Cybersecurity Best Practices Guide

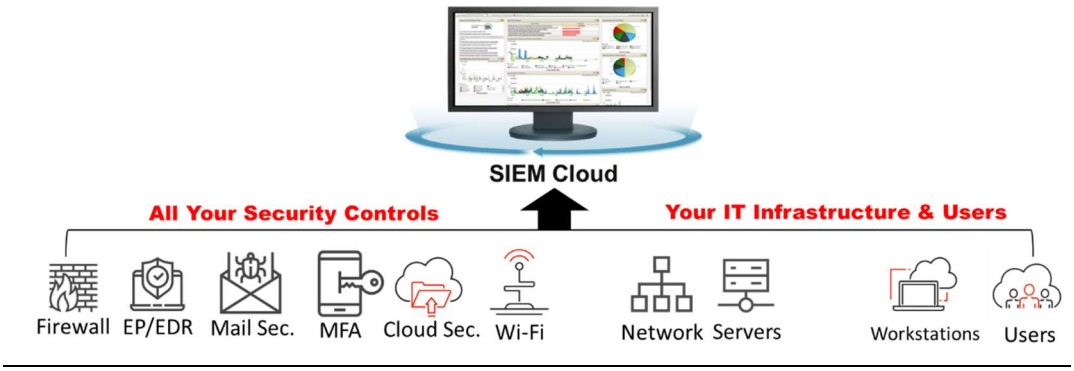
4 Reasons Companies Need a 24x7 SIEM-SOC

SIEM-SOC Overview

SIEMs provide the best **OVERALL** security monitoring of a company's security system. SIEMs provide top-level security MDR with the ability to broadly detect threats and attacks, analyze the attacks, prioritize attack severity, and determine appropriate mitigation options.

SIEMs also enable regulation compliance, support cyber insurance requirements, and satisfy the overall objectives of an **Information Security Management System (ISMS) process** by providing **Top-Level Detection and Response Solutions.**

SIEMS are managed by a **SOC Team** to configure, tune, and monitor for threats, attacks, and compromise. At a high level, SIEMs analyze Indications of Attack (IoA), discover Indications of Compromise (IoC), hunt down threats and discover vulnerabilities, alert and recommend remediation, contain attacks, and enable remediation.



SIEMs Enable Full System Monitoring

Unlike **Individual Security Product Monitoring or XDR Monitoring**, a SIEM is a tool that Ingests Security Information/Event Information from all security and core IT systems to provide real-time monitoring, alerting, and remediation information.

To accomplish this, SIEMs monitor Information gathered from ALL security devices and controls, core IT like servers and networks, vulnerability scans, threat feeds, and user behavior. The SIEM then correlates information and events from all sources, analyzes the information looking for IoAs & IoCs (using Std and Customized Rules & AI/ML). Threats attacks are blocked, and customers alerted. Alerts are generated and analyzed by a 24x7 technician who engages in **Threat Hunting** and **Forensics** to provide **Root Cause Analysis** and **Informed Remediation Information** to the company.

What Analysts Say about SIEM/SOCs

Managing cybersecurity is an overwhelming job, especially when trying to accomplish **real-time monitoring** of all related security information.

The **Cybersecurity Skills Shortage**, coupled with increasing levels of specialization required to manage a growing security infrastructure (like a SOC) makes IN-HOUSE management almost impossible even for enterprises. As a result, smaller companies have no chance.

Companies trying to staff all security themselves are experiencing skill shortages, high costs, training issues, and problems hiring or maintaining staff. Gartner's conclusion is that outsourcing SIEM SOCs to MSSPs is typically the right idea for nearly all small to medium-sized companies.

Why SOC/SIEM: 1a) Regulations

Generally, the biggest driver in utilizing a SIEM-Based SOC is **Regulation Compliance**. Regulations all require 3 major components of compliance: 3rd Party Risk Assessments to define gaps and help with planning, appropriate security controls, and active security management.

Management consists of the use of a **Risk Management Process** to assess, define, implement, and manage your security through prevention, detection, and response. Compliance is met through security monitoring that actively manages your controls and provides incidence response capability. **Outsourced Managed Security** through a SIEM SOC achieves the highest level of security monitoring attainment.

Why SOC/SIEM: 1b) Cyber Insurance

Along with Regulation Compliance, **Cyber Insurance** is increasing the requirements to qualify for policies annually. Cyber Insurance is becoming a major driver of increased security.

Insurance companies are losing money, claims are going up and they must decrease their risk. In result, cyber insurance companies are counteracting these changes through **higher rates** and **Increased requirements to qualify** for insurance. For companies buying cyber insurance, the need for Regulation Compliance-Level Security will become the standard to qualify.

Why SOC/SIEM: 2) Prevent Evasive Attacks

Today's cyber-attacks are highly evasive, eluding preventative controls. Over **20% of the attacks remain undiscovered** inside victim systems for months and another **10% are undiscovered for years**. APTs have become the norm for advanced attacks and strong detection solutions are needed, since many infections are not prevented.

SIEMS can catch attacks that move slowly through your IT systems. SIEMs correlate information and events from multiple sources, use AI/ML to look for IoA and IoC, and catch lateral movement of attacks that are part of APTs.

Why SOC/SIEM: 3) Balanced Security

Why should your company aim to achieve balanced security? Because attackers use the weakest link to breach your security. The goal of balanced security is to create the highest level of security with the least amount of cost. This is accomplished through knowing where your gaps are and prioritizing them, adding detection and response to your preventative solutions, and ensuring your security is tailored to your company's particular situation. The ability to detect and respond comes from a monitoring and detection solution like a SIEM/SOC.

Why SOC/SIEM: 4) Complete Picture

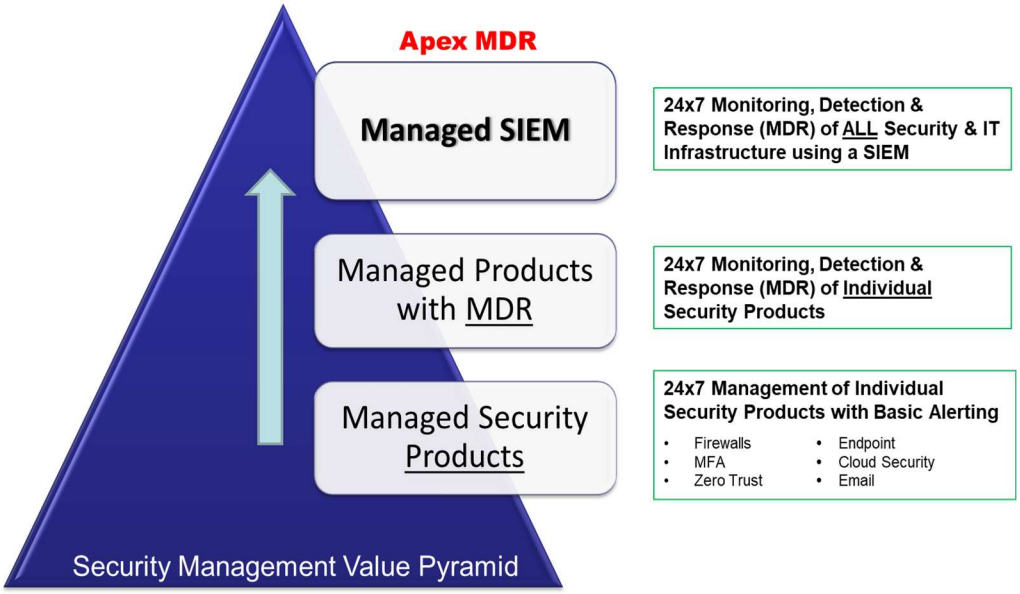
Information from any one (silo) source does not reveal overall risk. Single silo product capabilities don't provide a correlation of this information into one picture big picture of overall security and IT information. Likewise, individual security products don't generate analysis, alerts, and compliance-level reports of all IT information using **advanced rules** and **AI** to look for threats and attacks.

Ultimately, adequate threat/attack detection is accomplished by monitoring, correlating, and analyzing events and information from ALL your security and IT infrastructure. This includes real-time information from all your security products, your key IT (including network traffic, user access, servers, workstations), and all cloud and on-premises solutions.

SIEM-Based SOC provides a **complete picture of your security posture**. The monitoring, detection, and response (MDR) capabilities you get from each individual security product are silos of information (if they exist at all) and not a complete picture of your security.

Apex MDR = Managed SIEM/SOCs

Managed SIEMs are APEX solutions. Like the Great White Shark, they consume ALL security information and key IT system information in real-time. SIEMs are a compliance level solution that provides compliance-level assessments and reporting, correlates, analyzes, and alerts a SOC Team, allows for threat hunting and forensics, and helps define desired remediation, including **Threat Blocking** and **Long-Term Remediation.** SIEMS can work with all security products and XTM systems to provide a true top-level solution.



Security Management Value Pyramid

Let us put the various **types of Security Management** into perspective.

Starting at the Bottom:

Management of Individual Security Products

24x7 management of individual security products provides basic security alerting monitoring and offloads the burden of defining policies, configuration, management, maintenance, and adjustments. This security control management provides **individual silos of security management,** reducing hiring and training which allows the ability to focus on other IT topics.

Next up the Value Pyramid is Managed Products with MDR

24x7 Monitoring, Detection, and Response (MDR) of individual security products provides elevated management, monitoring & alerting using advanced security controls like EDR (versus basic Endpoint security). MDR requires security products that offer **advanced alerting of threats** and provide **threat hunting**, **forensic** and **remediation** tools.

A Managed SIEM

24x7 Monitoring, Detection & Response (MDR) of ALL security & IT infrastructure using a SIEM Is designed to monitor all security, key IT, and users to provide a complete security picture in real-time. With SIEM, correlation rules can be tailored, AI can be deployed, and alerts can trigger **Threat Hunting, Alerting, and Threat Containment.** When used in conjunction with Managed Services for products, overall security management, detection, and response can be elevated.

What's Needed to Manage a SEIM?

If you did try to manage your own SIEM you would need the right SIEM and the right team. This is qualified through redundantly trained expert staff sufficient to manage a **24x7 SIEM**, providing ongoing monitoring and adjustments to incorporate false positives and negatives. This staff must specialize in monitoring, analysis, threat hunting, and remediation.

Extensible Managed SIEM SOC with Managed Security Stack

eSecurity Solutions provides a full **Vendor-Agnostic Extensible Managed SIEM SOC** integrated with managed security products. eSecurity SOC Team provides value-added Services and support to our customers including **Pre-Implementation Baseline Reports**, **Ongoing Vulnerability Assessments, Compliance-Level Reports**, and **Advisories** during times of increased threats and attacks.

We have a dedicated team managing a full SIEM which includes **Host Vulnerability Assessments, File Integrity Monitor (FIM), and User Behavior Analysis (UBA).** Our SIEM-Based SOC promotes real-time monitoring of all multi-vendor security controls and key IT assets (like servers, PCs, networks, cloud) to provide event and information monitoring, correlation, analysis, threat hunting, alerting and response. We also offer optionally managed security controls in the areas of **Firewalls**, **Wi-Fi**, **EP**, **EDR**, **Email**, **MFA**, **Identity Management**, **Cloud Security**, **Zero Trust**, **Security Training**, and **Phishing Testing.**

Why eSecurity Solutions

We provide **Compliance-Level Security Solutions** for companies of all sizes. Our solutions start with Risk Assessments to define top priority gaps and solutions. Then, after defining the right security controls, we provide complete managed security solutions highlighted by the SIEM SOC. eSecurity Solution's mission is to provide full **Information Security Management System (ISMS) Cycle Solutions**. Our solutions are aligned with our customers' need to be compliant and secure.

With over 20 years of cybersecurity focused solutions and a broad customer base, eSecurity Solutions is a trusted expert in the security industry. We would love to start a conversation with you about the value eSecurity Solutions can bring to your company's security plan by becoming your trusted security partner.