KUDELSKI SECURITY

PARTNER PROGRAM

COMPROMISE ASSESSMENT

Determine if an active threat resides in your infrastructure using our exhaustive Compromise Assessment

Modern enterprises use multiple data centers, locations and devices – it's challenging to monitor and analyze data with confidence and establish if an active threat exists within your infrastructure.

Attacker dwell time can extend for months, creating the chance for pervasive data theft and other criminal activities.

To remove the threat, you need to go beyond traditional penetration testing toward a compromise assessment that includes advanced threat hunting over an extended period of time.

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 signs of compromise, mitigate the risk, and advance your internal threat hunting and response capabilities. Each assessment is carried out by a team of senior incident responders who are fully dedicated to perform advanced threat hunting every day of the engagement, using manual and automated methods.

APPROACH

- Scope the assessment.
- Identify malicious activity.
- Collect, monitor and analyze data.
- Identify breaches.
- Provide response recommendations.
- Provide engagement deliverables.

BENEFITS

- Improve understanding of the effectiveness of current technical controls and incident response.
- 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.
- Collect evidence for an effective response with law enforcement, partners, and customers.
- Improve internal capacity for incident detection, containment, and mitigation.