MANAGED SIEM

EVALUATION CHECKLIST

Netsurion®

Build your selection process with these strategic and tactical criteria to ensure success. This checklist was developed to guide you in addressing the range of requirements for your co-managed SIEM (Security Information and Event Management) project. Optimize your solution today to future-proof for tomorrow as your requirements, and cybersecurity threats, evolve over time.

1. Communicate Cybersecurity Risk to Executives

This checklist assists you in framing cybersecurity risk in business terms and not technical terms to involve stakeholders, identify the most crucial requirements, and gain funding. Organizations that are too conservative with an aversion to risk might overlook business advancements and opportunities, while a company that ignores business and technology risk is sure to face the consequences.

- ☐ Assess your cyber risk in view of your industry and its past cybersecurity incidents
- ☐ Determine your risk appetite regarding lost brand reputation or intellectual property
- ☐ Calculate the cost of downtime per hour to assist in ROI calculations
- ☐ Identify any compliance mandates or frameworks applicable to your organization
- ☐ Involve cross-functional executives across IT, security, HR, operations, and sales for example
- ☐ Position a SIEM solution as a cybersecurity investment that drives confident business growth
- ☐ Blend decision criteria like cost, control, onboarding, flexibility, and ROI

2. Solution Exploration and Planning

Enhance visibility and continuous monitoring for advanced threats in real time. If your organization does not possess the staff or skills for a SIEM solution, augment your capabilities with a co-managed solution. Plan ahead to avoid unnecessary operational and technical surprises.

- ☐ Identify business and technical requirements and stakeholders
- ☐ Evaluate whether you lean towards a DIY or Co-Managed SIEM solution
- ☐ Determine your organization's willingness to move log data off premises
- ☐ Document any findings if your organization has already attempted a SIEM implementation
- ☐ Ensure your project is approved and funded up front
- ☐ Assess your organization's cybersecurity maturity and readiness for a SIEM solution
- ☐ Develop qualitative and quantitative measure of success for the SIEM decision

3. SIEM Capabilities

Start developing your request for information (RFI) / request for proposal (RFP) with these crucial SOC-as-a-Service and SIEM requirements. Below are the comprehensive capabilities most often associated with a "next gen" SIEM solution.

- ☐ Log correlation and management
- ☐ 24/7/365 visibility and monitoring by a dedicated SOC
- ☐ Built-in Application Control for real-time endpoint response
- ☐ Integration of user and entity behavior analytics (UEBA)
- ☐ Proactive human-led threat hunting
- ☐ Security orchestration and automation
- ☐ Anomaly detection
- ☐ Known threat techniques and adversary actions mapped to reports and log correlation (MITRE ATT&CK)
- ☐ Addresses compliance management such as PCI DSS and HIPAA
- ☐ Long-term log and event storage, with an eye to compliance requirements
- ☐ Customer service in various formats
- ☐ Reports and dashboards for both executives and users

4. Solution and Supplier Selection

This checklist assists you in navigating the diverse range of technology and service provider choices while making an informed decision.

- ☐ Identify pilot or trial criteria with internal stakeholders
- ☐ Create a project plan for the trial as well as the future implementation
- ☐ Conduct pilot/demo/proof-of-concept (POC)
- ☐ Develop a short list of vendors that meet your customized criteria
- ☐ Document your "must-have" criteria from "nice-to-have" considerations
- ☐ If you plan to use one, create an RFI/RFP tailored to your organization's specific requirements
- ☐ Scope SIEM integration with your existing security products
- ☐ Determine if your organization will purchase via a channel partner or direct with a vendor
- ☐ Notify the selected vendor as well as those that were not selected of your decision
- ☐ Communicate the selection decision internally and thank those who participated in the evaluation process

5. Implementation and Onboarding

Apply knowledge gained regarding your organization, cybersecurity objectives, IT staffing model, and future requirements to apply the best-fit solution for your business.

- ☐ Inform employees of your "go live" date – and remember to celebrate
- ☐ Integrate log telemetry across apps, cloud, networks etc. for comprehensive visibility
- ☐ Implement sensors on all applicable servers and workstations
- ☐ Enforce least privilege and "need to know" access for users
- ☐ Train end users on the system and processes and involve executives in high level communication
- ☐ Determine who will review and follow up on future incident reports
- ☐ Tune the new SIEM solution or work with your third party provider to configure the system
- ☐ Pull reports and dashboards regularly from the Console or meet with your MSSP to review
- ☐ Follow up on alerts and threat mitigations quickly to minimize damage and data theft

6. Ongoing Operations

The wrong selection can have a long-lasting impact, be costly to maintain and support, and time consuming to tune, which is why many SIEM deployments end up abandoned and ROI unmet. Remain vigilant and prepared even after your startup and implementation. Cybersecurity is a journey, not a destination. With a co-managed service, you benefit from the proven track record of hundreds if not thousands of customer experiences.

- ☐ Meet regularly with your SIEM provider and customer success manager over time
- ☐ Implement Multi-Factor Authentication (MFA)
- ☐ Restrict users with a need-to-know using Role-based Access Controls (RBAC)
- ☐ Tune Application Control to block endpoint threats
- ☐ Integrate with existing applications and systems like remote monitoring and management (RMM) tools
- ☐ Continue to solicit key stakeholder feedback as your security posture evolves
- ☐ Add more endpoints and servers over time as needed
- ☐ Share results with your executives to show time-to-value

CONCLUSION

It is often unrealistic for most small-and-medium-sized businesses to hire, train, and retain in-house SOC staff and implement the state-of-the-art threat intelligence provided by SIEM and advanced Endpoint Protection solutions necessary to be effective. Attempting to implement DIY cybersecurity can result in underutilized security software that becomes shelfware and leads to gaping vulnerabilities.

Make a smarter investment with a Co-Managed SIEM from Netsurion. Our adaptive security approach tightly integrates SIEM, Endpoint Protection, and SOC-as-a-Service to deliver the optimal combination of people, processes, and technology. We enable you to predict, prevent, detect, and respond to security incidents when every minute matters in reducing attacker dwell times.

Find out more at
www.Netsurion.com

ABOUT NETSURION

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's Managed Detection and Response includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Extended Detection and Response (MXDR). Learn more at www.netsurion.com.


Netsurion®