Threat Detection and Response Services

What is threat detection and response?

Threat detection and response (TDR) refers to any advanced cybersecurity tool that identifies threats by correlating threat indicators or by analyzing the environment and user behaviors for malicious or abnormal activities.

Advantages TDRS

- Detection of abnormal user or network behavior or abuse of vulnerabilities.
- Early detection and strengthening of security measures contributes to avoiding unexpected costs.
- Through early detection and subsequent measures, the TDRS service reduces security risks and prevents security incidents.
- Demonstrating to external auditors that you have control over your IT security.

Features TDRS

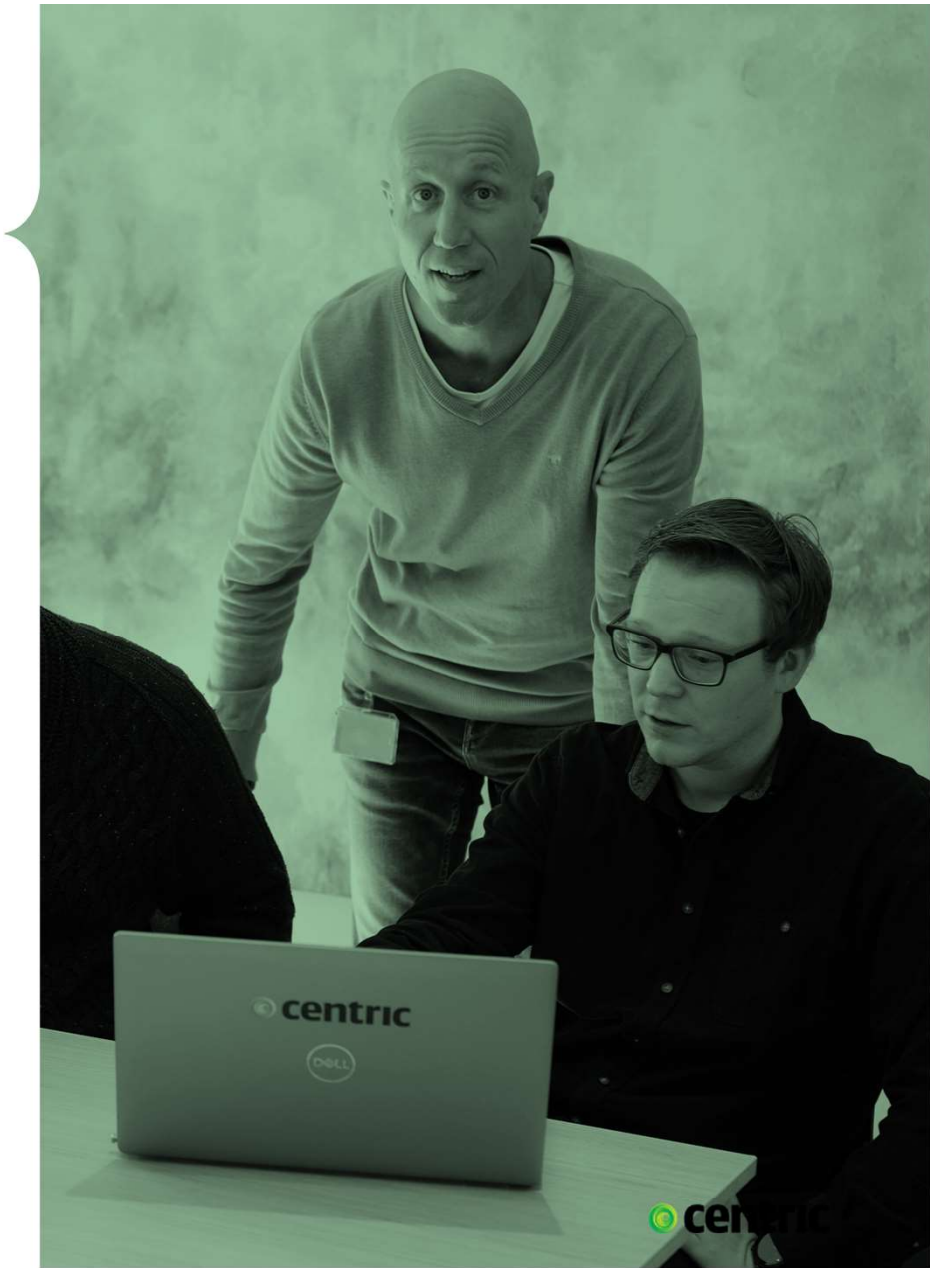
Centrally arranged security information and event management platform

- 7x24 monitoring of vital IT systems
- Detection of security incidents and follow-up based on security event logging
- Recommendations to mitigate security risks and incidents

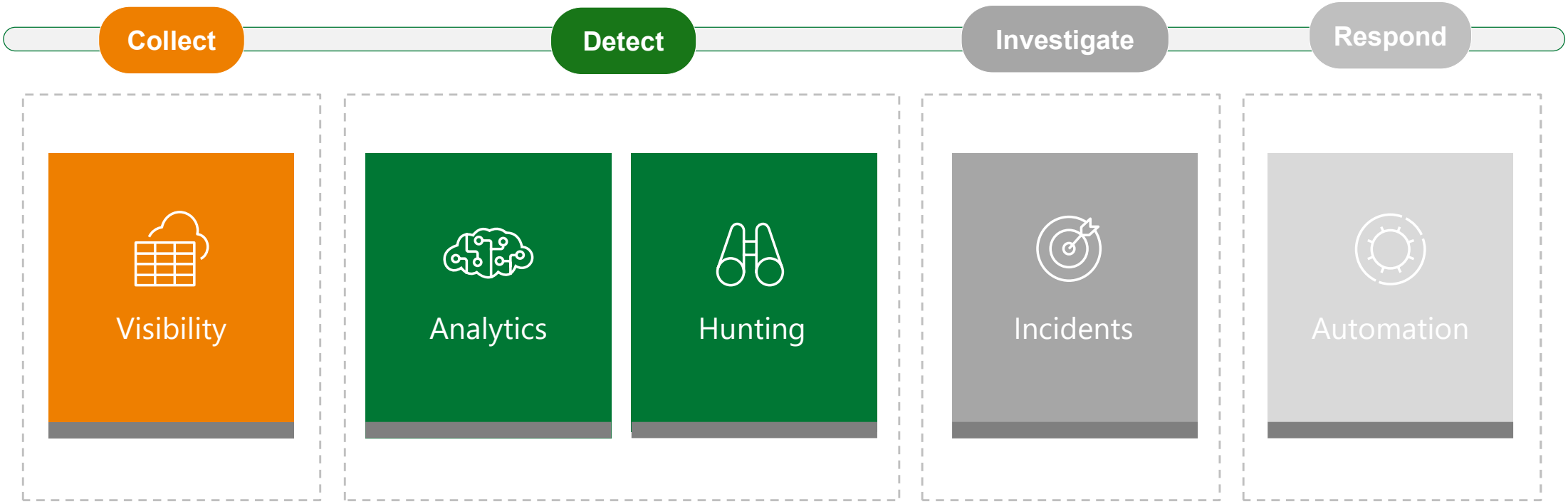
The TDRS security team is actively provided with information from various sources, by:

- Participation in the MSP-ISAC (NCSC) and Connect2Trust
- Threat information channels as components of our Security Information and Event Management (SIEM) and Advanced Threat Protection systems by our vendors and Malware Information Sharing Platform (MISP)

Flexible and transparent payment model



End-to-end solution for security operations



TDRS Services

TDRS – Scoping		Level - 1 (Basic)	Level - 2 (Advanced)	Level - 3 (Professional)	Level - 4 (Professional +)
TDRS Scope	Identity Protection (AAD and AD)	1 AAD, 1 On Prem AD (2 DC) - 35 Rules	1 AAD, 2 On Prem AD (8 DC) - 70 Rules	2 AAD, 2 On Prem AD (20 DC) - 111 Rules	4 AAD, 4 On Prem AD (40 DC) - 111 Rules
	Network Protection (Edge L3 Devices)	2 CIs - 14 Rules	6 CIs - 22 Rules	12 CIs (All Network Layer 3+ CIs) - 32 Rules	30 CIs (All Network Layer 3+ CIs) - 41 Rules
	App Security WAF		2 CIs - 14 Rules	6 CIs - 14 Rules	10 CIs - 14 Rules
	App Security IIS		5 CIs - 10 Rules	15 CIs - 21 Rules	30 CIs - 21 Rules
	App Security Syslog (Apache, Nginx, Linux)			15 CIs - 27 Rules	30 CIs - 27 Rules
	App Security Database			5 CIs - 15 Rules	10 CIs - 15 Rules
	Microsoft Defender for Endpoint (DFE)			Optional	Optional
	Microsoft Defender for Office (DFO)			Optional	Optional
Service Description	Retention period	90 days	90 days	180 days	180 days
	Reports	Weekly summary, monthly KPI report	Weekly summary, monthly KPI report	Weekly summary, monthly KPI report	Weekly summary, monthly KPI report
	Alert Investigation	Automated (7x24)	SOC (5x11 or 7x24)	SOC (5x11 or 7x24)	SOC (5x11 or 7x24)
	Customer Use Cases	On demand	On demand	On demand	On demand
	Infrastructure size (CIs)	Max 5 CIs	Max 22 CIs	Max 75 CIs	Max 154 CIs
	Number of Use Cases	49	116	220	229
Service Hours	Monitoring (hours per month)	0	8	43	68
	Threat Hunting (hours per month)	0	2	4	8


centric
connect.engage.succeed.

Additional information

Publisher	Centric Netherlands
Pricing	Depends on scope
Gold competencies	Security Cloud Productivity
Products	Microsoft Sentinel
Service type	Services
Country/Region	Netherlands
Also available in	EU