What is SIEM?

OVERVIEW

At its core, Security Incident and Event Management (SIEM) solutions offer organizations the ability to collect, aggregate, analyze, and store logs of network traffic and event data from various sources, including network devices, endpoint security, and intrusion prevention systems. SIEM technology enables businesses with the ability to monitor all access points and threats in one centralized location, freeing up time for IT security professionals to focus on other tasks.

2,244

cyber attacks occur every day

66%

of enterprises respond to between 1 and 25 cybersecurity incidents per month

$3.86M

is the average total cost businesses will spend responding to a data breach

Evolution of SIEM.

TRADITIONAL SIEM

The traditional SIEM solution was first brought to the information security market nearly two decades ago. Bringing together SEM (Security Event Management) and SIM (Security Incident Management), traditional SIEM solutions radicalized the way businesses managed cybersecurity.

NEXTGEN SIEM

Today's SIEM solutions have had to go beyond the traditional SIEM features of the past. Now, a modern NextGen SIEM solution includes extended functionalities like Security Orchestration Automation and Response (SOAR), User Event Behavioral Analysis (UEBA), and SOC-as-a-Service.

Features of NextGen SIEM.

SIEM solutions offer features that equip businesses with the necessary tools to gain a holistic insight into their attack surface, mitigate increasing risks, maintain compliance, and have peace of mind. Typically, the features of a SIEM solution will include the following:

LOG MANAGEMENT

To keep critical company assets secure and satisfy regulatory compliance requirements, log management must remain top of mind for businesses. In fact, according to the Center for Internet Security (CIS), the collection, storage and analysis of logs is a Critical Security Control. Without a robust log management solution in place, organizations.

REAL-TIME EVENT CORRELATION

With real-time event correlation, businesses can automatically sift through hundreds of thousands of network events, quickly isolate the ones that may pose risk to the business, and respond accordingly. Not only does this SIEM feature enable a deeper detection by providing IT staff with the ability to correlate seemingly harmless events.

SECURITY ORCHESTRATION & AUTOMATION

A key aspect of simplifying cybersecurity management is automating incident response workflows through SOAR. With Security Automation and Orchestration features, SIEM solutions allow for deeper automation of security monitoring, reporting and remediation tasks to dramatically increase response times to threats.

USER & ENTITY BEHAVIORAL ANALYSIS

Year after year, humans pose one of the largest threats to an organization's security. Even with proper security awareness training and security measures in place, humans are still likely to fall victim to a cyber attack. This means that businesses need a way to quickly identify and remediate any user or entity.

UNIFIED SECURITY DASHBOARD

Having the ability to monitor and control virtually every facet of your company's security efforts from a single pane of glass is essential, especially when it comes to measuring business impact. A SIEM solution should offer highly customizable dashboards that allow you to monitor security and performance of data for virtually every component detected in your network, including unified analytics across all environments, platforms, network devices, users, applications, and geographic locations in real-time.

OUT-OF-THE-BOX COMPLIANCE REPORTING

Whether your business is required to comply with HIPAA, PCI DSS, NIST 800-171, CMMC, ISO 27001, SOX, FISMA, GDPR or the plethora of other regulatory frameworks out there, maintaining that compliance is not an easy task. With a SIEM solution like ArmorPoint, you'll gain access to out-of-the-box reporting that allows you to quickly and automatically pull the required network data and information to demonstrate compliance at any time. Not to mention, you have the ability to export your logs instantly with ArmorPoint.

