MANAGED ATTACKER DECEPTION

Managed Security Services

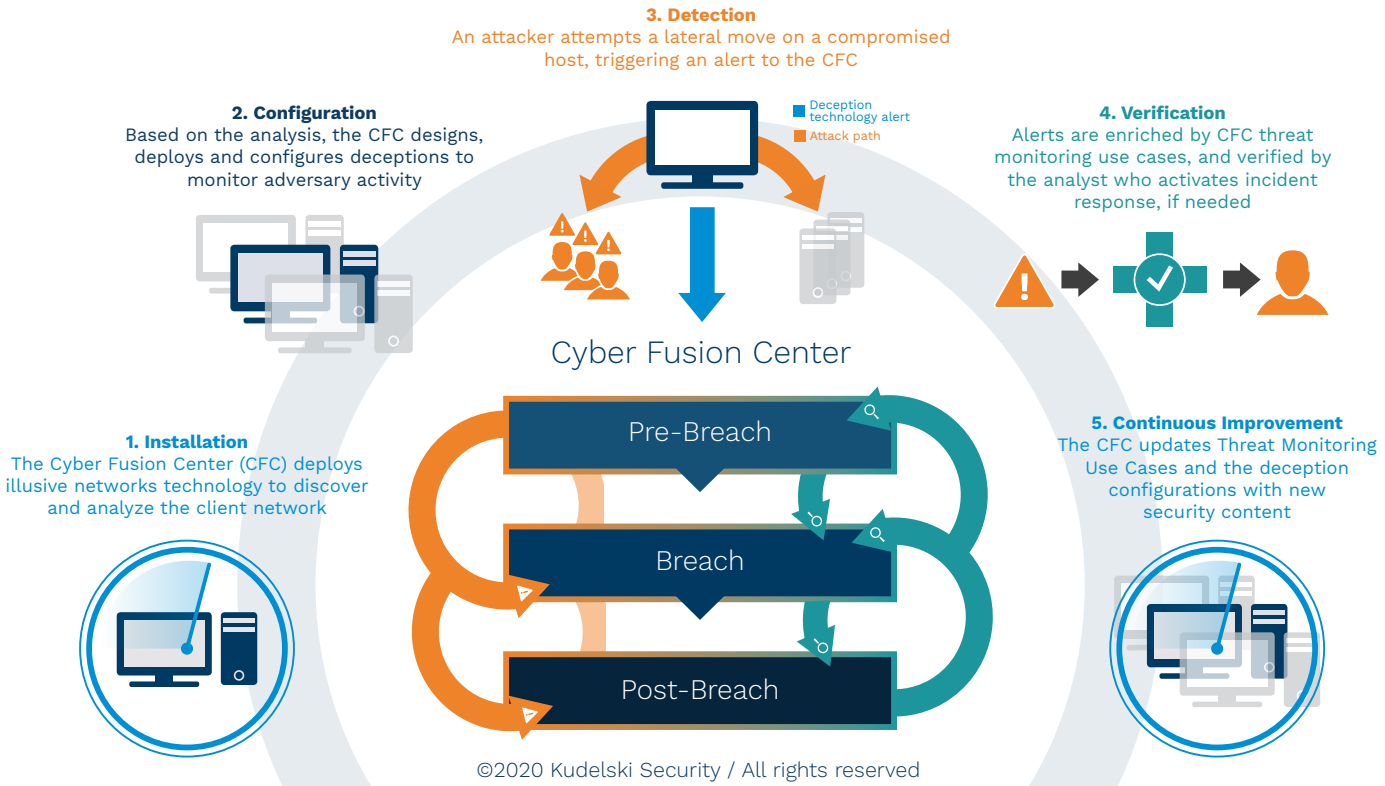
Gain the upper hand against cyber adversaries by forcing your attacker into an alternative reality, slowing them down while triggering a rapid response from the Cyber Fusion Center.

Modern attackers use a range of advanced techniques to compromise end-user endpoints and establish a foothold within an organization's network. Traditional managed security service providers offer solutions that do little more than alert clients to anomalies on the network, often leaving security teams to do the time-consuming work of identifying real threats and responding to breaches.

Kudelski Security's Managed Detection and Reponse (MDR) services include the Illusive Network 'Deception Everywhere' technology. Our MDR delivers rapid and effective detection and response services to better meet the security demands created by today's advanced adversaries. The technology creates an alternative network environment that behaves as a real network would; the attacker is confused and slowed down, while you receive relevant, contextualized, remediation guidance to contain the breach.

Managed Attacker Deception – How It Works

The Managed Attacker Deception Service is enabled by an advanced machine learning platform that preemptively identifies attack pathways and autonomously creates best-fit deceptions based on continuous real-time environment analysis. Attackers attempting to map out the network or move laterally within this environment trigger high-fidelity alerts to the Cyber Fusion Center (CFC) for investigation. The CFC's Threat Analysis team will quickly verify if there is a potential security incident, collect forensic data from impacted endpoints, and activate the client's incident response plan, all before any critical assets or sensitive data have been compromised.



How We Engage

Phase 1: Pre-implementation

Project scope is defined, the illusive network Deception Everywhere and Management System™ are deployed and deceptions are configured to seamlessly blend into the client's network.

Phase 2: Implementation

The illusive networks solution is integrated into the Cyber Fusion Center (CFC), the solution is fine-tuned by the MSS Implementation team, and connectivity to the client's environment is established. The CFC's Threat Analysis team will work closely with client contacts to ensure the solution is properly implemented and that deception profiles are customized in order to blend invisibly into the client's environment.

Phase 3: Go-live

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:

- 24x7x365 security event triage
- 24x7x365 health and performance monitoring of the attacker deception solution
- Proactive threat hunting
- Solution change and configuration management
- Incident containment
- Forensic data collection from impacted endpoints
- Reporting (incidents, escalations, trends, and real-time dashboards)

Key Benefits

Kudelski Security's Managed Attacker Deception Service is powered by our 24x7x365 Cyber Fusion Center (CFC), with global reach, multilingual support and operations in the United States and Switzerland.

- Rapidly reveals attacker lateral movements inside your network by leveraging innovative technology, Kudelski Security's deep expertise and CFC threat hunting capabilities
- Agentless solution, remotely managed, designed to avoid impact on business operations
- Enables better management of business risks
- Comprehensive cover, with deceptions deployed across all endpoints
- Collection of high-fidelity forensic data from impacted endpoints
- Reduces false positive alerts; enables security teams to focus on relevant threats
- Predictable cost of operations, scalable and designed to drive value
- illusive ransomware protects against ransomware, APT, and more

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY