


Supply, installation and service of industrial measuring instruments, analysers and continuous monitoring systems for gases, liquids and particles for environmental and process applications. Comprehensive solutions in the field of cybersecurity in accordance with NIS2 requirements.

Pure|Defense MDR Service for SMB

 Author and Solution Authority


SANS / GIAC Security Operations Manager (GSOM)

Igor Kapitančík

SANS / GIAC Certified Forensic Analyst (GCFA)

Security Service and Solution Architect
Certified Cybersecurity Operations Leader
Security Automation and Orchestration System Architect

Software Developer with Security Expertise
Senior Security & Monitoring Specialist / Analyst
Senior IT Administrator

 **MDR (Managed Detection and Response) Service** provides continuous threat **monitoring**, advanced **detection**, and rapid incident **response** through AI-driven & Expert-Led analytics, expert threat hunting, and adaptive cyber defense playbooks, ensuring fast threat neutralization and proactive containment against evolving cyber threats.

As an **MDR (Managed Detection and Response) provider**, we deliver a proactive, intelligence-driven, vendor-agnostic (X|EDR) cybersecurity solution designed to continuously monitor, detect, and rapidly respond to evolving cyber threats. By leveraging AI-driven & Expert-Led analytics, behavioral threat detection, and expert-led investigations, we provide real-time visibility into security incidents, enabling Fast-Acting Preliminary Security Threat Neutralization and Rapid Incident Containment. Our approach ensures that threats are mitigated before they escalate, minimizing operational disruptions and preventing breaches.

We operate with a Threat-Specific Adaptive Cyber Defense & Response Playbook, ensuring that Incident Quarantine Procedures & Threat Propagation Control are effectively implemented to contain attacks before they spread. Our service integrates Incident Handling Guidelines, Threat Mitigation Strategies & Risk Mitigation Advisory, aligning security operations with regulatory compliance and industry best practices. With our 24/7 SOC operations, proactive threat hunting, and automated response capabilities, we enhance cybersecurity resilience, delivering holistic threat containment and continuous security improvements to help organizations defend against advanced cyber adversaries.

Core Threat Detection & Response Framework

The **Core Threat Detection & Response Framework** is the foundational blueprint that defines how modern MDR services systematically identify, investigate, and respond to cyber threats in real time. The process typically begins with an **Event on Host**, such as an unauthorized process execution, suspicious login attempt, or anomalous system behavior. These events are first detected by **XDR (Extended Detection and Response) tools**, which not only provide rich telemetry across **endpoints, networks, cloud environments, and identities**, but also **automatically perform containment actions on known threats** to prevent their spread and reduce impact before further analysis begins. Once detected, the raw telemetry or events are then **ingested by a connector** into the centralized security platform for processing and enrichment, next are **stored and indexed by a Log Management system**, ensuring they are available for real-time and retrospective analysis. This structured data is then **correlated by the SIEM (Security Information and Event Management)**, which applies predefined detection rules, cross-references threat intelligence feeds, behavioral baselines and models, and known Indicators of Compromise (IoCs) to identify meaningful patterns.

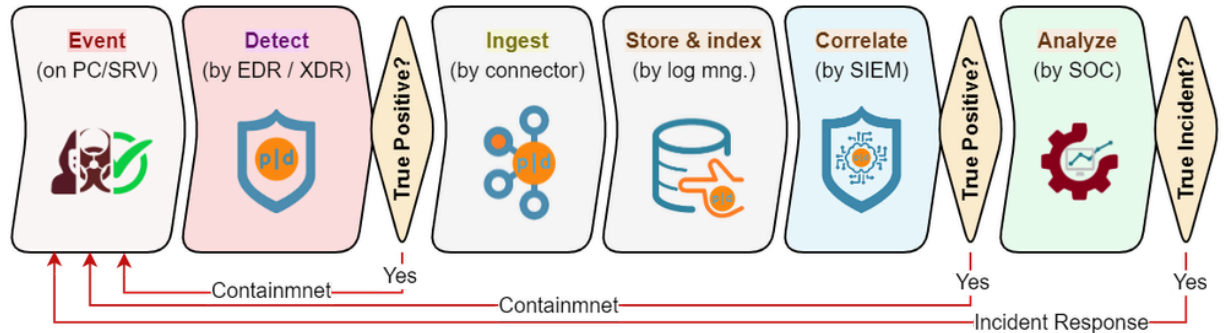
Alerts generated and enriched from this correlation are analyzed by the SOC team, where human analysts apply contextual understanding and threat hunting methodologies to assess severity, validate findings, investigate context, and determine whether the alert represents a true threat, a false positive, or a potential false negative due to detection gaps — initiating response actions if necessary. This framework supports seamless integration with **automated playbooks, containment workflows, and compliance-driven reporting** — ensuring both operational efficiency and regulatory adherence — enables continuous refinement through feedback loops, improving detection fidelity, threat triage efficiency, and response accuracy. By leveraging this layered approach—from detection to response—organizations can achieve faster mean time to detect (MTTD), reduce dwell time, and improve their overall cyber defense posture and integrating automated enrichment, playbook-driven responses, and escalation paths, the framework ensures that threats are **prioritized, contained, and remediated in a timely and structured manner**, forming the operational backbone of any modern MDR service.

Registered office:
ECM MONITORY, spol. s r.o.
Kuzmanyho 57
040 01 Kosice
Slovakia

Bank contact:
IBAN: SK02 1100 0000 0026 2572 1210
SWIFT/BIC: TATRSKBX

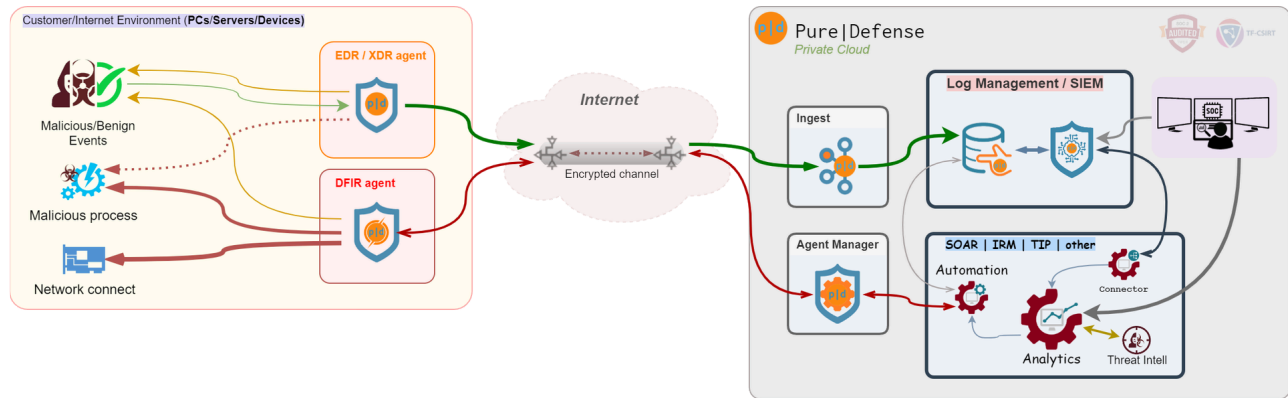
Company Registration Number: 31680372
VAT Registration Number: SK2020491495
Tax Registration Number: 2020491495

Core Threat Detection & Response Framework Chain



Pure|Defense MDR Service Delivery Models

Managed Detection and Response (MDR) Service Delivery Models define the structural and technological approach through which cybersecurity services are deployed, operated, and integrated into an organization's environment. The primary model is a **Private-Cloud Based MDR**, where all threat detection, telemetry ingestion, correlation, and response orchestration are hosted securely within a dedicated cloud infrastructure. This approach ensures high availability, scalability, and centralized threat intelligence while maintaining strong data privacy controls. It is particularly suited for organizations looking to leverage advanced security analytics and 24x7 monitoring without maintaining heavy on-premises infrastructure.



