KUDELSKI SECURITY

SOLUTION OVERVIEW

Managed Detection & Response Services

Managed Detection & Response

Protecting your Changing Environments with High-Touch, Customized Threat Detection and Response Services

AT A GLANCE

- **Complete Threat Visibility:** IT, OT, cloud, and endpoint
- **Rich Contextualization:** Threat detection and response architected to your unique business and threat model
- **Superior Value:** 99.9% reduction in noise; we escalate validated security incidents within an average of 10 minutes
- **Flexible Technology Deployment Options:** Fully managed and integrated with your environment
- **Intelligence-Driven, Human-Led Expertise:** Optimized and accelerated threat detection
- **Maturity Advancement:** Measurable security improvements and reduction in risk
- **Full Transparency:** Instant access to intuitive MSS Client Portal

CONTENT

A Different Approach to MDR

Kudelski Security's Managed Detection and Response (MDR) services enable security leaders to navigate an expanding threat landscape and demonstrate a measurable reduction in business risk to the board.

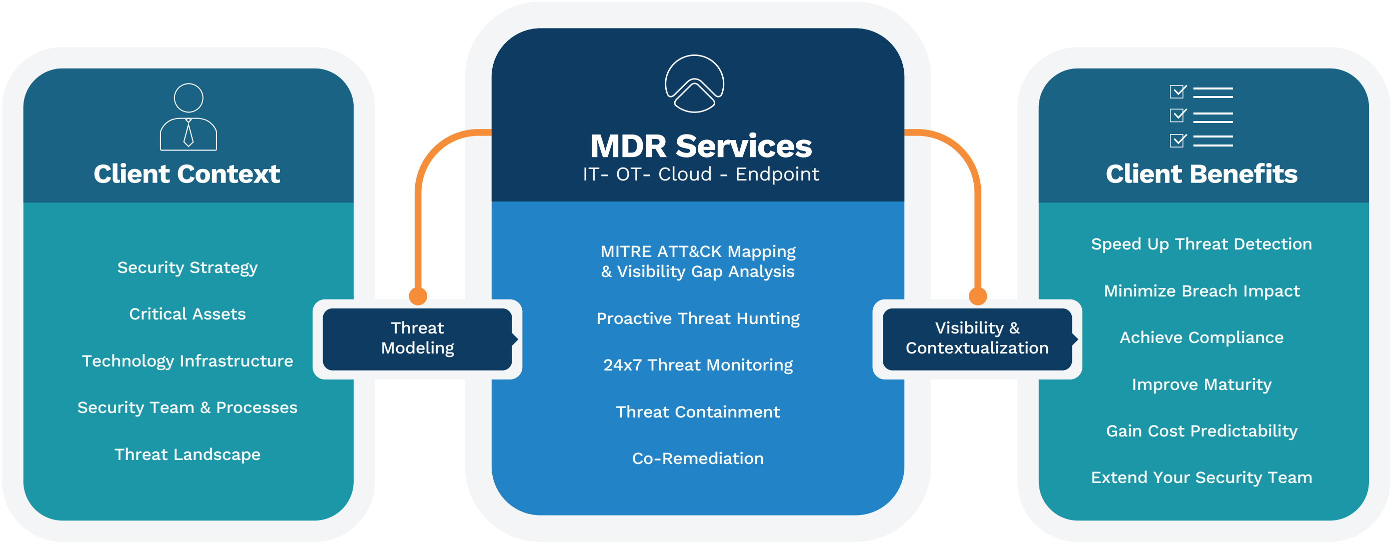
Our approach to MDR is built on personalization and rich contextualization. In the same way an attacker tailors their threats to your environment, we tailor our services. We deliver greater visibility, more relevant threat monitoring with hunting and more accurate threat detection, containment, and remediation.

We start by building a thorough understanding of your business – your strategy, risk exposure, and most likely threats. We use this to architect a threat detection and response model that addresses your unique needs and protects your data – wherever it resides.

Technologies change, but a proven methodology that puts contextualization center stage, has always enabled us to gain true visibility on threat data and deliver better security outcomes for clients.

A proprietary Use Case Framework, mapped to the Cyber Kill Chain and the latest MITRE ATT&CK techniques, is at the heart of our methodology. In close collaboration with your team, we customize the framework to your business by identifying and applying relevant detection use case scenarios.

Our analysts and threat hunters can then perform in-depth investigations on the threats that matter and will escalate validated, prioritized incidents to your team.



Client Context

Security Strategy

Critical Assets

Technology Infrastructure

Security Team & Processes

Threat Landscape

Threat Modeling

MDR Services

IT- OT- Cloud - Endpoint

MITRE ATT&CK Mapping & Visibility Gap Analysis

Proactive Threat Hunting

24x7 Threat Monitoring

Threat Containment

Co-Remediation

Visibility & Contextualization

Client Benefits

Speed Up Threat Detection

Minimize Breach Impact

Achieve Compliance

Improve Maturity

Gain Cost Predictability

Extend Your Security Team

MDR Services Overview

Reduce Threat Detection Time, Lessen Breach Impact, and Mature Security Posture

Our Managed Detection and Response (MDR) services address the multiple environments of a modern workplace: on-premise IT infrastructure, distributed endpoints, cloud, and OT/ICS environments. We focus on outcomes, not on managing security technologies. We deliver deep visibility and coverage to rapidly surface critical threats and provide your security team hands-on support to contain or remediate incidents.

Our MDR Services Include:

- Use case workshops to map your threat coverage to MITRE ATT&CK and build out your unique threat model
- Onboarding and fine tuning of service
- Advanced detection for common and emerging threats
- Continuous proactive threat hunting
- Incident response with threat containment and co-remediation
- 24/7 direct support from security analysts, hunters, and responders
- Real-time access to MSS Client Portal with KPI dashboards, reporting, SLA, and visibility into hunting activities
- Quarterly business review to ensure continuous service improvements

MDR FOR CLOUD

Get complete visibility into threats and misconfiguration issues across your cloud infrastructure and cloud applications. Our native MDR service for cloud detects and helps you respond to critical threats & misconfigurations in order to quickly mitigate risk and improve resilience.

MDR FOR IT

Shorten time-to-detect in your environment and ensure you have the necessary visibility and information to respond to incidents. We ingest relevant security logs and network data either natively or via your SIEM, and automatically process and fuse them with threat intelligence to generate rich contextualization. This enables us to hunt, detect, and respond faster to common and emerging threats.

MDR FOR ENDPOINTS

Secure the endpoint with next-generation detection, prevention, and deception technologies and stop attackers from establishing a foothold in your organization’s network. MDR service for endpoints rapidly identifies malicious activity, contains threats, and accelerates incident response measures.

MDR FOR OT/ICS

Reduce the attack surface of blended IT/OT environments with a complete, unique approach to security visibility into OT/ICS networks.
Our MDR service for OT/ICS networks helps ensure passive visibility into advanced threats and identifies weak points in your environment before costly exploits by threat actors, without causing downtime or disrupting critical operations.

MSS Client Portal: Holistic Security Visibility at Your Fingertips

Kudelski Security provides full transparency on all activity we carry out. Our intuitive MSS Client Portal gives you instant access to crisp and relevant threat information, helping you get a better grip on your security posture and level of risk.

FEATURES

- Real-time dashboards and reporting
- Use case detection benchmarking
- Insight into threat hunting activities
- Incident details with prioritized advice
- Visualized SLA performance
- Direct access to analysts, 24/7

The MSS Client Portal acts as a bridge between your security teams and Kudelski Security CFC analysts.

It gives you continuous visibility on vulnerabilities and risks as well as information on the most critical incidents – ones that have been contextualized and validated by our expert analyst team. We provide you actionable, prioritized advice on how to remediate these incidents, or you can track the steps we are taking to remediate on your behalf.

MDR Benefits

Driving Greater Value to Reduce Business Risk

- **Complete Visibility:** Services cover endpoints, on-premises, cloud, and OT/ICS networks, to eliminate blind spots.
- **Rapid & Accurate Threat Detection:** Current and emerging threats are identified and validated in minutes thanks to our methodology that fuses information about about attacker objectives and techniques with security data and business context.
- **Minimize Impact of Breach:** Speed of detection translates directly to containment of threats that may disrupt business.
- **Predict & Reduce Costs:** Budgets are optimized through MDR services that provide flexibility, predictability and greater return on investment.
- **Ease Burden on Your Security Team:** High-touch, personalized support from our 24/7 CFC analysts informs, and empowers security teams, focusing more resources on security priorities.
- **Ensure Compliance:** Regulatory compliance is facilitated through a proactive approach to threat detection and response, tailored to an organization’s unique business and risk profile.
- **Mature Your Security Posture:** Kudelski Security MDR delivers continuous improvements and risk reduction that elevate security posture over time.

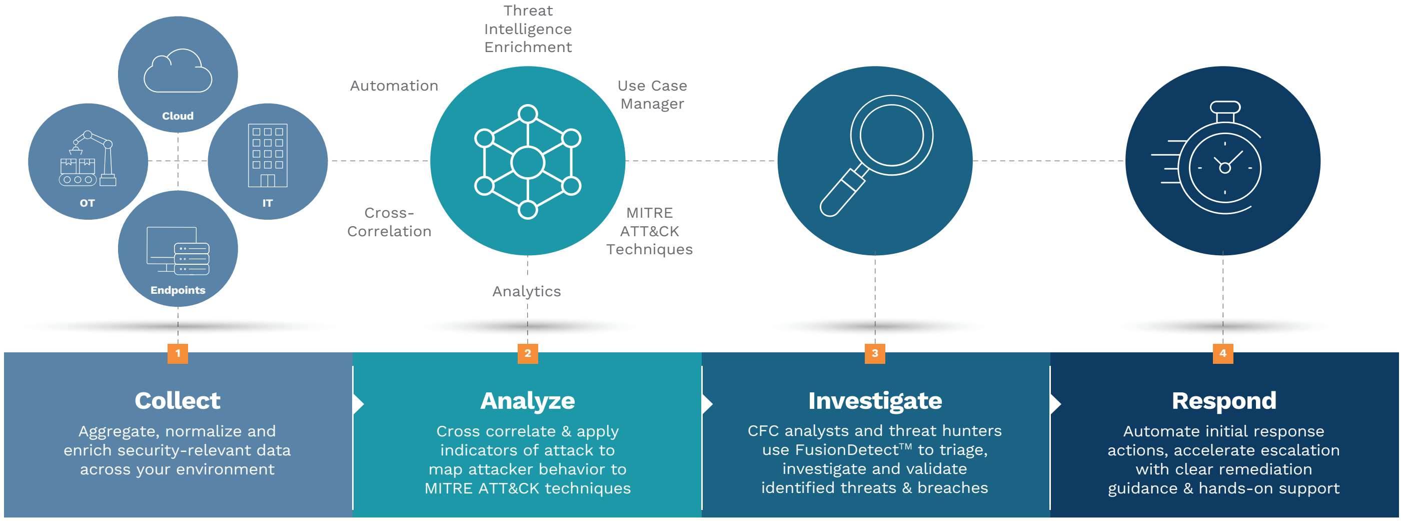
MDR Services Powered by FusionDetect™

Kudelski Security's Managed Detection and Response services are powered by FusionDetect™, our proprietary, cloud-native security analytics and response platform. FusionDetect™ works with leading-edge threat detection, deception, and response technologies as well as our native solutions, all monitored by the Cyber Fusion Center (CFC) team.

Leveraging our innovative Use Case Framework, mapped to the latest MITRE ATT&CK techniques and the Cyber Kill Chain, FusionDetect™ dramatically shrinks the time it takes to detect and respond to threats.

Through a multi-layered approach, Kudelski Security's FusionDetect™ enriches and cross-correlates security-relevant data from client environments while remaining infrastructure agnostic.

Intelligence in Action



Collect
Aggregate, normalize and enrich security-relevant data across your environment

Analyze
Cross correlate & apply indicators of attack to map attacker behavior to MITRE ATT&CK techniques

Investigate
CFC analysts and threat hunters use FusionDetect™ to triage, investigate and validate identified threats & breaches

Respond
Automate initial response actions, accelerate escalation with clear remediation guidance & hands-on support

1. COLLECT

FusionDetect™ collects and normalizes security-relevant logs, security event data or security alerts across your environments, to then enrich them with the latest global and organic threat intel (e.g. indicators of attack and knowledge about attacker tactics, techniques & procedures).

2. ANALYZE

FusionDetect™ applies the CFC Use Case Framework to map attack scenarios to latest MITRE ATT&CK techniques. The platform then cross-correlates multiple data sources and indicators of attack to rapidly surface suspicious behavior.

3. INVESTIGATE

FusionDetect™ enables our analysts to review each security event alert and perform in-depth investigations that identify likely attacker activity. CFC analysts can then provide your security team validated and prioritized security incidents with context on how they could impact your business.

4. RESPOND

The platform automates initial response actions. CFC analysts then take over, providing clear remediation guidance or carrying out the activity on your behalf, 24 hours a day, 7 days a week.

MDR Features

MONITOR	
Complete visibility across any environment: IT, cloud, OT/ICS, endpoint	✓
Award-winning client portal with real-time dashboards and reporting	✓
Use-case benchmarking and trends	✓
Curated, cutting-edge security technologies fully integrated with our CFC	✓
Direct, technology-agnostic raw log ingestion to FusionDetect™ platform	Optional
Data retention and investigation up to 12 months	Optional

DETECT & HUNT	
Data enrichment via open source, commercial and Kudelski Security organic threat intelligence	✓
Proprietary Use Case Framework mapped with the latest MITRE ATT&CK techniques	✓
24/7 advanced threat detection and expert-led investigations	✓
Human-led threat hunting, including retrospective hunting	✓
Threat Research and Detection Engineering team	✓
Dedicated analyst	Optional
Technical account manager	Optional

RESPOND	
Rapid alert triage and response	✓
Validated, prioritized incident escalation with remediation advice	✓
Threat containment and co-remediation	✓
Complex incident investigations and recovery support	Optional

MATURE	
High-touch, personalized services	✓
Insightful monthly threat intelligence summaries	✓
Regular security advisories on attacker activity, widely impactful vulnerabilities, and zero-day vulnerabilities	✓
Transparent SLA tracking and accountability	✓
API integration with your existing IT management tools	Optional
Feedback-driven operations enabled by Client Success Management team	✓
Monthly reporting and quarterly business reviews	✓
Monthly business reviews	Optional

FORRESTER WAVE LEADER 2020
Midsize Managed Security Services Providers
Gartner
IDC ANALYZE THE FUTURE
FROST & SULLIVAN
MSSP Alert Top 250 MSSPs™ 2020 EDITION
Bloor CHAMPION 2021 MANAGED DETECTION AND RESPONSE
CARNEGIE MELLON UNIVERSITY CERT IS A REGISTERED TRADEMARK OF CARNEGIE MELLON UNIVERSITY
CERT AUTHORIZED TO USE CERT
FIRST Improving Security Together
Microsoft Partner
Silver Cloud Platform
Silver Security

FROM OUR CLIENTS

"Kudelski Security offers true visibility into the threats that can impact us. They have also proven they can reduce detection time to just a few hours, enabling a proactive response against advanced attacks."

- Chris Anderson, CISO, Pernod Ricard

"With Kudelski Security on our team, we can now react faster to cyber-attacks. At the same time, we still retain ownership and control, since the comprehensive processes were defined together."

- CISO, RHI Magnesita

FROM INDUSTRY ANALYSTS

"Kudelski Security customizes its MDR approach based on what clients want. Security leaders needing a high-touch, customized version of MDR and a vendor that blends MSS and MDR together seamlessly, should engage with Kudelski Security [...] Kudelski Security's extensive collaboration capability helps clients understand and resolve incidents more effectively."

- Forrester Wave™: MDR Service Providers (MSSP), Q1 2021

"Organisations looking for a hands-on MDR service that spans their entire enterprise network, including deep expertise in operational and ICS environments, should consider the differentiated approach from Kudelski Security. Whilst MDR is a specialty, Kudelski is an MSSP in its own right and offers a range of complementary services that help their customers to build and maintain strong security program."

- Bloor Research Lead Security Analyst, Feb. 2021

Level up your threat detection and response. Get in touch today

Request a Demo | info@kudelskisecurity.com | www.kudelskisecurity.com

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.