Nedscaper

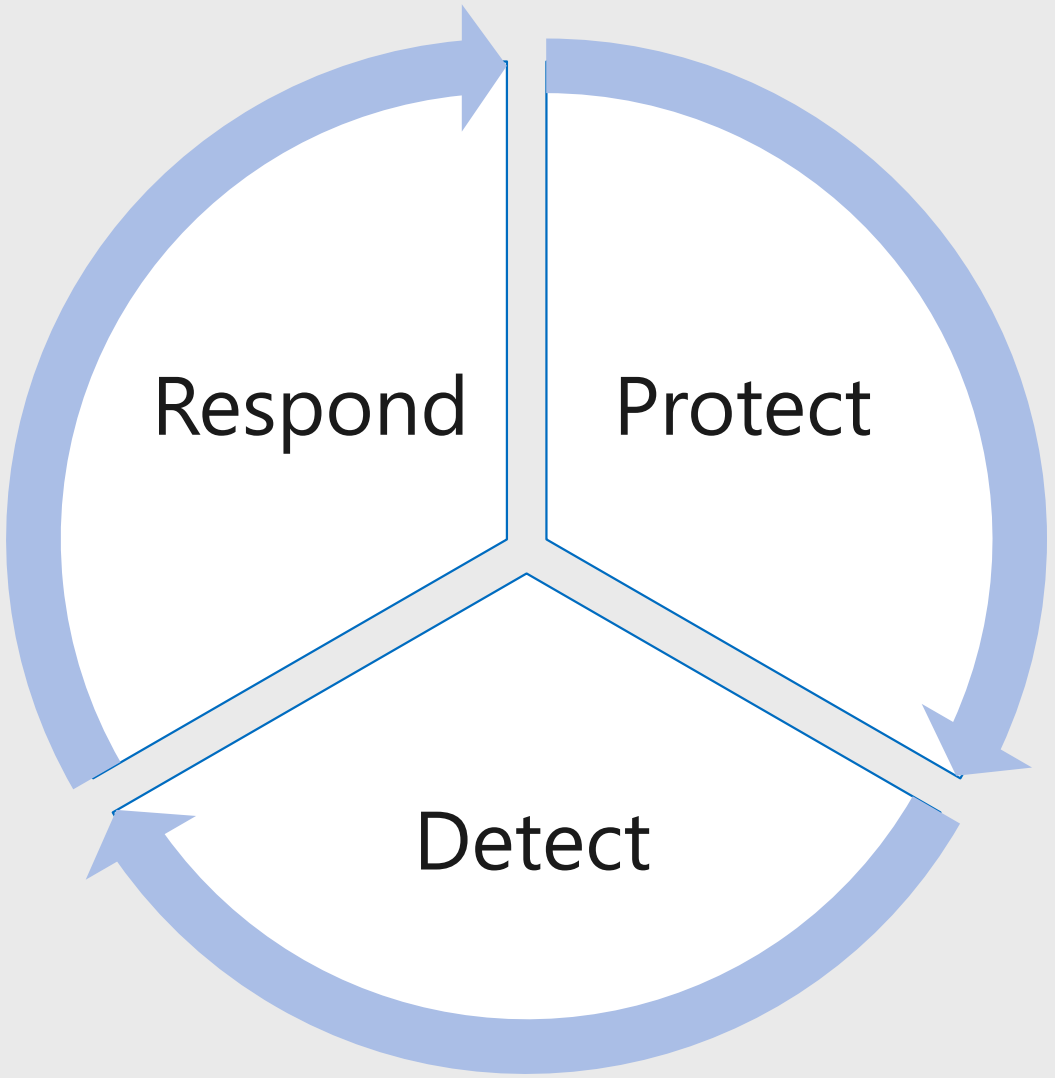
Nedscaper platform overview

// SECURING CLOUDS AND GIVING BACK

Protecting against today's threat landscape

Thomas Verwer
Founder

Cybersecurity Lifecycle



Its about **technology**, **processes** and **people** together. You address cybersecurity threats with one of them alone.

Nedscaper

Nedscaper

Legenda

- Event Log Based Monitoring
- Investigation & Proactive Hunting
- Outsourcing
- Consulting and Escalation
- Native Resource Monitoring

Improve & Learn by Measuring:

Responsiveness - Mean time to Acknowledge (MTTA)

Effectiveness- Mean Time to Remediate (MTTR)

Broad Enterprise View

Correlated/Unified Incident View

Case Management

Machine Learning (ML) & AI

Behavioral Analytics (UEBA)

Security Orchestration, Automation, and Remediation (SOAR)

Security Data Lake

Security Incident & Event Management (SIEM)

Classic SIEM

ArcSight, Radar, splunk>, ...

Alert integration - Graph Security API

Intelligent Security Graph (ISG)
Integrated Threat Intelligence & Deep Human Expertise

SOAR reduces analyst effort/time per incident, increasing overall SOC capacity

Nedscaper

Expert Assistance

Enabling analysts with scarce skills

- Incident Response, Recovery, & CyberOps Services
- Microsoft Threat Experts
- Managed Detection and Response Using Microsoft Threat Protections
- Classic Managed Security Services Provider

Deep Insights

Actionable alerts derived from deep knowledge of assets, and ML/UEBA

Raw Logs

Security & Activity Logs

Security & Network

Provide actionable security alerts, raw logs, or both

Carbon Black., Symantec, FORTINET, SOPHOS, zscaler, FIREEYE, CYBERARK, Lookout, DUO, paloalto, Check Point, f5, CROWDSTRIKE, Barracuda, ...

Microsoft Threat Protection (MTP)

(SOAR)

- Azure Security Center
- Azure ATP
- Azure AD Identity Protection
- Microsoft Defender Advanced Threat Protection (ATP)
- Office 365 ATP
- Cloud App Security

Information Protection

Hybrid Infrastructure and Apps

Java, JBoss, HTML, Microsoft .net, php, .NET, ..., vmware, aws, ...

Identity & Access Management

{LDAP}, Ping, ..., okta, ORACLE, SailPoint

Endpoint & Mobile

...

Modern & SaaS Applications

Office 365, ..., SAML, ...

Information

ORACLE, SQL Server, MySQL, IBM DB2, ...

NEDSCAPER

Platform capabilities

Powered by

Nedscaper

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security appliances

Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response

Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (Log Analytics)

Integrate

Nedscaper ServiceNow

Multiclient CI/CD

Nedscaper Git

Azure