Orange Cyberdefense

Managed Threat Detection
SIEM

Terabytes of information do not equal knowledge. Only a good threat hunter can recognize and stop attacks that bypass automatic systems

Tighten your defenses

No protection is infallible. It is therefore all the more important to be prepared for the case when attackers undermine or circumvent protective measures.

Reliably detecting intrusions is the essential foundation for successful cyber-attack prevention and a key feature for organizations to protect themselves from cyberattack damage.

The cyber security analysts in our CyberSOCs, with ten globally dispersed hubs, use state-of-the-art technology and processes to monitor the IT environments of our customers.

Whether it‘s a mid-size manufacturing company or a global technology group, we‘re on the trail of the assailants, ensuring that you‘re aware of emerging threats, security risks and breaches, hence providing you with help and advice.

Network & Infrastructure

- Security Information and Event Management (SIEM)
- Network Intrusion Detection (NIDS)
- Network Behavior Analysis (NBA)
- Sandboxing
- Threat Intelligence
- System Monitoring

User & Identity

- User and Entity Behavior Analysis (UEBA)
- Cloud Access

Endpoint & Application

- Endpoint Behavior Analytics
- Hostbased Intrusion Detection (HIDS)
- File Integrity Monitoring (FIM)

Managed Threat Detection SIEM – Managed SIEM

Problem:

The SIEM is the cyber defense alarm system, but only if it works and is armed does it serve its purpose. This requires experts who ensure the functionality of your SIEM system, 24 hours a day, 365 days a year.

Solution:

With Managed Threat Detection - Managed SIEM, we take care of all aspects of your SIEM system and make it available to you as a powerful defense against cyber attacks.

The Managed SIEM package includes:

- Incident Management
- Remote Troubleshooting
- Remote Fault Remedy
- SIEM Monitoring
- Hardware Monitoring (for hardware appliances)
- OS and Application Monitoring
- System Function Monitoring
- Log Source Monitoring
- Lifecycle Management
- Configuration Change Management
- Backup & Restore
- Content Updates
- Software Upgrades
- 8×5 or 24×7 Service

Pro Service

Find out more on how to detect attacks before they cause damage on:
orangecyberdefense.com/gb/detect/

Managed Threat Detection SIEM – Security Analysis

Problem:

Many SIEM implementations fail because massive amounts of data are fed into the SIEM, but this provides limited added value out-of-the-box. Even the most numerous supplied detection use cases are often usable only to a very limited extent. Some can be used after extensive adjustments. With our standard use cases we cover widespread attack scenarios and create immediate added value.

If SIEM installations are not continually updated to detect new threats, their benefits decline rapidly.

Solution:

Even though the analysis of safety-relevant data can be highly automated, machines cannot take you all the way. Only those who succeed in combining state-of-the-art analysis technology with the know-how of human experts will remain a step ahead of the attack.

This is precisely the approach we take in our advanced Cyber SOCs, where we combine state-of-the-art sensors and analytical methods with the expertise of our Cyber Security Analysts and make them available to our customers in the form of our Security Analysis Service.

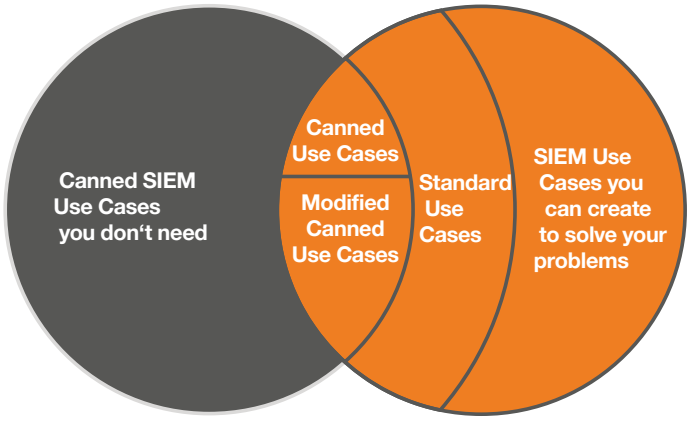
Managed Threat Detection SIEM - Security Analysis is based on the analysis of security-relevant log data from the IT infrastructure of our customers. This log data is collected by a SIEM system that is integrated into the customers infrastructure.

A SIEM ensures good transparency and visibility with regard to security-relevant events. But collecting data is one step, drawing the right conclusions is another.

The collected data must be correlated and enriched with further information before it can be interpreted by experts. Only then is it possible to deduce important findings from it in order to take the right measures to prevent or contain security incidents.

We constantly develop new detection methods for attack indicators, which are integrated into our standard use cases. Your investment in your SIEM system is thus permanently protected!

Use-Case-based Approach



Source: based upon Dr. Anton Chuvakin, Research VP, Gartner's GTP Security and Risk Management Group

Our standard use cases cover common attack scenarios. They meet the requirements of various security standards and frameworks such as CIS Critical Security Controls, ISO/IEC 27001 or PCI-DSS.

The Managed SIEM - Security Analysis package includes:

- 8×5 or 24×7 Service
- Use-Case-based analytics approach vor reliable incident recognition
- Standard Use Cases inlcuded – Standard Use Cases instantly puts your SIEM into operational mode
- **Optional:** Surveilance of add-on use cases – thus we integrate very specific recognition scenarios seamlessly according to customer specifics
- **Optional:** Threat Hunting – The ideal supplement for the deterministic approach of a SIEM to uncover new attack vectors and analyze the necessary indicators to keep recognition patterns up to date

For more information check
https://orangecyberdefense.com/gb/

Orange Cyberdefense
Waterloo Road, London SE1 8RD

info@gb.orangecyberdefense.com
+31 88 1234 200