netcetera

SECURITY OPERATIONS CENTRE (SOC) SERVICES

A GUIDE TO OUR SOC SERVICES

Introduction

This brochure explains our Security Operations Centre (SOC) services in more detail and is designed to answer some of the initial questions that you may have.

If you have any further questions, one of our partner specialists will be happy to answer them.

Contents

Page Contents

Security Operations Centre (SOC) services

Our fully managed SOC service ensures that your digital assets are secure and protected against cybercrime.

We aim to help our partners maintain the health of your security devices and pro-actively identify vulnerabilities and threats, while easing the burden on in-house IT teams.

How does it work?

Security Platform

We provide a fully managed Security Operations Centre (SOC) service with real-time monitoring of security events related to your digital infrastructure.

Whether you use an EDR or fully managed SOC model, our cloud-based security platform monitors your network and devices in the cloud, on-premises and in remote locations 24/7, helping you to detect threats virtually anywhere.

The Security Platform will monitor the following areas.

- **System Compromise:** Behaviour indicating a compromised system.
- **Exploitation & Installation:** Behaviour indicating a successful exploit of a vulnerability or backdoor/RAT being installed on a system.
- **Delivery & Attack:** Behaviour indicating an attempted delivery of an exploit.
- **Reconnaissance & Probing:** Behaviour indicating an actor attempt to discover information about your network.
- **Environmental Awareness:** Behaviour indicating policy violations, vulnerable software, or suspicious communications.

Security events related to the above areas are captured by the Security Platform, correlated with the custom rules and then reported as alarms.

Security Alarm Service Process

Below are the levels of services we offer:

- Level 1:
  The L1 security analyst monitors and reviews the latest alarms that have the highest criticality or severity. Should further investigation be required, L1 security analyst will escalate the issue to a L2 security analyst.

- Level 2:
  Examine the alarms escalated by L1 analyst and determine whether these are positives or false positives. If an alarm is identified as positive and cannot be handled at L2, then these are escalated to Level 3. Otherwise L2 analyst will close the incident while informing L1 and SOC supervisor.

- Level 3:
  Analyse the security events escalated by L2 analyst to de termine their impact on your network. Each attack will differ in terms of the appropriate remediation steps to take on the affected systems.

L3 analyst will also determine whether further action such as threat hunting, memory forensics, etc. are required to determine the extent of the compromise.

SOC services

Features

Our SOC service includes the following features:

› Asset discovery & inventory
› Vulnerability assessment
› Intrusion detection
› SIEM event correlation
› Incident response
› Log management
› Compliance reports
› Email alerts
› Automated incident response & forensics
› Supports PCI log storage requirements
› Endpoint Detection and Response

Coverage

We'll detail which devices we are supporting and when we are supporting them within your contract. You can add, decrease and make changes to your list of supported devices at any time in any given month.

Our SOC service is provided 24 hours a day, 7 days a week, 365 days a year.

Types of devices and plugins

The Security Platform supports many types of standard devices such as:

› Firewalls
› Servers
› Manageable switches
› Anti-Virus servers
› Databases
› Endpoints, etc.

What we ask of you

To help things run smoothly there are a few things that we need you to do:

You need to let us know if a server has been decommissioned or is no longer required. If a supported device is shown as unavailable we'll ask you to verify whether the agent has been decommissioned or has connectivity issues. In the case of decommissioning, we will remove the monitoring agent.

You also need to ensure that we have remote access to all supported devices.

Reports

Types of Reports

We will generate and submit the following types of reports for the security incidents detected by the security platform.

Report Type	Frequency
Initial breach assessment	Prior to installation
Alarms - top attackers, attacked hosts and destination ports	Weekly
Vulnerability assessment. Active hunting	Every six months
User activity	Monthly
Compliance	Upon client request

SOC Service
Standard

Strengthen your existing security by implementing a managed Endpoint Detection and Response (EDR) solution.

For businesses who are entering the managed security domain to shield their digital assets, but with a budget.

Cloud endpoint security is a critical part of cybersecurity and often the most targeted area by attackers. EDR offers discovery and visibility, adding a robust level of endpoint protection along with a signature-based anti-virus.

Our standard service includes the following:

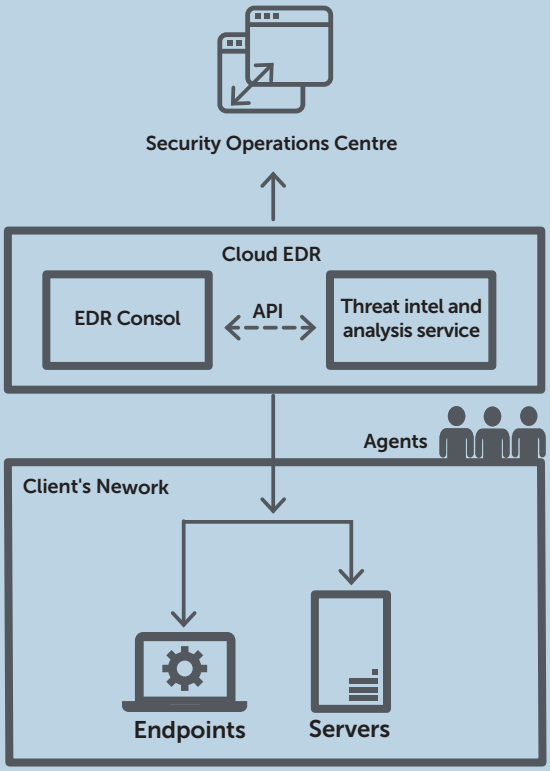
› 24/7/365 managed EDR
› Incident notification
› Assisting malware analysis
› Incident response
› Analysis report
› Scan reports

Additional services

EDR standalone installation still has limitations. To produce artefacts and objectives people and process factors should be met. This is why our EDR comes with 24/7/365 monitoring, along with L1 and L2 cybersecurity professionals that will monitor the infrastructure for any anomalous process inside the endpoint, including:

› The unification of endpoint data.
› Increased visibility throughout a whole IT environment.
› The ability to monitor endpoints either roaming or on premise.
› The ability to detect malware and store endpoint events.
› The ability to respond to an event in real-time.
› Integration with additional security tools.

EDR Deployment Architecture



SOC services

SOC Service
Premium

The strongest suite of cyber-security services. Fully managed SOC services to help reduce risk, respond to threats faster, achieve compliance and ensure continuity.

For businesses who are looking for a complete suite of managed security solutions and cyber-security services.

Our fully managed SOC provides real-time monitoring of security events related to your digital infrastructure. The monitoring is carried out 24/7/365 to detect, identify and notify you of the security risks on your digital assets. Security events captured by the security platform will be correlated with the custom rules and then reported as alarms to the team to investigate.

- Asset discovery & inventory
- Continuous monitoring
- Dark web monitoring
- Email notification
- File integrity monitoring
- Intrusion detection
- Log management
- Proactive tuning
- Real time threat detection
- Reports
- SIEM event correlation
- Vulnerability Assessment (Internal)

