



CyberSecurity

Cyber Incident Response

Get assistance with managing your security incidents 24/7

Short description:

Global support through each stage of the incident response process: detection, containment, remediation, and crisis monitoring.

Key benefits:

Manage your critical and targeted security incidents and ensure appropriate containment and remediation thanks to our CSIRT (Computer Security Incident Response Team) experts.

Service family:

- Advanced Incident Response 



<p>Detailed description</p>	<ul style="list-style-type: none"> • Preparation of incident response using the appropriate tools. • Incident response conducted in compliance with SANS process and best practice. • Detection and in-depth analysis of current cyber and APT threats to your network and endpoints. • Recommendations and support for containment. • Continuous monitoring during and after the incident, both onsite and remotely. • Confidential custom detection rules to identify targeted and furtive attacks. • Support and coordination of activities by a dedicated incident manager. • Remediation and existing protection improvement. • Joint drafting of an incident prevention strategy and key security processes, taking lessons learnt into consideration. • Assistance with incident communication management, internally and externally (on request). <p>A service desk is included as standard.</p>
<p>Service level agreement</p>	<p>Immediate intervention following first contact.</p>
<p>Operational follow-up</p>	<ul style="list-style-type: none"> • Kick-off meeting with the customer. • Weekly technical reports (or more frequently, if required). • Status update at the end of each phase of the incident response process.
<p>Deliverables</p>	<ul style="list-style-type: none"> • Detailed investigation report: <ul style="list-style-type: none"> - Executive summary - Threat assessment - Attack timeline and persistence - Containment recommendations - Remediation recommendations • Malware analysis reports (on request). • Detection rules (on request). <p>A secure and dedicated web portal is available to access and exchange documents.</p>
<p>Available offers</p>	<p>Personalised service packages available, to include:</p> <ul style="list-style-type: none"> • Detection and analysis of cyber threats. • Containment and remediation measures.