24/7 INCIDENT RESPONSE
Advisory Services

KUDELSKI SECURITY

Augment your incident response capabilities with Kudelski Security's advanced, 24/7, local emergency support teams.

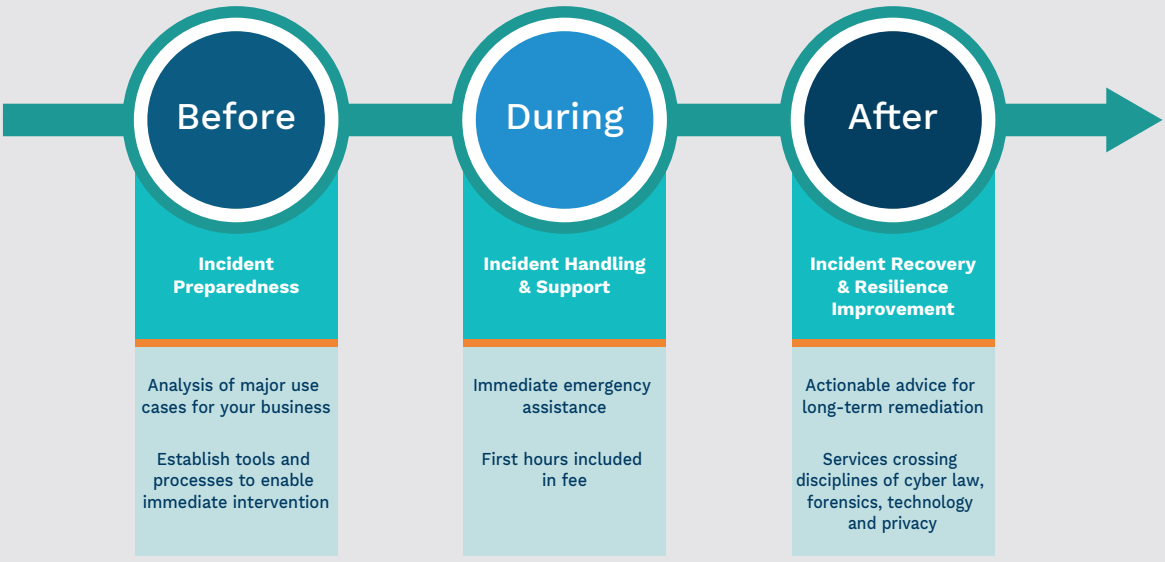
With cyberattacks increasing in frequency and complexity, organizations must be prepared for any type of attack or damages to the business or reputation. Having a clear plan of action for when a breach occurs is paramount in reducing the impact and returning to business as usual as quickly as possible. However, creating and executing a swift and effective response strategy requires a large investment in technology, people and processes that many organizations do not have the means or skill sets to achieve without a trusted partner.

Kudelski Security's 24/7 Incident Response Services helps ensure you have the right organization-wide response plan and capabilities in place to effectively respond to cyber threats. You'll benefit from rich security expertise as well as advanced incident response techniques for swift incident resolution based on best practices for cyber resilience.

24/7 Incident Response - A Comprehensive Approach

Key Outcomes

- Greater assurance that your organization is prepared to respond effectively to security incidents
- Subscription-based model with preparation phase, an emergency response hotline with security experts on standby, and first hours of investigation included in fee
- A cyber resilience maturity review that identifies incident response capability gaps and provides steps to improve response maturity
- Dedicated team of consultants and technical experts familiar with your industry and company



Our Response Methodology

In the event of a cyber incident, our consultants will carry out the following activities:

- Immediate response via hotline with 2-hour SLA for CSIRT investigation (subscribed clients)
- Information gathering for strategic and tactical data points
- Initial recommendations for incident containment
- Advanced situational awareness that defines the threat profile, attack scope, critical business disruptions, and suspected attack vectors
- Continuous containment recommendations as the incident evolves
- Identify the most effective remediation strategy for returning the business to a “pre-breach state”
- Remediation recommendations to avoid further breaches by limiting or mitigating the identified vulnerabilities or gaps

24/7 Incident Response Service

When dealing with a cybersecurity incident, one of the most crucial factors in returning to business as usual is to be appropriately prepared. The 24/7 Incident Response Service prepares clients by proactively developing a client-specific Service Level Framework (SLF) that defines how Kudelski Security will provide incident response support. In the event of an incident, our response retainers ensure a Kudelski Security incident response team is on standby to quickly intervene and protect your business from additional attack.

Service Level Framework (SLF) for Efficient Preparation

The Service Level Framework is a pre-established, coordinated approach to incident response that ensures Kudelski Security consultants can move swiftly and unimpeded when responding to an incident. In collaboration with the client team, a senior security consultant will gather the necessary information to prepare the SLF, which includes the incident response use cases, existing technologies, roles and responsibilities, incident response procedures, and a chain of command/communication procedures. All necessary tools, processes and communication methods will be setup ahead of time to reduce response time and overall business impacts of a cyber incident.

24/7 Emergency Response Retainers

Kudelski Security’s response retainer program ensures an experienced emergency response team is at the ready to enact the response plan, reducing time to action and diminishing the overall impact to the business. With a monthly retainer in place, clients have access to our 365x24x7 hotline and a standby CSIRT expert team that has more than 20 years of forensic investigation and response experience.

Incident Response Support Levels

Level 1	Level 2	Level 3
Immediate Response	2 Hours Remote Assistance	4 Hours Remote Assistance 24 Hours Onsite
First line support, gather initial information, determine escalation requirements and client "technical" availability	Cyber incident response by a specialist, mostly done remotely and sufficient for about 80% of the incident types	Advanced incident response team for critical business impacting incidents
German	German	German
French	French	French
English	English	English
Italian		
Call Center	Security Professional	Incident Response Team

Info@kudelskisecurity.com | www.kudelskisecurity.com