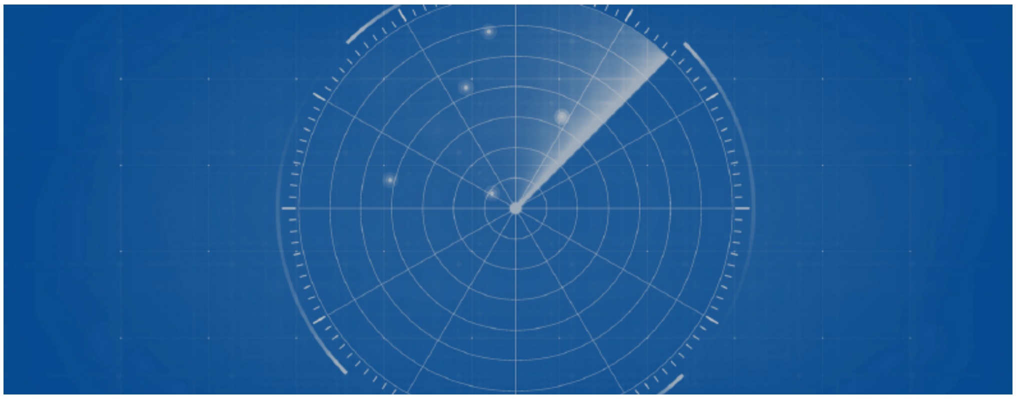
SIEM
OKIOK

MONITORING MADE EASY

Implement a managed, hassle-free monitoring and incident response solution



Today, all organizations, large and small, need to implement effective monitoring of their information assets to detect suspicious activity as early as possible. Moreover, it is not enough to detect suspicious activity, it is necessary to be able to quickly analyze it in order to make quick decisions and apply effective preventive measures as soon as possible.

One of the problems often reported by our customers is that their monitoring service provider does not react quickly enough to suspicious situations, while any delay can lead to catastrophic impacts.

Traditional SIEM solutions require specialized expertise and attention to achieve and maintain state-of-the-art detection capabilities and require a dedicated team of analysts to evolve the solution to keep it effective as well as to operate it on a daily basis.

Unfortunately, the challenge of hiring and maintaining a specialized team makes it nearly impossible for most companies to implement such solutions.

A simple and effective solution

The OKIOK SIEM solution is a managed incident detection and response solution offered in service mode, which puts high-performance, constantly evolving technology at your fingertips, taking full advantage of the experience and expertise of the OKIOK penetration testing team.

Continuous protection, every day, 24 hours a day

Logs from your sources are ingested, consolidated, normalized, stored, and analyzed 24 hours a day.

Risk situations are automatically detected by applying sophisticated analysis algorithms, based on use cases drawn from our experience and the MITRE ATT&CK reference framework.

The resulting alerts are prioritized and enriched to include the contextual information needed for a quick and efficient resolution and automatically forwarded to your technical team through the agreed upon channels.

The solution can automatically take action on your various platforms to limit the impact of an attack.

OKIOK's expertise at your service

The OKIOK team develops and evolves monitoring cases based on the concrete knowledge gained in the field during the hundreds of intrusion tests and incident response mandates carried out each year.

Plus, you can count on complementary professional services from the industry's leading experts to support your team and help you make informed decisions. These services range from in-depth event analysis to supporting your major incident response strategy.

Eliminate the human factor

Quickly analyzing suspicious activity, making the right decisions and initiating critical actions are not easy tasks for even the most seasoned analysts. Malicious software is becoming increasingly sophisticated and effective at hiding its tracks and confusing analysts.

In this regard, we believe that we should aim to eliminate the human factor in event analysis in addition to automating responses that can help reduce risk by eliminating response times.

Eliminating the human factor in the analysis, decision and response chain helps reduce errors and initiate critical actions in the shortest possible time.

OKIOK SIEM

Automate to respond quickly

The OKIOK SIEM solution includes Security Orchestration, Automation and Response (SOAR) features that automate responses to alerts and events to reduce risk and maintain control over the potential deluge of alerts.

Eliminate the cost and hassle of hiring and retaining staff

The OKIOK SIEM solution allows your company to realize even greater benefits by allowing you to focus your most precious resource, human capital, on value-added tasks related to your mission.

Robustness and virtually unlimited ingestion capacity

The OKIOK SIEM solution is a pure cloud solution that takes advantage of the robustness and virtually unlimited capacity of the AWS cloud infrastructure. In fact, the solution adapts to your company's data flow, whether it is small or large.

In addition, the solution is designed so that no information is lost, even in the event of a network or technology failure.

Compliance and security of your data

Sleep easy, your data is adequately protected in transit and at rest when supported by SIEM OKIOK. In addition, data is stored in data repositories located in your country or in the area of your choice to ensure compliance with normative and required hosting frameworks.

Get results quickly

The OKIOK SIEM solution can be implemented very quickly by having our experts integrate your city assets and infrastructures with the log collection and consolidation service.

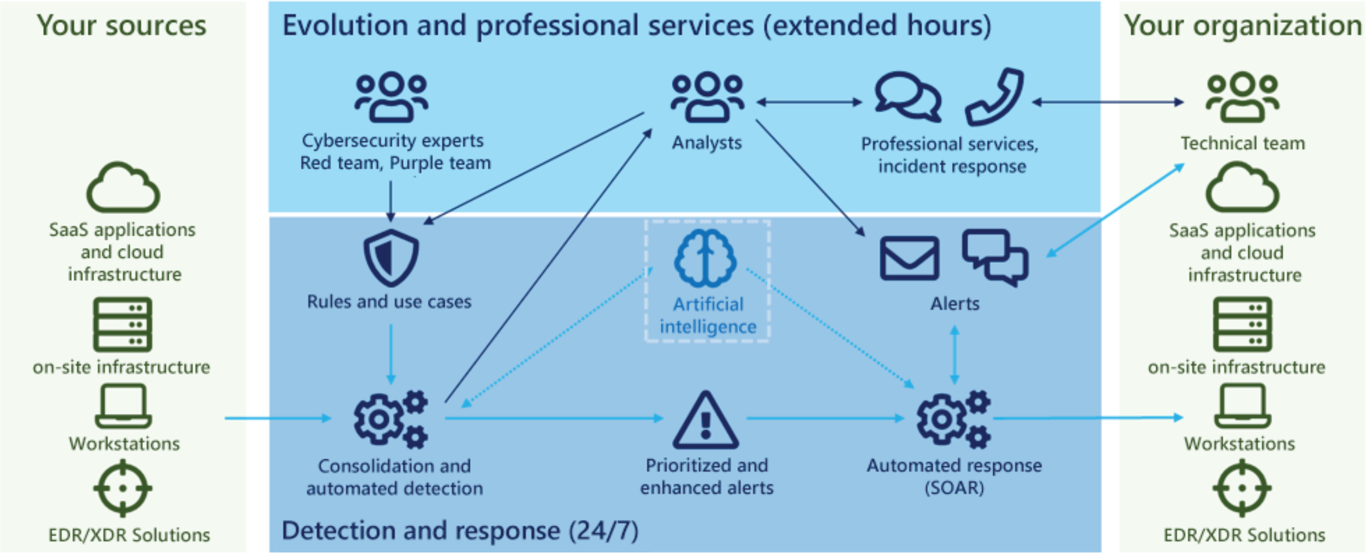
Integration capacity

SIEM OKIOK™ integrates easily with virtually any information system and infrastructure component. The solution can ingest all standard and non-standard log formats, including logs produced by legacy systems, gatekeepers and infrastructure components such as Active Directory (AD), LDAP directories, SQL databases, as well as for cloud applications and infrastructures such as Office 365, Microsoft Azure, Google Cloud Platform, AWS, etc.

This flexible architecture allows SIEM
OKIOKTM to easily adapt to any existing and future technical environment.

EDR and XDR solutions

SIEM OKIOK integrates with EDR / XDR solutions such as Sentinel One and takes advantage of their local detection and automated response capabilities.


Your sources
SaaS applications and cloud infrastructure
on-site infrastructure
Workstations
EDR/XDR Solutions
Evolution and professional services (extended hours)
Cybersecurity experts Red team, Purple team
Analysts
Professional services, incident response
Rules and use cases
Artificial intelligence
Alerts
Consolidation and automated detection
Prioritized and enhanced alerts
Automated response (SOAR)
Detection and response (24/7)
Your organization
Technical team
SaaS applications and cloud infrastructure
on-site infrastructure
Workstations
EDR/XDR Solutions

OKIOK is a leader in the field of information security. Since 1973, the company has distinguished itself through the excellence of its products and the high quality of its services. OKIOK offers a wide range of integrated solutions designed to meet the needs of organizations of all sizes.

www.okiok.com | info@okiok.com | 1 877 561-1681

Revision date: December 2022 Trademarks are the property of their respective owners