THREAT MONITORING & HUNTING

Managed Security Services

Detect security incidents faster with 24x7x365, intelligence-infused threat monitoring and analysis from our Cyber Fusion Center.

The rise of sophisticated threats is outpacing the ability of most organizations to combat them, and the average attack now goes undetected for 56 days. Successful and more rapid detection of advanced attacks requires a different approach, one that provides greater contextual relevance and is built on an adpative response in an ever-changing threat landscape.

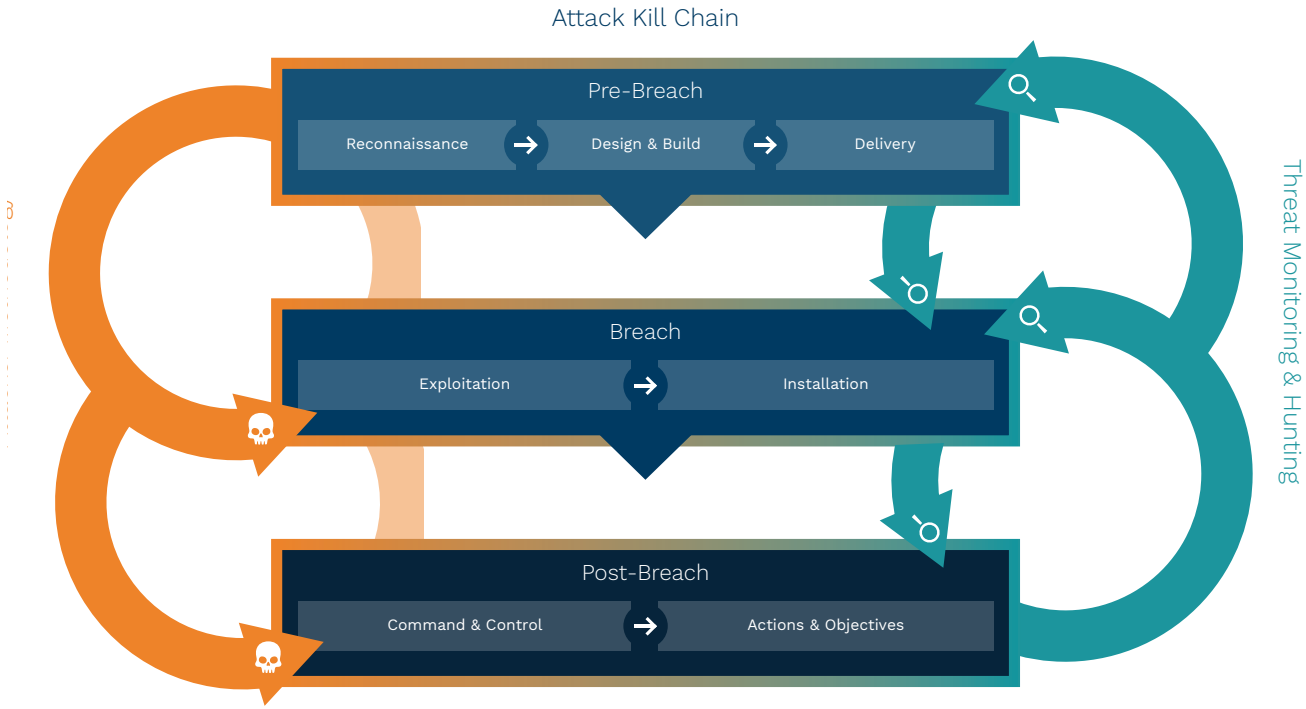
Kudelski Security's Threat Monitoring & Hunting Service is part of the suite of Managed Detection Response (MDR) services. Our MDR capabilities enable us to reduce detection time from months to just a few hours – whatever the environment, wherever the data resides. Delivered by our Cyber Fusion Center (CFC), the service relies on high-end commercial and proprietary tools, technologies, deep experience, and threat intelligence. This unique combination enables rapid identification of threats and incident management – including containment and clear remediation guidance – and helps strengthen your overall cyber resilience.

Threat Monitoring – How It Works

Kudelski Security's Threat Monitoring provides long-range visibility into threats and cyber adversaries.

The CFC is able to analyze and detect threats faster than most MSSPs. We gather security data from all environments (traditional IT, cloud, OT / industrial control systems, IoT), automatically correlating it with threat intelligence to generate rich and contextual threat content.

Leveraging cutting-edge technologies, methodologies, and human expertise, we detect and hunt for anomalies that can indicate suspicious behavior. If we find a match, we instantly generate alerts for analysis by the CFC. In the event of a breach, we rapidly activate the client's incident response plan, containing and isolating the attack and providing clear steps for remediation.



How We Engage

Kudelski Security's Managed Security Services are built from the ground up to drive greater value to the client. They leverage a proven four-phase onboarding and operational process.

Phase 1: Pre-implementation

Threat monitoring use cases are reviewed and security rules to support identified use cases are configured and tuned to generate high-fidelity security alerts.

Phase 2: Implementation

The MSS Implementation team collects information, establishes connectivity to devices, and determines security incident notification procedures.

Phase 3: Go-live

The service is thoroughly validated by the CFC Threat Analysis team to ensure smooth day-to-day operations and monitoring.

Phase 4: Ongoing Operations

Once the service is operational, CFC threat analysts support clients daily through several activities:

- Management and maintenance of threat hunting and monitoring use cases
- Security event triage and anomaly detection
- Automated and manual security content updates
- Change management
- Incident containment
- Reporting (incidents, escalation, trends, and real-time dashboards)

Unlike other MSSPs, our systems automatically enrich the security data from a client's managed devices with threat intelligence the moment it is ingested, allowing analysts to hunt for threats retroactively and carry out more efficient triage and analysis of security events.

Our attack detection is nonlinear, imitating the ad-hoc way an attacker moves through a network. We rewind the cyber kill chain, automatically reevaluating security data and comparing it against newly gathered threat intelligence regarding attacker tactics, techniques, and procedures.

Key Benefits

Kudelski Security's Threat Monitoring Service is powered by our 24x7x365 Cyber Fusion Center, with global reach, multilingual support and operations in the United States and Switzerland.

- Extend your security team with dedicated guidance and support from our CFC expert analysts, threat hunters and responders
- Drastically reduce the time to detect and respond to threats through contextual intelligence automatically fused into our analytics process and tools
- Optimize cost predictability and scalability of security operations
- Meet regulatory and compliance requirements
- Get real-time, high-fidelity alerts as well as dashboards and reports from the Client Fusion Portal. Gain comprehensive visibility of your security posture across all environments: IT, OT/ICS, cloud

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.

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY