Incident Response: The First 24 Hours

The decisions you make in the first day of a security incident decide how much damage it does. Work through this checklist in order, tick items off as you go, and record what you did and when.

Golden rule: do not power off or wipe affected systems. Disconnect them from the network instead. Turning a machine off destroys evidence held in memory that investigators may need.

1. Confirm and declare

Hour 0 – 1

- [ ] Confirm the alert or report is a real incident, not a false positive.
- [ ] Appoint one **incident lead** who makes decisions and coordinates everyone else.
- [ ] Start an **incident log**: every action, decision and finding, with the time and who did it.
- [ ] Activate your incident response plan and call in your response team or retained responders.
- [ ] Move sensitive discussion off systems that may be compromised, such as corporate email or chat, onto a separate channel.
- [ ] Note the time you became aware of the incident. Regulatory deadlines run from this moment.

2. Contain the damage

Hour 1 – 4

- [ ] Isolate affected devices from the network, using your EDR tool or by unplugging the network cable. Keep them powered on.
- [ ] Disable or reset compromised accounts, and revoke their active sessions and access tokens.
- [ ] Block known malicious IP addresses, domains and file hashes at the firewall, proxy, email gateway and EDR.
- [ ] Protect your backups: take them offline or confirm they are immutable before attackers can reach them.
- [ ] Restrict administrative access to the minimum needed while you investigate.
- [ ] If ransomware is involved, do not contact the attackers or pay without legal and specialist advice.

3. Preserve evidence

Hour 1 – 6

- [ ] Capture memory images from key affected systems before rebooting anything.
- [ ] Take forensic disk images, or snapshots for cloud virtual machines.
- [ ] Export and secure logs: firewall, VPN, identity provider, email, EDR, cloud audit logs and the SIEM.
- [ ] Increase log retention so evidence is not overwritten automatically.
- [ ] Record a chain of custody for all evidence: who collected it, when, how, and where it is stored.

4. Assess and notify

Hour 4 – 12

- [ ] Scope the incident: which systems, accounts and data are affected, and how the attacker got in.
- [ ] Decide whether personal data is involved. Under UK and EU GDPR, a notifiable breach must be reported to the regulator (the ICO in the UK) within **72 hours** of becoming aware of it.
- [ ] Check other obligations: your cyber insurer, contracts with clients, sector regulators and card schemes.
- [ ] Consider reporting to law enforcement (Action Fraud and the NCSC in the UK).
- [ ] Brief senior leadership with facts, impact and next steps. Avoid speculation.
- [ ] Agree one spokesperson and prepare holding statements for staff, customers and media.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution

5. Eradicate and plan recovery

Hour 12 – 24

- [ ] Identify the root cause and every place the attacker gained a foothold, including persistence mechanisms.
- [ ] Remove malware, malicious accounts, scheduled tasks and unauthorised remote access tools.
- [ ] Patch or reconfigure the weakness the attacker used.
- [ ] Plan restoration from known-clean backups, in priority order of business impact.
- [ ] Reset credentials more widely where needed, including service and privileged accounts.
- [ ] Increase monitoring on affected systems, because attackers often try to return.

Key contacts

Fill this in before you need it, and keep a printed copy somewhere you can reach without your network.

Role	Name	Phone (out of hours)
Incident lead		
IT / security lead		
Executive sponsor		
Legal / data protection officer		
Communications / PR		
Cyber insurer (policy no.)		
Incident response retainer	Scarlet Dragonfly	+44 7389 051440

Do

- Keep a timed log of everything.
- Isolate, don't power off.
- Use a separate communication channel.
- Get legal advice early.

Don't

- Wipe or rebuild systems before evidence is captured.
- Alert the attacker by announcing it on systems they can see.
- Pay a ransom without specialist advice.
- Speculate publicly about the cause.

This checklist is general guidance and does not replace legal advice or a tailored incident response plan. Need help now or want a plan built for your organisation? Contact Scarlet Dragonfly at scarlet-dragonfly.com or +44 7389 051440.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution