Cybersecurity, don’t overlook the human element

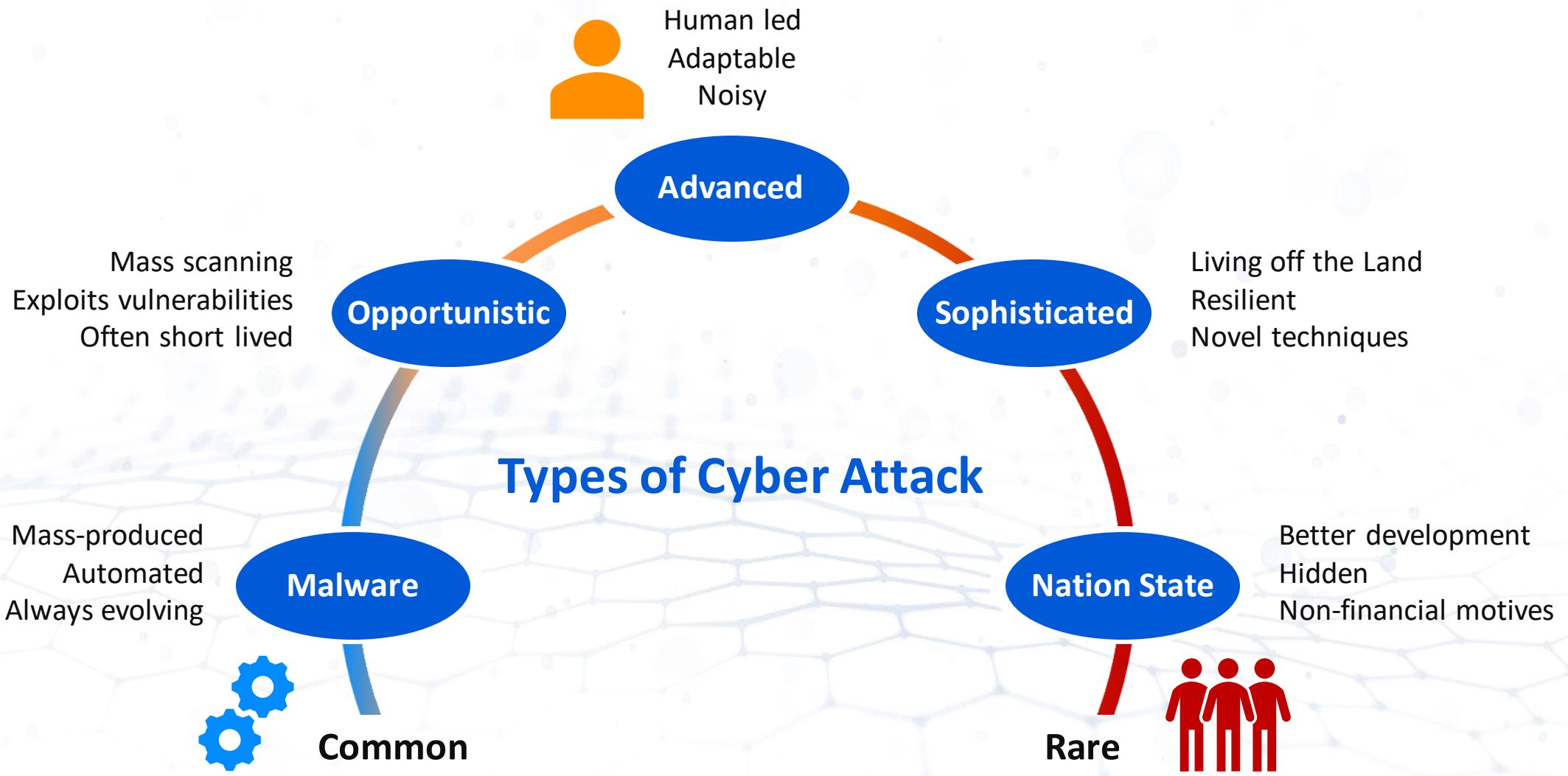
Paul Jacobs
Team Lead – Rapid Response

SOPHOS

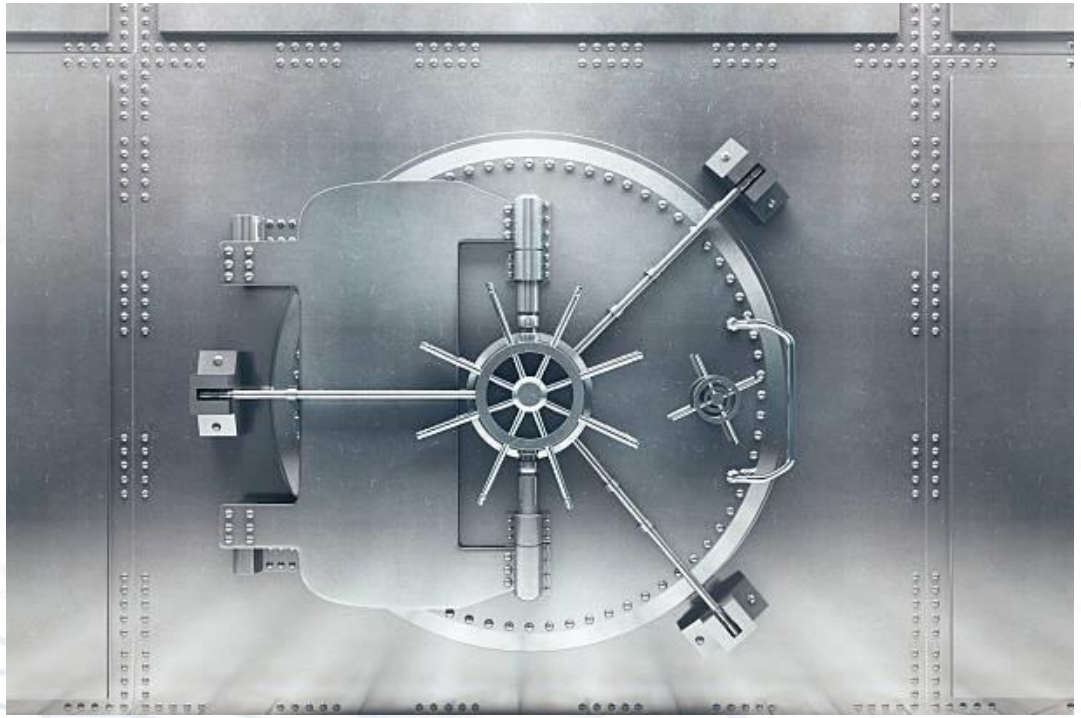
Topics Covered

- Why both technology and people are critical for an effective cybersecurity strategy
- Assume the attack succeeded: Why a post-incident investigation is crucial
- Why is the education sector a target?
- Real-world cyberattack walkthroughs: Two attack timelines from Education providers who were attacked by ransomware groups
- Tips to help minimise the risk of significant attacks being successful

Why technology and people are critical for an effective cybersecurity strategy



