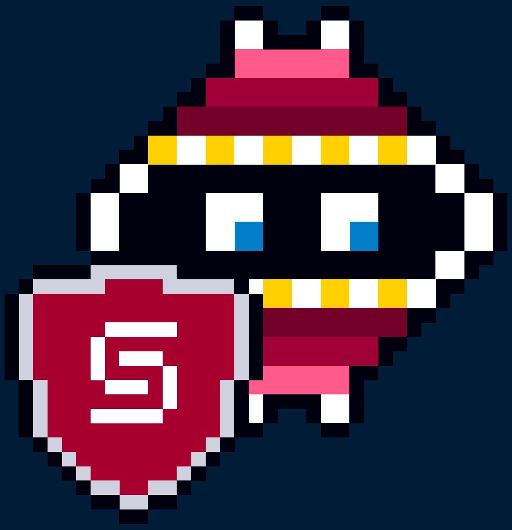
Netsecurity

MDR - Managed Detection and Response

Service Overview - December 2024

Microsoft Azure Marketplace

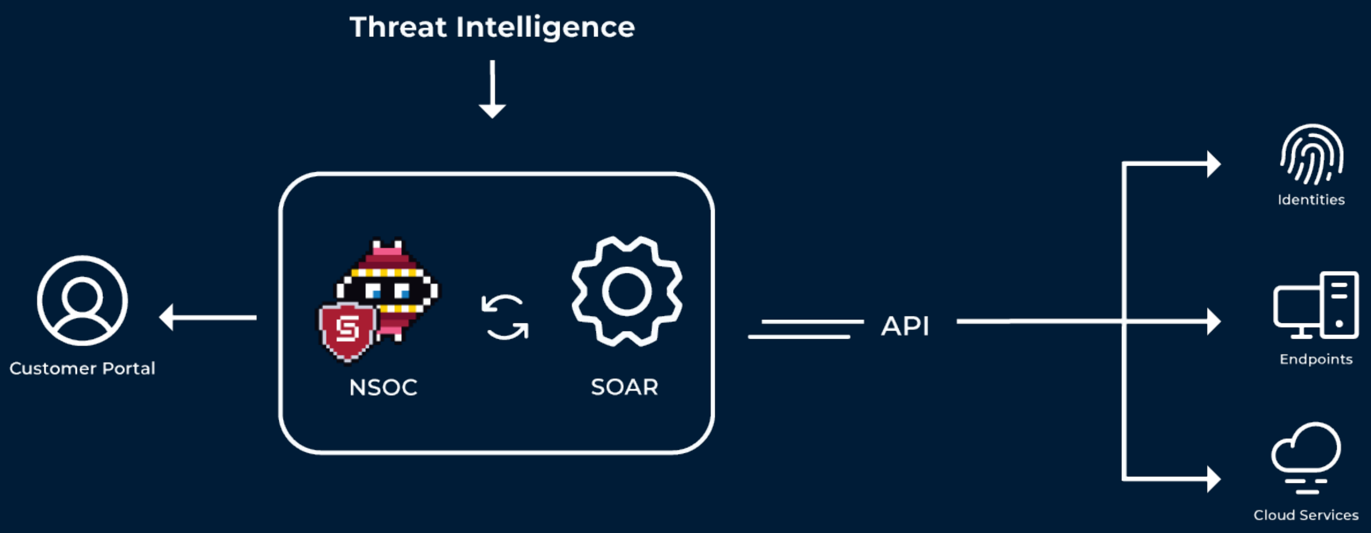


Why it's important to use MDR

The threat landscape is constantly and swiftly changing. Attackers are getting more sophisticated, outsmarting their victims as organizations move quickly into the digital world with limited security resources. The rapid shift to hybrid cloud solutions and outsourcing leaves these organizations with less control over what security measurements they have in place. Compounding the problem, there is an increasing gap between attackers' capabilities, speed, and their agility compared with organizations' ability to secure their business with traditional security technology and operational best practices.

How it works

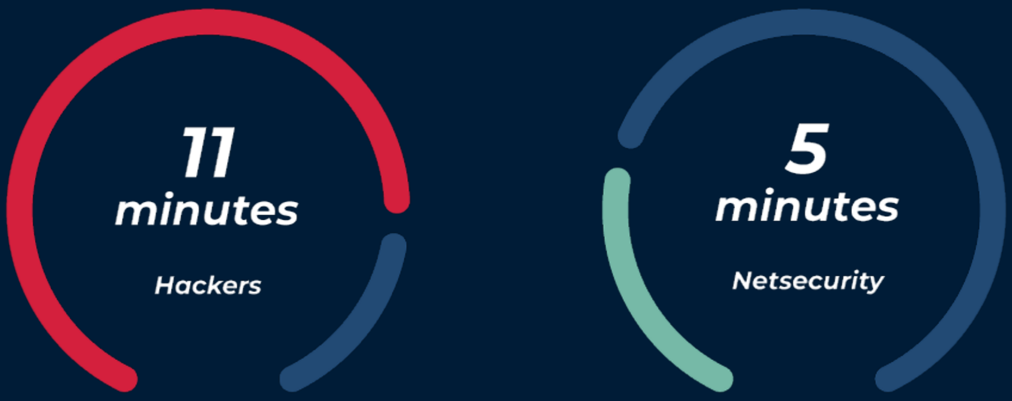
Netsecurity Secure Operations MDR is part of a complete service offering addressing the increasing gap between the threat landscape and the need for rapid adaption to changing business needs without the increased cyber risk. Netsecurity MDR service provides 24/7 protection and stable security for your business. We protect your IT-assets from potential threats, and if you are under attack, we provide rapid response and damage control.

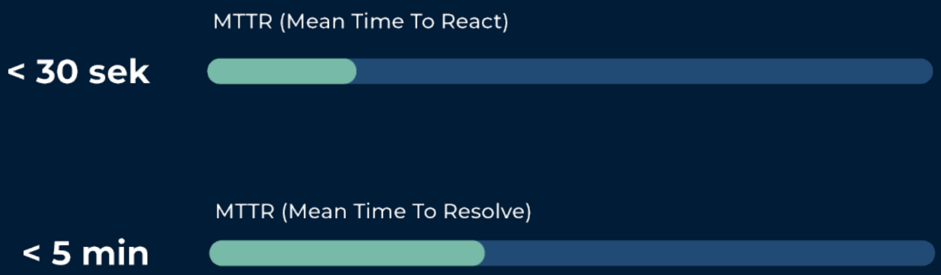


We provide detailed reports regarding insights and incidents so you can be well informed about what types of incidents you have, thereby being kept in the loop on what's going on. With both our experts in NSOC and our long time experience with SOAR, we make sure you are safe and secure 24/7/365.

Resolve

Containing a cyber threat within a short time frame is critical to maintain system integrity and stability. On average, the fastest hackers can breach your defenses within 11 minutes. But our MDR-service swiftly detects and contains, responding within 5 minutes. Our rapid response allows us to uphold security and minimize issues. We are confident that our response time will provide excellent security measurements and protection for you.





Detection

To effectively detect alerts and security incidents we collect, analyze and compile necessary information from IT and IT security solutions. This grants us the ability to detect suspicious activity. Microsoft's modern security solutions detect anomalies and security deviations. We take full advantage of these features for our service offering. These modern solutions draw data from various sources, including:

Identities

Identity monitoring is crucial when it comes to cyber security. You need constant surveillance because digital identities are one of the most targeted possibilities to breach your business. Two factors authenticating reduce the risk of a successful attack, but monitoring suspicious activity is crucial for good detection of a possible security breach. Netsecurity provide excellent identity security in monitoring:

- Azure Identity protection (Microsoft 365 and Azure Active Directory)
- MS Defender for identity (Active Directory, on-premise Microsoft domain)
- User Account, Password protection

We respond to suspicious activity with deactivating/and or activating user accounts, forcing password change and ending active sessions.

Endpoints

Traditional antivirus cannot protect against modern and automated attacks and must be replaced with proactive solutions that can protect against unknown and new vulnerabilities and methods. Modern endpoint solutions leverage the infinite capacity of the cloud to protect against even the most advanced attacks. Endpoint security in combination with network security offers great benefits such as:

- Full protection of all devices
- Faster threat detection
- Reduced risk of data breaches

Cloud Security
Cloud security is about roles, responsibility models, processes and technology. Cloud providers deliver some of this, but not all, and those of us who use the cloud are responsible for the data that is sent to, stored in, accessed, produced and processed in the cloud. We provide cloud users with sufficient insight, control and protection to fulfill their part of the responsibility.

- Full cloud visibility, identify and manage anomalies, threats and incidents
- Full protection of your own and your company's data
- Full adherence to compliance requirements – monitor and report deviations

Analyze

When an alert is detected, we conduct an extensive classification of the alert and then start the automated gathering of correlating information for the analysis to start. This process involves evaluating the stage of the attack at which the alert was detected, using the MITRE ATT&CK framework as a reference. The identified tactic serves as the starting point for retrieving relevant information from all integrated data sources within the service. Following an extensive sequence of automated information retrieval, analysis and assessment tasks, the criticality of the alert is determined. Based on this assessment, an appropriate response is then selected and initiated.

Response

After analysis, all alerts will undergo an appropriate response. Some alerts will change to an incident based on the severity:

- Alerts that are considered false positives will automatically be closed while also providing reasoning for this decision and more information

- Incidents that are considered to reveal suspicious activity will initiate technical response measures to stop or gain control of the situation.

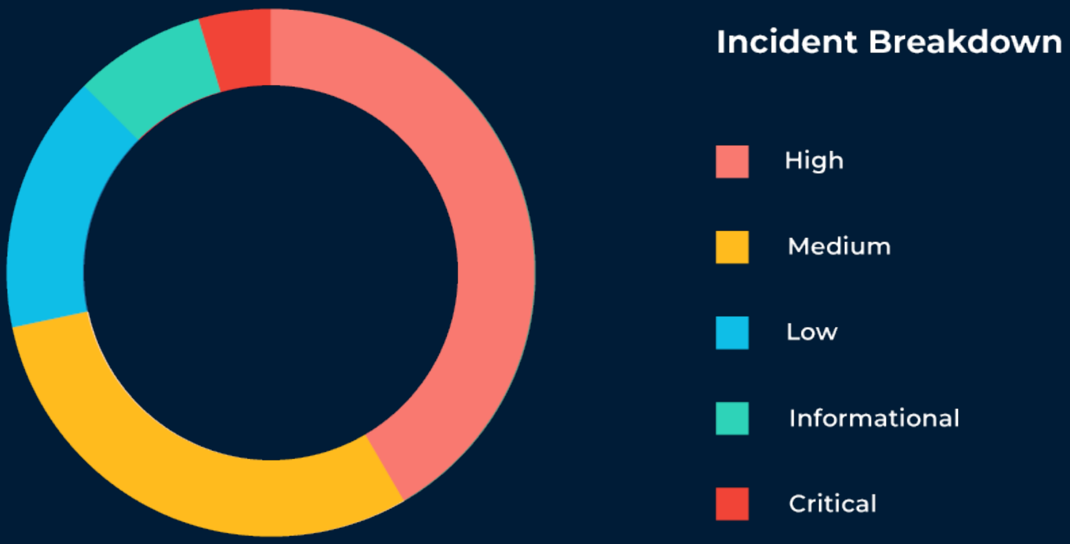
- Incidents that indicate that the customer is under attack and there is activity that cannot be mitigated will be reported to the customer and/or escalated to higher-level incident management.

Read more about our renowned Incident Response Team (IRT)

Benefits

To ensure the safest possible environment for our customers, we strive to adapt our service with a flexible and future proof approach. While also maintaining advanced industry standard benefits:

- **24/7** – Monitoring, detection and response around the clock
- **Risk reduction** - Stable reduction of risks
- **Multilayer prevention** - We stop and hinder ongoing attacks across network, endpoint and cloud assets
- **Insights** – Detailed dashboard with continuous and detailed information
- **Alerts** - Immediate notification and response in the event of incidents for you and affected users
- **Assistance** – Help and follow-up advice from our experts



NSOC (Netsecurity SOC)

NSOC is the hub for our services and operations. NSOC is a modern SOC operation where our security experts, along with market-leading security technology, sophisticated delivery process, supporting operations and continuous improvement, enable us to deliver a world-class security service. This is the foundation of our security monitoring services and is staffed with expert security personnel 24/7. They work with incident management which is supported by our own custom SOAR solution.

The security monitoring center's technical platform is built around automation of repetitive tasks and a logic for orchestration, enabling extremely fast initial analysis and response in the service to prevent and mitigate ingoing and newly intitated attacks against our customers. We have developed an operation that leverages technology to the maximum, while simultaneously using human resources optimally.

About Netsecurity

Netsecurity is a Norwegian owned company delivering services from Norway, focused and specialized within cybersecurity. The cybersecurity market is constantly evolving, with new challenges impacting enterprises and organizations. Insight and intelligence are at the core of every top-class security operation. Netsecurity's holistic security approach is built around our world class Secure Operations. We have developed a market leading cybersecurity operation, by investing in breakthrough innovation and best-of-breed-technology.

Our customers have access to an agile security organization that embeds security into every aspect of their operations, aligning it with each customers specific business needs. In building resilience from the core, our customers businesses can operate and grow confidently even in today's rapidly evolving threat landscape.

Discover more at www.netsecurity.no