SOPHOS

SOPHOS DIGITAL FORENSICS AND INCIDENT RESPONSE

Take action when a cyber emergency strikes.

Sophos Digital Forensics and Incident Response (DFIR) 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.

ACCREDITATIONS

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

WHAT SOPHOS DFIR DELIVERS

Four outcomes. One expert-led response.

Expert-led response

Rely on an experienced team of DFIR experts that brings vast expertise into every engagement.

- Experience from active incidents for thousands of customers
- Backgrounds spanning military, organizational CSIRTs, law enforcement and intelligence agencies
- Remote and onsite response available

Rapid deployment

Enable quick action to triage, contain, and neutralize threats with immediate expert response.

- 24/7 rapid assistance to capture existing forensic data
- Start initial analysis and develop containment action
- Deploy added technology and analytics to expand visibility

Understanding the threat

Response driven by in-depth knowledge of the threat landscape and current adversary behaviors.

- Threat intelligence curated from thousands of annual engagements
- Continuously updated insights from active investigations and threat research
- Real-world adversary behavior embedded into every response

Minimal disruption

Restore normal operations and strengthen your ability to withstand future attacks.

- Rapid threat elimination and return to steady-state operations
- Expert-guided remediation to close security gaps
- Stronger security posture to reduce future risk

START HERE

Learn more at **sophos.com/DFIR →**

2026-06-22 SB-EN (MC)