Solution Brief

Sophos Emergency Incident Response

Take action when a cyber emergency strikes

Sophos Emergency Incident Response provides full-service assistance when you experience a cyberattack, focused on neutralizing the threat, identifying root cause, and assessing security posture and recommending actions to prevent future incidents. Our team of cross-functional experts apply their years of experience and learnings to rapidly triage, contain, and neutralize active threats, and eject adversaries to prevent additional damage.

Use Cases

1 | EXPERT-LED RESPONSE

Desired Outcome: Rely on an experienced team of incident response experts.

Solution: Whether onsite or remote, Sophos Emergency Incident Response specialists bring vast expertise into every engagement, from working active incidents for thousands of customers, and with backgrounds spanning national, military, organizational Computer Security Incident Response Teams (CSIRTs), law enforcement and intelligence agencies.

2 | RAPID DEPLOYMENT

Desired Outcome: Enable quick action to triage, contain, and neutralize threats.

Solution: Sophos Emergency Incident Response gets to work for you immediately, providing 24/7 rapid assistance to capture existing forensic data, start initial analysis, develop containment action, and deploy any additional technology and analytics to quickly expand visibility of your environment.

3 | UNDERSTANDING THE THREAT

Desired Outcome: Response driven by in-depth knowledge of the threat landscape.

Solution: Effective incident response requires a thorough understanding of current adversary behaviors. Sophos Emergency Incident Response personnel continually curate threat intelligence through the combination of insights gathered via thousands of engagements annually and up-to-date threat research infused throughout analysis and investigative activities.

4 | MINIMAL DISRUPTION

Desired Outcome: Restore normal operations for your business.

Solution: Sophos Emergency Incident Response eliminates threats and restores your organization to steady-state operations. Our expert-driven remediation guidance helps you recover, strengthen your security posture, and guard against future attacks.

The Sophos Incident Response practice is accredited by multiple organizations, including CIR Standard and Enhanced by the NCSC in the UK, SSS in Japan, and BSI in Germany.

Learn more:

sophos.com/emergency-response

2025-06-04 SB-EN (NP)