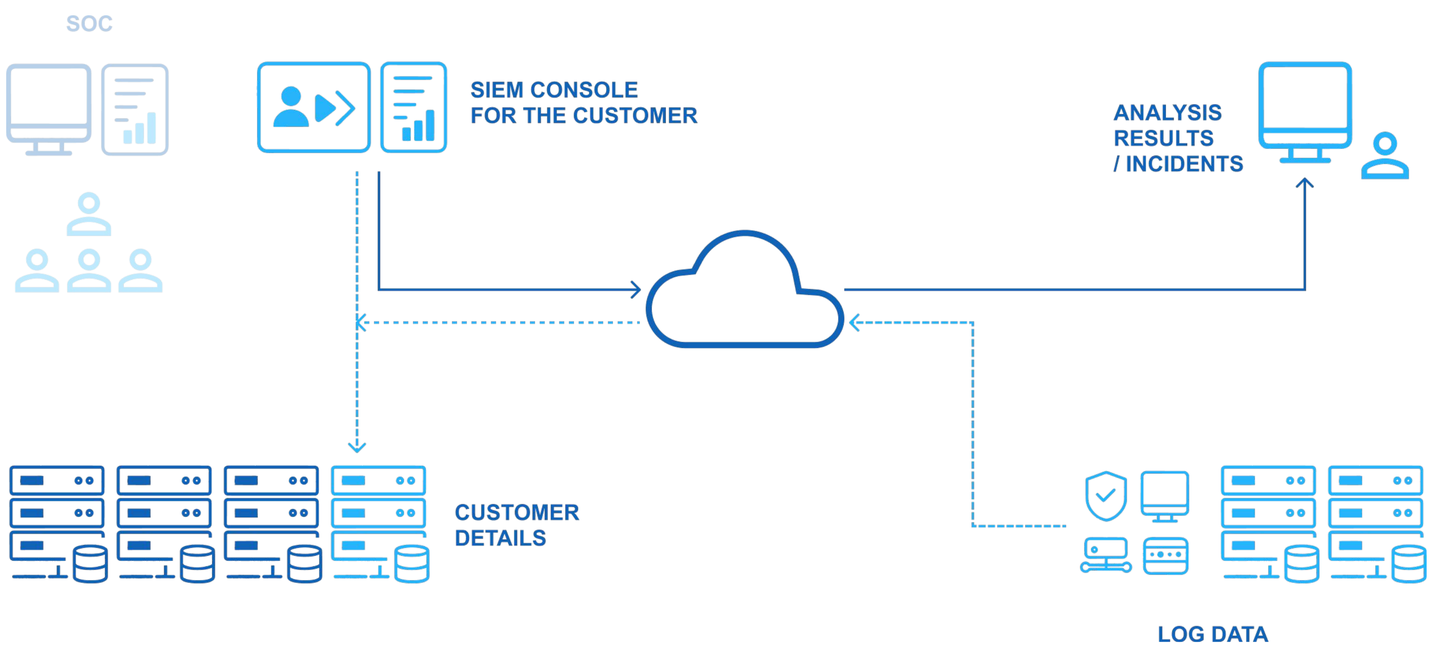
OUR SERVICES
DATA COLLECTION AND PROCESSING MODELS

MINIMUM OPTION – MANAGED SIEM

The minimum option - Managed SIEM allows you to take full advantage of SIEM/SOAR/XDR technology without having to install, configure and maintain it in your own infrastructure. All necessary configurations and integrations are performed by NonStop SOC engineers in accordance with the customer's requirements, as are all system maintenance responsibilities. The customer can use all the system's functionalities as if it were part of their own infrastructure. In this model, the collected data and logs are processed and stored in the NonStop SOC data centre.



NonStop SOC infrastructure (SIEM, SOAR, XDR, TI)

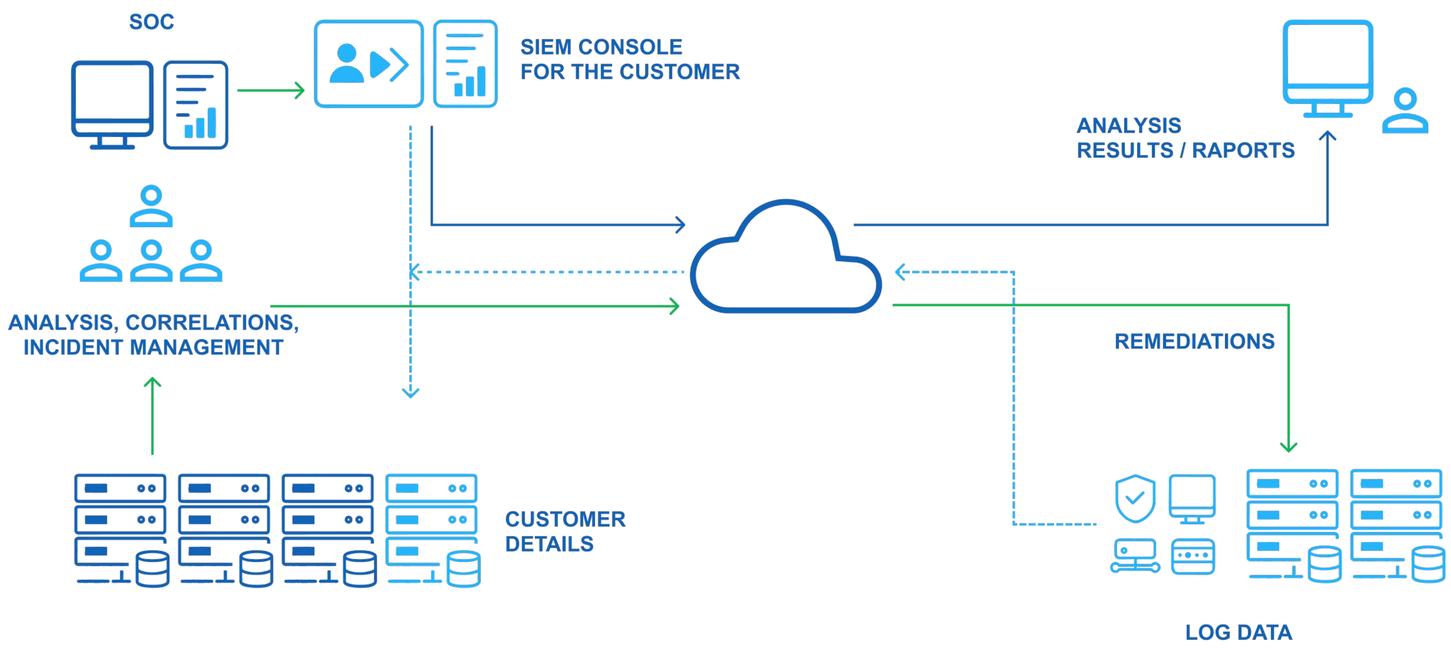
- Data processing at DC NonStop SOC
- Information and operational console for the customer in the NonStop SOC infrastructure

Customer infrastructure

- Transfer of all data to NonStop SOC
- Access to a full information and operational console for the customer in the NonStop SOC infrastructure

MINIMUM OPTION – MANAGED SOC AND SIEM

Minimum option – Managed SOC and SIEM ensures the use of SIEM/SOAR/XDR technologies to monitor information systems and manage security incidents on behalf of the customer by the NonStop team. As in the Managed SIEM option, the customer can use all the system's functionalities and additionally receives the full range of Managed SOC services. All necessary SIEM/SOAR/XDR configurations and integrations are carried out by NonStop SOC engineers in accordance with the customer's requirements, and all responsibilities related to system maintenance remain with the service provider. In this model, as in the previous one, the collected data and logs are processed and stored in the NonStop SOC data centre.



NonStop SOC infrastructure (SIEM, SOAR, XDR, TI)

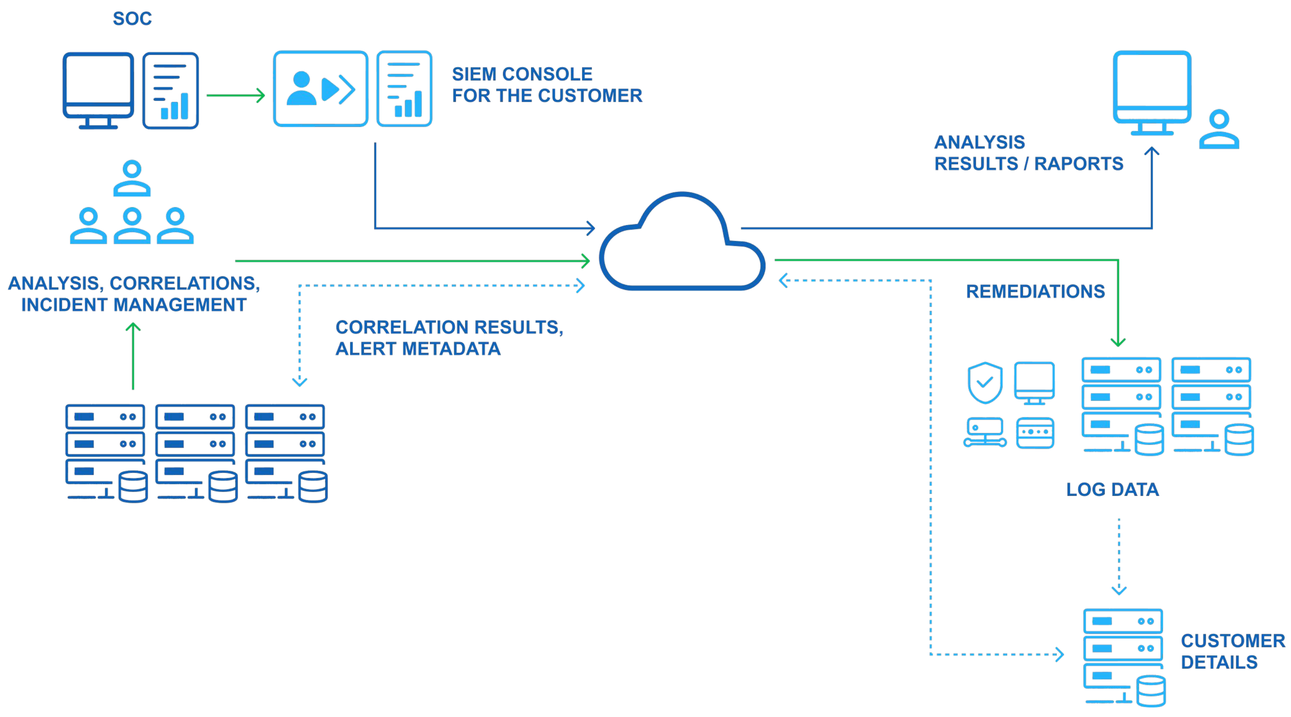
- Ongoing monitoring and incident management (managed SOC services)
- Data processing at DC NonStop SOC
- Information and operational console for the customer in the NonStop SOC infrastructure

Customer infrastructure

- Transfer of all data/logs to NonStop SOC
- Access to the information console for the customer in the NonStop SOC infrastructure
- Remediation, information and analysis (resulting from managed SOC services)

OPTIMAL OPTION – MANAGED SOC, MIXED SIEM

The optimal option - Managed SOC, Mixed SIEM enables the use of SIEM/SOAR/XDR technologies to monitor information systems and manage security incidents on behalf of the customer by the NonStop SOC team. As in the Managed SIEM option, the customer can use all the system's functionalities and additionally receives the full range of Managed SOC services. All necessary configurations SIEM/SOAR/XDR integrations are implemented by NonStop SOC engineers in accordance with customer requirements. In this model, unlike the previous ones, the collected data and logs are processed and stored in the customer's infrastructure, without the need to transfer them to the NonStop SOC data centre. This solution is particularly beneficial for customers who want to keep their data and logs in their own environment, while ensuring compliance with accepted compliance rules.



NonStop SOC infrastructure (SIEM, SOAR, XDR, TI)

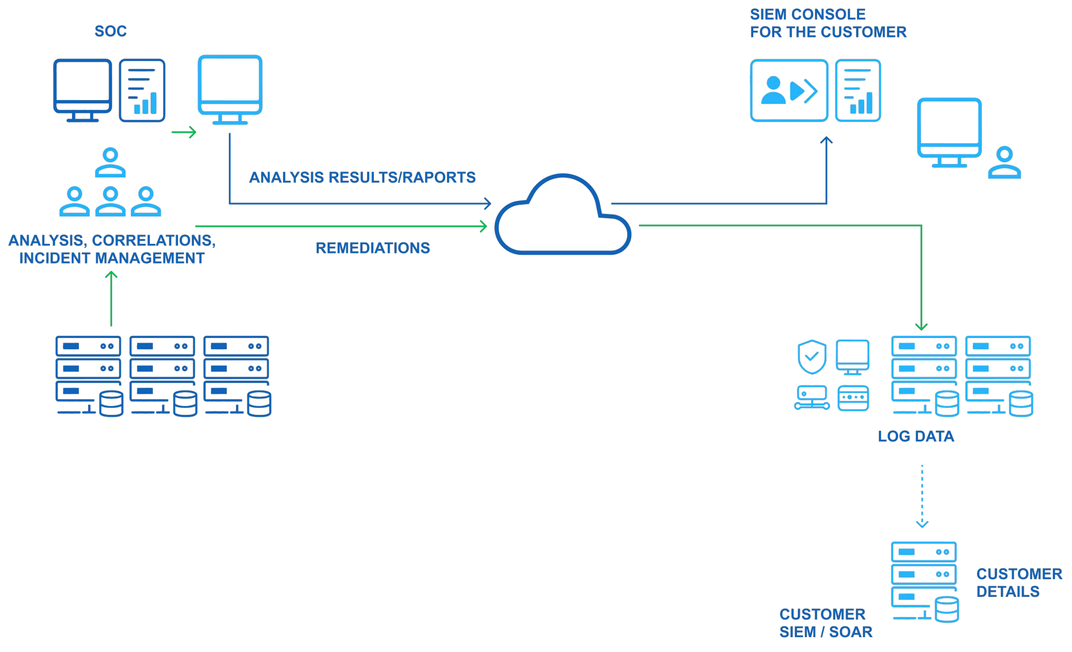
- Ongoing monitoring and incident management (managed SOC services)
- Only correlation results and alert metadata are processed in the NonStop SOC DC
- Customer console in the NonStop SOC infrastructure

Customer Infrastructure

- All data and logs remain in the customer's data centre
- Access to the information and operational console for the customer in the NonStop SOC infrastructure.

EXTERNAL OPTION – MANAGED SOC, CUSTOMER SIEM

The external variant - Managed SOC, Customer SIEM provides monitoring of information systems and security incident management (Managed SOC services) on behalf of the customer by the NonStop SOC team, using the customer's SIEM/SOAR/XDR technology. The necessary SIEM/SOAR/XDR configurations and integrations can be performed by NonStop SOC engineers in accordance with the customer's requirements and the needs of the processes designed for the SOC. In this model, the collected data and logs are processed and stored in the customer's data centre without the need to transfer them to the NonStop SOC data centre. This solution is particularly beneficial for customers who already have SIEM/SOAR/XDR technology and would like to strengthen their cyber security by using SOC services.



NonStop SOC infrastructure (SIEM, SOAR, XDR, TI)

- Ongoing monitoring and incident management (managed SOC services)

Customer infrastructure

- All data and logs remain in the customer's SIEM/SOAR.
- Access to the information and operational console for NonStop SOC in the customer's infrastructure.

nonstop soc

SERVICE CATALOGUE

The service catalogue has been developed based on the recognised FIRST industry standard for SOC/CSIRT operations, which enables the exchange of information between various participants in the cybersecurity management process at different levels the customer, SOC and CSIRT – and to select SOC services depending on needs and organisational maturity. The minimum NonStop SOC service package includes basic services in the area of security event management and security incident management. Other services in other areas may be provided depending on the customer's choice and needs.

SECURITY EVENTS MANAGEMENT

Basic services

1. Monitoring and detection

- Log and sensor management
- Use case management
- Contextual data management

2. Event analysis

- Correlation
- Qualification

SECURITY INCIDENT MANAGEMENT

Basic services

1. Report acceptance Incident

- Receipt of incident reports
- Incident assessment and processing

2. Incident analysis and response

- Incident triage (prioritisation and categorisation)
- Information gathering
- Coordination of detailed analysis
- Root cause analysis
- Correlation between incidents
- Incident response

Additional services

3. Artifact and Forensic Evidence Analysis

- Analysis of carriers or other media
- Reverse engineering
- Start-up or dynamic analysis
- Comparative analysis

4. Mitigation and data recovery

- Establishment of a response plan
- Ad hoc measures and containment of incident impact
- System restoration
- Support for responsible entities for information security

5. Incident coordination

- Communication
- Distribution of notifications
- Coordination of activities
- Reporting
- Communication with the media

6. Crisis management support

- Distribution of information to recipients
- Reporting on the state of information security
- Communication regarding strategic decisions

VULNERABILITY MANAGEMENT

Basic services

1. Detection and investigation of security breaches

- Incident vulnerability detection
- Detection of vulnerabilities from public sources
- Threat vulnerability assessment

2. Receiving reports on vulnerabilities

- Receiving vulnerability reports
- Triage and processing of vulnerability reports

3. Vulnerability analysis

- Vulnerability selection (validation and categorisation)
- Root cause analysis of vulnerabilities
- Development of countermeasures

Additional services

4. Vulnerability Coordination

- Vulnerability notification / reporting
- Vulnerability stakeholder coordination

5. Vulnerability disclosure

- Vulnerability disclosure policy
- Infrastructure maintenance
- Vulnerability announcement / Communication / Dissemination
- Post-disclosure feedback

6. Susceptibility response

- Vulnerability detection/scanning
- Vulnerability removal

SITUATIONAL AWARENESS

Additional services

1. Data acquisition

- Policy aggregation and filtering, understanding guidelines
- Mapping assets to functions, roles, activities, and key risks
- Data collection
- Data processing and preparation

2. Analytics and synthesis

- Forecasting and inference
- Event detection (through alerting and / or hunting)
- Decision support related to incident management
- Estimating the impact on security status

3. Communication

- Internal and external communication
- Reporting and implementation of recommendations
- Dissemination / integration / sharing of information
- Information exchange management
- Feedback

KNOWLEDGE AND ITS TRANSFER

Additional services

1. Building awareness

- Research and information gathering
- Preparation of reports and information materials
- Dissemination of information
- Reaching audiences

2. Training and education

- Gathering requirements regarding knowledge, skills and abilities
- Developing educational and training materials
- Delivering content
- Mentoring
- Professional development of SOC staff

3. Exercises

- Requirements analysis
- Development of exercise formats and environment
- Development of scenarios
- Conducting exercises
- Reviewing exercise results

4. Technical consulting

- Risk management support
- Support in business continuity planning and disaster recovery
- Support in creating policies, processes and procedures
- Technical consulting

CONTACT US

Telephone: +48 22 570 13 60

E-mail: kontakt@nonstopsoc.com.pl