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.

SERVICE OPTIONS

1
Up To
250
ENDPOINTS

SCOPE

Access to
1 Data Center or Location

Monitor for
15 consecutive days

Review up to
4 events each day

2
Up To
500
ENDPOINTS

SCOPE

Access to
2 Data Centers or Locations

Monitor for
30 consecutive days

Review up to
12 events each day

3
Up To
1000
ENDPOINTS*

SCOPE

Access to
3 Data Centers or Locations

Monitor for
30 consecutive days

Review up to
20 events each day

KEY DELIVERABLES

- **Cyber Resilience Maturity Presentation:** Executive presentation with core information.
- **Compromise Assessment Report:** Analysis of identified evidence, business impact, and technical summary of findings.
- **Initiative Summary:** Outline of prioritized cyber initiatives, according to cyber resilience maturity level, threats, risks, and required level of effort and investment.
- **Strategic Roadmap:** Visual illustration of prioritized initiatives, key milestones and associated dates over a 24-month period.
- **Threat Hunting Guide and Technical Training:** Training modules, adapted to the client technology, available on request.

**For larger enterprises, contact us for a custom proposal*

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY