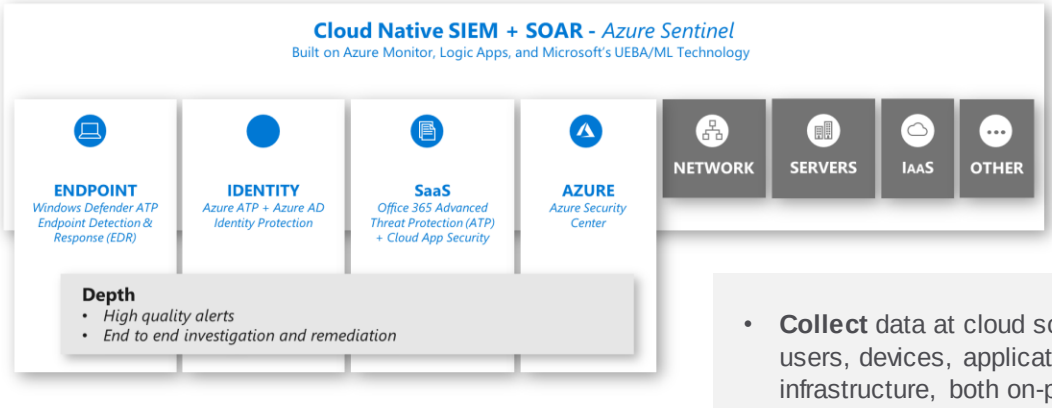
Azure Sentinel Managed SIEM Service

The challenge

Cybersecurity can be a never-ending saga—a chronicle of increasingly sophisticated attacks, volumes of alerts, and long resolution timeframes where today's Security Information and Event Management (SIEM) products can't keep pace. SecOps teams are inundated with a very high volume of alerts and spend far too much time in tasks like infrastructure set up and maintenance. As a result, many legitimate threats go unnoticed.

The solution

Our Azure Sentinel Managed SIEM Service makes it easy to collect security data across your entire hybrid organization from devices, to users, to apps, to servers on any cloud. It uses the power of artificial intelligence to ensure you are identifying real threats quickly and unleashes you from the burden of traditional SIEMs by eliminating the need to spend time on setting up, maintaining, and scaling infrastructure.



The value

Azure Sentinel Managed SIEM Service is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution timeframes.

- **Collect** data at cloud scale – across all users, devices, applications and infrastructure, both on-premises and in multiple clouds
- **Detect** previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft
- **Respond** to incidents rapidly with built-in orchestration and automation of common tasks
- **Investigate** threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft

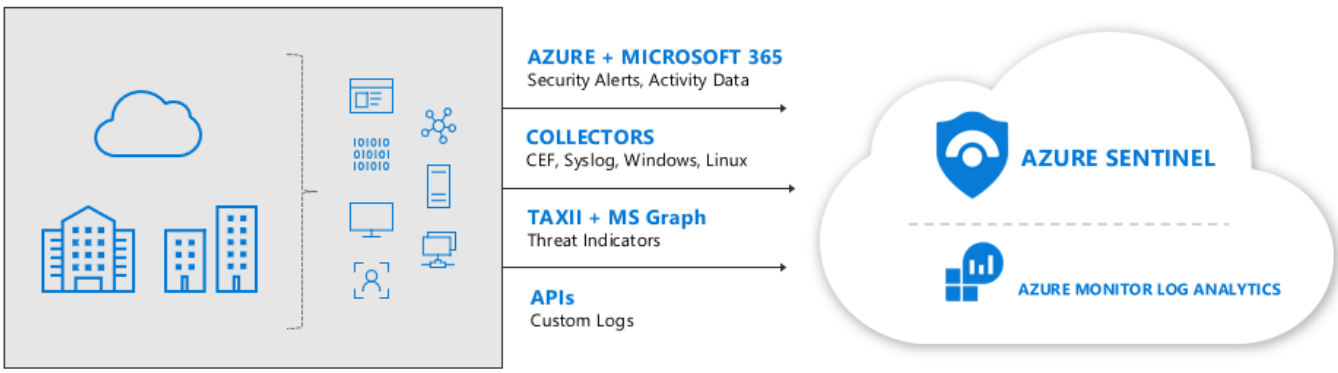
Contact us
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

Azure Sentinel Managed SIEM Service

The how

With the Azure Sentinel Managed SIEM Service we will simplify security orchestration. Our goal is to make it easy to collect data across all sources within your organization. Azure Sentinel has built-in connectors that help you do just that:

- One-click integration with Microsoft solutions
- Data connectors for growing list of other technologies – on-premises and cross-cloud
- Support for standard log formats (CEF/Syslog and WEF)
- Specialized TAXII and Graph connectors for threat intelligence data
- REST API for connecting to cloud solutions
- Proven log analytics platform with more than 10Pb of daily data ingestion



Why Enfo

Our values are at the core of our actions; collaboration, trust, continuous development and expertise. We walk beside our customers in their data-driven business transformation, taking ownership of their transformation as if it were our own.

Mastering complexity

Confidence in cloud

Genuine care

Contact us
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400