Proactive SOC 1.0

Service Description

13/01/2026

GlobalConnect

GlobalConnect

Content

1. Introduction

A Security Operation Centre (SOC) provides continuous protection, visibility and response against cybersecurity threats. The Proactive SOC is GlobalConnect's SOC-as-a-service offering, designed to meet customers' cybersecurity needs. The service is provided through GlobalConnect's Security Partner Netsecurity AS.

With Proactive SOC, GlobalConnect offers the customers a single point of contact during security incidents and ensures the customer has access to a cybersecurity Incident Response (IR) team.

Proactive SOC consists of the following services:

- Managed Detection and Response Service (MDR)
  - The MDR service offers real-time monitoring, detection, and response to cyber threats. It integrates advanced technology with expert analysis to monitor and act on user behavior, and secure endpoints and cloud environments. This service ensures comprehensive protection tailored to businesses of all sizes.
- Incident Response Service (IRS)
  - The Incident Response Service consists of a dedicated team of cybersecurity experts equipped to handle, mitigate, and resolve security incidents in the most efficient way possible.

The service enhances the customers' ability to tackle cybersecurity challenges by offering early detection, expert analysis, proactive response, and swift recovery support to maintain business continuity during security incidents.

Proactive SOC service emphasizes compliance, adaptability, and collaboration to secure customers organization with a proactive and resilient cybersecurity posture.

2. Methodology and framework

Proactive SOC uses reliable frameworks for a systematic approach to incident management, ensuring accuracy, efficiency, and verification that the process is followed correctly.

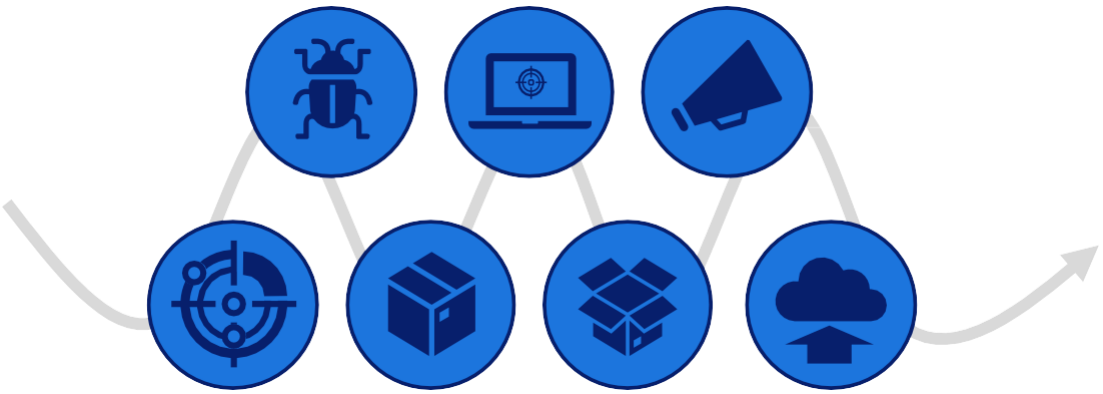
To ensure continued effectiveness in a rapidly evolving threat landscape, the methodology used to deliver this service may be adapted over time.

2.1. PICERL

For incident management, the PICERL framework is used: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. This approach ensures thorough preparation, effective detection, containment, removal of threats, system recovery, and analysis for future improvements.

2.2. ATT&CK for Enterprise Kill Chain framework

The ATT&CK framework, based on the Cyber Kill Chain, consists of real-world attack tactics and techniques. Proactive SOC uses this framework to classify, understand, and manage threats. By leveraging the Mitre ATT&CK™ framework, Proactive SOC ensures product-agnostic and independent mitigation plans, aligning with ISO27001 and GDPR standards.



3. Service Features

3.1. Managed Detection and Response (MDR)

GlobalConnect's MDR service, part of the Proactive SOC offering, provides continuous monitoring and response to cyber threats using advanced technology and frameworks. It identifies and mitigates attacks both on-premises and in the cloud, leveraging identity and endpoint.

The service includes:

- Orchestration and Automation (SOAR): Streamlined alarm analysis using Security Orchestration, Automation, and Response for efficient incident management.
- SOAR Tenant: Each customer receives a separate tenant, ensuring security and GDPR compliance.
- Endpoint Monitoring (EDR): In-depth monitoring of endpoints using Endpoint Detection and Response technology.
- Intrusion Detection: Real-time detection of intrusions and suspicious activities.
- Cloud Services Monitoring: Monitoring of cloud services like Microsoft, AWS, Google, etc., via APIs to ensure cloud security. SCPN and CNAP are not included.
- Key Performance Indicators (KPI) Reporting: Detailed reports with relevant KPIs to assess security status.
- Integration with Microsoft Azure Sentinel: Consolidates data from network resources for comprehensive analysis. This is an add-on and not included in the base package.

3.1.1 Reporting

Monthly reports are prepared and reviewed, with the review process tailored to the customer's preferences during onboarding. The reports include:

- Alarm statistics and risk scoring
- Representation of alarms within the MITRE ATT&CK framework
- Comparison of customer alarms against overall trends
- Details of users involved in alarms or incidents
- Indicators from emails and suspicious domains from the last month
- External and internal IP addresses involved in incidents

These reports are continuously refined and improved to ensure relevance and accuracy.

3.2. Incident Response Service (IRS)

As part of the Proactive SOC offering, the Incident Response Service (IRS) is crucial for identifying and addressing IT security incidents. These occur when there is unwanted access to information systems, or suspicion thereof, with intentions to compromise confidentiality, authenticity, integrity, or availability.

GlobalConnect's security partner commits to responding within 1 hour, deploying a team of skilled professionals to tackle security challenges promptly

3.2.1 The Incident Response Process

The incident response process within the Proactive SOC involves a comprehensive approach:

- Identification and Classification: Determine the nature of the incident, including involved actors, malware, attack vectors, tools, and methods used by the attacker
- Access Mapping: Assess how unauthorized access occurred and the extent of the intruder's activities within the information systems
- Limit and Prevent Further Activity: Take immediate action to restrict and prevent additional unauthorized activities, while documenting procedures
- Secure Electronic Evidence: Gather and preserve electronic evidence to support investigations and potential legal actions
- System Restoration: Restore affected systems to their normal state, minimizing downtime
- Learning Points and Recommendations: Extract insights from the incident and recommend measures to enhance security posture
- Customer Reporting: Provide detailed reports outlining the scope, impact, and response to the incident

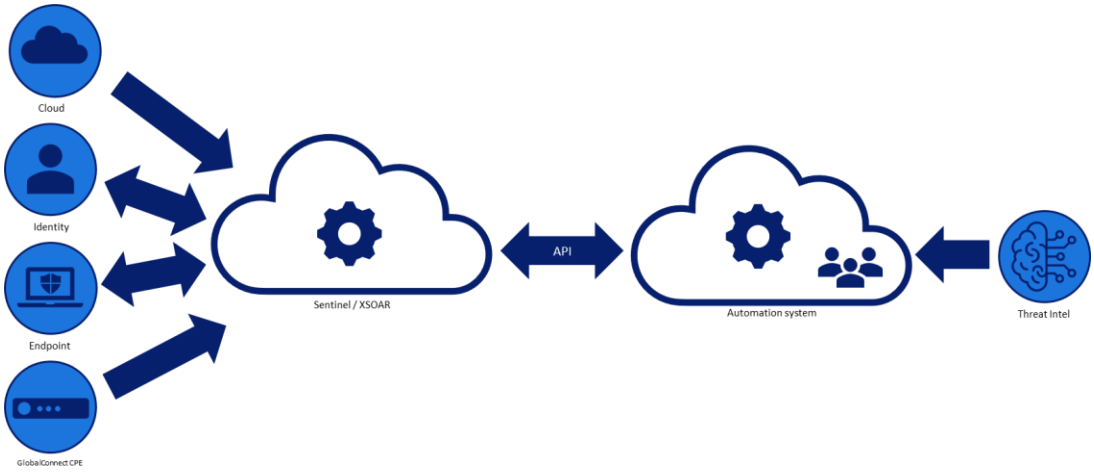
3.3. Service onboarding

The Proactive SOC onboarding process covers both MDR and IRS services, ensuring comprehensive security management

3.3.1 MDR Service Onboarding

The MDR service begins with establishing an API connection by the customer, enabling efficient exchange of alarm data and automated responses. No physical components are required, and the service supports over 900 integrations, with options for custom adaptations to your systems. The effectiveness of the service depends on the level of access granted to the customer's systems; broader access enables more comprehensive protection and response capabilities.

During onboarding, contact information, notification matrices, and collaboration details are exchanged to ensure smooth operation. The integration allows for automatic responses to events and alarms, ensuring timely threat mitigation. Two-way synchronization with systems like ticketing platforms keeps the customer informed of all response actions, ensuring seamless integration with existing security solutions.



3.3.2 IRS Service Onboarding

The IRS service builds on the MDR foundation and starts with preparation talks, exchanging documentation, access, and communication channels as part of the standard onboarding. When an incident occurs, the IRS process activates, utilizing the established MDR infrastructure to respond effectively and manage the incident.

4. Packaging

4.1. Base package

The following SOC services are included in the base package:

- MDR and IRS onboarding (one-time charge)
- Dedicated SOAR tenant
- Protection of 50 identities (Entra ID)
- Protection of 50 endpoints
- Protection of 5 servers
- Service Level Agreement (SLA)

4.2. Add-on packages

Proactive SOC allows for the following additional services:

- Identity (Entra ID) protection, in increments of 50 identities
- Endpoint protection, in increments of 50 endpoints
- Server protection in increments of 5 servers

4.3. Logging packages

GlobalConnect offers customers the option to have Managed SIEM Sentinel within their Microsoft tenant for an additional fee.

This service enables the collection and processing of telemetry from sources that does not support agent-based monitoring such as IoT devices and network infrastructure.

Managed SIEM Sentinel includes:

- Verification and control of data connector setup into Sentinel, ensuring that the sources to be included are configured correctly.
- Log setup and maintenance of sources without ready-made data connectors, so that they can also utilize Sentinel.
- Detection rules beyond Microsoft's built-in ones. Allowing events outside the standard to be uncovered and handled through Sentinel.
- Relaying of alarms from Sentinel to Netsecurity SOC platform for processing.

The base configuration of Managed SIEM Sentinel includes:

- 150GB of SIEM data log amount
- 1x of SIEM log sources

Additional storage and log sources can be purchased for an extra fee.

5. Service Level Agreement (SLA)

The terms and conditions outlined in this SLA are distinct and separate from the standard SLAs that may apply to other services from GlobalConnect.

MDR services are delivered for alerts/notifications that are generated in the Customer's environment and that are made available to and received by the Provider. The Customer is responsible for maintaining the necessary licensing level and configuration to ensure the generation and transmission of alerts. If alerts are not generated or do not reach the Provider as a result of insufficient or changed licensing, the service's response-time commitments do not apply for the affected scope.

The Incident Response Service (IRS) response time is calculated from when the Customer contacts the Netsecurity 24/7-365 staffed alarm telephone, or when the SOC has escalated the case to the Incident Response team to handle the incident.

Any customer inquiries should always go to Netsecurity's 24/7-365 staffed alarm telephone. Requests by email is not a support channel that is covered by the SLA.

The SLA guarantees a response time within 1 hour to "hands on keyboard" or "key in car".

In case hours from the Incident response team are needed to mitigate an attack, based upon customer's approval, GlobalConnect will invoice the customer for used hours according to the existing price list. No costs for responding to the incident will be incurred without the customer's approval. For ICT incidents, the customer shall report this to the Netsecurity 24/7-365 staffed alarm telephone.

5.1. Service Level and Warranty Overview

Availability period – service hours	24/7/365
Availability (uptime within availability period) *	99 %
Security Monitoring – Guaranteed Resolution Time *The time from detection, via analysis/enrichment to response.*	

"Critical" classified detections/possible security incidents	30 minutes
“High” classified detections/possible security incidents	2 hours
“Medium” classified detections/possible security incidents	24 hours
“Low” classified detections/possible security incidents	48 hours
"Information" classified detections/possible security incidents	Report
Technical resources, follow-up and other services	
Customer portal for registration and follow-up of cases	Included
Incident management – response time *The time from the need reported to the IRT team until they are in the process of handling the incident (hands-on-keyboard)*	
Incidents escalated from the SOC service	1 hour
Incidents escalated from the Customer	2 hours
Physical attendance at the customer's premises	By appointment

Note - Downtime caused by the Customer, external factors, planned maintenance or other circumstances for which the Supplier is not responsible is not covered by the warranty*

5.2. Notification routines

Notification routines are collaboratively established with the customer at the start of the service. This includes designated contact people, escalation routines and more. All cases detected by the Supplier will be classified and categorized by the Supplier and registered against the applicable SLA. SLA deviations are internally escalated, assessed for impact, and reported to the customer using the agreed method

5.3. Compensation for Accessibility Violations

Standardized compensation is calculated based on the total ongoing monthly charges for the service for the month in which guaranteed availability has not been met in relation to the relevant customer. It is the customer’s responsibility to notify GlobalConnect if entitled to compensation in accordance with the table below:

Availability in %	Compensation
99.0 to 98%	15 %
98 to 97%	25 %
97 to 96%	35 %
96 to 90%	50 %
Under 90%	80 %

5.4. Compensation in the event of a breach of the agreed resolution time

SLA is measured on all alarms and is calculated per calendar month based on the percentage of alarms resolved within and outside the agreed resolution time. Standardised compensation is calculated based on the percentage of the resolution time that ex-ceeds the agreed resolution time. It is the customer’s responsibility to notify GlobalCon-nect if entitled to compensation in accordance with the table below:

Resolution time - deviation in %	Compensation
1 to 2%	5 %
2 to 3%	10 %
3 to 4%	15 %
4 to 5%	25 %
Over 5%	45 %

6. Glossary

Abbreviations	Definition
SOC	Security Operations Centre
IRS	Incident Response Service
MDR	Managed Detection and Response
SLA	Service Level Agreement
CPE	Customer Placed Equipment
ICT	Information and Communication Technology
KPI	Key Performance Indicator
SOAR	Security Orchestration, Automation, and Response
Hands on keyboard	Start of billable, remote incident response work
Keys in car	Indicates the start of billable, customer required on-site response work, including travel time

.