certego

Platform & Services
Packages

Unified Security Operations Platform
& SecOps Services

Platform & Services Packages

certego

PanOptikon®
Unified Security Operations Platform

	Standard	Premium
Multi-Tenant SaaS	✓	✓
Raw Telemetry Visibility	✓	✓
Query and Integrations APIs	✓	✓
Sub-Tenant Groups Management	✓	✓
MSSP License Consumption Dashboard	✓	✓
MSSP Partner Visibility	✓	✓
Security Orchestration, Automation & Response (SOAR)	✓	✓
Automated Response and Remediation (Playbooks)	✓	✓
3rd-party Integration	✓	✓
Customized Playbooks	✗	✓

Platform & Services Packages

Security Operations Services

	Standard	Premium
Coverage 24/7/365	✓	✓
Managed Detection and Response (MDR) Services	✓	✓
Guided Onboarding & Deployment Services	✓	✓
Training Services	✓	✓
Executable Analysis (Sandbox)	✓	✓
On-demand Threat Analysis	✓	✓
Incident Report	Standard	Custom
Service Review	Up to 1/y	Up to 2/y
Custom SLA	✗	✓
Certego Service Specialist	✗	Add-on
Digital Forensics	✗	Add-on

Platform & Services Packages

Threat Intelligence

	Standard	Premium
Proprietary Threat Intelligence Platform	✓	✓
Log Integration	✓	Custom
Threat Intelligence IOCs	✓	✓
Threat Intelligence BIOCs	✓	✓
Monthly Threat Intelligence Report	✓	✓
Credential Theft Monitoring	✗	✓
Custom Ticket Classification	✗	✓
Custom Severity	✗	✓
Custom Correlation	✗	✓
Custom Threat Hunting	✗	✓

Platform & Services Packages

Endpoint Detection & Response (EDR)

	Standard	Premium
Secure Remote Shell	✓	✓
Automatic Remediation	✓	✓
Active Directory Integration	✓	✓
File & Process Events Monitoring & Logging	✓	✓
Threat Hunting	✓	✓
Remediation Playbooks	✓	✓
Application and Endpoint Inventory	✓	✓
Windows Events Logging	✓	✓
Windows Events Visibility	✓	✓

Platform & Services Packages

Endpoint Prevention

	Standard	Premium
Next Generation Antivirus (NGVA)	✓	✓
Ransomware Protection	✓	✓
Malware Protection	✓	✓
Exploit Protection	✓	✓
Critical Component Protection	✓	✓
File & Documents Protection	✓	✓
Device Control	✓	✓
Credentials Theft Protection	✗	✓

Platform & Services Packages

certego

Network Detection & Response (NDR)

	Standard	Premium
Network Scan Detection	✓	✓
Log Collection & Correlation	✓	✓
Malware Callback Detection	✓	✓
DNS Attack Detection	✓	✓
Domain Filtering	✓	✓
Port Scanning Detection	✓	✓
Zero-day & APT Detection	✓	✓
Intrusion Detection System (IDS)	✓	✓

Platform & Services Packages

User Behavior Analytics (UBA)

	Standard	Premium
User Visibility	✓	✓
User Threat Level	✓	✓
Lateral Movement Detections	✓	✓
Login Anomaly Detection	✓	✓