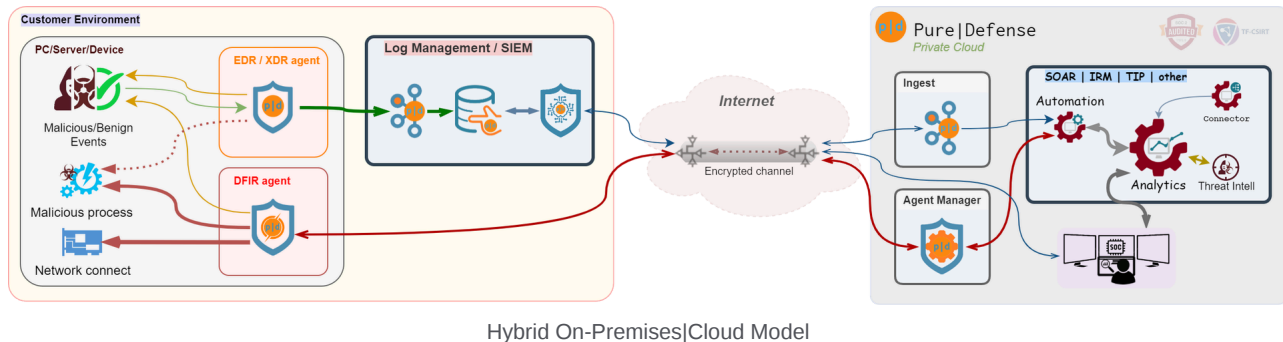
Private-Cloud Based Model

For organizations with strict data residency requirements, regulatory constraints, or a need for localized control, the MDR service can be extended to incorporate an **On-Premises Cybersecurity Analytics Platform**. This enables the creation of a **Hybrid Cloud/On-Premises MDR model**, which blends the flexibility of cloud-based analytics with the control and sovereignty of on-prem deployments. In this model, sensitive telemetry, logs are processed and retained locally, while benefiting from cloud-based correlation engines, global threat intelligence, and centralized SOC support. This hybrid model offers a balanced approach—providing operational agility, data control, and enhanced compliance alignment tailored to complex enterprise or regulated environments.

Registered office:
ECM MONITORY, spol. s r.o.
Kuzmanyho 57
040 01 Kosice
Slovakia

Bank contact:
IBAN: SK02 1100 0000 0026 2572 1210
SWIFT/BIC: TATRSKBX

Company Registration Number: 31680372
VAT Registration Number: SK2020491495
Tax Registration Number: 2020491495

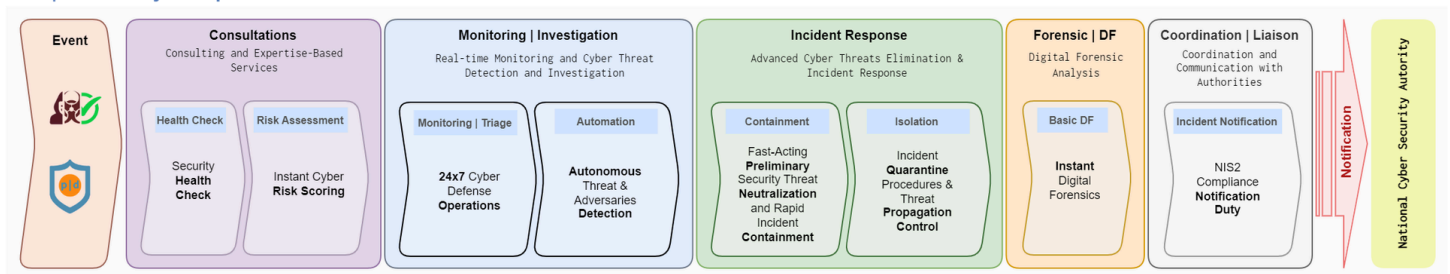


Pure|Defense Cyber Operations Process Flow

The **Cyber Defense Operations Process Flow** defines the structured, end-to-end methodology through which organizations monitor, detect, analyze, and respond to cyber threats in a continuous and resilient manner. At the core of this process is the operation of **24x7 Cyber Defense Operations**, driven by a combination of **Autonomous Threat & Adversaries Detection** and expert-led **Live Cyber Threat Hunting Operations**. This real-time vigilance enables security teams to identify abnormal behavior early and initiate **Fast-Acting Preliminary Security Threat Neutralization** to prevent escalation.

Once a threat is validated, the process transitions into **Rapid Incident Containment**, leveraging **Incident Quarantine Procedures** and **Threat Propagation Control** to isolate affected assets and halt lateral movement. These actions are orchestrated through the **Cyber Defense & Incident Response Hub**, which provides visibility and operational command via **Cyber Defense Key Performance Indicators & Metrics Dashboards**. The entire flow is supported by **Real-Time Security Incident Life-Cycle Management & Escalation**, ensuring timely mitigation and compliance with regulatory obligations such as the **NIS2 Compliance Notification Duty**. Capabilities such as **Security Health Check**, and **Risk Assessment** are utilized during on-boarding phase to validate and enhance the cyber defense posture. This dynamic and adaptive process ensures organizations remain both resilient and compliant in the face of evolving cyber threats.

Pure|Defense Cyber Operations Process Flow



MDR Service Features & Capabilities

MDR Service Features & Capabilities refer to the core functionalities and advanced security measures that enable continuous threat monitoring, proactive attack detection, rapid incident response, and automated threat containment.

Our **MDR service function** is built on a proactive, intelligence-driven approach to cybersecurity, delivering continuous threat monitoring, advanced detection, and rapid incident response to protect organizations from sophisticated cyber threats. We operate using a combination of AI-powered & Expert-Led analytics, real-time threat intelligence, and expert-led threat hunting, enabling fast-acting preliminary security threat neutralization and rapid incident containment to prevent breach escalation. Through automated detection and response mechanisms, we empower security teams to swiftly identify, investigate, and remediate security incidents with minimal impact on business operations.

Real-time Monitoring and Cyber Threat Detection and Investigation

Monitoring | Investigation

Real-time monitoring and cyber threat detection ensure continuous **visibility** and proactive **mitigation**. AI-driven & Expert-Led analytics and expert analysis rapidly detect threats, assess risks, and contain incidents. Strategic asset surveillance and real-time risk assessment enhance security, aligning with ISO 27001 standards, NIS2 direction and other for incident response and risk management.

Function	pure defense SMB	Description
24x7 Cyber Defense Operations <div>Monitoring Triage</div>	INCLUDE	<p>Ensures continuous threat monitoring, rapid incident response, and proactive risk mitigation to protect organizations from evolving cyber threats in real time.</p>
Autonomous Threat & Adversaries Detection <div>Automation</div>	INCLUDE	<p>AI-driven security approach that leverages machine learning, behavioral analytics, and threat intelligence to identify, analyze, and respond to cyber threats and adversarial activities in real time without manual intervention.</p>
Cyber Security Expert-Driven Cyber Threat Detection <div>Investigation</div>	8X5	<p>Combines human intelligence, advanced analytics, and threat hunting to analyze complex attack patterns, identify sophisticated threats, and conduct deep forensic investigations, ensuring precise and adaptive incident response.</p>
Root Cause & Origin Analysis <div>Analysis</div>	ADD-ON	<p>Identification of the underlying cause, attack entry point, and threat vectors of a security incident to enable effective remediation and future risk prevention.</p>
Strategic Asset Cyber Surveillance & Extended Monitoring <div>Critical Asset Monitoring</div>	ADD-ON	<p>A proactive security approach that ensures continuous oversight, threat detection, and risk assessment of critical assets to prevent cyber threats and maintain operational resilience.</p>

Registered office:
ECM MONITORY, spol. s r.o.
Kuzmanyho 57
040 01 Kosice
Slovakia

Bank contact:
IBAN: SK02 1100 0000 0026 2572 1210
SWIFT/BIC: TATRSKBX

Company Registration Number: 31680372
VAT Registration Number: SK2020491495
Tax Registration Number: 2020491495

Advanced Cyber Threats Elimination & Incident Response

Incident Response

A **proactive, intelligence-driven approach** that leverages AI-powered threat detection, expert-led analysis, and automated response mechanisms to rapidly identify, **contain**, and **neutralize** sophisticated cyber threats. By integrating real-time risk assessment, forensic investigations, and adaptive mitigation strategies, it ensures minimal impact, operational resilience, and continuous security posture improvement.

Function	pure defense SMB	Description
Fast-Acting Preliminary Security Threat Neutralization and Rapid Incident Containment Containment	INCLUDE	ⓘ A proactive cybersecurity approach that ensures immediate threat suppression, swift incident isolation, and mitigation to prevent escalation and minimize operational impact. By leveraging automated response mechanisms and expert-driven analysis , it enables efficient containment and accelerated recovery from cyber incidents.
Threat-Specific Adaptive Cyber Defense & Response Playbooks Playbooks	INCLUDE	ⓘ Dynamic, intelligence-driven security protocols that provide customized threat mitigation, rapid incident response, and adaptive defense strategies tailored to specific cyber threats.
Incident Quarantine Procedures & Threat Propagation Control Isolation	INCLUDE	ⓘ Critical cybersecurity measures that isolate compromised systems, contain threats, and prevent lateral movement through automated response mechanisms , ensuring minimal impact and rapid threat neutralization .
Incident Handling Guidelines, Threat Mitigation Strategies & Risk Mitigation Advisory Advisory	ADD-ON	ⓘ Provide structured response protocols, proactive threat containment measures, and strategic risk reduction guidance to ensure effective incident management, minimal impact, and enhanced cybersecurity resilience .

Presentation, Reporting, Integration and Notification (of Detection, Incident and Response)

Portal | Reports | Notification

Ensures real-time threat **visibility**, streamlined incident response, and data-driven security improvements. Through the Cyber Defense & Incident Response Hub, security teams leverage Key Performance Indicators, Incident Life-Cycle Management, and Context-Aware Notifications to prioritize threats, enhance intelligence sharing, and automate remediation, strengthening cyber resilience and operational readiness.

Function	pure defense SMB	Description
Cyber Defense & Incident Response Hub <div>Portal</div>	INCLUDE	<p>i A centralized security operations platform that integrates real-time threat detection, incident management, and automated response workflows. It enables efficient threat mitigation, rapid incident resolution, and continuous cybersecurity posture improvement across the constituency.</p>
Cyber Defense Key Performance Indicators & Metrics Dashboards <div>Dashboards</div>	INCLUDE	<p>i Provide real-time visibility into security operations, threat trends, and incident response effectiveness. By aggregating critical cybersecurity metrics, these dashboards enable proactive risk assessment, performance monitoring, and compliance tracking, ensuring data-driven decision-making and continuous security improvement.</p>
Cybersecurity Performance & Metrics Regular Review <div>Reports</div>	MONTHLY	<p>i A structured assessment process that evaluates threat detection efficiency, incident response effectiveness, and overall security posture based on key performance indicators (KPIs) and real-time metrics. By analyzing historical trends, remediation success rates, and compliance adherence, organizations can identify gaps, optimize security strategies, and enhance cyber resilience against evolving threats.</p>
Real-Time Security Incident Life-Cycle Management (include Escalation) <div>Incident Life-Cycle Escalation</div>	INCLUDE	<p>i A structured, end-to-end approach to detecting, analyzing, containing, and resolving security incidents in real time. By integrating automated detection, AI-driven threat intelligence, and escalation protocols, it ensures rapid incident prioritization, efficient response coordination, and minimal operational disruption, strengthening an organization's overall cyber resilience.</p>

Comprehensive Cyber Threat Hunting

Threat Hunting | TH

A **proactive, intelligence-driven approach** that leverages Advanced Threat Profiling for Risk Mitigation, Threat-Specific Hunting Operations, and Ongoing Worldwide Cyber Attack Tactical Surveillance to detect and neutralize sophisticated cyber threats. By utilizing Live Cyber Threat Hunting Operations and Forensic-Based In-Depth Threat Investigation, security teams can identify adversarial tactics, analyze attack footprints, and mitigate risks in real time. This continuous, expert-led process strengthens cyber resilience, reduces dwell time, and enhances proactive defense against evolving threats.

Function	pure defense SMB	Description
Live Cyber Threat Hunting Operations Operational TH	INCLUDE	i Proactive security approach that leverages advanced threat intelligence, behavioral analytics, and AI-driven anomaly detection to identify and neutralize cyber threats as they emerge. By integrating continuous monitoring, forensic-driven investigation, and rapid response mechanisms, it enables immediate detection, containment, and mitigation of sophisticated adversarial activities, reducing dwell time and strengthening cyber resilience.

Cyber Threat Intelligence

Threat Intelligence | CTI

A **proactive, intelligence-driven approach** that leverages Threat Actor Attribution & Incident Contextualization to identify, analyze, and mitigate evolving cyber threats. By integrating Deep Web Intelligence-Driven Threat Surveillance and Cyber Threat Intelligence Hub, organizations gain real-time threat visibility, enhance detection capabilities, and strengthen their cybersecurity posture against adversarial tactics and emerging attack vectors.

Function	pure defense SMB	Description
Proactive Intelligence-Driven Threat Management CTI	ANNOUNCE	i Leverages real-time threat intelligence, adversary profiling, and automated detection to anticipate, detect, and mitigate cyber threats before they escalate, ensuring early risk mitigation and adaptive defense strategies.

Digital Forensic Analysis

Forensic | DF

Digital Forensic Analysis is a **systematic process of collecting, examining, and interpreting digital evidence** to investigate cyber incidents, data breaches, and malicious activities. By leveraging **Instant Digital Forensics, Fundamental Malware Analysis, and Full-Fledged & Legally Sound Digital Forensics**, security teams can rapidly identify threats, ensure evidence integrity, and support legal and incident response efforts.

Function	pure defense SMB	Description
Instant Digital Forensics Basic DF	INCLUDE	<p>i A real-time, intelligence-driven approach to rapidly analyzing, identifying, and responding to security incidents. By leveraging Live Digital Forensic techniques, security teams can immediately extract and examine digital evidence, define Indicators of Compromise (IoCs) and Indicators of Attack (IoAs), and accelerate threat containment and remediation.</p>
Fundamental Malware Analysis Reverse Engineering	PHISH-FORENSICS	<p>i A core cybersecurity process that involves examining malicious code to identify its behavior, capabilities, and impact. By leveraging static and dynamic analysis techniques, security teams can detect Indicators of Compromise (IoCs), uncover attack vectors, and assess potential risks, enabling effective threat mitigation and response.</p>

Coordination and Communication with Authorities

Coordination | Liaison

Coordination and Communication with Authorities refers to the structured engagement between an organization's cybersecurity team and relevant governmental, regulatory, and law enforcement bodies. This ensures compliance with legal requirements, facilitates threat intelligence sharing, enables timely incident reporting, and supports crisis management efforts. Effective coordination helps mitigate risks, improve response times, and strengthen overall cybersecurity resilience.