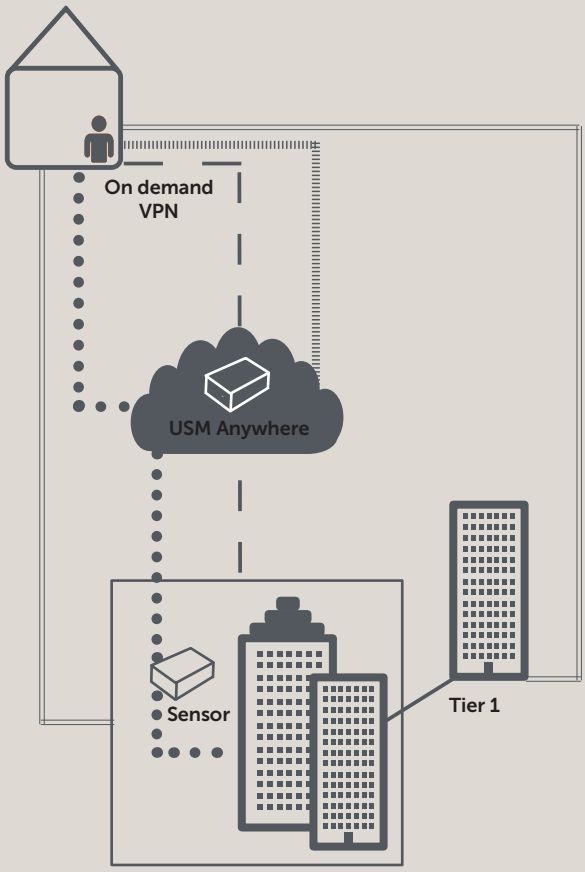
Resolution

Resolution involves an event being identified as a positive event or declared as a "false positive". We will submit recommendations to you upon investigating the alarms.

Target response times

Resolution Time	High	Medium	Low
Response Time	90 Minutes	2 Hour	N/A
Method	Email and SMS	Email and SMS	Weekly Report

Deployment Architecture



Elements	Description
— —	On demand VPN connection from your side, for troubleshooting when required
Sensor	Security appliance in cloud environment (AWS)
• • • •	Alarms and events
|||||||||||||||||	SOC ream monitors alarms
═══	Customised dashboard for viewing

SOC services

Service Offering Grid

Services	Device Count				
	10	25	50	>50	>199
› Asset Discovery & Inventory	✓	✓	✓	✓	✓
› Breach Assessment (One Time)	✓	✓	✓	✓	✓
› Continuous Monitoring	✓	✓	✓	✓	✓
› Dark Web Monitoring	✓	✓	✓	✓	✓
› Email Notification	✓	✓	✓	✓	✓
› File Integrity Monitoring	✓	✓	✓	✓	✓
› Event Search – Real Time	15 Days	15 Days	30 Days	30 Days	30 Days
› Incident Response	✓	✓	✓	✓	✓
› Intrusion Detection	✓	✓	✓	✓	✓
› Log Management	✓	✓	✓	✓	✓
› Proactive Tuning	✓	✓	✓	✓	✓
› Real Time Threat Detection	✓	✓	✓	✓	✓
› Reports	✓	✓	✓	✓	✓
› SIEM Event Correlation	✓	✓	✓	✓	✓
› SOC Managed	✓	✓	✓	✓	✓
› Vulnerability Assessment (Internal)	✓	✓	✓	✓	✓

SOC services

Value Added Services

SOC add-ons

SOC add-ons require project planning that involves determining and documenting a list of specific tasks, deadlines and the additional costs involved. The outcome for any add-on is to provide an effective and repeatable process for security services, as well as quantifying the overall integrity, coverage and thoroughness of the engagement.

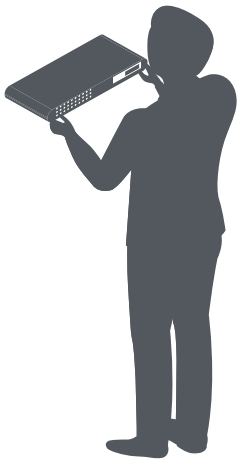
We provide the following SOC add-ons:

- Vulnerability Assessment (External)
- Vulnerability Assessment (Internal)
- Penetration Testing
- Web Application Vulnerability Assessment & Penetration
- Testing
- Mobile Application Penetration Testing
- Breach Assessment
- Threat Hunting
- Deep Learning for Network Traffic Analysis
- Deception Technology

We will assist your business by recommending the remedial measures based on the outcome of the assessment. You have the option to escalate recommendation to our NOC if appropriate services are purchased and are within the scope.

Third-party vendor coordination and management

During the installation process and thereafter, there could be instances where the services of third parties, mostly for device or application management support, are required. In such instances, we will require assistance in obtaining the prompt support from the third party. We will not be responsible for any failure of the security, due to delay in third party support.



Service Level Agreement (SLA)

We offer a comprehensive SLA covering our Security Operations Centre (SOC)

Incident Alarms

Alarm Type	High	Medium	Low
Response Time	30 Minutes	1 Hour	24 Hours
Method	Voice, Email and SMS	Email and SMS	Email

› **Low priority:** Events that do not seem to have any impact on you device/system/information

› **Medium priority:** The event or the series of events that do not have a significant effect on you device/system/Information and therefore does not warrant an immediate action.

› **High priority:** Alarm generated due to an event or series of events that could have a significant impact on your device/system/information that requires an immediate action.

Examples of Events

› **Low priority:** General port scans, wrong password, account lockout, etc.

› **Medium priority:** Targeted attempts to connect, targeted port scans, account lockouts, behavioural anomalies, etc,

› **High priority:** Malware and virus infections, unauthorised software installation, policy violations, unauthorised connections etc.

The above list is not exhaustive. The final categorisation of alarms will depend on your security policy or the requirement of security to support the business operation.

Response time starts when the event first appears with the relevant alarm category on the L1 Operator Dashboard. Security alerts will be informed only to the nominated contact person.

Escalation process

Our goal is to provide a response within the stated SLA and to ensure that we exceed your expectations.

Contact Details

You are required to provide primary and secondary contact details as a nominated point of contact. This individual will be contacted by the SOC Supervisor in regards to any security incidences.

We will provide you with the contact details of the SOC to ensure you have two way communication with our security team.

Internal Escalations

If a high or a medium alarm is found to be positive, then we will adopt the following process based on your consent.

- Our security team will remotely access the device and carry out a threat hunting.
- If the device is compromised, then the above process will require carrying out a threat hunting on other devices that are connected to the compromised device.
- If you agree our security team will carry out a memory forensics to identify the level of compromise.
- If you agree our team will carry out malware reverse engineering to find out more details about the malware and its impact on your business operations.

Security and compliance

We are committed to ensuring that security is considered and maintained within all aspects of our operation. We have implemented the following security control measures within our SOC.

SOC Security Measures

Human resources

- Employment history verification
- ID document checks
- Professional qualifications verification
- Minimum of 2 verified references
- Criminal record checks
- NDAs and confidentiality agreements in place for every employee

Physical

- 24/7 on-site security
- Biometric access control system with dual authentication
- Night vision enabled CCTV system throughout the suite

Infrastructure

- Access to information controlled by principle of least access
- Domain controlled environment utilising group policy, enabling access control and monitoring
- Multi-factor authentication to further control access to infrastructure resources and tools
- Remote access sessions AES-256 encrypted
- All systems kept current with security patches, anti-virus and anti-malware software and definitions
- All operations performed as per ITIL best practice

Redundancy

- 24/7 backup generator and UPS facilities
- Redundant Internet connectivity based on wired and wireless technologies
- Cloud-based SaaS and IaaS environments are used for critical business systems e.g. VoIP telephony, call management and PSA functions
- Business continuity/disaster recovery plan with standby disaster recovery suite

Customer data

- Your data is stored on a hosted SSAE 16 Type 11 certified secure CRM and ticketing system
- Your credentials (if supplied) are stored within a secure database utility with options for cloud-based or local storage dependent on regulatory requirement
- All data stored within IT Glue is stored on EU servers to comply with GDPR regulation

Compliance and certifications

- ISO 27001:2013 certification
- PCI DSS compliance
- HIPAA/HITECH regulated clients via Business Associate Agreement*
- GDPR compliance

Netcetera
The Dataport
Ballasalla
Isle of Man
IM9 2AP