KUDELSKI SECURITY

Managed Security Services

Powered by the Cyber Fusion Center

Our Managed Security Services blend innovative technologies and advanced threat analysis to provide CISOs the resources and intelligence necessary to navigate today's complex threat landscape.

With an ever-increasing number of sophisticated and targeted threats, it is commonly accepted that security breaches will occur. In order to protect critical assets, data, and reputation, CISOs need trusted cybersecurity partners who can help them reduce the complexity of managing cybersecurity programs while maximizing the value of their investments.

Kudelski Security's Managed Security Services have been designed to address gaps in traditional managed security services and deliver what organizations need most: to reduce the time it takes to detect threats. The Cyber Fusion Center (CFC) has built custom technology, tools, and processes to reduce detection time and ensure clients have the information they need to react effectively to verified security threats.

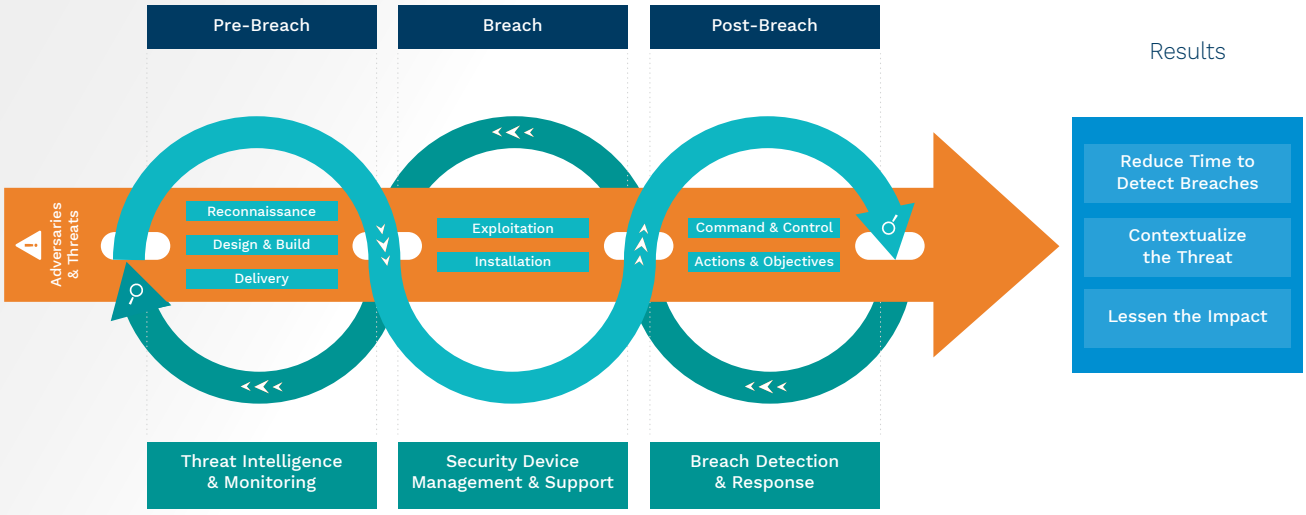
Cyber Fusion Center

The Cyber Fusion Center (CFC) operates 24x7x365, powering Kudelski Security's state-of-the-art Managed Security Services.

Traditional MSSP solutions lack the advanced capabilities required to combat advanced adversaries. The CFC goes beyond standard solutions, combining expert analysts, threat monitoring, intelligence sharing, and innovative technologies to rapidly detect and respond to threats.

We take a nonlinear approach to the traditional phases of the kill chain, enabling us to identify patterns and disrupt adversary movements throughout the stages of an attack. Clients benefit from a continuous improvement in their security posture, remediating security issues faster and protecting their assets and reputation.

DISRUPTING THE KILL CHAIN WITH KUDELSKI SECURITY



Managed Security Service Offerings

Kudelski Security's 24x7x365 Managed Security Services are aligned to the different stages of an attack, which can be broadly divided into pre-breach, breach, and post-breach.

Threat Intelligence & Monitoring

The CFC's threat intelligence collection and analysis capabilities give us superior insight and long-range visibility on threats and the tactics, techniques, and procedures used by adversaries. We automatically enrich data from your organization with threat intelligence. Analysts use this rich content to investigate and hunt for known and unknown threats, reducing detection time and increasing accuracy.

Vulnerability Scanning

The CFC will conduct regular scans of your external and internal networks and web applications in order to identify vulnerabilities that can be exploited by attackers. Clients consume the information via our Client Portal and receive scan reports and remediation recommendations.

Threat Monitoring

The CFC gathers security data, automatically correlating it with threat intelligence to generate rich and contextual threat content. Our analysts filter out routine alerts from real incidents, hunt for known and unknown threats, and provide guidance for incident containment and prioritized remediation.

Security Device Management & Support

Our vendor-certified experts act as an extension of your team, providing specialized 24x7x365 security device support and management, freeing up your staff time, and helping you see the full value of investments.

Security Device Management

The CFC will manage, monitor, and maintain a wide range of security devices from leading technology vendors, including F5, Cisco, Palo Alto Networks, Juniper, RSA, and LogRhythm.

Security Device Support

The CFC will complement your in-house team by providing a 24x7x365 hotline with expertly trained staff, ready to assist in troubleshooting potentially complex issues. The Intelligent Outage Management Process includes incident, problem, and risk management activities.

Breach Detection & Response

Our advanced Breach Detection and Response services leverage innovative tools from leading technology vendors to detect and respond to the most evasive threats that organizations face. When a potential threat is identified, the CFC's Threat Analysis team receives an alert, quickly verifies if there is a potential security incident, collects forensic information from impacted endpoints, and activates your response plan.

Endpoint Detection & Response

The CFC uses CrowdStrike's Falcon technology to collect, enrich, correlate, and analyze all security-relevant information from endpoints.

Managed Attacker Deception

The CFC attacker deception solution, powered by Illusive Networks, creates a transparent alternate reality. Attackers attempting to map out the network or move laterally are led into this alternate reality while high-fidelity alerts are sent to the CFC for investigation.

KUDELSKI SECURITY

info@kudelskisecurity.com | www.kudelskisecurity.com