CYBERTHREAT UPDATE
YOU WILL BE BREACHED

TAKEAWAYS, FIRST

- Cybersecurity is business risk management.
- EVERY business owner CONSTANTLY does risk management.

Accept

Acknowledge and live with the risk

Transfer

Shift consequences of the risk to another party

Control

Reduce likelihood or impact of the risk

Avoid

Eliminate exposure to risk

TAKEAWAYS, FIRST

- Solid cybersecurity does NOT make you immune to loss.

- Cybersecurity works to:
    - Minimize threat actors’ opportunities to do you harm.
    - Detect high-risk, suspicious activity as early as possible.
    - Investigate and respond to suspicious indicators.
    - Minimize business disruption and recover.

TAKEAWAYS, FIRST

“Cybersecurity” is NOT an installable product, it’s a combination of…

TOOLS

PEOPLE

PROCESSES

CULTURE

TAKEAWAYS, FIRST

Tools

- Air-gapped Data Backup
- E-Mail, Teams Security Filtering
- Managed Detection & Response (MDR)
- Conditional Multi-Factor Authentication
- Security Information & Event Management (SIEM)
- External Vulnerability Scanning

People

- IT Team
- Cybersecurity Insurer
- Attorney
- Internal security response team
- Security Operations Center (SOC)

Processes

- Incident Response Plan

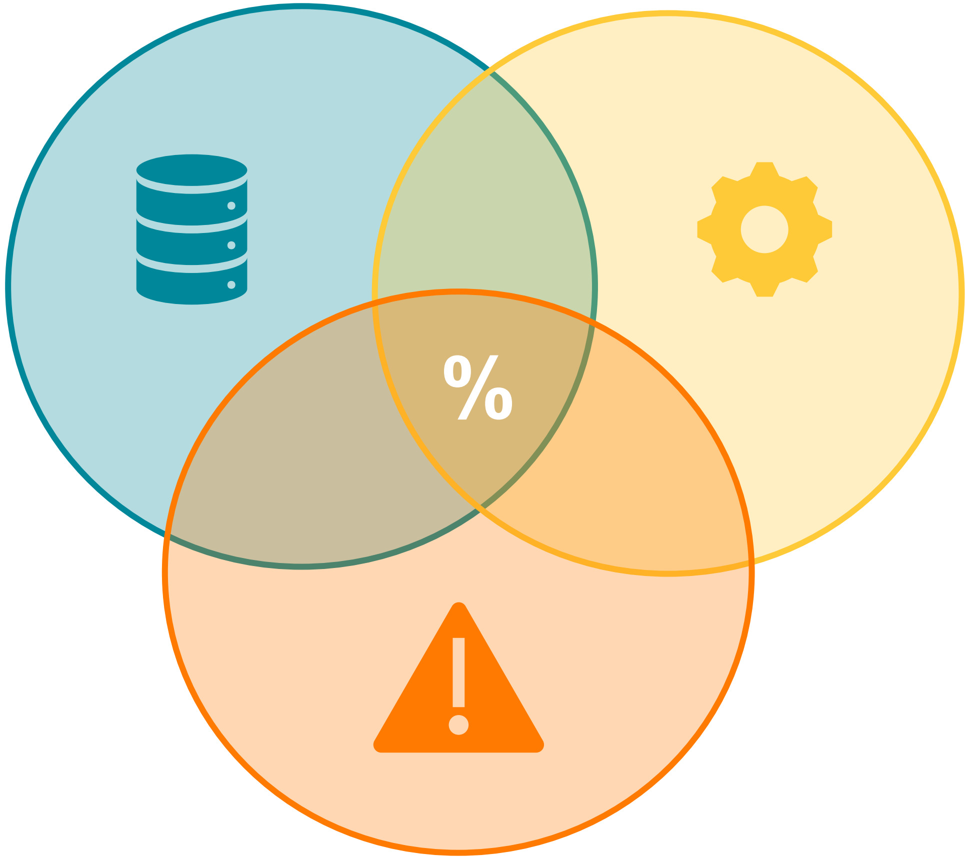
Culture

- Leadership team driving security

ASSESSING RISK LIKELIHOOD

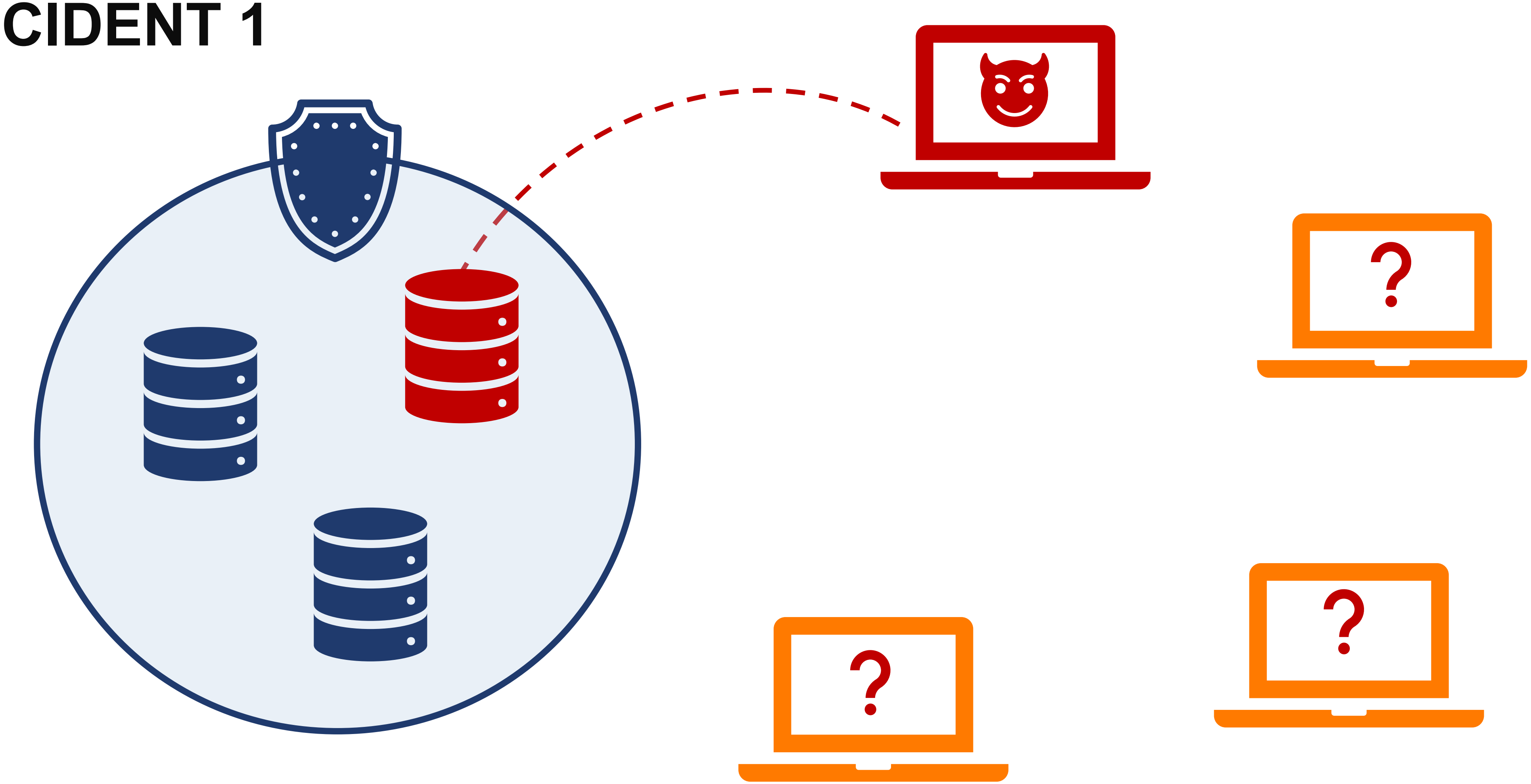
“Incidents” happen at the confluence of:

- An **active threat attempt**, and
- An **asset** you care about, and
- A **vulnerability**



INCIDENT 1:
LAW FIRM

INCIDENT 1



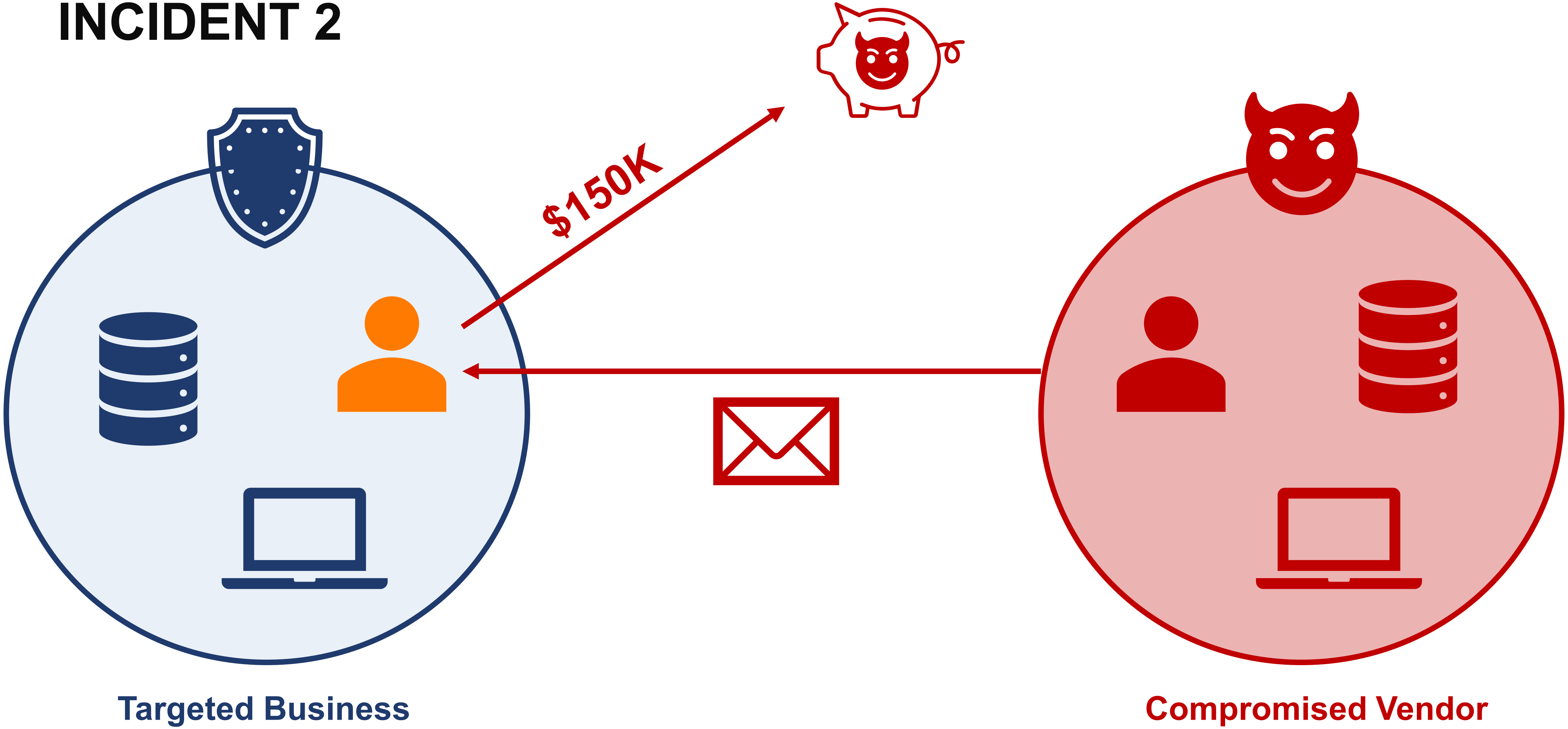
INCIDENT 1 IMPACTS

- 2 weeks’ business downtime (~$200K)
  - 11 attorneys unable to bill at full rate or access files
  - Extraordinary measures required to meet court, filing deadlines
- Uncertainty of privileged client information exposure
- Emergency replaced all computers (~$30K)
- Emergency replaced older network firewall (~$5K)
- Emergency replaced older server instances (~$15K)
- Emergency response, recovery (~$15K)

INCIDENT 2:

MANAGED CARE PROVIDER

INCIDENT 2



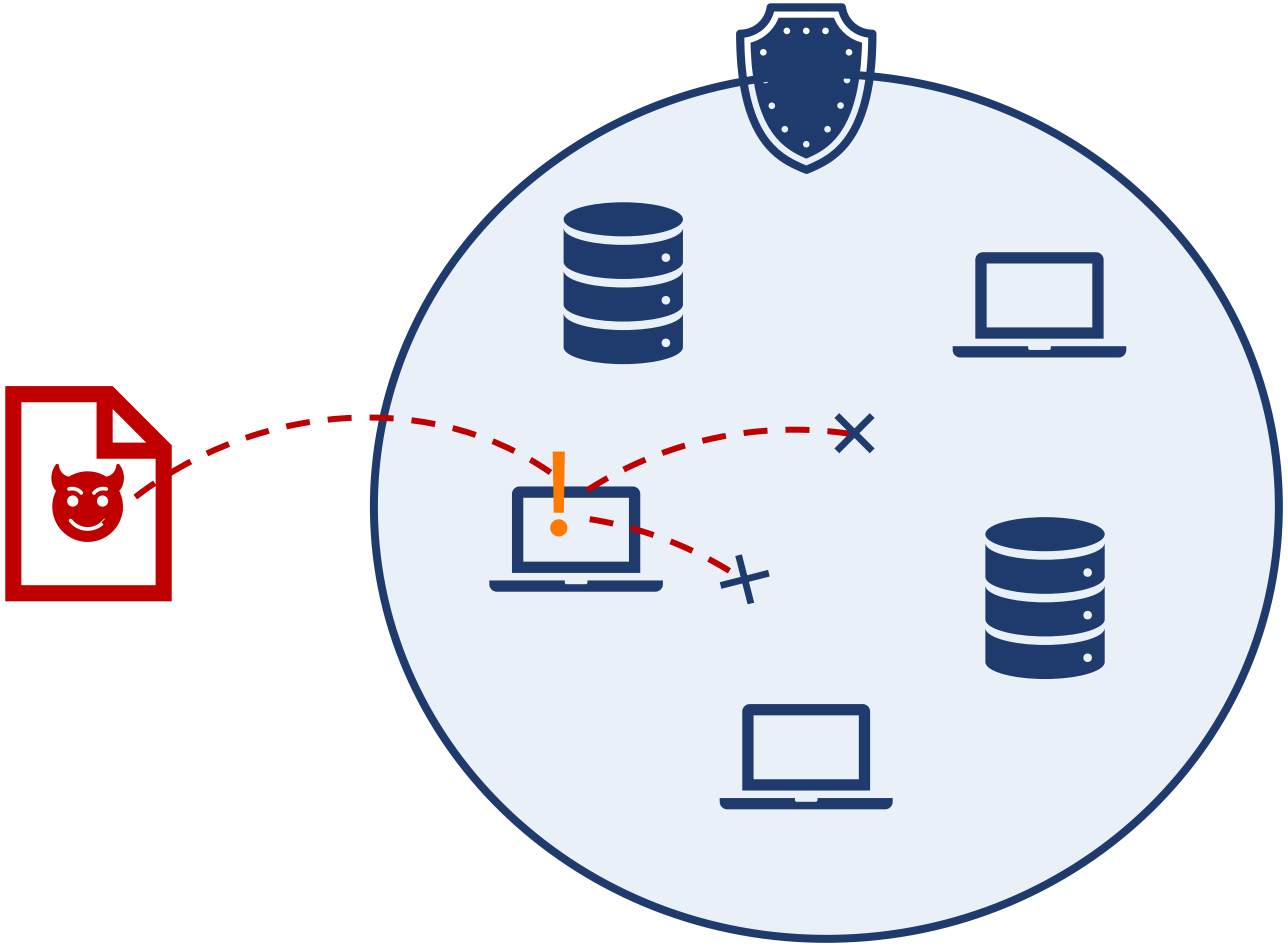
INCIDENT 2 IMPACTS

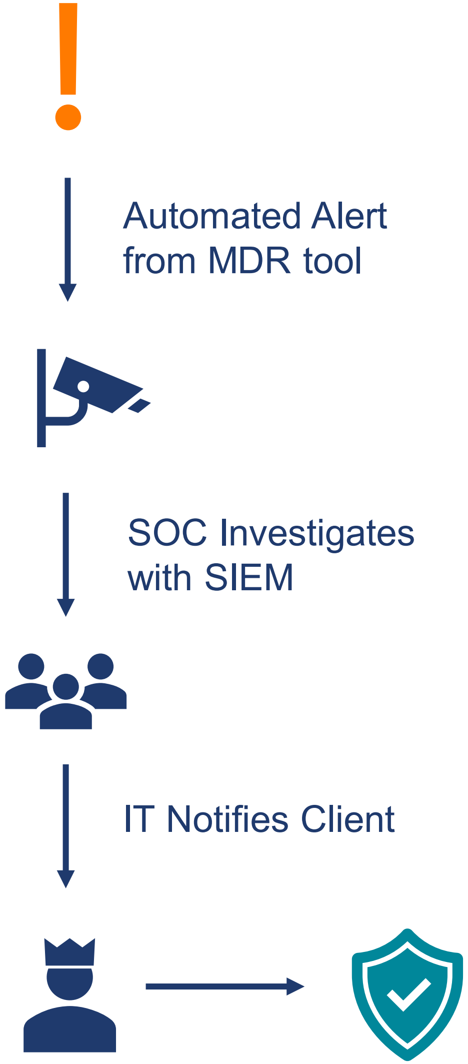
- >$100K wire fraud loss
  - Eventually recovered through international law enforcement, banking
- Full executive team + legal response for 3 weeks (~$80K)
- Full accounting team awareness, attention (~$50K)
- HIPAA patient information exposure; regulatory exposure
- Patient privacy mitigation expenses
- Third-party trust impacts; compromised accounts used as jumping-off pts

INCIDENT 3:
INSURANCE BROKERAGE

Event: November 7, 2023

INCIDENT 3: INTERCEPTED





Automated Alert from MDR tool

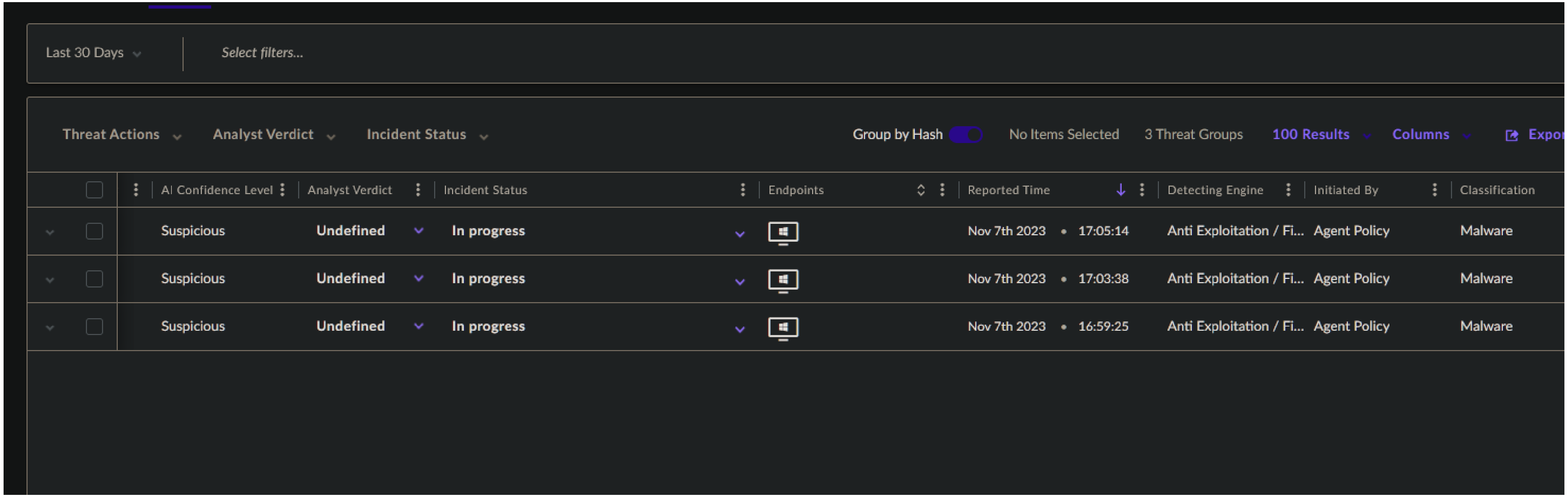
SOC Investigates with SIEM

IT Notifies Client

Security Incident Completely Resolved

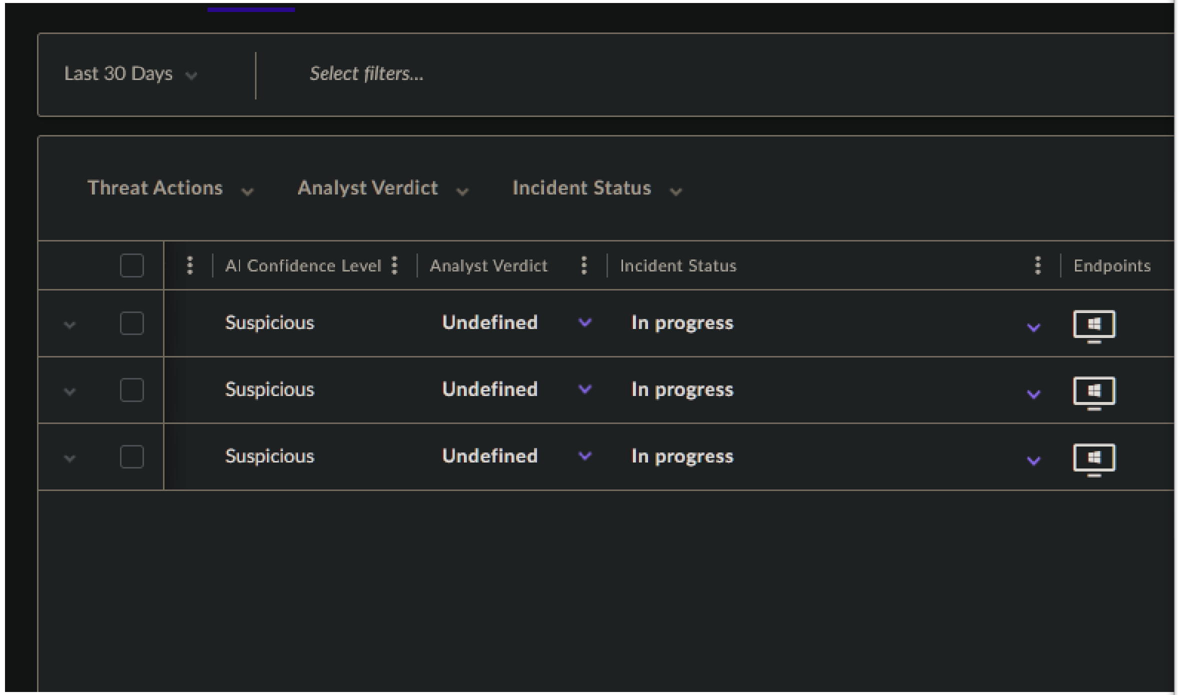
Time from alert to resolution: **2 hours and 30 minutes**

INCIDENT 3: INTERCEPTED



AI Confidence Level	Analyst Verdict	Incident Status	Endpoints	Reported Time	Detecting Engine	Initiated By	Classification
Suspicious	Undefined	In progress		Nov 7th 2023 • 17:05:14	Anti Exploitation / Fi...	Agent Policy	Malware
Suspicious	Undefined	In progress		Nov 7th 2023 • 17:03:38	Anti Exploitation / Fi...	Agent Policy	Malware
Suspicious	Undefined	In progress		Nov 7th 2023 • 16:59:25	Anti Exploitation / Fi...	Agent Policy	Malware

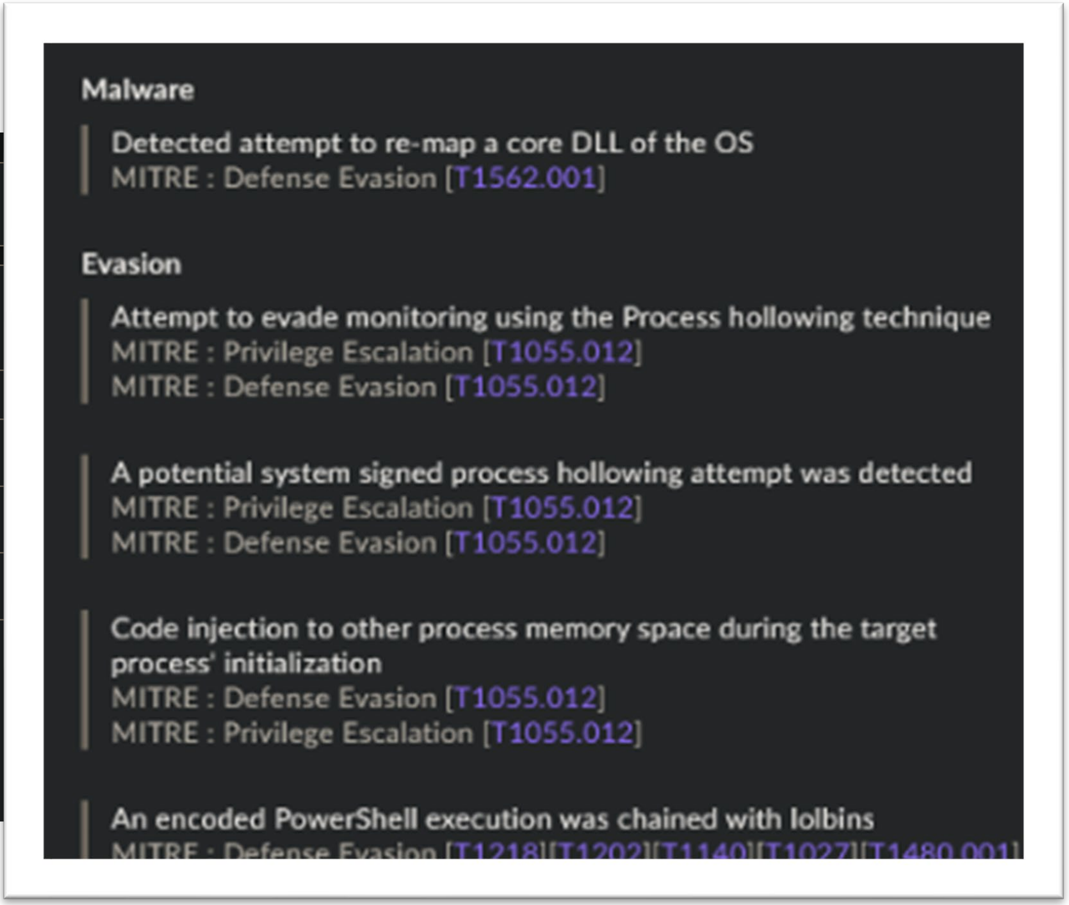
INCIDENT 3: INTERCEPTED



Last 30 Days ⌄ | *Select filters...*

Threat Actions ⌄ Analyst Verdict ⌄ Incident Status ⌄

	□	AI Confidence Level	Analyst Verdict	Incident Status	Endpoints
⌄	□	Suspicious	Undefined ⌄	In progress ⌄	🖥
⌄	□	Suspicious	Undefined ⌄	In progress ⌄	🖥
⌄	□	Suspicious	Undefined ⌄	In progress ⌄	🖥



Malware

Detected attempt to re-map a core DLL of the OS
MITRE : Defense Evasion [T1562.001]

Evasion

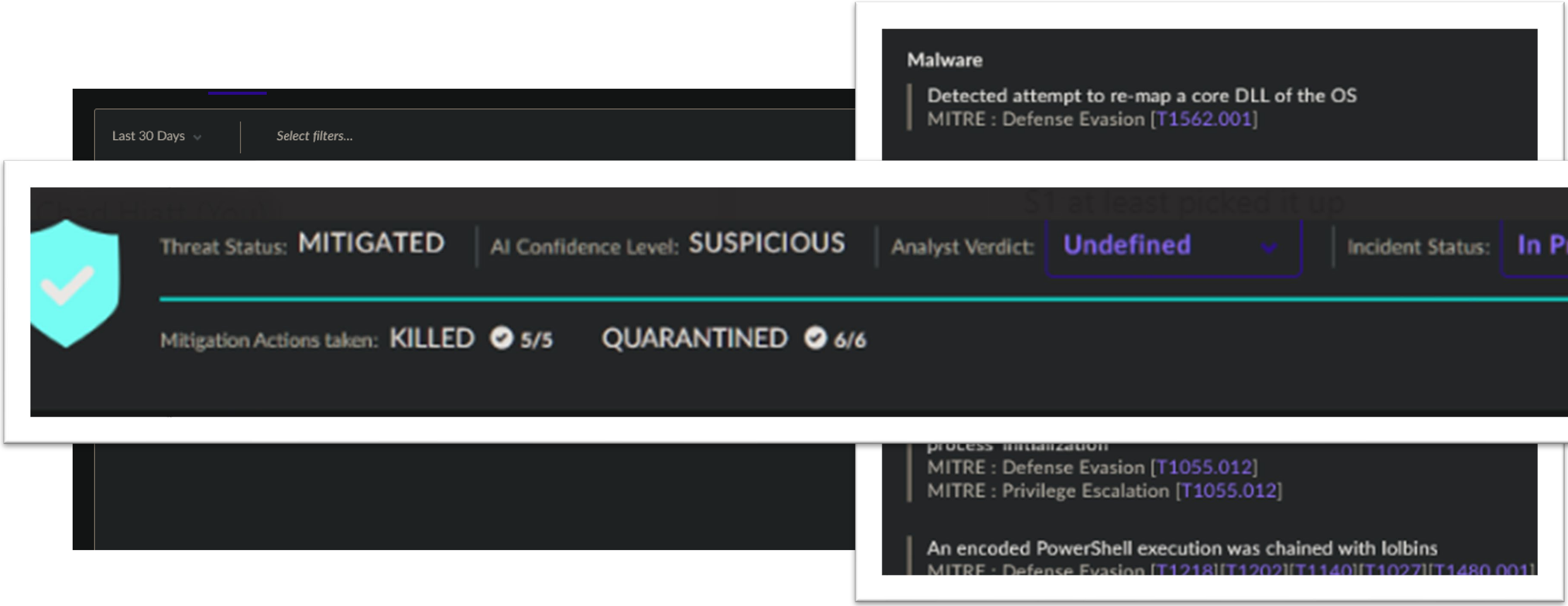
Attempt to evade monitoring using the Process hollowing technique
MITRE : Privilege Escalation [T1055.012]
MITRE : Defense Evasion [T1055.012]

A potential system signed process hollowing attempt was detected
MITRE : Privilege Escalation [T1055.012]
MITRE : Defense Evasion [T1055.012]

Code injection to other process memory space during the target process' initialization
MITRE : Defense Evasion [T1055.012]
MITRE : Privilege Escalation [T1055.012]

An encoded PowerShell execution was chained with lolbins
MITRE : Defense Evasion [T1218][T1202][T1140][T1027][T1480.001]

INCIDENT 3: INTERCEPTED



Last 30 Days

Select filters...

Malware

Detected attempt to re-map a core DLL of the OS
MITRE : Defense Evasion [T1562.001]

S1 at least picked it up

Threat Status: MITIGATED

AI Confidence Level: SUSPICIOUS

Analyst Verdict: Undefined

Incident Status: In Prog

Mitigation Actions taken: KILLED ✓ 5/5 QUARANTINED ✓ 6/6

process initialization
MITRE : Defense Evasion [T1055.012]
MITRE : Privilege Escalation [T1055.012]

An encoded PowerShell execution was chained with lolbins
MITRE : Defense Evasion [T1218][T1202][T1140][T1027][T1480.001]

INCIDENT 3: INTERCEPTED

- **4:59 PM**: Script action detected by protection tools on notebook.
- **4:59 PM**: MDR identified event as suspicious **and interrupted it**.
- **5:09 PM**: Security Operations Center 24x7 investigated, correlated.
- **5:31 PM**: Escalation to Aldridge IT team ("3 suspicious events interrupted")
- **5:50 PM**: Suspect **computer network-isolated** + full scan initiated.
- **5:55 PM:** Client main point of contact notified.
- **6:00 PM**: User account activity reviewed; **credential + MFA reset** initiated.
- **6:20 PM**: Environment assessment opened for **correlated events**.
- **6:30 PM**: **Source/activity origin investigation** opened.

INCIDENT 3: INTERCEPTED

- **Security Awareness Training and Phishing Testing**
  - User was conscientious enough to abort at "Grant admin?" prompt

- **Aldridge Managed Detection & Response (MDR)**
  - Detected the malicious executable's attempted actions, and blocked automatically.
  - Alerted SOC team via SIEM.

- **Aldridge Advanced MFA for Microsoft 365**
  - Prevented the malicious executable from reporting usable credentials for the user; over 20 invalid login attempts to Microsoft 365 during same 1 hour period.

- **24x7 Security Operations Center (SOC)**
- **Aldridge Network Operations Center**, **Rapid Response Team**, and **L3 Team**
  - Human eyes on the situation; human communication, investigation, response, recovery

HOW DO I PROTECT MY BUSINESS?

1 Have a plan, move forward in steps

2 Build resilience – start with the fundamental security tools

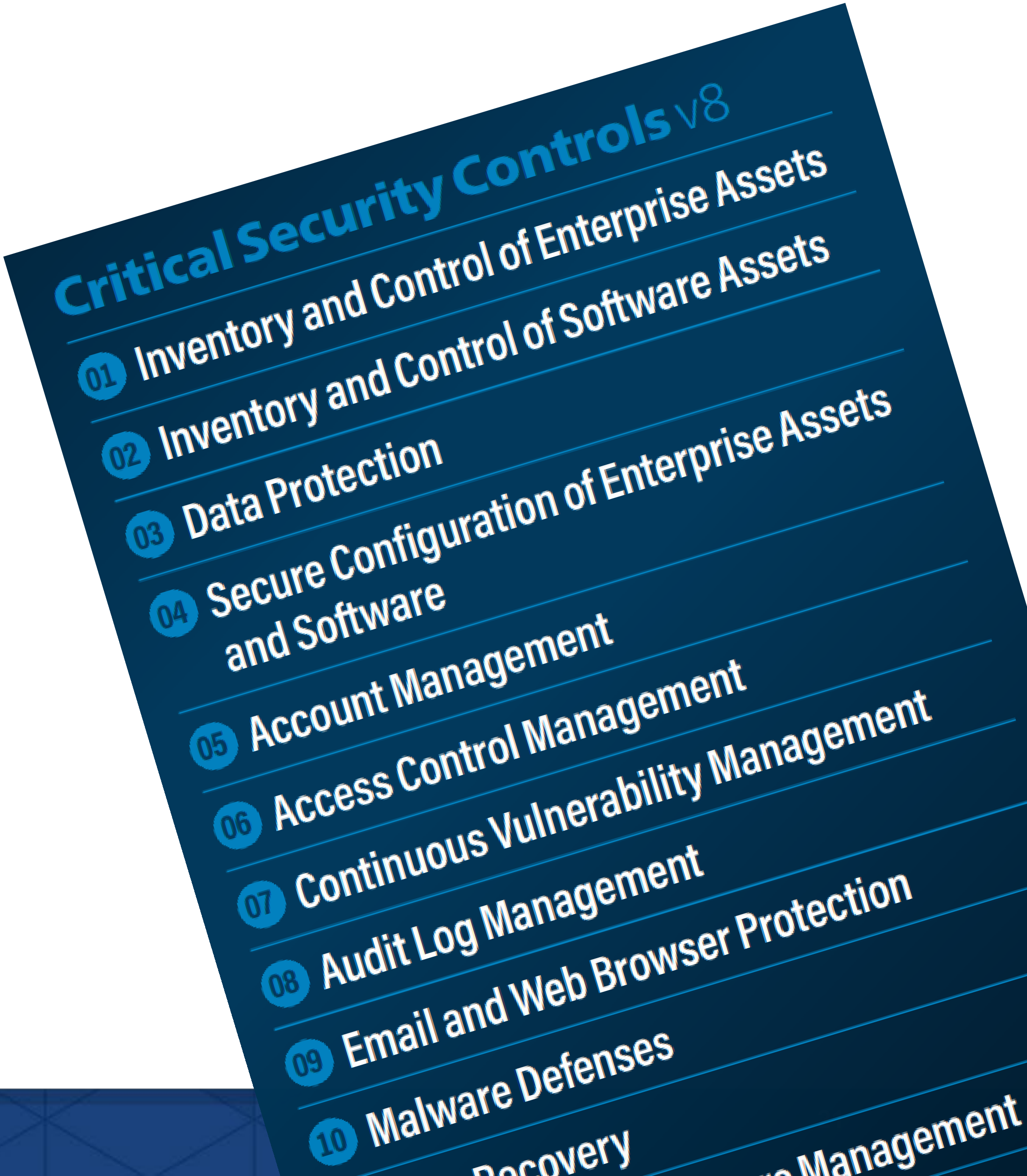
3 Inventory your IT assets (before the threat actors do)

4 Think through and put an initial Incident Response Plan in place

1 HAVE A PLAN

Center for Internet Security (CIS)
Critical Security Controls,
Implementation Group 1 (CIS IG1)

- 18 Controls encompassing 56 Safeguards
- Mix of technical and business components
- https://www.cisecurity.org/controls



Critical Security Controls v8

01 Inventory and Control of Enterprise Assets

02 Inventory and Control of Software Assets

03 Data Protection

04 Secure Configuration of Enterprise Assets and Software

05 Account Management

06 Access Control Management

07 Continuous Vulnerability Management

08 Audit Log Management

09 Email and Web Browser Protection

10 Malware Defenses

Recovery

Management

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

What does a “V1” Incident Plan look like?

- Ideally, only 1 to 2 pages.
- “Quick reference” guide of key business factors, decisions, contacts.
- Defines the severity level and how your business reacts to the threat.
- Enumerates high-level, predetermined response guidance.
- Published within your organization, known to exist, trained, ready to use.

ALDRIDGE
SECURITY INCIDENT RESPONSE PLAN
aldridge.com
Scope:
Objectives:
Roles and
SECURITY INCIDENT RESPONSE PLAN
2
3

4 IMPLEMENT YOUR "V1" INCIDENT PLAN

Sample Contents

- Your Responsibilities
- When to Activate
- Communication
- Assess Severity
- Key Contacts
- Who's In Charge
- Asset Protection, Validation
- Evidence Preservation
- Response Processes

ALDRIDGE

SECURITY
INCIDENT
RESPONSE PLAN

aldridge.com

The purpose of this doc
event of a security incid
(SIRP) is designed to
addressed in a timely
organization's system

Scope:

This plan applies t
have access to ou

Objectives:

The main objec

To detect secu
To contain se
To investigate
To recover fr
To documen
To continuo
Roles and

The follow

Incident
incidents
Incident
overse
availab
Techn
of the
Communication
with stakeholders and coo
Legal Lead: The Legal Lead is respons
complies with all legal and regulatory requirements.
Incident Reporter: Any employee, contractor, or vendor who det
is responsible for reporting it to the IRT.
Security Incident Response Process:
The following process will be followed in the event of a security incident:

2

URITY INCIDENT RESPONSE PLAN

urity incident must report it to the
ity level based on its impact and

s scope and impact.
impact of the incident.

e.
lan.

rations.
normal operations

necessary.

akeholders
dures will be

ssary.
tions are consistent

anization's systems
t regular security
sure that all

3

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

Sample Contents

- Your Responsibilities
- When to Activate
- Communication
- **Assess Severity**
- Key Contacts
- Who’s In Charge
- Asset Protection, Validation
- Evidence Preservation
- **Response Processes**

ALDRIDGE

SECURITY
INCIDENT
RESPONSE PLAN

aldridge.com

The purpose of this doc
event of a security incid
(SIRP) is designed to
addressed in a timely
organization's system

Scope:

This plan applies t
have access to ou

Objectives:

The main objec

To detect secu
To contain se
To investigate
To recover fr
To documen
To continuo

Roles and

The follow

Incident
incidents
Incident
oversee
availab
Techn
of the
Communication
with stakeholders and coo
Legal Lead: The Legal Lead is respons
complies with all legal and regulatory requirements.
Incident Reporter: Any employee, contractor, or vendor who dete
is responsible for reporting it to the IRT.
Security Incident Response Process:
The following process will be followed in the event of a security incident:

2

URITY INCIDENT RESPONSE PLAN

curity incident must report it to the
ity level based on its impact and

s scope and impact.
impact of the incident.

e.
lan.

rations.
normal operations

necessary.

akeholders
dures will be

ssary,
ations are consistent

anization's systems
t regular security
sure that all

3

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

Sample “Assessing Severity”

High Severity

- Our customer commitments are at imminent risk due to the event.
- One or more of the following High Confidentiality-sensitive assets is likely at imminent risk due to the event: xxx, yyy, zzz.
- One or more of the following High Integrity-sensitive assets is at imminent risk or is likely in an untrusted state due to the event: …
- One or more of the following High Availability-sensitive assets is at imminent risk or is unavailable due to the event: …

4 IMPLEMENT YOUR "V1" INCIDENT PLAN

Sample "High Severity" response

1. First responder is incident lead until a 1st tier contact is engaged.
2. Notify or delegate to notify 1st tier contacts via e-mail, Teams, text, and phone (voice) on first indication; provide facts, status of investigation, potential concern.
3. Assume this is an attack until evidenced it is not.
4. Investigation and rapid initial response
   - Internal communication to managers that an investigation is in progress.
   - Assess high- and medium-priority asset state and integrity.
   - Protect and isolate unaffected priority assets.
   - Preserve state and evidence.
5. If high confidence,
   - You are pre-approved to interrupt customer delivery and systems.

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

- Start with, “I’ve seen this indicator, I want to let you know we’re investigating. So far, I have these people involved.”

- Communicating and training on an Incident Response Plan can prompt people to use “**incident**” or “**breach**” prematurely.
  - Do not use the word “**incident**” until you’re sure it’s an incident.
  - Do not use the word “**breach**” until you’re sure it’s a breach.
  - Include guidance on use of these terms in your training and communication.

EXAMPLE TRAINING GUIDANCE

"Within our organization, we should all continue conscientiously talking about 'cybersecurity.'

There are many terms used in modern cybersecurity, some of which have specific implications to our customers, our vendors, and our industry. Notably, the terms, 'cybersecurity incident' or 'breach' do have specific implications to our business and denote qualified and verified risk events that may also impact the people we serve and do business with.

*Because it requires specific knowledge and consideration of the actual event details, the impacts, and our trusted relationships and obligations, **<u>only our Chief Executive Officer</u>** can determine if a 'cybersecurity incident,' or 'cybersecurity breach,' has occurred. Those mean very specific things to us and our community, so aren't terms you should ever use casually.*

With your continued help we hope to never have such an event occur, but should it ever happen, this is an important part of our business and community communication, safety, and recovery planning."

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

Having the right plans in place – ready, decided, trained, maintained – can reduce the severity (cost) of an event.

- Shift your defensive response as far left in the attack chain as feasible.
- Emphasize awareness and early detection throughout the organization.
- Communicate, communicate, communicate.

4 IMPLEMENT YOUR “V1” INCIDENT PLAN

It is NOT an IT - only problem

It is NOT a stable step-by-step process