
Nedscaper
Protecting against
today's threat landscape
SECURING CLOUDS AND GIVING BACK

Nedscaper company profile

Nedscaper, your partner for next-generation managed security services and consulting. We drive E5 and Azure Sentinel, all day every day 24x7.The company name Nedscaper is derived from Netherlands and Cape Town and is a verb making it our our MDR (SOC) brand.

Nedscaper's Managed Detect and Respond service is powered by Microsoft Azure Sentinel. Nedscaper's offering will guide your organization enhance security monitoring, threat detection, and response services. Nedscaper Cloud SOC helps simplify and strengthen security operations by collecting security data across the entire hybrid enterprise by using built-in artificial intelligence to quickly and accurately identify security threats and runs within your own MS Azure infrastructure. During every last week of the month, the platform is populated with updates of new intellectual property in the form of Azure Playbooks, KQL Queries and further automation.

The Nedscaper Cloud SOC aims to detect, analyse, and respond to cybersecurity incidents using a combination of technological solutions, skilled people and processes. The main advantage of having a Cloud SOC is to improve the detection of security incidents through continuous monitoring and analysis of data activity. Nedscaper provides this Cloud Security service based on Azure Sentinel, a cloud-native SIEM and SOAR solution, and the accompanying high-quality technological intellectual property and support.

Nedscaper's Head Offices are based in Amsterdam, The Netherlands with the Security Operations Center located in Cape Town, South Africa. Nedscaper is a Microsoft Gold partner and supports a multitude of global clients in a variety of industries.

Nedscaper was founded in April 2020, in 2020 through 3 quarters the annual revenue hit 400.000 EUR with a profit margin of 21%. For 2021 the targeted revenue is 2.500.000 EUR with an equal profit margin whilst still being self funded.

Nedscaper article in FD newspaper and Trouw

https://fd.nl/economie-politiek/1377545/een-hippere-plek-voor-offshoring-dan-kaapstad-is-er-niet-npg1caMdrC1I

https://www.trouw.nl/buitenland/zuid-afrika-populair-voor-offshoring-we-geven-onze-medewerkers-wel-een-cursusje-hollandse-directheid~b2a65c0f/

Nedscaper facts and capabilities

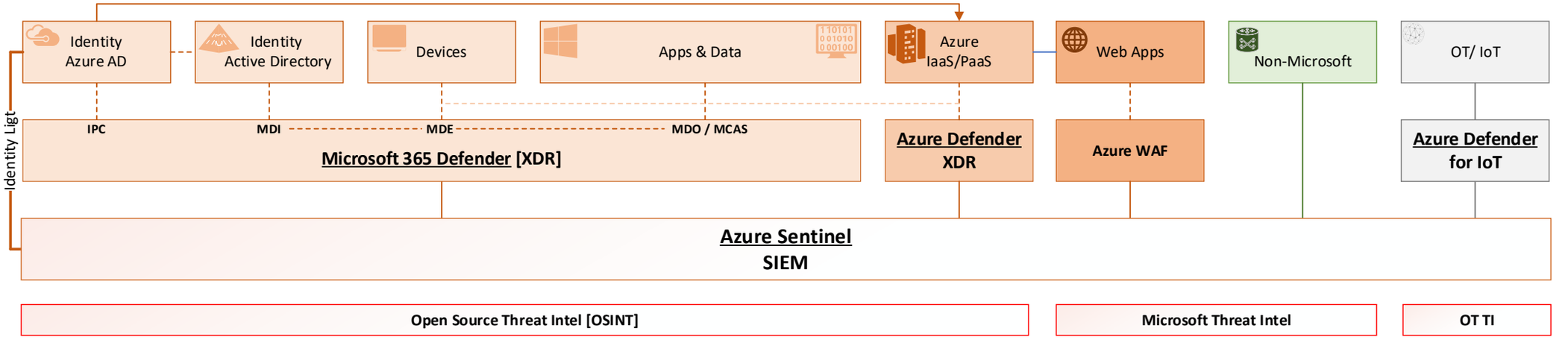
- **Team consistency Amsterdam, Netherlands – Headcount 23**
  - Cloud Security Consultants: 12
  - Cloud Security Analysts: 4
  - Cloud Security Developers: 4
  - Management / HR / account execs: 3

- **Team consistency Cape Town, South Africa – Headcount 8**
  - Cloud Security Consultants: 1
  - Cloud Security Analysts: 4
  - Cloud Security Developers: 1
  - Management / Marketing: 2

- **The Nedscaper Managed Detect and Respond (MDR) Platform**
  - Is based on Azure Sentinel and Microsoft 365 Defender
  - Tier 1 bank: 25,000 users
  - Tier 1 bank: 20,000 users
  - IT system integrator: 2000 users
  - Dutch supermarket chain: 1500 users
  - Agricultural business 3000 users
  - Construction company 5000 users
  - Oil and gas industry business 2000 users
  - Largest Dutch Coffee company 12.5000 users
  - Tier 1 law firm: 2000 users
  - Tier 1 security business: 4000 users
  - SA fintech e-payment company – Nedscaper monitoring the complex hybrid Azure architecture

Nedscaper MDR architecture

- **Microsoft 365 Defender** for the Modern Workplace
- **Azure Defender** for Azure IaaS & PaaS
- **Azure Sentinel** as the MDR and 3rd party ingestion
- **Azure Defender for IoT** (Design Partner)



XDR ❤ MDR

E5 ❤ AZURE SENTINEL

What to expect from a good SOC?

An effective SOC should have the capability to detect incidents at its heart, investigate them in order to decide on an appropriate course of action, and act upon that. It should strive to identify indications of an attack at the earliest possible stage (moving from detect to predict), in order to maximise the opportunity of mitigating the threat before it effectuates and impacts the business. To this end, an effective SOC should be able to understand threats, the cyber terrain as well as the business in which it is actively operating.

The diagram below depicts the six requirements of a good and effective SOC:

Modernized

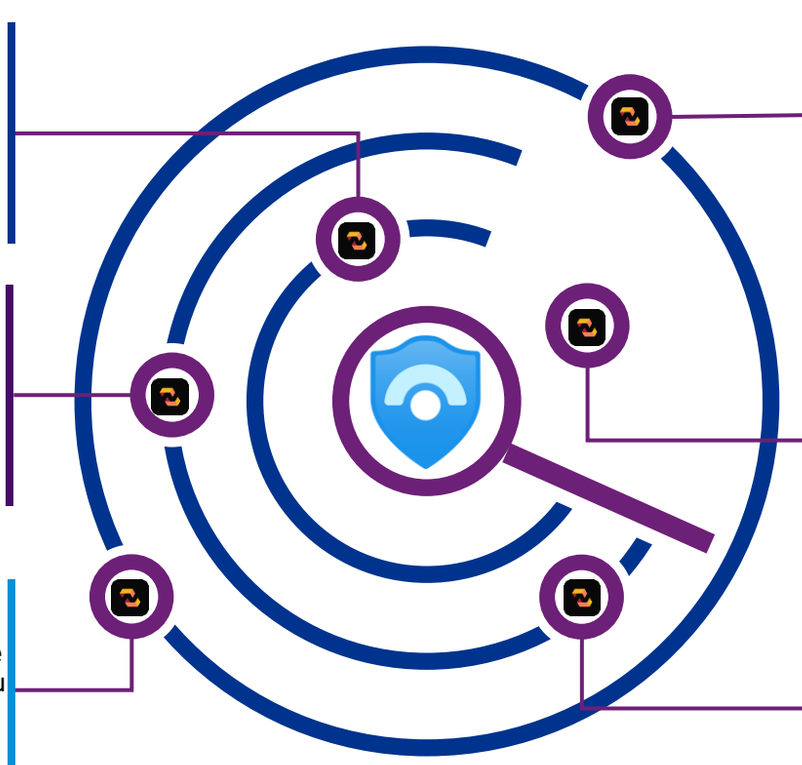
Covering your entire organization, following a cloud native consistent approach, to ensure you avoid blind spots based on broad industry standards.

Threat-led

Enabling effective detection capability for threats applicable to your organization, leveraging threat intelligence sources to determine your priorities and decide how you should respond.

Intelligent

Using a cloud native architecture, flexible and adaptive analytical tools to allow you to make effective, fast decisions based on real-time insights.



Automated

Leveraging SOAR (Security Orchestration, Automation and Response) tooling to accelerate response, increase productivity and allow your team to focus their attention where it really matters.

Agile and scalable

Being able to adapt and respond to the ongoing organizational changes and rapid shift in your attack surface based on automated Microsoft and Nedscaper capabilities.

Integrated and holistic

Enabling overall solution and business integration, integrating cyber detection and response capabilities and identifying synergies where appropriate.

Our approach

Our vision on Security Operations

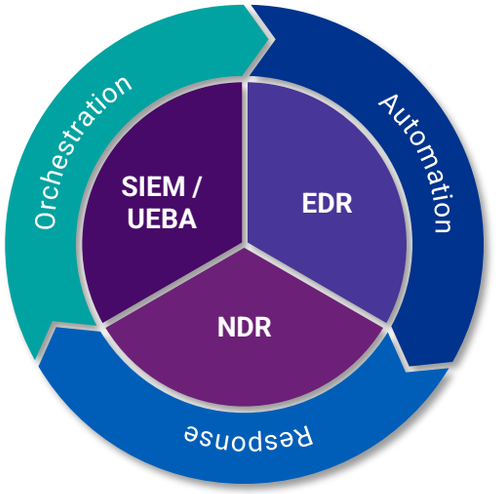
The image on the right depicts the conceptual positioning of the SOC within the global Information Security Function and the Contoso Ecosystem. Such a function consists of the following 4 main functions and their goals:

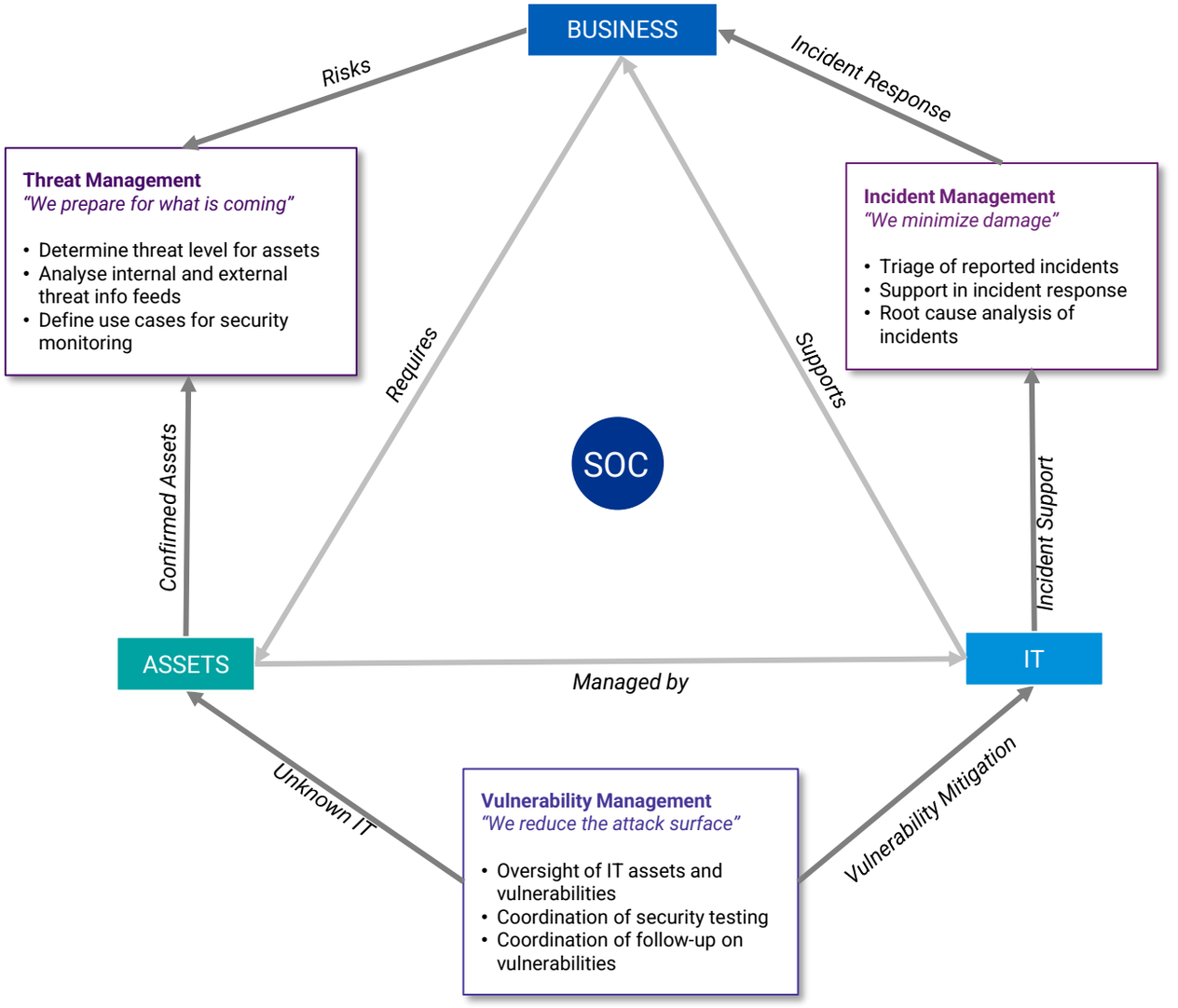
1. **Threat Management** – *'Proactively preparing for what is coming'*
2. **Vulnerability Management** – *'Reducing Contoso's attack surface'*
3. **Incident Management** – *'Minimizing damage and contributing to Contoso's compliance posture'*
4. **Security Monitoring** – *'Detecting potential malicious behavior on Contoso's network and systems'*

Traditionally, a SOC is responsible for Security Monitoring, and may additionally perform one or more of the functions above. In Contoso's context, in addition to Security Monitoring the SOC also performs Threat Management and Security Orchestrated Automated Response.

Building onto the latest industry progress, Nedscaper envisions the SOC from a holistic standpoint within Cyber Defense, combining the latest advancements in ML/AI correlated response throughout the networking and endpoint detection surface by Microsoft 365 and Azure.

Through our proposal with Nedscaper, we are able to encompass all core SecOps capabilities ***as per Contoso needs and requests***; and deploy a highly scalable SOC architecture with vast observability.





Our approach

Nedscaper SOC Target Operating Model

The SOC as an important capability must be driven by a coherent and streamlined operating model that leverages the right arrangement of **people**, **processes** and **technology**.
The Target Operating Model (TOM) establishes the standards for SOC processes, data sources and tools, roles and responsibilities, competencies and learning, stakeholder engagement, governance and performance management. The TOM encompasses the Organization & Governance elements (roles and responsibilities) as well as the required service definition and processes, defining and supporting daily activities for the SOC as part of the Management Framework.

Together with the project team and ongoing operational teams, the IT Ecosystem and the supporting Technology, the content of a TOM is the foundation for effective SOC operation and continuous improvement.

A TOM will be highly customized based on the identified improvements and your ambition level. Some examples of what you can expect a TOM to contain are show in the diagram below.

Nedscaper Security highlights

- **Offensive Services**

- **Azure Defender for IoT and OT Design Partner**
- **Security Design Partner (Microsoft IL)** for MDI, M365D, MDE, MCAS, IPC

RE: PrintNightmare

DN Daniel Naim <Daniel.Naim@microsoft.com>
To Nir Avnery; Derk van der Woude; Raymond Roethof; Mor Rubin; Yaron Kaner; Dana Iris Gutkind
Cc Ofir Shlomo
You replied to this message on 14/07/2021 13:40.

Promised an update – thanks for your finding we found out an edge case that was not covered. Kindly check if with version **2.154.14267.35601** the detection works!

Thanks,
Daniel

#PrintNightmare