COMPROMISE ASSESSMENT

Incident Response & Cyber Resilience

KUDELSKI SECURITY

Quickly confirm and respond to active threats by improving hunting and response capabilities

Modern business environments produce data sprawl among diverse corporate infrastructures that can be difficult to properly monitor and analyze. Active threats may go undetected for months, creating a gap between compromise, detection, and response that opens the door for data theft.

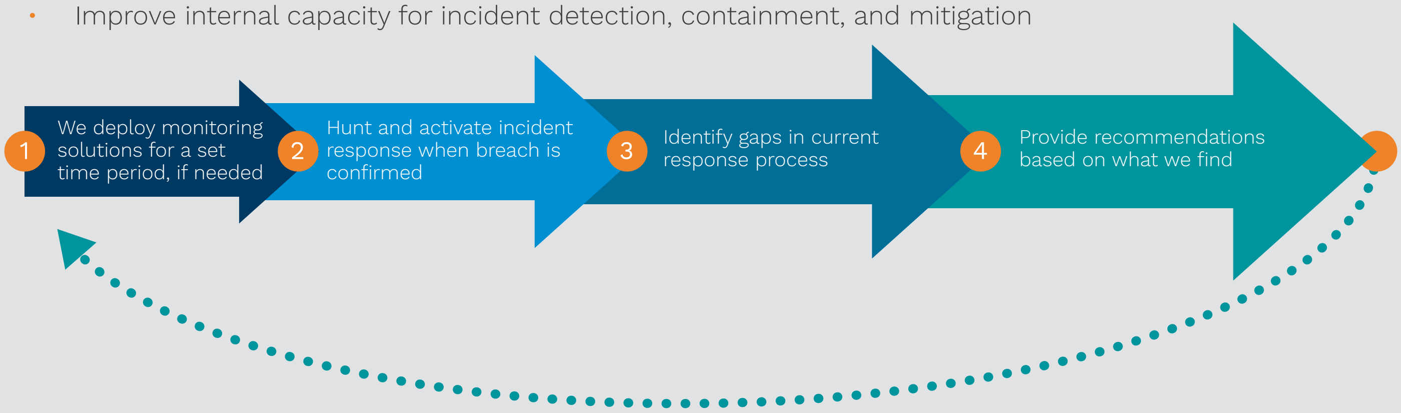
If you suspect you've been compromised, need a new approach to traditional network penetration testing, or want to build your threat hunting capacity, Kudelski Security's Compromise Assessment can help.

Over an agreed upon time period, a senior team of incident responders will carry out a proactive investigation of your computing environment to detect, analyze, and respond to active threats. The team leverages threat intelligence from our Cyber Fusion Center to monitor for indicators of compromise (IoC) and performs in-depth investigations to validate attacks. For confirmed attacks, you will receive guidance on impact mitigation as well as recommendations for advancing threat hunting capacity to reduce dwell time and impact of breaches.

Compromise Assessment Service

Key Outcomes

- Gain visibility of malicious activity, identify, and confirm a breach that evaded existing controls
- Reduce the impact of a breach due to faster discovery and optimized incident response process
- Improve understanding of the effectiveness and limitations of current technical controls and incident response processes and capabilities
- Collect evidence for an effective response with law enforcement, partners, and customers
- Improve internal capacity for incident detection, containment, and mitigation



1 We deploy monitoring solutions for a set time period, if needed

2 Hunt and activate incident response when breach is confirmed

3 Identify gaps in current response process

4 Provide recommendations based on what we find

The Kudelski Security Advantage

Identify process and control deficiencies-aligned to industry-established frameworks

Customized to your technologies and threat landscape

Full-time focus of advanced threat hunters for agreed length of time

How We Engage

Scope & Goals

Scope and goals based on client's business requirements and computing environment.

Data Capture

Output from detection technology and logs is analyzed to identify malicious behavior, collect incident data, and provide insight into overall security posture.

Monitoring & Response

Over an agreed upon time period, data is monitored and analyzed to establish patterns of unauthorized activity and identify signs of compromise. Identified breaches are immediately communicated and response recommendations provided.

Reporting & Recommendations

Final reports, analysis, and recommendations are delivered, including a review of current cyber resilience maturity and a 24-month strategic roadmap for incident response program.

Ongoing Monitoring

After the engagement has concluded, the service can be extended with customized monitoring packages.

Service Description

Kudelski Security's Compromise Assessment is typically a 30-day engagement that delivers immediate results. It is designed to quickly confirm a compromised or non-compromised state, identify and mitigate signs of compromise, and develop the client's internal threat hunting and response capabilities. Each assessment is carried out by a team of senior incident responders who perform advanced threat hunting every day of the engagement, using manual and automated methods.

The investigation leverages data collected from client's detection technologies and logs. If needed, we can deploy our own detection technology that includes a host-based agent, a network-based monitor and cloud-based agents. Tools, configurations, and analysis are refined, based on evidence found internally and externally (e.g. Dark Web and Threat Intelligence Discovery), to improve detection and deliver the most comprehensive, relevant results.

When the team detects signs of compromise, they perform an in-depth investigation to validate that the attack took place, if it was targeted, and what the root causes and the potentially leaked information were. This level of visibility enables clients to confirm compromised data and get the information they need for effective response.

Engagement Deliverables:

- Cyber Resilience Maturity Executive Presentation
- Compromise Assessment Report – including analysis of identified evidence, its business impact, and a technical summary of findings
- Initiative Summary – outlining prioritized cyber initiatives according to cyber resilience maturity level, threats, risks, level of effort, and investment required
- Strategic Roadmap – visually illustrating the prioritized initiatives, key milestones, and associated dates over a 24-month period
- A threat hunting guide and technical training, adapted to the client's technology is available on request.

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