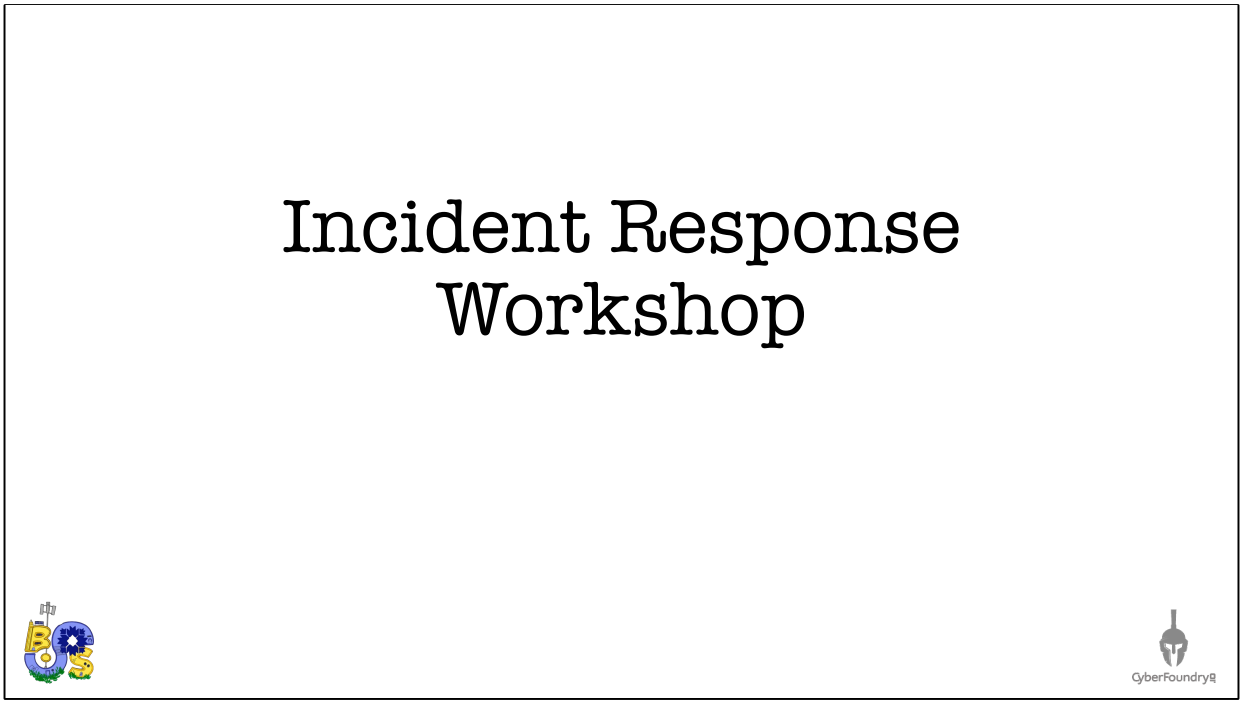
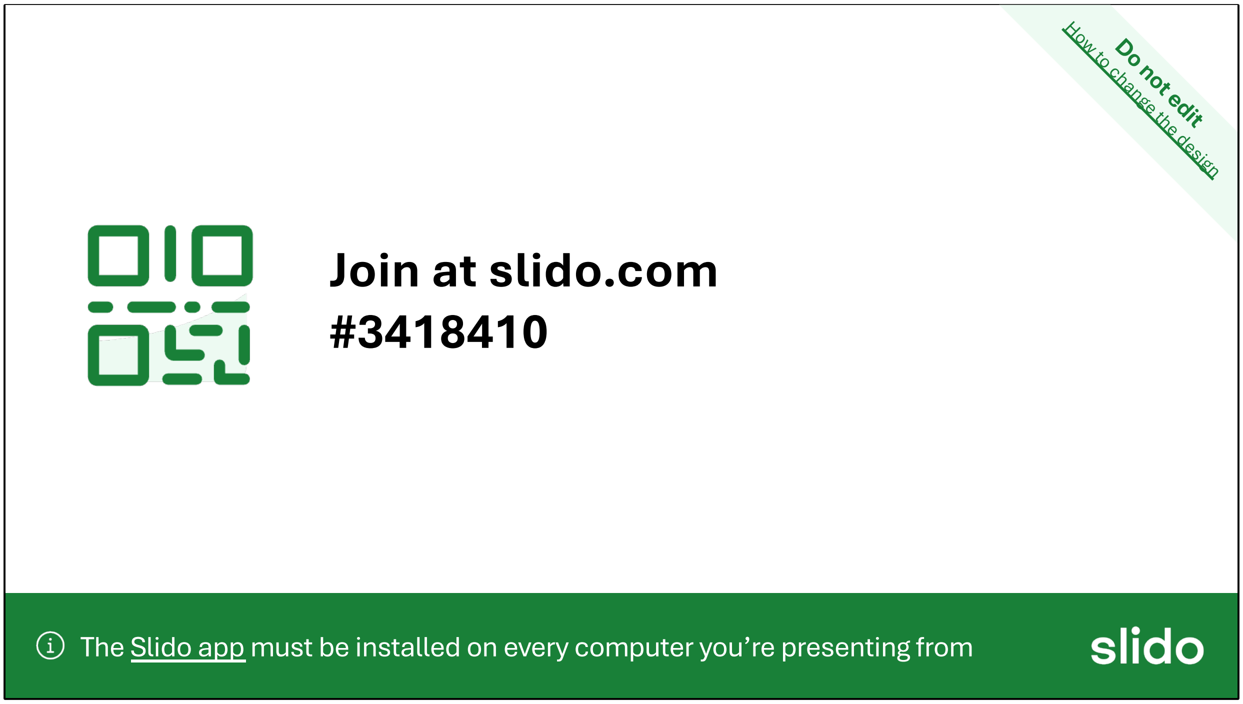


Incident Response Workshop

CyberFoundry



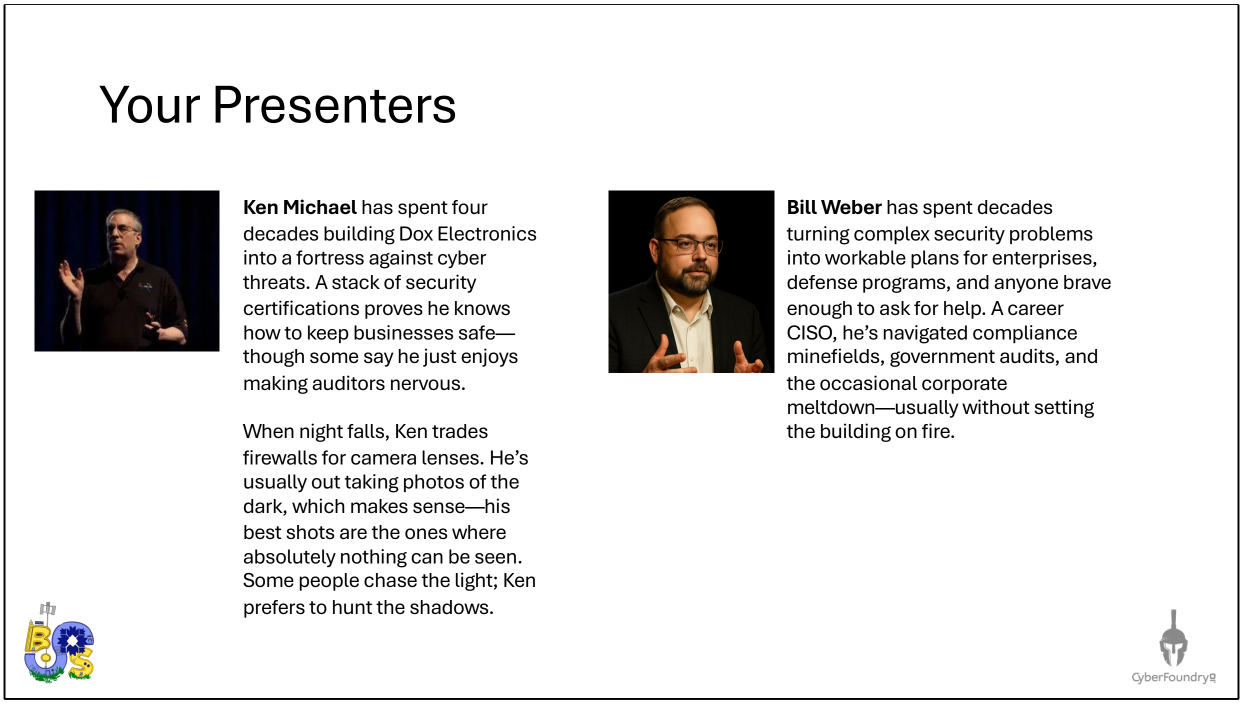
Do not edit

How to change the design

Join at slido.com
#3418410

ⓘ The Slido app must be installed on every computer you're presenting from

slido



Your Presenters

Ken Michael has spent four decades building Dox Electronics into a fortress against cyber threats. A stack of security certifications proves he knows how to keep businesses safe—though some say he just enjoys making auditors nervous.

When night falls, Ken trades firewalls for camera lenses. He's usually out taking photos of the dark, which makes sense—his best shots are the ones where absolutely nothing can be seen. Some people chase the light; Ken prefers to hunt the shadows.

Bill Weber has spent decades turning complex security problems into workable plans for enterprises, defense programs, and anyone brave enough to ask for help. A career CISO, he's navigated compliance minefields, government audits, and the occasional corporate meltdown—usually without setting the building on fire.

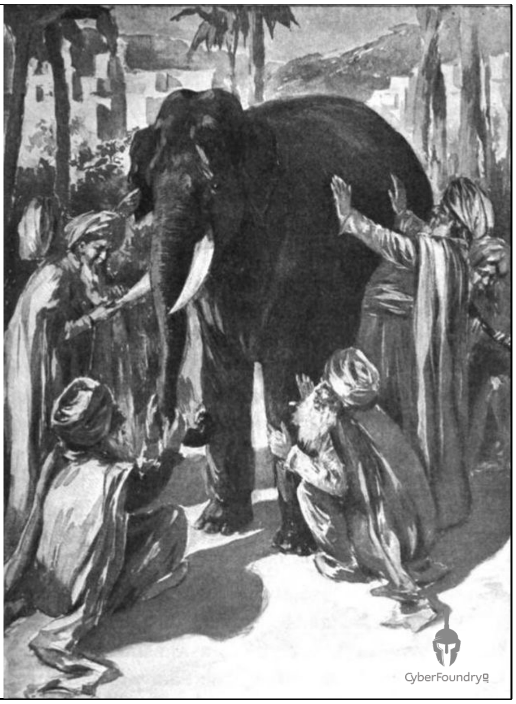
agenda

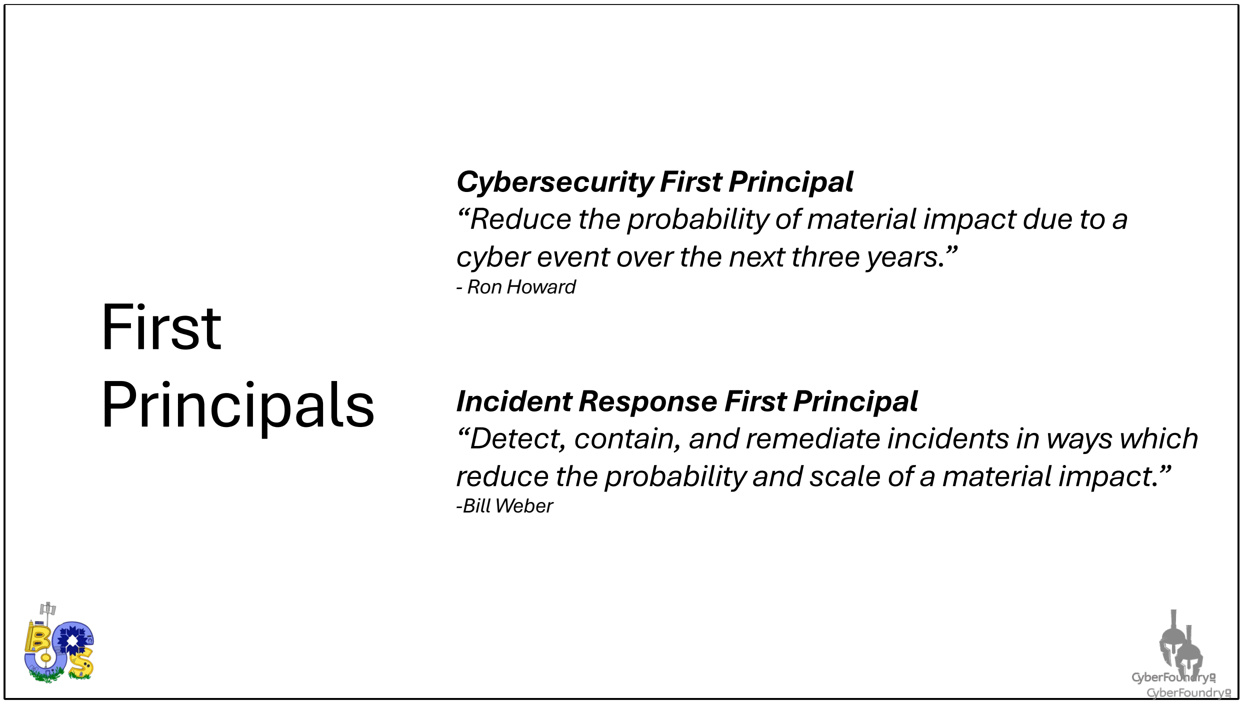
Part 1
Understanding the Incident Response Plan

Part 2
Tabletop Exercise

Part 1

Understanding the Incident Response Plan





First Principals

Cybersecurity First Principal

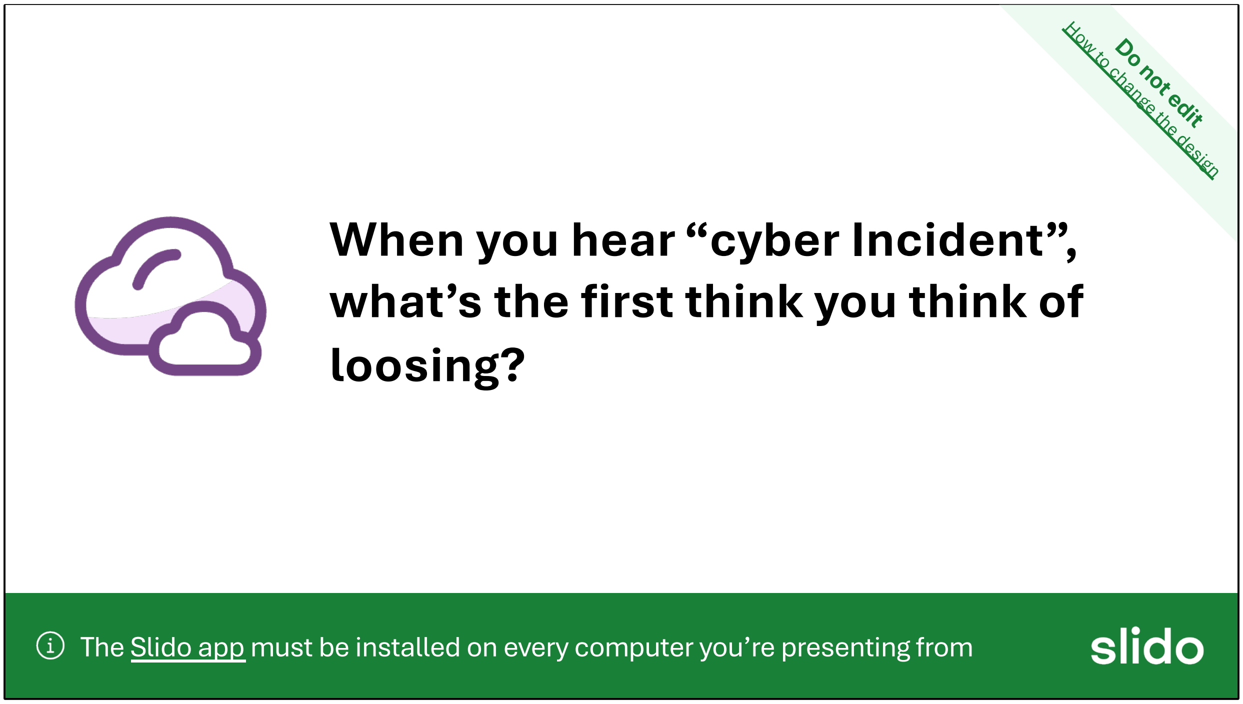
“Reduce the probability of material impact due to a cyber event over the next three years.”

- Ron Howard

Incident Response First Principal

“Detect, contain, and remediate incidents in ways which reduce the probability and scale of a material impact.”