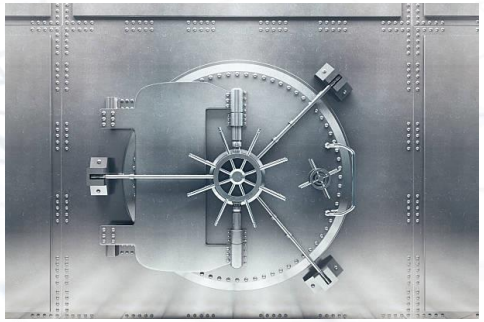
Cybersecurity is the same as physical security



Cybersecurity is the same as physical security

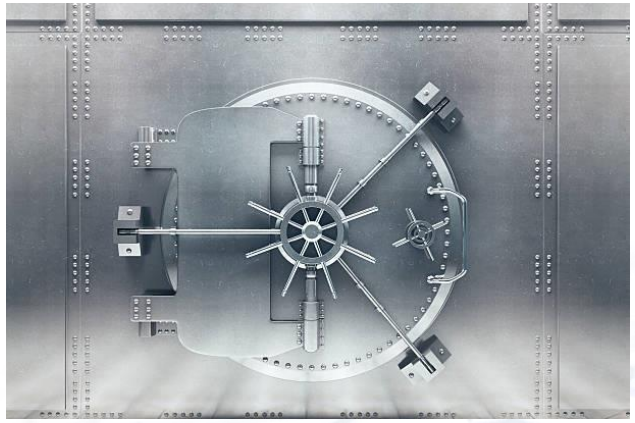
Firewall breached → Admin credentials stolen → Network scanned → Domain controllers identified → Domain Admin credentials stolen → Customer data exfiltrated → Backups deleted → Ransomware deployed to all devices → All business operations stop

00:00

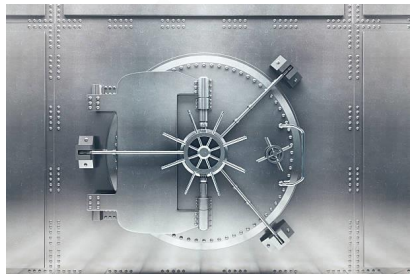


SOPHOS

Cybersecurity is the same as physical security



What you want vs What you have



Anti-Virus

XDR

SOC

One person responsible

for Everything!

SOPHOS

Assume the attack succeeded: why post-incident investigation is crucial

Wiping a machine

Pros

It's simple

It's fast

It removes unknown threats

It provides peace of mind

Cons

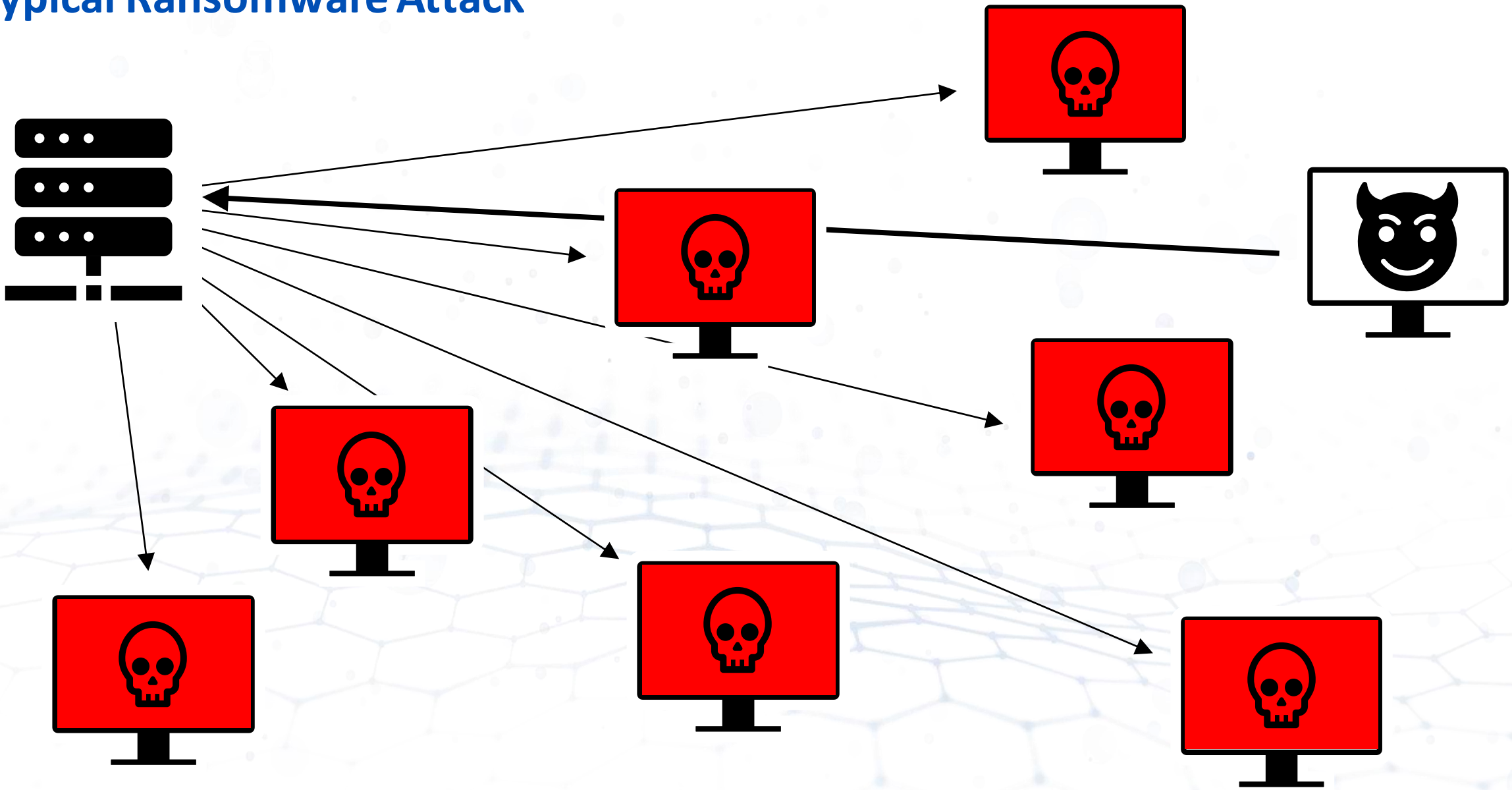
Destruction of evidence

Doesn't address root cause

Doesn't remove all threats

False sense of security

Typical Ransomware Attack



Why is the education sector a target

- May be seen as an easier target
- May have resources that could be exploited for Crypto mining
- Education Sector may have intellectual data that might be valuable
- PII data for Staff and Students might be valuable
- Raises the profile of the attack group via Media attention
- Victim may pay the ransom

Walkthrough of a Ransomware Attack – Case Study 1

Day 1 – VMware Horizon device exploited via Log4j.

Day 22 – PowerShell command executed to download and install Cobalt Strike from a C2

Day 24

- 12:00pm – Net.exe utility used to enumerate domain accounts
- 12:30 pm - PowerShell command to query all AD joined devices and IP addresses and then checked servers were online via ping.
- 1:00pm - Domain admin accounts compromised (believed via LSSAS dumps) and lateral movement from initial access device to other devices begins to occur.
- 8:00pm – Cobalt Strike installed on 2 more servers, including Veeam Backup
- 10:00pm – AnyDesk, Atera and Splashtop were installed on several more servers
- 11:00pm – WinRAR used to archive data and upload 10GB uploaded to mega.nz

Day 25

- 2:00am – SSH on the ESXi servers enabled and attacker manually access devices to deploy ransomware
- 4:00am – New administrator account created by attacker
- 4:05am - Scheduled task created via Group Policy to execute ransomware across all domain joined devices.

Walkthrough of a Ransomware Attack – Case Study 2

Day 1

8pm – Initial Access via RDP. Password compromised via Brute Force.

(2 weeks)

Day 14

9am – Unauthorised RDP logon from external IP (could be different attacker)

(7 weeks)

Day 65

10pm – Unauthorised RDP logon from external IP (could be different attacker)

(3 weeks)

Day 86 – 6am - Unauthorised RDP logon from external IP (could be different attacker)

3 days later …

Walkthrough of a Ransomware Attack – Case Study 2

Day 89

- 11 am - Unauthorised RDP logon from external IP
- 12pm – Attacker browsed numerous network locations from initial access device
- 12pm – Attacker utilised a network scanner to enumerate the environment.
- 12pm – Attacker attempted to use Psexec against another server. Blocked by application control.

Day 92

- 3pm – Attacker comes back via RDP
- 3pm – Attacker deploys a credential harvesting tool called Mimikatz
- 4pm – Attacker begins to laterally move from initial access device to other servers within the network
- 5pm – Anydesk installed by attacker on several servers for persistence
- 6pm – Powershell commands ran by attacker on one of the servers to download a suite of tools including Cobalt Strike
- 7pm – Attempts to install PSExec service Exchange server, blocked by Application Control
- 7pm – Attacker manually accessed Backup Servers and destroyed all backup files..
- 7pm – Ransomware was deployed from a single device via a batch file which contained all the IP addresses of target devices and encrypted files via network shares
- 8pm – Event logs were cleared by the attacker on several servers.

How to minimise the risk of significant attacks being successful

- Make sure your entire IT infrastructure is not run and supported by a single person
- Ensure you have protected or offline backups. This is so important.
- Ensure you have Multi-Factor Authentication implemented for all users.
- Do not use software that is no longer vendor supported
- Be prepared with an Incident Response plan and test it regularly. Even if it is just a table top walk through.
- Take an honest overview of your Security Posture and prioritise areas for improvement.
- If you don't have the skills in-house to deal with cyber incidents then consider using a managed service.
- Use tools such as Shodan.io, Censys.io to help understand your perimeter exposure
- Pingcastle.com has a tool that can help you understand some of the security issues present in your environment.
- Conduct regular audits of domain accounts, services and software in use.
- Have a patch management plan which incorporates how you identify and mitigate new vulnerabilities
- Research how others in your sector have dealt with attacks.
  - The following Podcast is a good example and relates to an attack at Dundee and Angus College (https://www.jisc.ac.uk/podcasts/tech-takes-the-impact-of-ransomware-attacks-02-mar-2022)

Sophos Managed Detection & Response

24/7 threat hunting, detection, and response delivered by an expert team as a fully-managed service

Sophos.com/MDR

Sophos Rapid Response

Sophos.com/RapidResponse

SOPHOS

SOPHOS

Cybersecurity delivered.