Function	pure defense SMB	Description
NIS2 Compliance Notification Duty <div>Incident Notification</div>	INCLUDE	<p>i A mandatory regulatory requirement under the NIS2 Directive, requiring organizations to promptly report significant cybersecurity incidents to relevant authorities. This obligation ensures transparent communication, rapid threat containment, and regulatory compliance, enabling authorities to assess risks, coordinate responses, and mitigate potential disruptions to critical infrastructure and essential services.</p>
NIS2 Regulatory & Cybersecurity Compliance Liaison <div>Authority Communication</div>	ADD-ON	<p>i A designated security professional responsible for ensuring compliance with the NIS2 Directive, managing incident reporting, regulatory communication, and cybersecurity governance. This role facilitates coordination with authorities, oversees the NIS2 Compliance Notification Duty, and ensures adherence to legal and industry cybersecurity requirements, strengthening the organization's regulatory posture and resilience against cyber threats.</p>
Dedicated Incident Response Commander <div>Dedicated Commander</div>	AD-HOC CONTACT SALES	<p>i A senior security leader responsible for overseeing and coordinating all aspects of cyber incident response. This role ensures rapid threat containment, regulatory compliance, and seamless communication with internal teams and external authorities, including fulfilling NIS2 Compliance Notification Duty and managing Emergency Incident Response Hotlines to minimize operational impact and strengthen cyber resilience.</p>

Tel.: ++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Supply, installation and service of industrial measuring instruments, analysers and continuous monitoring systems for gases, liquids and particles for environmental and process applications. Comprehensive solutions in the field of cybersecurity in accordance with NIS2 requirements.

Consulting and Expertise-Based Services

Consultations

Specialized cybersecurity advisory, risk assessments, and strategic guidance to help organizations enhance security posture, mitigate threats, and achieve regulatory compliance. By leveraging Security Health Checks, Instant Cyber Risk Scoring, and Live Exploitability Analysis, security experts deliver tailored solutions for Compliance-Driven Security Framework Implementation, Cybersecurity Governance Integration, and SOC operations, ensuring proactive defense and resilience against evolving cyber threats.

Function	pure defense SMB	Description
Security Health Check Health Check	INCLUDE	<p>i A comprehensive assessment of an organization's cybersecurity posture, identifying vulnerabilities, misconfigurations, and potential risks. By leveraging Instant Cyber Risk Scoring, Live Exploitability Analysis, and Compliance-Driven Security Framework Implementation, it provides actionable insights to strengthen defenses, enhance threat resilience, and ensure regulatory compliance.</p>
Instant Cyber Risk Scoring Risk Assessment	INCLUDE	<p>i A initial evaluation of an organization's security posture, analyzing vulnerabilities, threat exposure, and exploitability to provide immediate risk quantification. By leveraging Live Exploitability Analysis, Security Health Checks, and Compliance-Driven Security Framework Implementation, it enables organizations to prioritize mitigation efforts, enhance threat resilience, and maintain regulatory compliance.</p>
On-Prem Cybersecurity Analytics Platform On-Prem SecMonitoring	CONTACT SALES	<p>i A locally deployed security solution that enables organizations to analyze threats, detect anomalies, and respond to incidents in real time within their own infrastructure. By leveraging Live Exploitability Analysis, Compliance-Driven Security Framework Implementation, and Enterprise Security Operations Center (SOC) integration, it ensures full data control, regulatory compliance, and enhanced threat intelligence while minimizing reliance on external cloud-based security services.</p>

Registered office:
ECM MONITORY, spol. s r.o.
Kuzmanyho 57
040 01 Kosice
Slovakia

Bank contact:
IBAN: SK02 1100 0000 0026 2572 1210
SWIFT/BIC: TATRSKBX

Company Registration Number: 31680372
VAT Registration Number: SK2020491495
Tax Registration Number: 2020491495