tracealert

Gain access to the data you need to proactively investigate and resolve unauthorized network events and anomalies.

Network vulnerabilities exist and cyber threats continue to grow.

Networks are larger and more complex than ever before, and protecting them against increasingly sophisticated cyber threats is an ongoing challenge for organizations today. Complex attack methodologies coupled with advanced social engineering attacks have resulted in the grim reality that vulnerabilities exist in every organization, regardless of size.

To protect critical information assets, intellectual property, maintain real-time visibility into IT environments and avoid business disruption, Security Information and Event Management (SIEM) solutions have become a necessary element in the security strategy of organizations today.

The limitations of traditional SIEMs.

By centralizing and processing data from a wide range of sources, SIEM solutions offer a more advanced approach to identifying and managing network security threats. However, most organizations generate thousands of event and system logs every second — potentially creating millions of security events per day.

For this reason, traditional SIEMs can be difficult to utilize and extremely time-consuming to maintain. A certain level of expertise as well as extensive IT resources are required to operate the system, continually monitor event and system logs, and identify potential security threats. Not to mention the expense and time associated with configuring rules to ensure the system remains up-to-date with the latest threat information.

Furthermore, due to the massive amounts of data produced daily, IT departments are often overwhelmed by the sheer number of security alerts, only to realize many of which are false positives. Unfortunately, this can result in an organization's inability to identify relevant security threats and lead to undetected data breaches.

Detect incidents that would otherwise remain unexposed.

With TraceAlert, you have access to an affordable, fully managed SIEM solution that empowers you to instantly improve network security. No longer do you need to sift through massive amounts of data related to potential security threats and attempt to perform meaningful analysis.

Our cloud-based solution enables your organization to automatically address growing cyber threats and quickly respond to critical network security vulnerabilities, all without having to invest in expensive infrastructure, hardware, or additional IT resources.

Features and Benefits

- Fully managed SIEM solution — from rule configuration to data analysis to alerts to ongoing maintenance, we manage everything for you
- Our team of cybersecurity experts actively monitor your event and system logs 24 hours a day, 7 days a week, 365 days a year
- All extraneous data is filtered out, which means the only alerts your organization receives are those that are relevant and associated with credible security threats
- Detailed reports are delivered directly to you that include actionable information and instructions to help you respond quickly to all identified vulnerabilities
- IT resources are able to focus on relevant alerts and as a result, have more time to devote to other strategic initiatives
- Suspicious trends and behaviors are identified as they occur and rules are updated accordingly
- Specifically designed to help your organization address complex regulatory guidelines and risk management needs