Focusing on only Critical alerts, leaving Medium and Low-priority alerts untouched. Unfortunately, threat actors know most organizations ignore the Mediums and Lows and use this to hide in their environments for months.

Critical Start's human-driven MDR approach ensures that our security experts provide nuanced threat detection and analysis, identifying complex attack patterns and behaviors that automated systems might miss. Our team adapts response strategies to fit your organization's evolving risk profile.

4. WHAT HAPPENS WHEN AN ALERT IS 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.

Critical Start uses multi-vendor flexibility and seamless workflow integration to help organizations turn broad, contextual SIEM alerts into definitive write-ups for executive and technical resources and provides clear guidance and active remediation support throughout incidents. (***Fig 6***)

We tailor Rules of Engagement (**ROE**) specific to your environment for your for specific hosts, devices, and users that cover notifications, escalations, and responses. We also provide guided response as appropriate for SIEM implementations to align with your business objectives.

Our investigation procedures show precisely what steps analysts took when investigating every alert and provide contextual, human-driven analysis (including using a two-person integrity review) augmented by automation to provide actionable findings and ensure every alert is resolved, regardless of criticality, resulting in a more robust security posture across your organization.

The Critical Start Security Operations Center (**SOC**) is open to multiple people on your team (not just a single point of contact) to ask questions and request response actions. Tailored information configured to your organization is available through our security value dashboards.

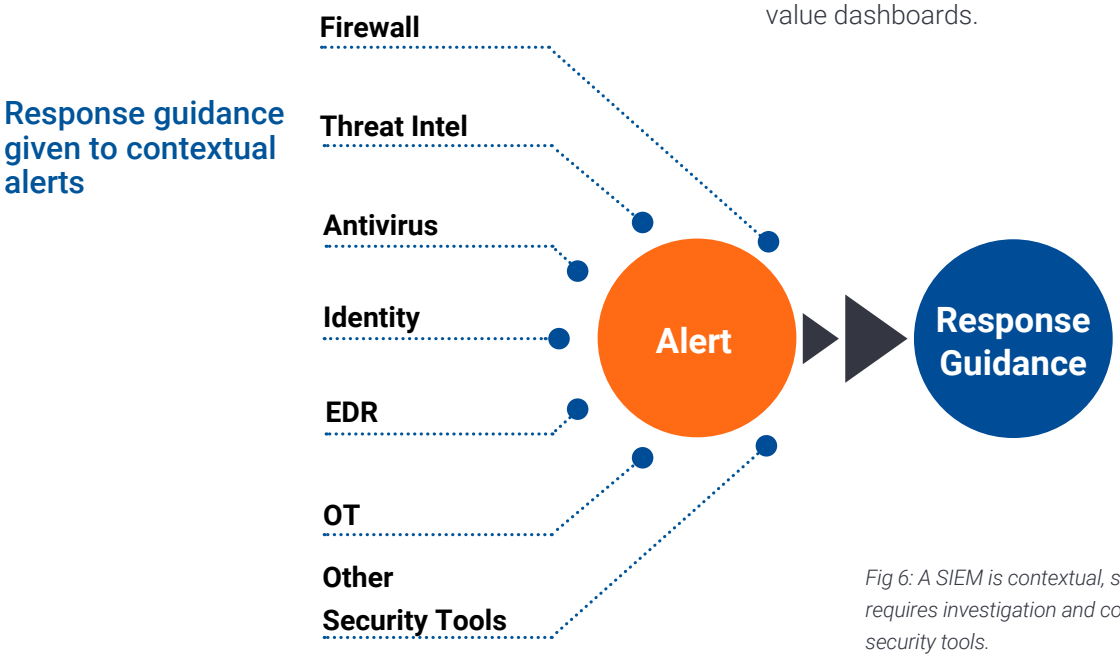

Fig 6: A SIEM is contextual, so effective response guidance requires investigation and correlation across multiple security tools.

4. REDUCING ATTACKER DWELL TIME WITH CONTRACTUAL SLAS

Critical Start has contractual SLAs of 10-minute notifications for Critical alerts and 60-minute or less **Median Time to Resolution (MTTR).**

Our **MTTR** is 60 minutes from when a threat alert is generated until a resolution action is taken. Resolution actions include:

- Response action on behalf of the customer
- 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 providers with experience responding to events using your full security toolset. They 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.

Managed SIEM and MDR Services
Provider Checklist

Use this checklist to compare key capabilities and features across providers to ensure you are getting a service that meets your needs and includes a dedicated team of security experts to help you derive maximum value from your SIEM investment.

CAPABILITY/FEATURE	CRITICAL START	Provider #2	Provider #3
CONTENT			
Deployment of use cases across various log sources and types of threats + compliance	✓		
Creation of detection content (translating alerts into 'English' to send back to the customer)	✓		
Customized log sources and content – 5 per contract year	✓		
Log source prioritization and management	✓		
Designing and building detection and reporting content for compliance	✓		
Alert enrichment with details about IPs, hashes, and domains to provide additional context	✓		
IT Help Desk	✓		
IT Ops	✓		
CONFIGURATION			
Installation + configuration of the log collection and management platform/SIEM, data sources; onboarding and configuration of SIEM UI	✓		
Configuration of APIs	✓		
Data onboarding and dashboards/app implementation for Supported Data Sources	✓		
Installation of vendor-supported apps for common security vendors' dashboards and reports	✓		
Configuration of log parsers for Supported Data Sources	✓		
Configuration of SIEM applications for SIEMs that have an app marketplace	✓		
Conduct or assist in configuring the source device to log to the SIEM	✓		
Custom SIEM dashboards for compliance	✓		
Architecture review of your existing configuration	✓		
OPERATIONS and PLATFORM HEALTH			
Log Health reporting for Supported Data Sources (including Zero-Log Ingest Alerts)	✓		
Spend-related support to optimize spend	✓		

Managed SIEM and MDR Services
Provider Checklist (*cont.*)

CAPABILITY/FEATURE	CRITICAL START	Provider #2	Provider #3
SECURITY ALERT MONITORING, THREAT DETECTION, INVESTIGATION, and ESCALATIONS			
24x7x365 real-time threat monitoring, detection, and response	✓		
Threat Intelligence operationalized with native detections that increase the effectiveness of your investment in detecting attacks	✓		
Playbook orchestration and alert routing to appropriate groups or users	✓		
Contractual SLAs of 10-minute notification for Critical alerts and 60-minutes or less for Time to Detect (**TTD**) and Median Time to Resolution (**MTTR**) for ALL alerts, regardless of priority	✓		
Monitoring and support for Supported Log Collectors	✓		
Two-person integrity review on every action to be taken	✓		
Direct, 24x7x365 collaboration with SOC analysts for rapid investigation and response	✓		
Analyst response actions or Incident containment on-the-go (e.g., host isolation, disabling user accounts, email removal) from your phone via a native MOBILE**SOC**® app	✓		
Custom rules of engagement for notification and response actions tailored to your environment	✓		
Automatic, facilitated, and managed remediation options	✓		
Retain technical artifacts such as policy configurations and custom detections	✓		
Provable metrics, peer benchmarking, shared customer learnings and best practices	✓		
NIST CSF maturity and MITRE ATT&CK® Framework coverage reporting for effective response	✓		
Complete transparency (full access to the CORR platform, investigation tools, and audit activity)	✓		
Detection personalization specific to your business, network appliances and users	✓		

Maximizing the ROI on your SIEM investment
Critical Start Security Services for SIEM Solution

What does it take to reduce cyber risk, prevent breaches, and stop business disruption?
Choosing a partner to enable better threat detection through SIEM telemetry readiness and MDR integration is not easy in a world where security leaders' time is also taken up with concerns about the

- Security risks of complex and disparate security environments
- Lack of resources to dedicate to Tier 1 and Tier 2 SOC support and repetitve (but necessary) tasks
- Increased risk of a breach due to alert fatigue, security coverage gaps, misconfigured logs, etc.
- Difficulty justifying security spend, measuring ROI, and presenting outcome-driven metrics to the Board and other stakeholders
- Talent shortage
- Threat of employee burnout

As you evaluate service providers to address your major pain points and unique needs, ensure they can also provide support to help with all of your other concerns, too. Use this Buyer's Guide for its expert insights and guidance to help streamline your evaluation and buying process, answer any questions you may have, and methodically check to see which providers can meet your needs.

Afterall, when it comes to optimizing the total value of your SIEM solution and uncovering hidden threats, it's not about choosing the right MDR provider — it's about choosing the MDR provider right for *your* organization.

For organizations seeking to unleash the full potential of their SIEM investment and proactively manage risk with a more comprehensive MDR service, **Critical Start Security Services for SIEM** offers a unified solution that combines improved threat detection and comprehensive coverage with streamlined cost optimization.

We collaborate closely with you and your team to understand your unique security needs and goals, allowing us to optimize your SIEM deployment for maximum risk reduction and ROI. By elevating MDR through our unique approach of integrating security intelligence, flexible deployment options, and human-driven expertise, we ensure that your organization receives unmatched protection and value. Our flexible pricing model and value-based approach ensure you receive the most effective solution for your specific requirements.

Contact us to learn more and discuss how you can achieve the full operational and 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.

> **Security Services for SIEM gives you the best of both worlds — the ability to focus your internal resources on projects that achieve your goals while adding an MDR provider to handle the urgent day-to-day tasks triggered by security alerts.**

Contact us for more information about Critical Start Security Services for SIEM, or schedule a demo at:

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