Digital Intelligence

BAE SYSTEMS

Incident Response
The first hours

Evidence of a potential attack

- Unusual network traffic
- Security monitoring alert
- Suspicious or anomalous DNS queries
- Indicators of potential insider activity
- Unexplained financial transactions funds transfer
- A tip off from an external party

When evidence of a potentially serious attack is detected, you need to REACT

R

Resource

Assign an incident handler with appropriate authority to manage the incident, coordinate with internal stakeholders, work with specialists and authorise containment, eradication and recovery actions.

E

Evidence

Ensure logging is maximised, with sufficient storage, on key devices like firewalls, proxies and active directory servers - but don't install new software to collect data.

Stop using known infected machines and don't take them offline or shut down until the risks are understood. Preserve evidence in accordance with recognised digital forensics and chain-of-custody principles. If the case might go to court, keep detailed records of all actions taken and engage legal professionals.

A

Assess

Initial assessment should focus on identifying any immediate risks and potential business impacts based on the information known so far. This will inform the response strategy and also help identify any reporting requirements and key stakeholders.

C

Contact

Engage specialist investigators, if needed, who can guide you through the response while minimising the impact of the attack on your business. Use an alternate form of encrypted communication if there is a risk your corporate email is compromised.

T

Take Action

Consult with specialists before undertaking irreversible actions. Avoid actions that could alert the attacker prematurely or destroy forensic artefacts. Likely first actions will be to notify business leadership and start developing internal and external communications. It may also be appropriate to implement proportionate containment measures such as network segmentation, credential resets, disabling compromised accounts or limiting bandwidth to reduce the risk of data exfiltration.

Incident Response Readiness

- This guide to the first hours of an incident response is intended for emergency use only.
- We recommend that you develop processes that are tailored to your own business.
- Call us if you would like support creating an incident response plan or training your staff.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/digital

linkedin.com/company/baesystemsdigital @BAESystemsDigi

Assured Service Provider

CREST

in association with National Cyber Security Centre

Victim of a cyber attack?
Contact our emergency response team on:

UK & International: +44 330 158 5263
Email: cyberresponse@baesystems.com