Infigo
MODULE_01XDF_99_3
Infigo
SIEM
MODULE_01XDF_99_3
Security and compliance with multitenancy on-premises and in the cloud
www.infigosiem.com

# What Can You Do With Infigo SIEM?

We have built Infigo SIEM (Security Information and Event Management) to give its users the power to turn raw data into something useful. And that means that organizations can transform their data into information, into insights, into something actionable. Something that has value not just for a few stakeholders, but an organization as a whole.

It was made by using Splunk as its base, with rewritten parts that we deemed are not as fast or as efficient as they should be, with more than 20 years of real-world information security experience on defensive and offensive side put into shaping detection scenarios.

Here are just a few of the things Infigo SIEM can do for you out of the box.

**01**
Enhance your security posture

**02**
Detect threats before they become breaches

**03**
Get only relevant alerts, reduce alert fatigue

**04**
Investigate suspicious activities in detail

**05**
Be compliant with various regulations

**06**
Get reports tailored to stakeholders' needs and wants

**07**
Add multiple tenants out of the box

**08**
Gain insight into your assets with dynamic discovery

**09**
Give access to the SIEM through role-based access

**10**
Integrate on-premises or in the cloud

**11**
Visualize complex events in a simple and clean way

**12**
And much more!

# Full Visibility, Full Control

Enhance your organization's security posture with Infigo SIEM, ensuring **comprehensive visibility and eliminating blind spots**. Our solution empowers you with all the necessary information to effectively defend against a myriad of cyber threats. **Beyond security**, leverage this wealth of information to address questions from internal stakeholders and meet compliance requirements.

Infigo SIEM incorporates **powerful features** designed and tested through thousands of engineer hours by Infigo IS. The combination of usability and power provides a robust platform that will **give your analyst the right tool for today's cybersecurity challenges.**

## 1 AGGREGATION

Aggregation involves the collection and consolidation of data from various sources within an organization's IT environment. It is the process of bringing together diverse sets of information from multiple sources to provide a centralized view and serve as the foundation for further operations.

- Supporting thousands of sources
- Asset information
- Automatic network range discovery
- Enrichment
- Integration with other tools
- Multitenancy (central data collection, scattered data collection, hybrid)
- Scalability (terabytes per day) and redundancy

## 2 CORRELATION

Correlation is the process of transforming raw data into useful and actionable information. It aims to make sense of the vast amount of data collected by the SIEM system and to detect potential security incidents and is, by default, a critical step for SIEM to function.

- Detection – real-time, near real-time, scheduled, or ad-hoc
- Anomaly Detection
- Dynamic Thresholds
- Threat Intelligence
- SIEM Rules (creation, management...)
- SOAR (Security Orchestration, Automation, and Response) capabilities integrated in Infigo SIEM; we call it PAC, or Post Alert Creation

## 3 ALERTING

Since alerting is a critical feature of every SIEM, we have rewritten this Splunk mechanism to give us advanced incident workflow under the new name – Infigo Meerkat. It enables organizations to promptly identify and respond to potential security threats, minimizing the impact of incidents.

- Infigo Meerkat (a completely new extension of Splunk alerting mechanism with advanced incident workflows)
- MITRE ATT&CK Framework
- Rule-based Alerts
- Real-time Alerts
- Severity Levels
- Risk Context Alerting

## 4 INCIDENT INVESTIGATION

Incident Investigation is the process of examining and analyzing security events or alerts to gain a deeper understanding of a potential security incident. This phase involves detailed examination, correlation, and contextualization of information to determine the scope, impact, and root cause of a security event.

- Drill-down to raw events
- Alert auto close
- Allowlisting
- Case management
- Custom searches
- Data retention/warehousing for forensic analysis
- Dynamic severity
- Load balancing searches
- Pivot investigation
- Tagging

## 5 REPORTING

Reporting involves the generation of detailed and customizable reports to provide insights into the security events, compliance status, and overall performance of the SIEM system. A crucial part of communication, analysis, and regulatory compliance.

- Customizable reports
- Reporting dashboards (Authentication, Email, Endpoint, IDS, Malware, Network, Web...)
- Reporting through email or ticketing service

## 6 VISUALIZATION

The presentation of security-related data and insights in a graphical format through a web-based GUI. Infigo SIEM helps make complex data more understandable, enabling security professionals to quickly identify patterns, trends, and anomalies.

- Dashboards that are multitenancy aware
- Built-in documentation
- Dashboard tooltips
- User role-based access

HACK

**Your logs are an untapped resource; with Infigo SIEM, use them to answer important questions, boost your security posture, and stay on regulators' good side**

What happens next is up to you - let us make your life easier

# www.infigosiem.com


**INFIGO IS d.o.o.**
Karlovačka 24a
10020 Zagreb
**Croatia**
+385 1 4662 700
info@infigo.is

**INFIGO IS d.o.o.**
Hasana Brkića 2
71000 Sarajevo
**Bosnia and Herzegovina**
+387 33 821 245
info@infigo.ba

**INFIGO Software Design LLC**
2902, Level 29, Marina Plaza
Dubai Marina, Dubai
PO Box 5000307
**United Arab Emirates**
+ 971 4 512 4081
info@infigo.ae

**INFIGO IS d.o.o.**
Tivolska cesta 50
1000 Ljubljana
**Slovenia**
+386 1 777 89 00
info@infigo.si

**INFIGO IS d.o.o.**
Ul. Metodija Shatorov Sharlo br. 30/2-17
1000 Skopje
**North Macedonia**
+389 (0)2 3151 203
info@infigo.mk