VULNERABILITY MANAGEMENT

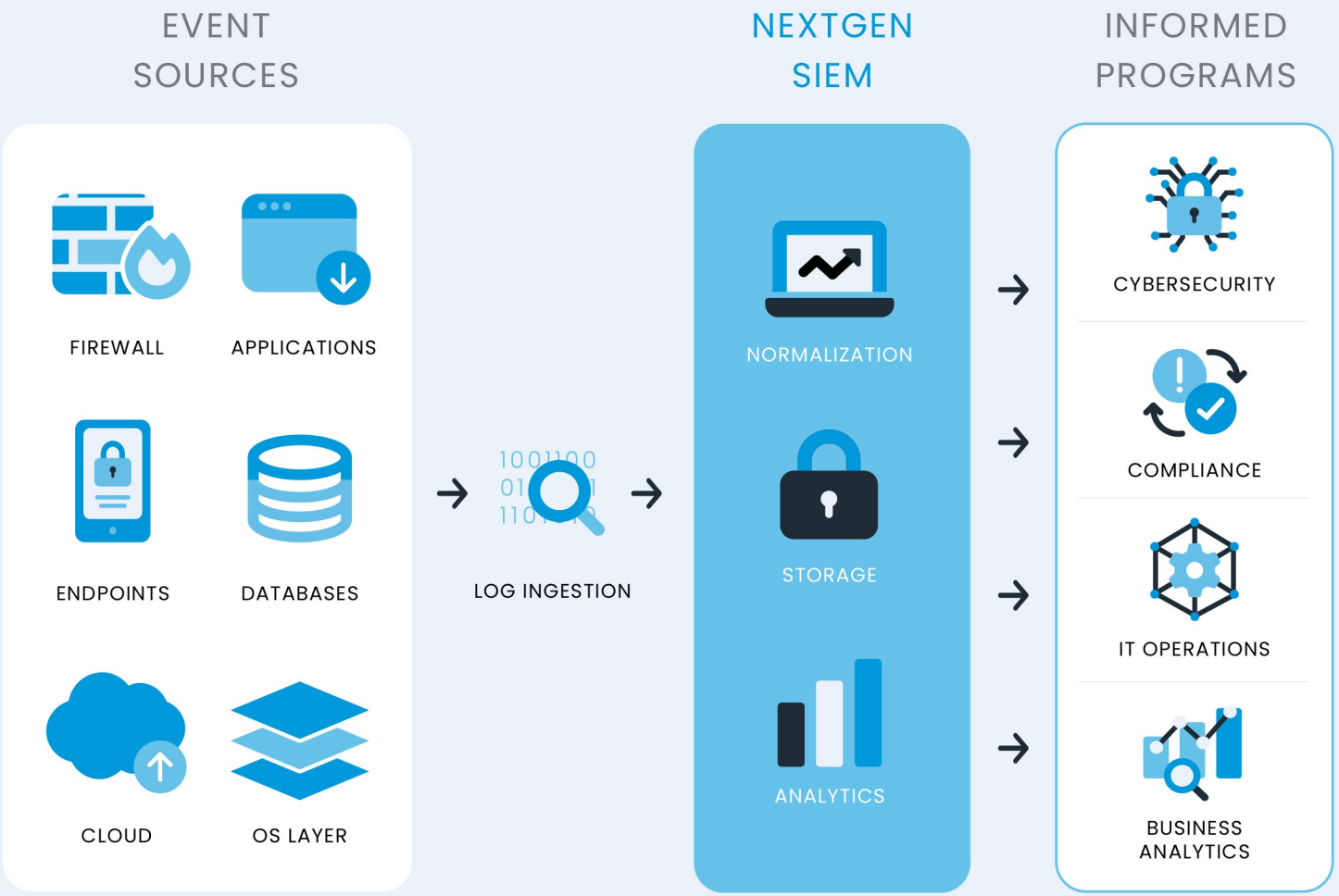
A SIEM's vulnerability management capabilities allow you to continuously hunt your network for malicious activity, securely mitigate threats, and use the knowledge gained to optimize response methods and processes in the future to completely minimize network vulnerabilities. Through vulnerability scanning, remediation strategy planning, and risk scoring, businesses will have a clear way to identify, minimize, and respond to threats in a way that will minimize the vulnerability's impact on the business.

FILE INTEGRITY MONITORING

While UEBA automatically detects and monitors all user activity on the company network, regardless of device, application, or geographic location to thwart any malicious or inadvertent activity that could put critical company files and applications at risk. With fi le integrity monitoring, businesses will have the intelligence and agility needed to detect and mitigate threats that could compromise the integrity of the files.

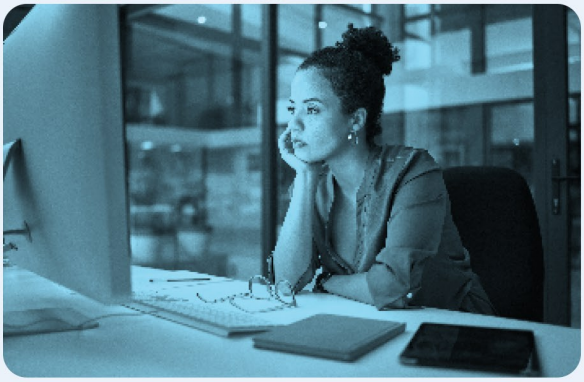
SIEM Architecture.

Modern NextGen SIEM solutions vary in quality, but they are built to function in the same way. First, the SIEM solution will ingest data across your entire organization through various collectors. This includes logs from security devices, network devices, cloud environments, applications, workstations, and servers. Once collected, the correlation engine will then aggregate, normalize, and analyze the event log data, which then kicks off the main features of the SIEM: threat detection, alerts, reports, forensic analysis, automated responses, and custom dashboards. Finally, the logs are sent to a storage database for at least one year.



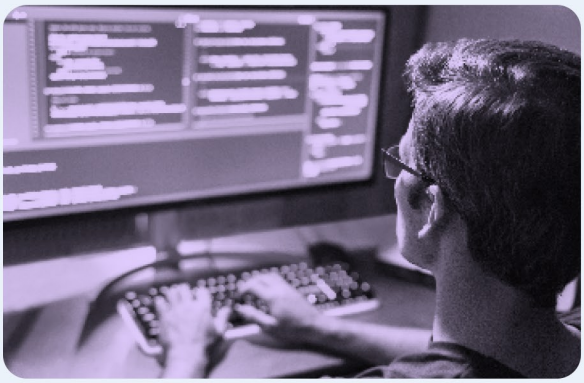
SIEM Use Cases.

SIEM solutions offer features that equip businesses with the necessary tools to gain a holistic insight into their attack surface, mitigate increasing risks, maintain compliance, and have peace of mind. Typically, the features of a SIEM solution will include the following:



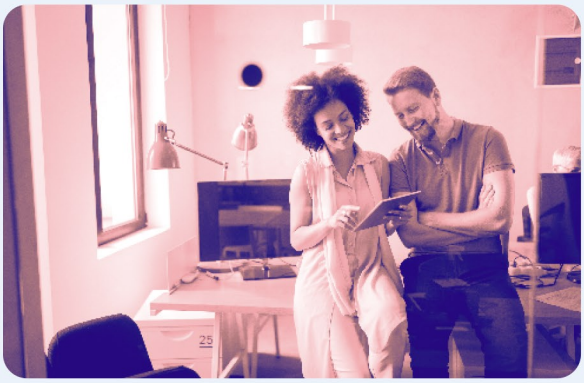
SIEM for Compliance.

Whether it's the strict requirements, lengthy legalese, or steep fines and penalities, hearing the word "compliance" makes most people uneasy. With out-of-the-box and custom compliance reporting available, SIEM solutions help businesses streamline their compliance efforts. Preparing for an audit like PCI DSS, HIPAA, SOX, FISMA, ISO 27001, GDPR, or CMMC is streamlined because you'll have instant access to your logs.



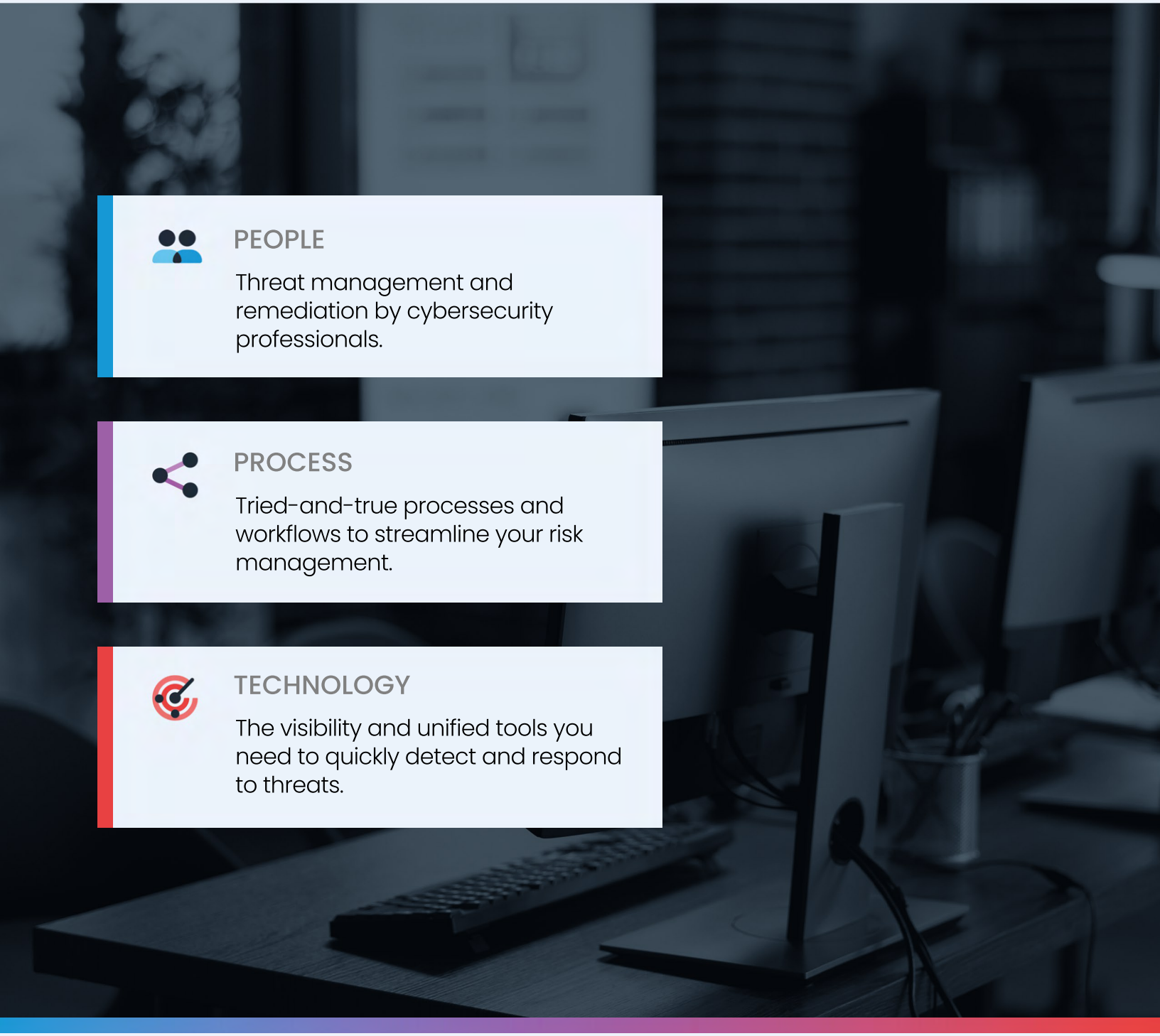
SIEM for Threat Intelligence.

When it comes to an organization's security, being proactive rather than reactive is always a best practice. While you should always have an incident response plan in place, having a robust threat intelligience solution that keeps you ahead of security incidents is paramount. Leveraging your SIEM solution for threat intelligence is a great way to gain holistic insight into the threats you're up against. SIEMs typically can integrate with threat intel.



SIEM for Incident Response.

Regardless of how robust your information security management system is, all businesses are susceptible to falling victim of a cyber attack. However, the hard truth is that when many companies experience a malicious incident, their incident response plan is inadequate. SIEM solutions offer a streamlined, automated approach to incident response -- an approach that can decrease the time it takes to contain and remediate the incident.



PEOPLE

Threat management and remediation by cybersecurity professionals.

PROCESS

Tried-and-true processes and workflows to streamline your risk management.

TECHNOLOGY

The visibility and unified tools you need to quickly detect and respond to threats.

Whether you're an individual, small business, or large corporation, our team of experts can help safeguard your online presence and ensure your peace of mind.

Take control of your online security today and contact us for expert guidance and support.

- @ArmorPoint
- linkedin.com/company/armorpoint
- ArmorPoint

armorpoint.com