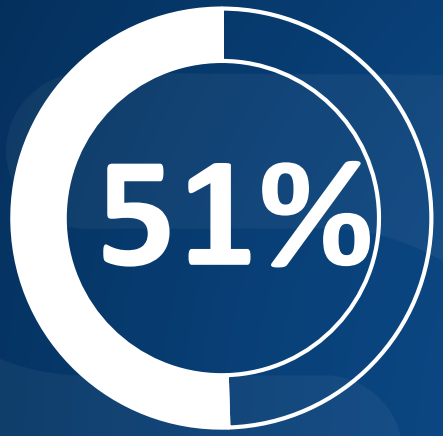
SOPHOS
Cybersecurity evolved.

CYBERSECURITY INCIDENT RESPONSE BEST PRACTICES

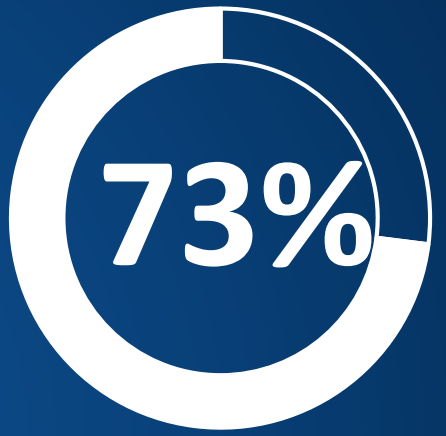
FOUR COMMON MISTAKES AND HOW TO BUILD AN EFFECTIVE INCIDENT RESPONSE PLAN

Geoff Morrison
Cyber Security Sales Engineer
Wednesday, 10 February 2021

HD IT
IT for business...



of organizations were hit by ransomware in the last year



of attack victims said the cybercriminal succeeded in encrypting their data

The State of Ransomware 2020, Sophos

HD IT
IT for business...

SOPHOS

FOUR COMMON CYBERSECURITY INCIDENT RESPONSE MISTAKES

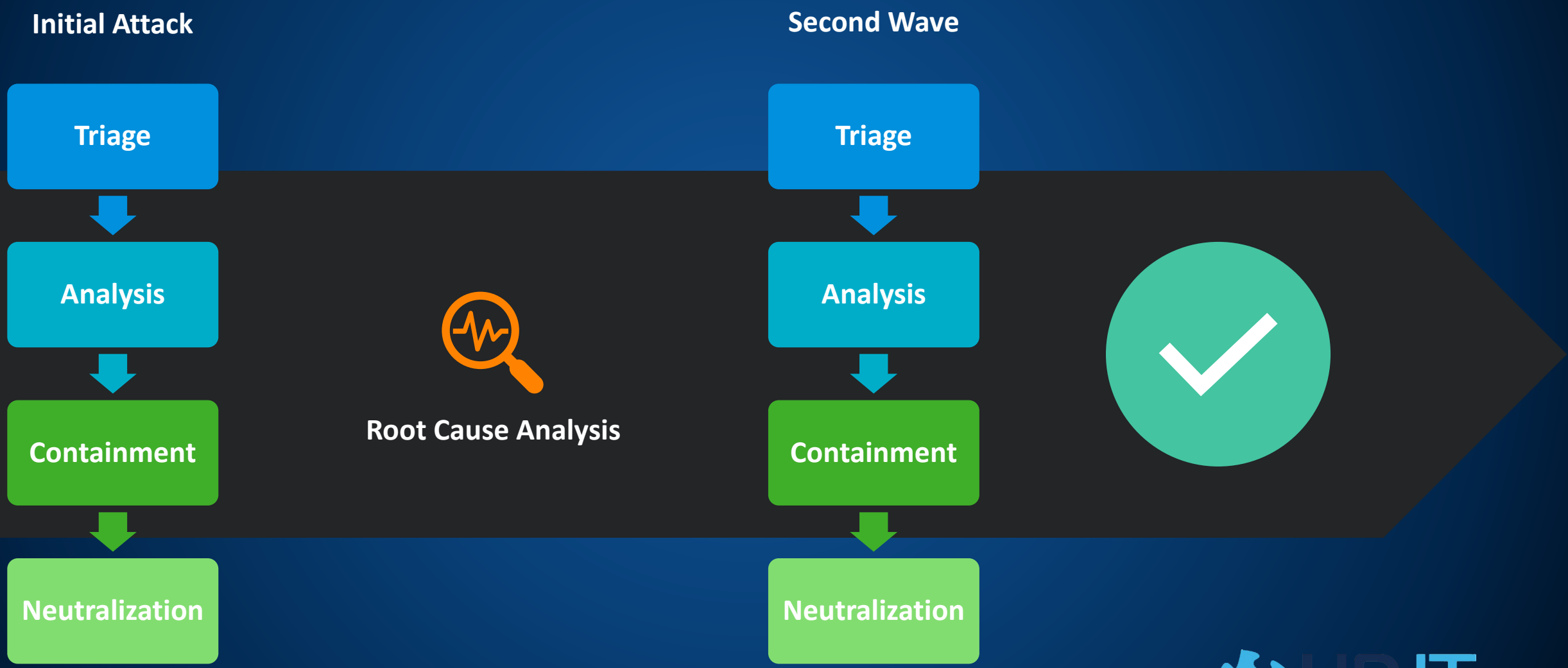
HD IT
IT for business...

SOPHOS

1. WAITING TOO LONG TO REACT

- Lack of context = lack of urgency
- Attacks hit at inopportune times
- Understaffed and/or inexperienced teams
- Teams are overwhelmed

2. DECLARING "MISSION ACCOMPLISHED" TOO SOON



CASEBOOK

BLOCKING A $15M RANSOMWARE ATTACK

DAYS 1-3: THE ATTACK BEGINS

Operators compromise computer on target's network

DAYS 4-5: CALM BEFORE STORM

The attackers wait for a day when the target's security team wouldn't be working

DAY 6: THE FIRST ATTACK

The attack was launched on a Sunday, using a compromised domain admin account

DAY 7: SOPHOS ENGAGED

Sophos Rapid Response team engaged. Compromised account identified, malicious files removed, attacker C2 blocked

DAY 8: NEUTRALIZATION

Sophos continued to investigate and blocked additional files and accounts

DAY 9: THE SECOND ATTACK

The attackers launched a new attack via a different compromised account

DAY 9: ATTACK II THWARTED

Sophos Intercept X and the Rapid Response team stopped and cleaned up the attack

DAY 9: THIRD TIME LUCKY?

The attackers distributed the ransomware payload inside a virtual machine

DAY 9: ATTACK III THWARTED

The Sophos Rapid Response team detected and stopped the attack. No files were encrypted

3. RELYING ON INCOMPLETE VISIBILITY

COLLECTING SIGNALS

- Tools
- Tactics
- Procedures

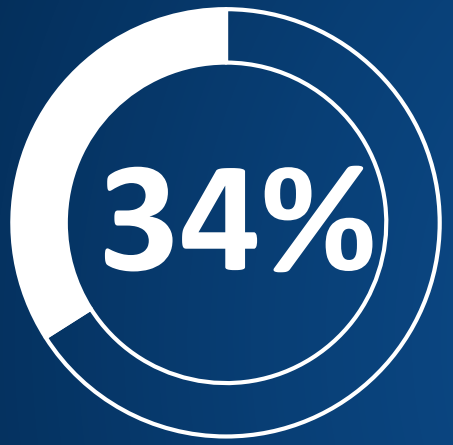
REDUCING NOISE

- Data collection/storage costs
- Alert fatigue
- Time wasted on false positives

APPLYING CONTEXT

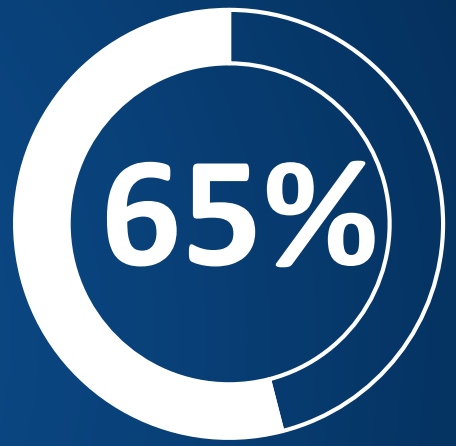
- Pinpoint signal origin
- Identify current stage + related events
- Outline potential business impact

4. ASSUMING YOU CAN HANDLE IT ON YOUR OWN



Say lack of skilled resources is their biggest challenge when it comes to determining the attack chain and root cause of an incident

ESG

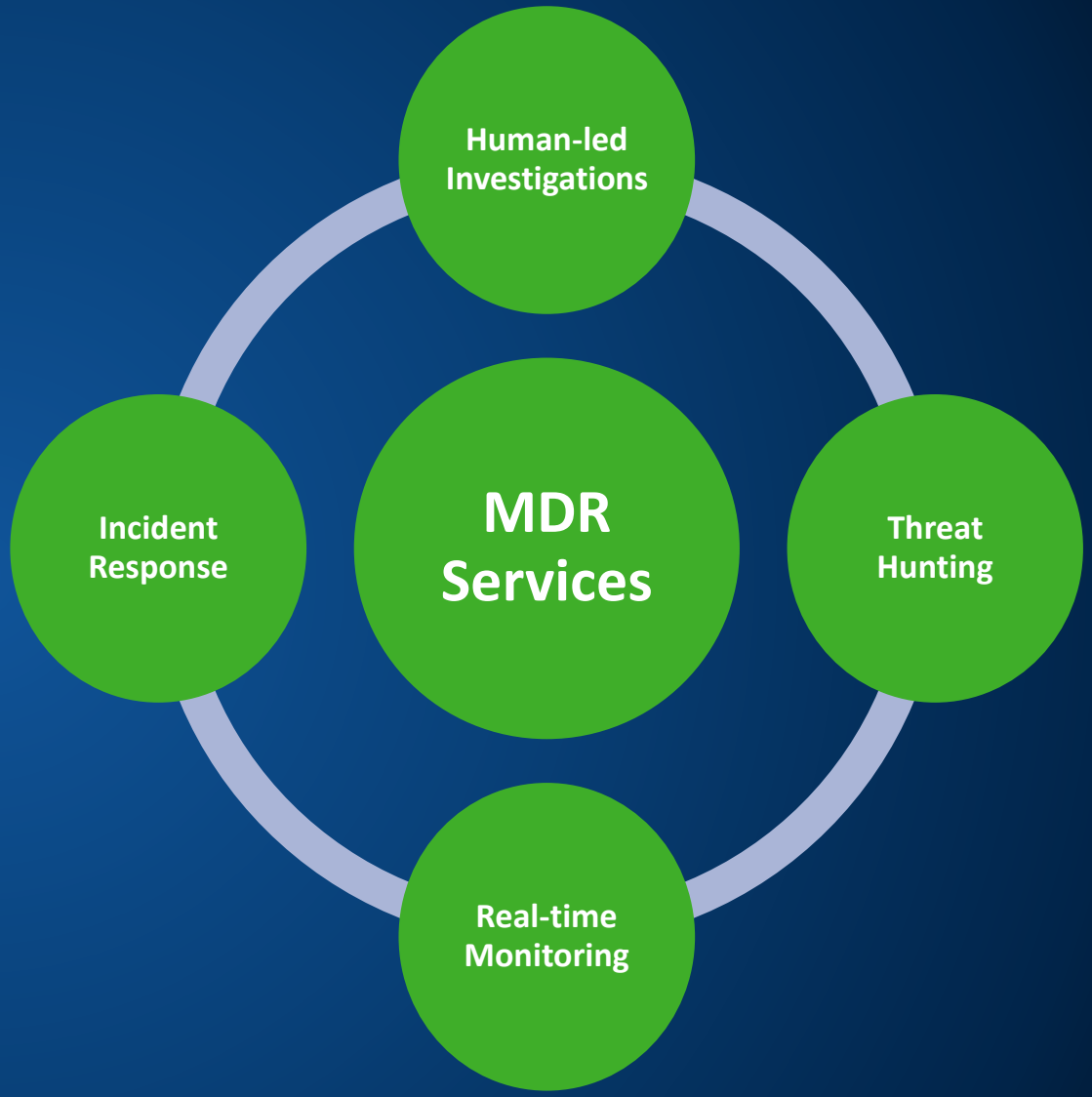


of organizations already outsource some/all of their IT security efforts. This is set to rise to 72% by 2022.

Cybersecurity: The Human Challenge
Sophos 2020 Survey of 5,000 IT Managers

of organizations will be using MDR services by 2025 (up from less than 5% in 2019).

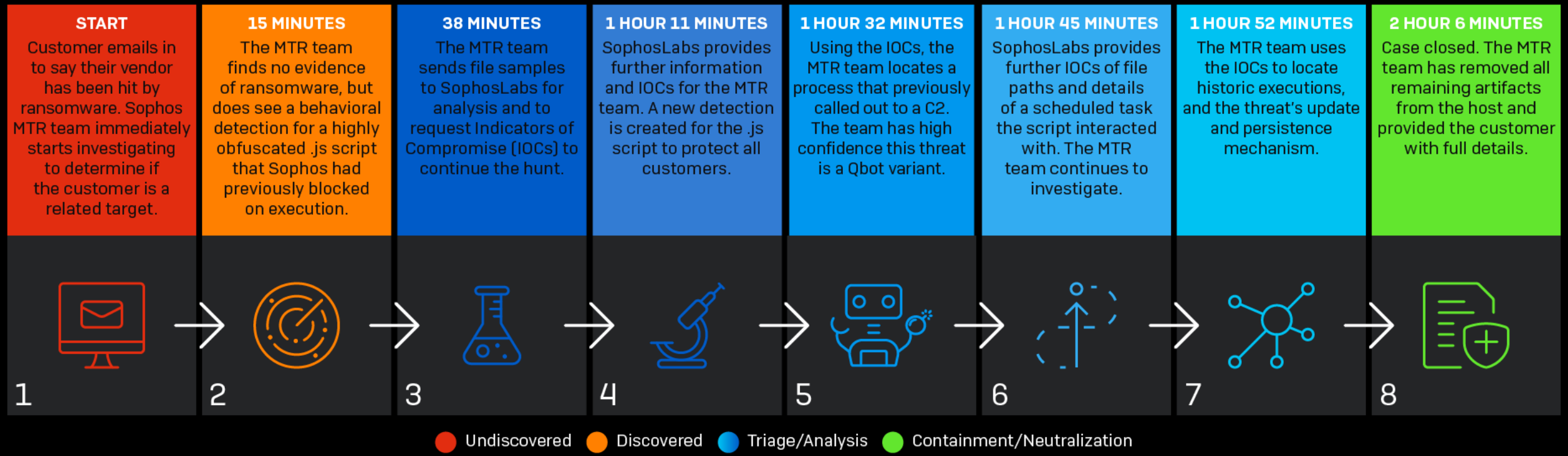
Gartner Market Guide for Managed Detection and Response Services*



*26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

CASEBOOK

A RANSOMWARE HUNT THAT UNEARTHED A HISTORIC BANKING TROJAN



news.sophos.com 🔍 **'MTR Casebook'**

SUMMARY

1. REACT AS QUICKLY AS POSSIBLE
2. DON'T DECLARE "MISSION ACCOMPLISHED" TOO SOON
3. ENSURE YOU HAVE COMPLETE VISIBILITY
4. ACCEPT THAT IT IS OK TO ASK FOR HELP

10 STEPS TO AN EFFECTIVE CYBERSECURITY INCIDENT RESPONSE PLAN

HD IT
IT for business...

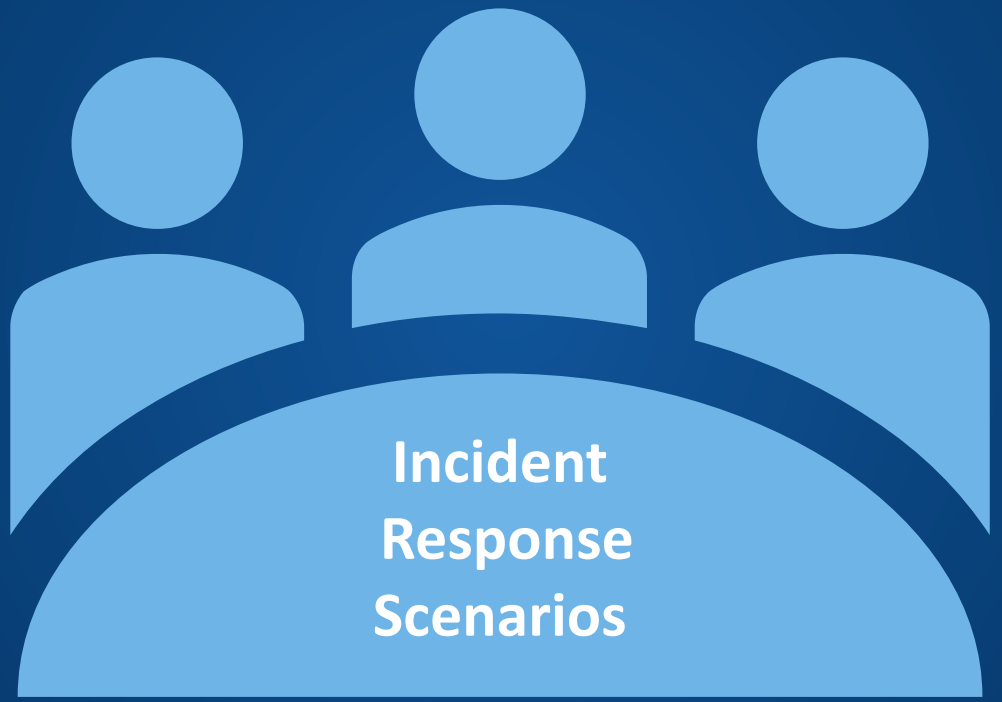
SOPHOS

1. DETERMINE KEY STAKEHOLDERS

2. IDENTIFY CRITICAL ASSETS

- Data
- People
- Infrastructure
- Applications

3. RUN TABLE-TOP EXERCISES



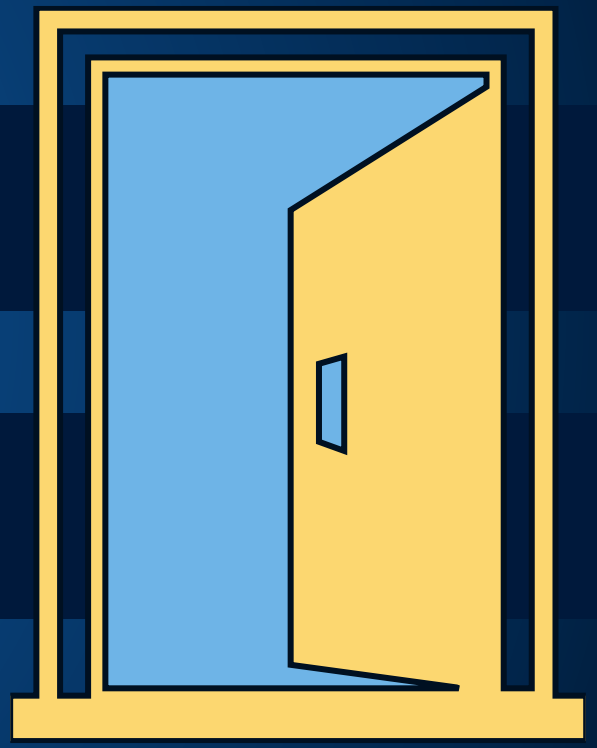
SCENARIO #1 - ACTIVE ADVERSARY DETECTED IN NETWORK

- Was an attacker able to infiltrate?
- What tools, tactics, techniques, and procedures did they use?
- What was targeted?
- Did they have established persistence?

SCENARIO #2 - SUCCESSFUL DATA BREACH

? What was exfiltrated?

? How was it exfiltrated?



SCENARIO #3 - SUCCESSFUL RANSOMWARE ATTACK

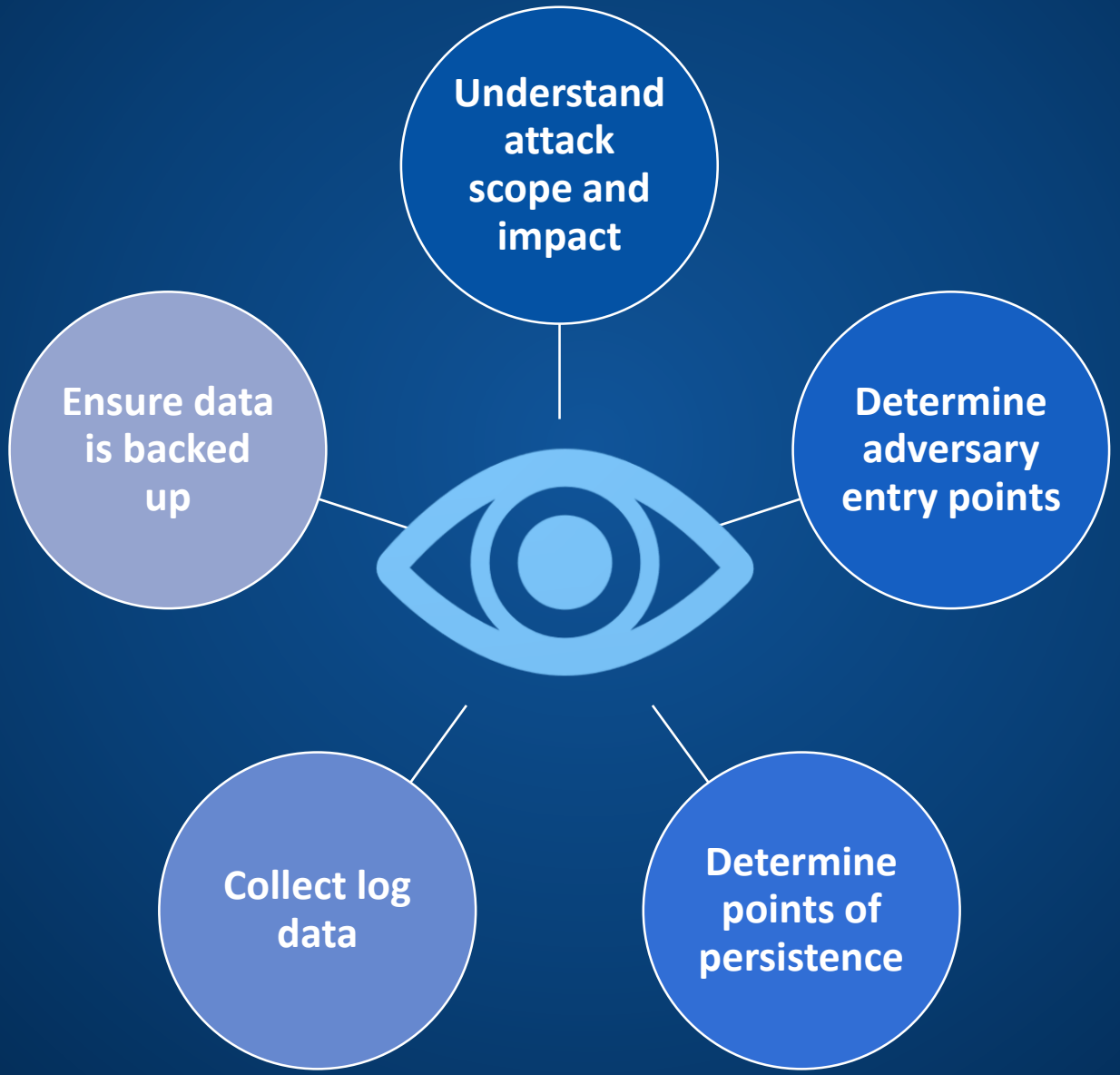
- Follow a plan to recover losses
- Include a process to restore systems from backups
- Investigate if the adversary's access has been cut off
- Consider the impact of paying the ransom

SCENARIO #4 – HIGH-PRIORITY SYSTEM COMPROMISED

Consider a business recovery plan

4. DEPLOY PROTECTION TOOLS

5. ENSURE YOU HAVE MAXIMUM VISIBILITY



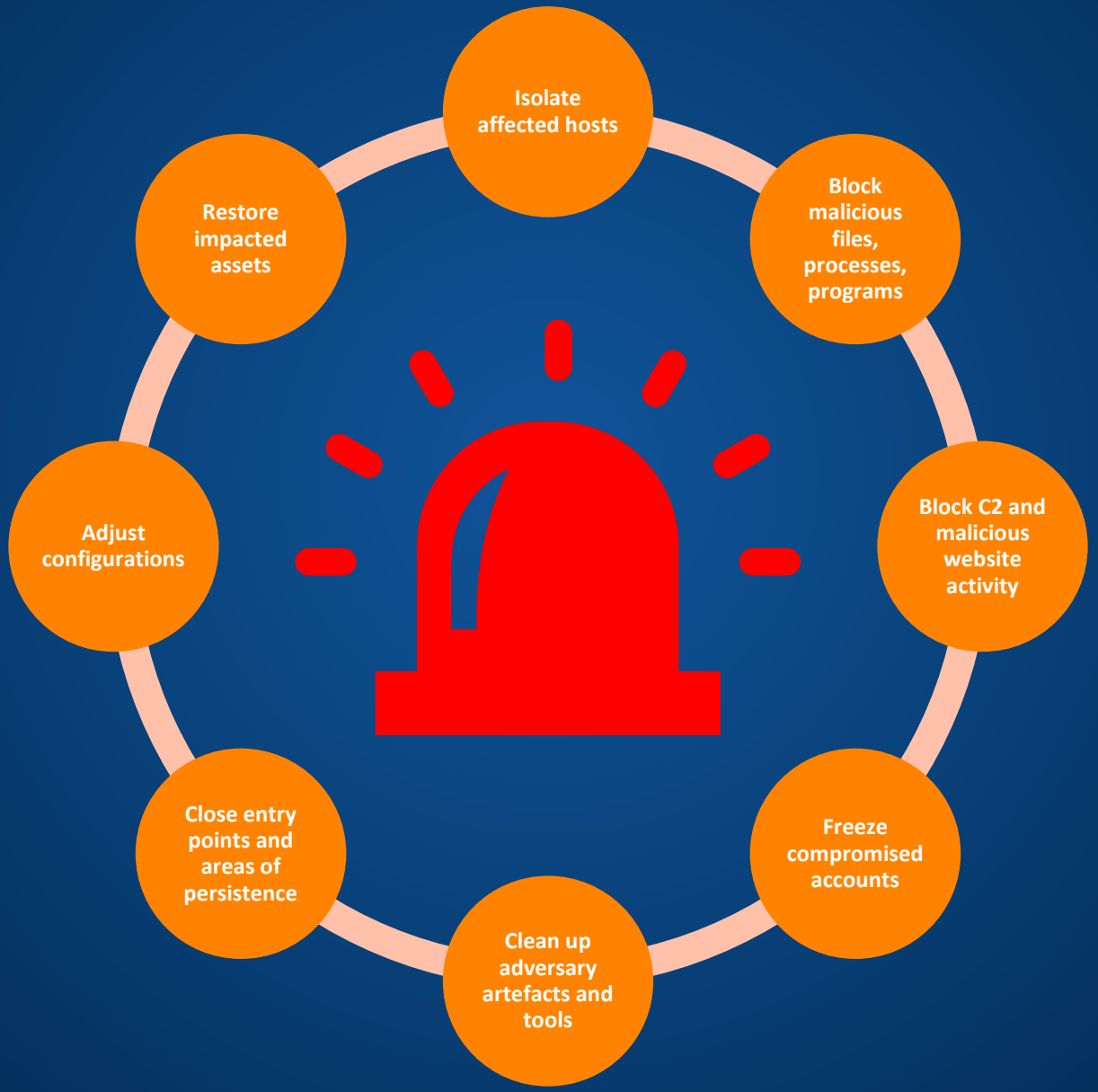
6. IMPLEMENT ACCESS CONTROL

- Deploy MFA
- Limit Admin Privileges
- Change Default Passwords
- Reduce Number of Access Points

7. INVEST IN INVESTIGATION TOOLS

- Hunt across your environment to detect IOCs and IOAs
- Help analysts pinpoint compromised assets
- Help determine attack scope and impact

8. ESTABLISH RESPONSE ACTIONS

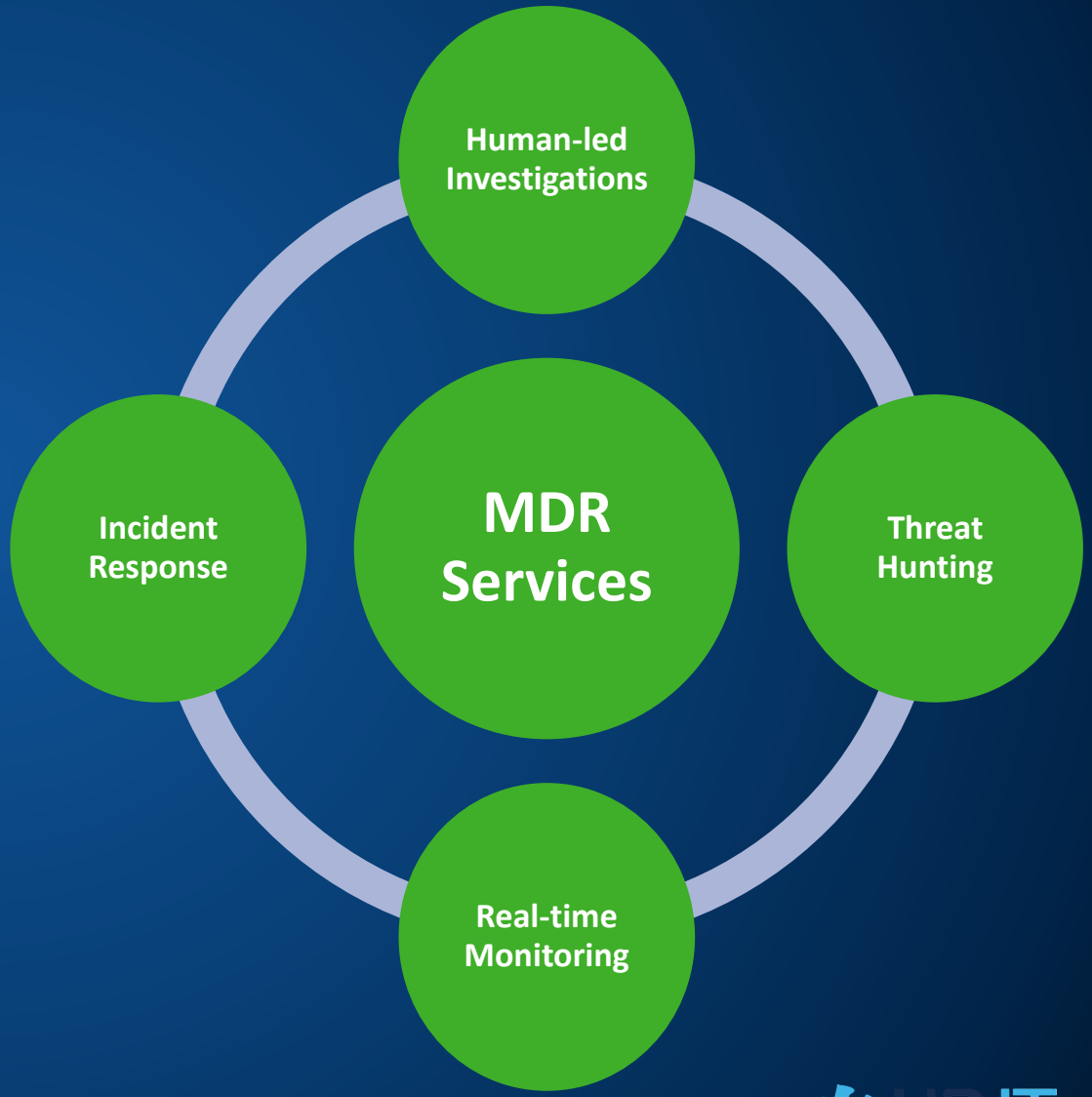


9. CONDUCT AWARENESS TRAINING

10. HIRE A MANAGED SECURITY SERVICE

of organizations will be using MDR services by 2025 (up from less than 5% in 2019).

Gartner Market Guide for Managed Detection and Response Services*



*26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

YOUR TEN-STEP PLAN

1. DETERMINE KEY STAKEHOLDERS
2. IDENTIFY CRITICAL ASSETS
3. RUN TABLE-TOP EXERCISES
4. DEPLOY PROTECTION TOOLS
5. ENSURE MAXIMUM VISIBILITY
6. IMPLEMENT ACCESS CONTROL
7. INVEST IN INVESTIGATION TOOLS
8. ESTABLISH RESPONSE ACTIONS
9. CONDUCT AWARENESS TRAINING
10. HIRE A MANAGED SECURITY SERVICE

HOW SOPHOS & HDIT CAN HELP

HD IT
IT for business...

SOPHOS

Protection. Visibility. Expertise.

24/7/365
Proactive Service

EDR for Security Analysts
and IT Administrators

The World's Best
Endpoint Protection

Sophos Managed Threat Response (MTR)

- 24/7 human-led threat hunting.
- We investigate suspicious activity, not just detections.
- Others Stop at Notification. We Take Action.

Analyst-Led Threat Hunting and Response

Targeted Actions to Neutralize Threats

Complete Transparency and Control

Sophos Rapid Response

- Remote Incident Response
- 24/7 Team
- Dedicated Point of Contact
- 45 Day Fixed-cost Service
- Rapid Deployment
- Transition to MTR Advanced

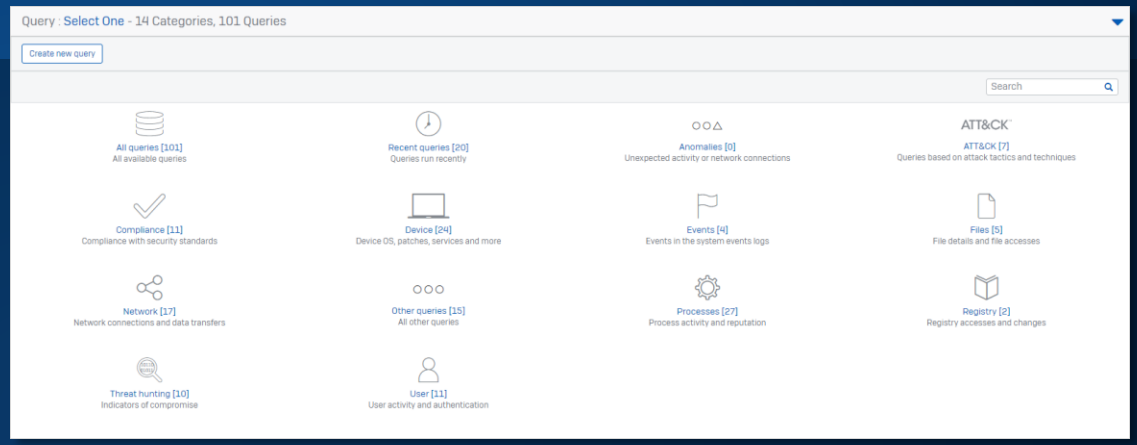
SOPHOS

HD IT
IT for business...

Sophos EDR: Ask, Answer and Respond - *Fast*

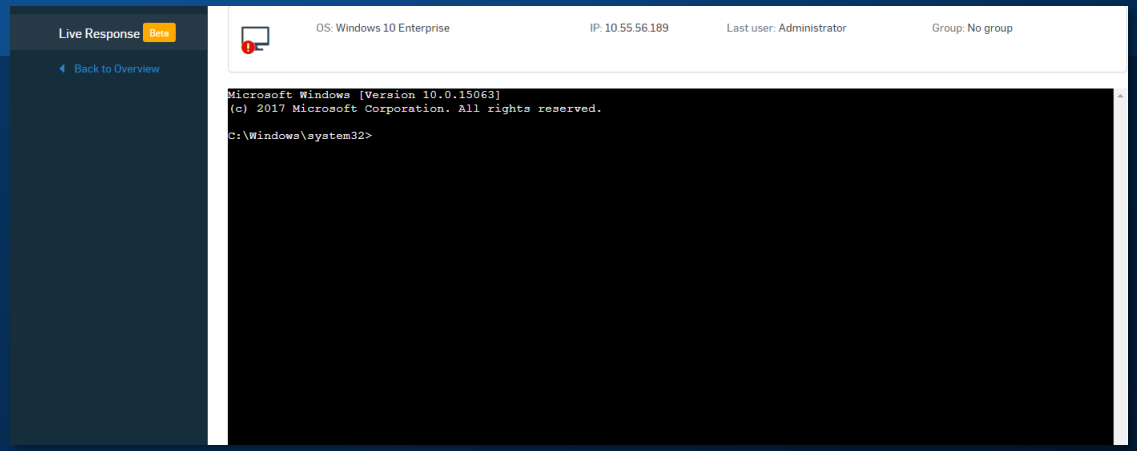
Live Discover

- Rich endpoint search capabilities
- Pre-written, customizable SQL queries
- Up to 90 days on-disk live and historic data

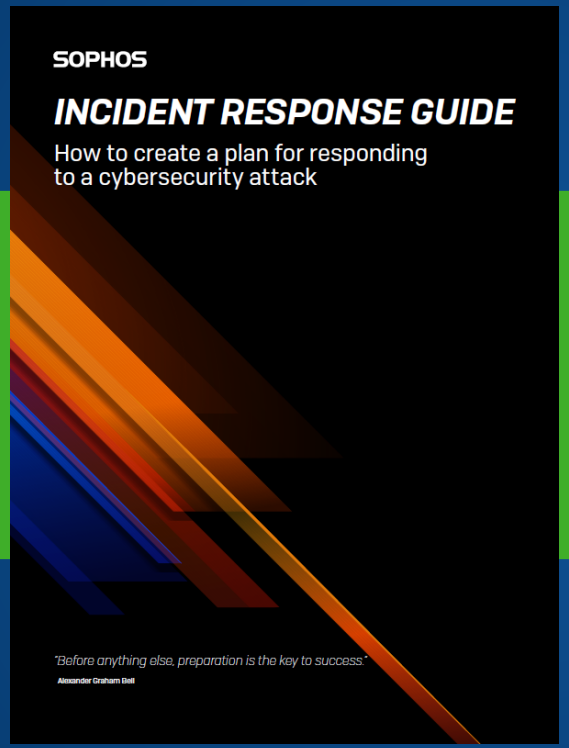


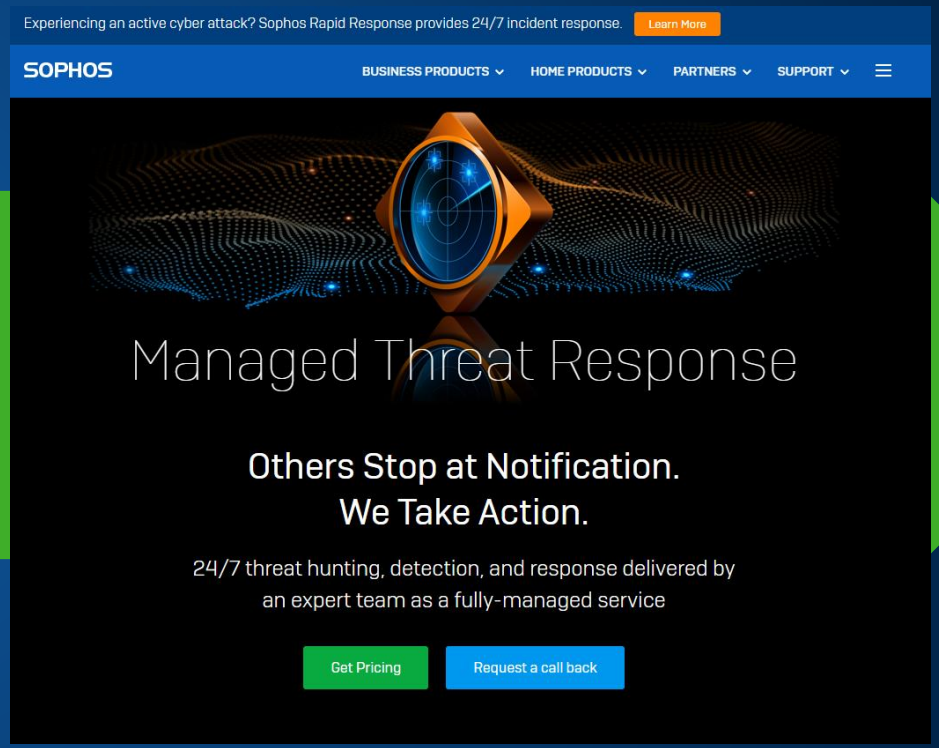
Live Response

- Remotely remediate managed devices
- Powerful cmdline interface
- Audit logs and MFA included



NEXT STEPS





SOPHOS.COM/PLAN

SOPHOS.COM/MTR
SOPHOS.COM/RAPIDRESPONSE

ANY QUESTIONS?

CYBERSECURITY EVOLVED.

HD IT
IT for business...