ENDPOINT DETECTION & RESPONSE

Managed Security Services

Detect threats and respond faster with expanded endpoint visibility.

The modern threat landscape continues to evolve and threat actors are no longer concentrating their efforts on an organization's perimeter. Decreasing network visibility, increasing numbers of remote workers, and the interconnected nature of enterprise networks have now made the end user and their endpoints the growing focus of attackers.

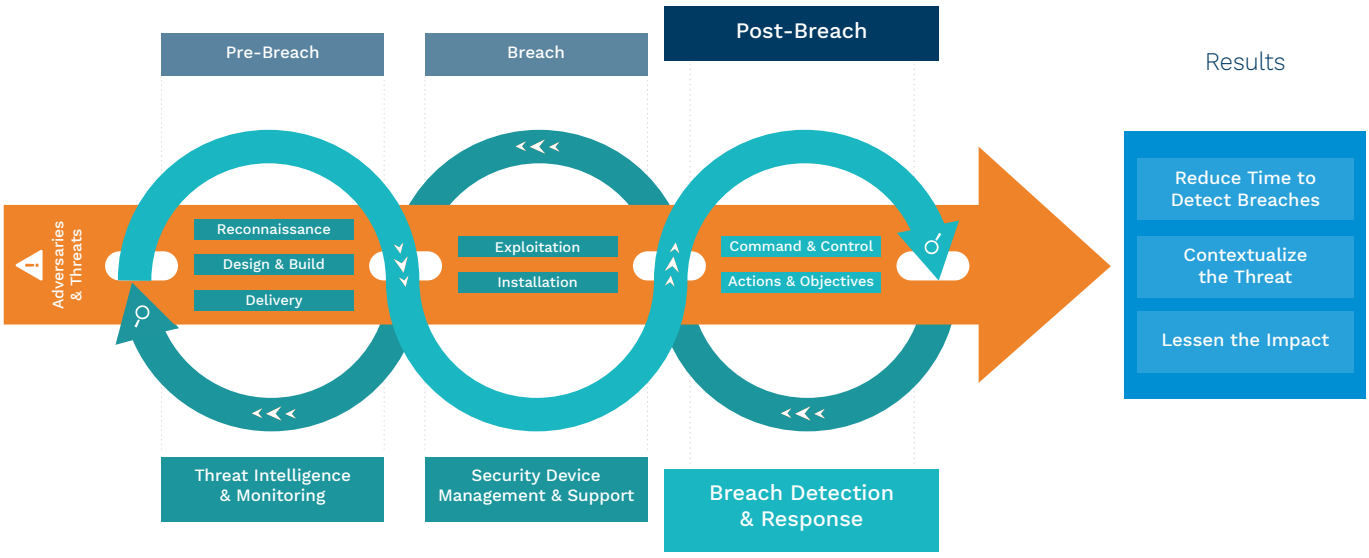
It is now commonly accepted that breaches will occur; it's no longer a question of if or when an attack occurs, it's how quickly it can be identified and mitigated. In order to combat security threats and help our clients protect their endpoints, Kudelski Security provides an Endpoint Detection and Response Service as part of its Managed Detection and Response capabilities. This service, delivered from the Cyber Fusion Center (CFC), aims to quickly identify malicious activity and accelerate incident response actions to safeguard critical assets and data.

Endpoint Detection & Response – How It Works

The Endpoint Detection and Response Service is a key part of our approach to disrupting the cyber kill chain. Leveraging CrowdStrike's advanced capabilities, the CFC Threat Analysis team can significantly reduce the risk of damaging, long-lasting, data breaches by detecting anomalies and disrupting adversary movements through the stages of an attack.

To combat advanced attacks targeting the end user and to hunt for new threats, suspicious patterns, and indicators of compromise, a lightweight agent is deployed to endpoint fleets. The agent continuously collects and transmits security relevant data about files, application activity, network connections, processes, and memory, while excluding personally identifiable information.

DISRUPTING THE KILL CHAIN WITH KUDELSKI SECURITY



How We Engage

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

Phase 1: Pre-implementation

Project scope is defined, the CrowdStrike Falcon™ host agent is deployed, and Falcon Orchestrator Platform is installed and configured.

Phase 2: Implementation

The CrowdStrike platform is integrated into the CFC, the solution is fine-tuned by the MSS Implementation team, and connectivity to the client's environment is established.

Phase 3: Go-live

The CFC Threat Analysis team validates the service 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
- Indicators of Compromise (IOC) management
- Proactive threat hunting
- Solution health and performance monitoring
- Quiet endpoint monitoring
- Change and configuration management
- Incident containment
- Forensic data collection
- Reporting

Security data collected by the CrowdStrike Falcon™ host platform is enriched with up-to-the-minute threat intelligence and processed through our custom analytics. Potential threats and alerts are analyzed for signs of malicious activity by the CFC Threat Analysis team.

Key Benefits

Kudelski Security's Endpoint Detection and Response Service is powered by our 24x7x365 CFC, with global reach, multilingual support and operations in the United States and Switzerland.

- Detect threats that evade conventional security controls by leveraging unrivalled endpoint visibility, deep expertise and our CFC threat hunting capabilities
- Reduce the time to detection with Crowdstrike's leading endpoint protection solution and our contextual intelligence, automatically fused into the analytics process
- Accelerate incident response with direct access to impacted endpoints and in-depth forensics data
- Reduce cost of operations and ease the complexity of endpoint security
- A Managed Detection and Response service (MDR) that reduces threat detection time to hours, or minutes even, is available for organizations needing an advanced level of protection

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY