SIEM/MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

With Great Visibility.... Comes a Lot of Noise

Cybersecurity Starts with Visibility. Visibility Starts with SIEM.

A Security Information and Event Management (SIEM) system is the foundation of any cybersecurity program, but implementing and managing SIEM solutions can be complex and resource-intensive. Without the right expertise, it's easy to be overwhelmed by irrelevant data, false positives, and missed threats.

The challenge has only grown with the rise of disparate data sources across endpoints, on-prem networks, cloud infrastructure, and SaaS applications. While SIEM is essential, ask yourself if your organization needs a more comprehensive solution.

The Case for Managed SIEM Services

Many organizations are turning to managed SIEM services for the right mix of technology and expertise to enhance visibility and threat mitigation. But the market is crowded, with services like Managed SIEM, SOC-as-a-Service, and Managed Detection and Response (MDR), each offering different levels of coverage.

Still considering a DIY approach?

Here are the 3 most underestimated challenges of building and managing your own SIEM or SOC:

TECHNOLOGY

SIEM is just the start. You'll also need IDS/IPS, vulnerability assessment tools, EDR, advanced analytics, reporting tools, and more. Automation can help, but human expertise and process discipline are crucial to interpreting and acting on the data.

PROCESSES

Your organization needs detailed incident response playbooks for handling ransomware, malware, DDoS attacks, and other threats—24/7, because attackers don't take breaks.

PEOPLE

Staffing is the toughest part. A fully functional SOC requires skilled analysts across three shifts, plus Tier 2 and Tier 3 experts for threat hunting, malware analysis, and advanced response.

Key Benefits

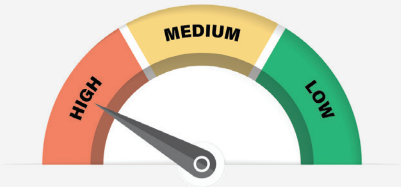
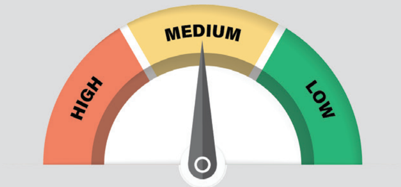
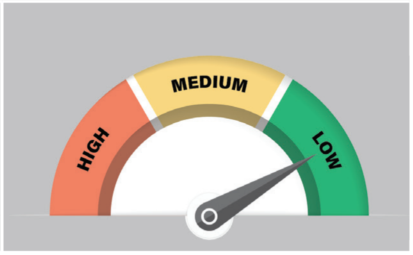
1. Reduced Complexity and Increased Scalability/Flexibility
2. Frees Up Valuable IT Resources
3. Experienced Security Professionals
4. Rapid Deployment
5. Improved Reporting and Analytics Capabilities

To learn more, call us toll-free at 866.490.MAIN (6246) or speak with your Mainline Account Executive.

SIEM/MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

It's a common misconception that a SOC can be effectively staffed with just three analysts—one per shift. This leaves no room for time off, training, or thorough forensic investigations. A more realistic approach requires a minimum of 8 to 10 analysts to ensure 24/7 coverage. Additionally, there are significant costs to consider, such as real estate for the SOC, telecommunications, and other hidden operational expenses. It's crucial to find the right SOC model that aligns with your organization's risk tolerance and operational needs.

Company Risk Profile for SIEM/MXDR

	Build	Buy	Partner
Pros	• Full control	• Full control and existing staffing • Established processes	• No up front costs • Immediate profit center • Fast time to market • Flexible business growth
Cons	• High up front Cost • Complex implementation • Long time to value • Staffing Challenges	• High up front cost requires financing • Business and IT integration • Slow time to market • Staffing challenges	• Business and IT integration
Risk Profile			

Partnering with Mainline's Cyber Ninjas not only removes the stress of building and managing a SOC but also eliminates the challenge of staffing. Our Cyber Ninjas hold top-tier industry certifications and continuously expand their expertise to meet evolving requirements. Whether you need fully managed, co-managed, or Level 3 Analyst support, we provide a team of security experts equipped with the right technology and proven processes, tailored to your specific needs. It's clear why a managed SIEM/MXDR solution from Mainline offers both practical and cost-effective advantages, delivering quick time-to-value while addressing today's complex IT security challenges.