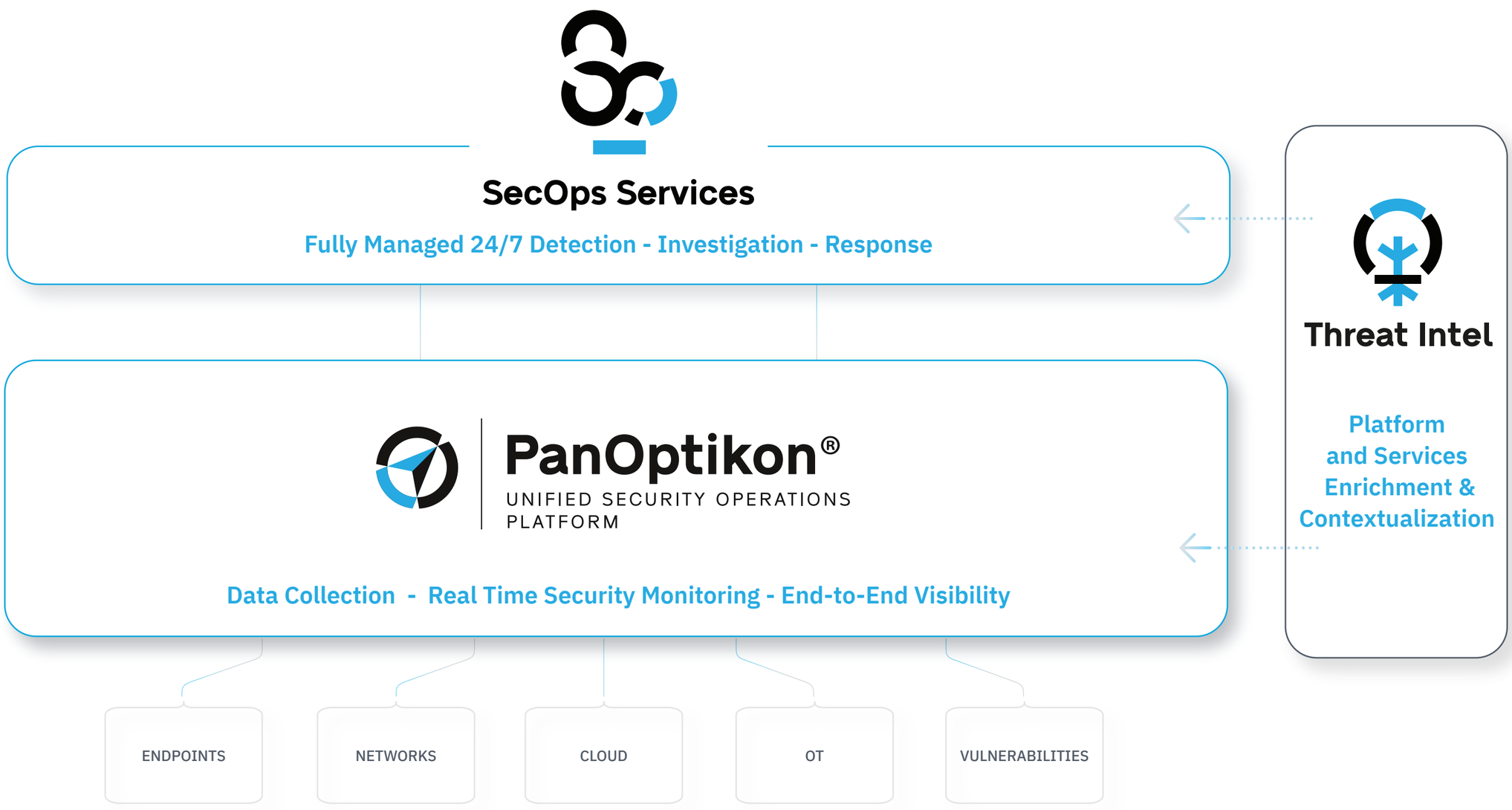
Centralized Log Management

	Standard	Premium
EDR Data Retention	✓	Add-on
3rd-party logs (Firewall, Web Filtering, Email filt, etc)	✗	✓
SaaS Application Data Retention	✗	✓

Pure-play MDR provider con oltre di 11 anni di esperienza nella lotta al cybercrime

Il fulcro dell'offerta di Certego si articola attorno a tre pilastri che, integrati tra loro in modo sinergico, costituiscono la base della sua forza: la **piattaforma di Unified Security Operations "PanOptikon®"**, un team dedicato di **Security Operations Services** e un'intensa attività di ricerca nell'ambito della **Cyber Threat Intelligence**.

La stretta interconnessione tra tecnologia avanzata, competenze umane altamente specializzate e analisi approfondita delle minacce, posiziona Certego come player all'avanguardia nei servizi di **Managed Detection & Response**.



24/7 **Sempre pronti a proteggerti**

200+ **Clienti Attivi**

1M+ **Asset Monitorati**

110K **Allarmi Gestiti** (2023)

10K **Incidenti Gestiti** (2023)

Via F. Lamborghini 81, 41121 Modena (MO)