-Bill Weber



Do not edit

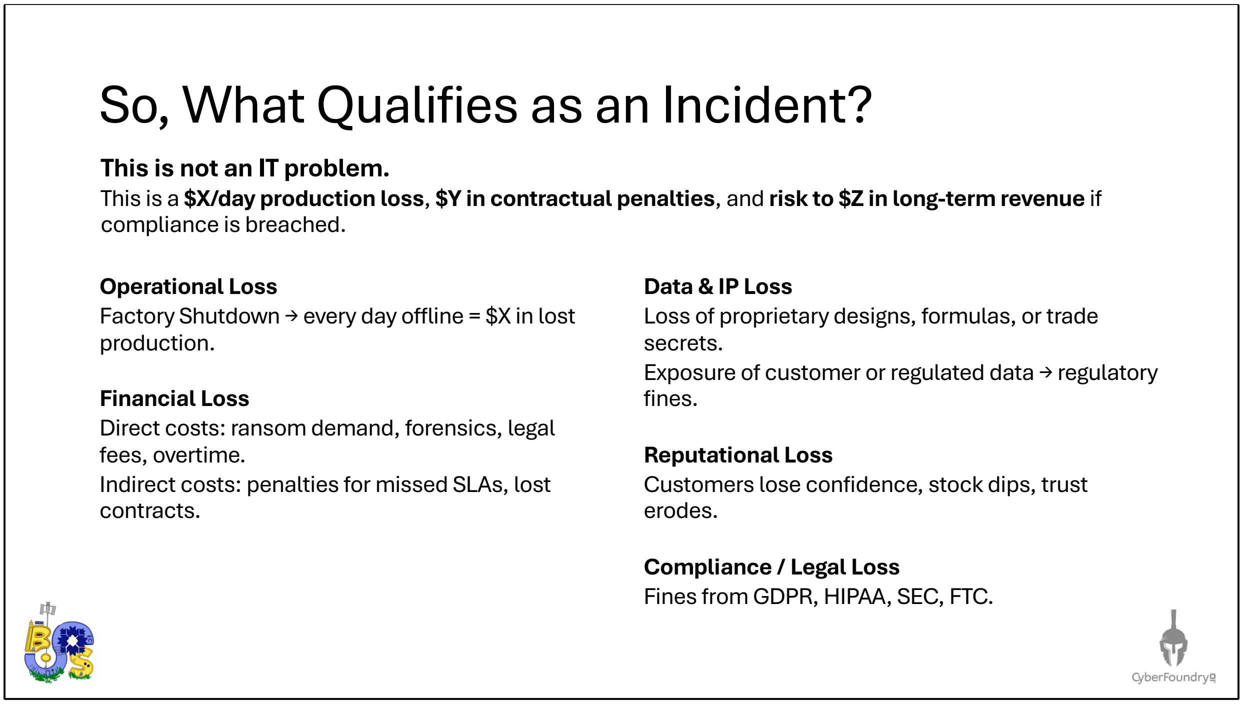
How to change the design

When you hear “cyber Incident”, what’s the first think you think of loosing?

The Slido app must be installed on every computer you’re presenting from

slido

What does an incident look like?



So, What Qualifies as an Incident?

This is not an IT problem.

This is a **$X/day production loss**, **$Y in contractual penalties**, and **risk to $Z in long-term revenue** if compliance is breached.

Operational Loss

Factory Shutdown → every day offline = $X in lost production.

Financial Loss

Direct costs: ransom demand, forensics, legal fees, overtime.

Indirect costs: penalties for missed SLAs, lost contracts.

Data & IP Loss

Loss of proprietary designs, formulas, or trade secrets.

Exposure of customer or regulated data → regulatory fines.

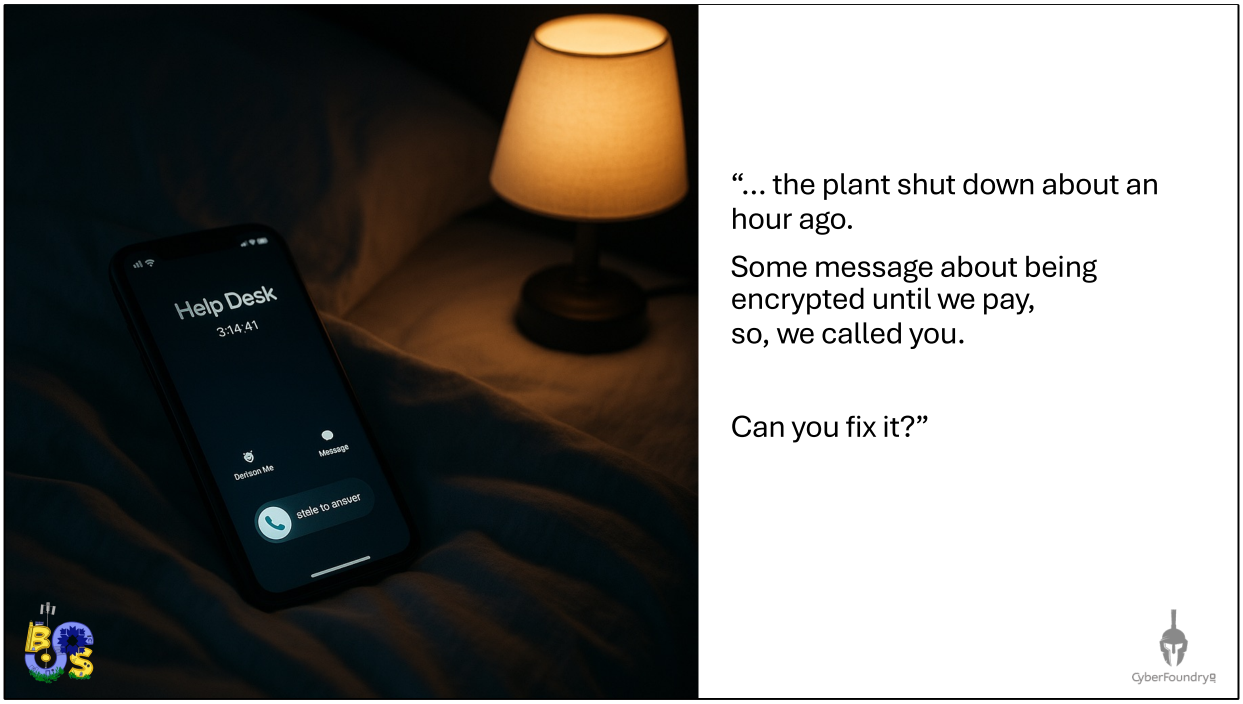
Reputational Loss

Customers lose confidence, stock dips, trust erodes.

Compliance / Legal Loss

Fines from GDPR, HIPAA, SEC, FTC.

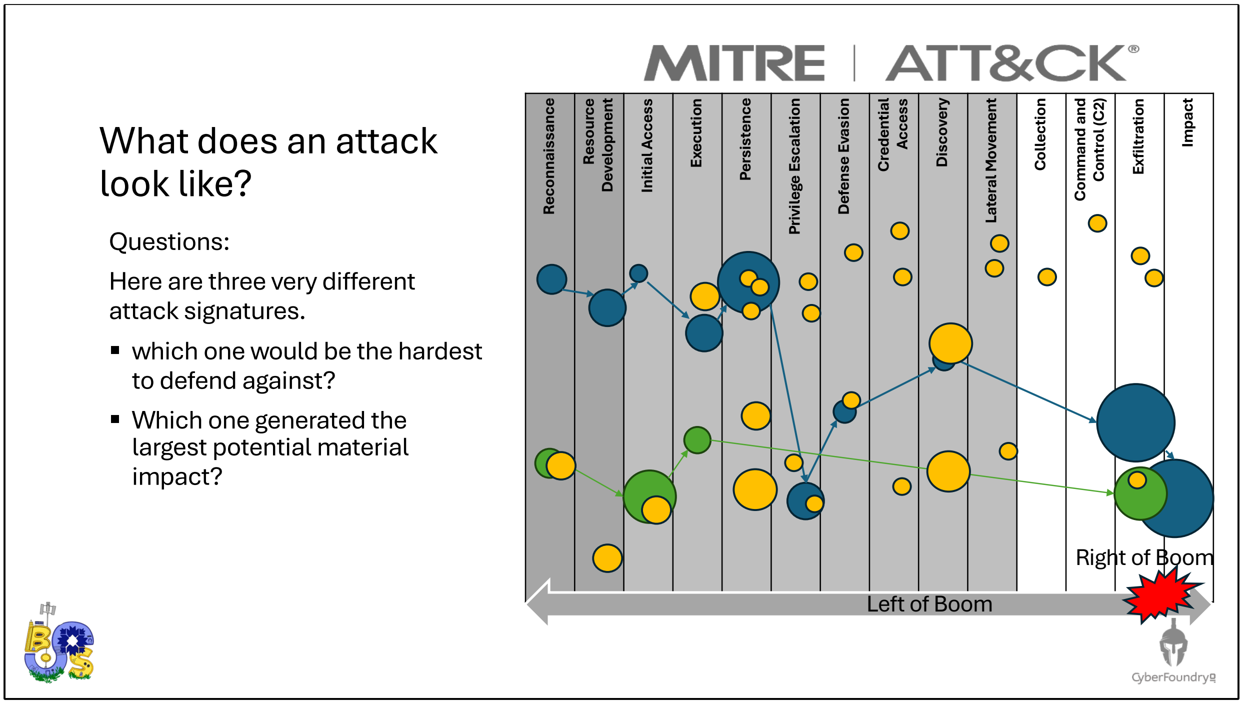
CyberFoundry



"… the plant shut down about an hour ago.

Some message about being encrypted until we pay,
so, we called you.

Can you fix it?"



What does an attack look like?

Questions:

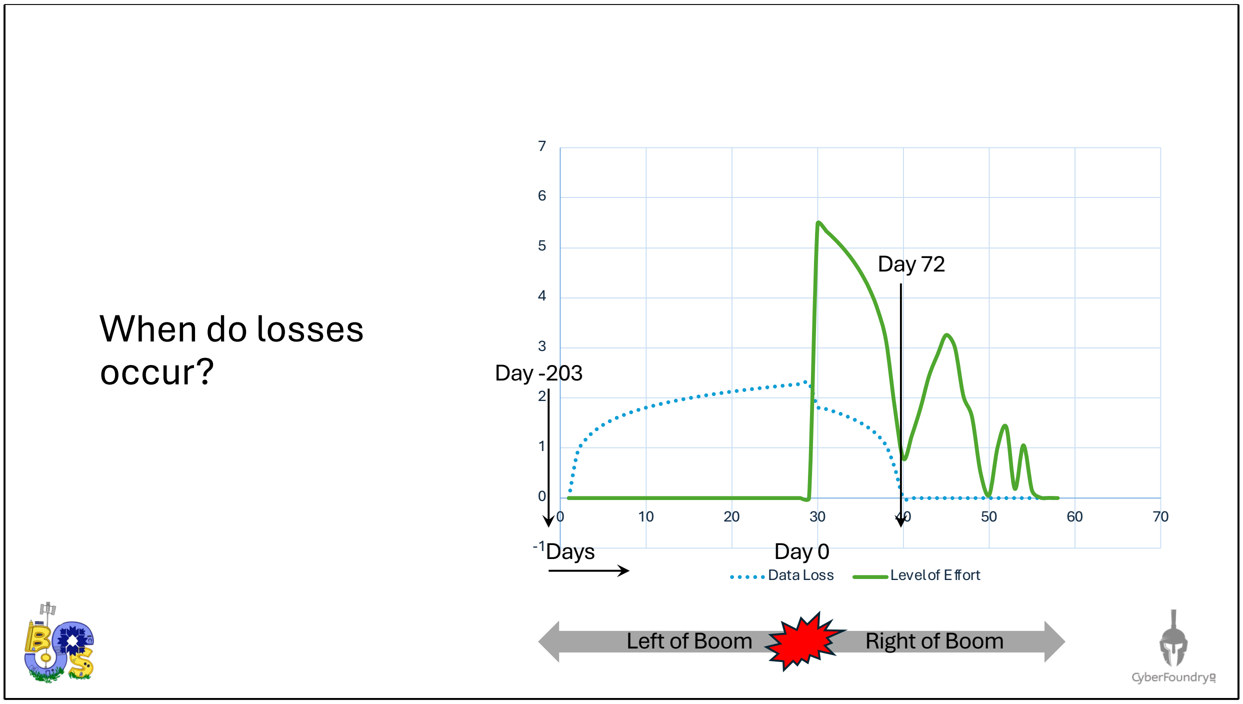
Here are three very different attack signatures.

- which one would be the hardest to defend against?
- Which one generated the largest potential material impact?

https://www.cyberfoundry.io/wp-content/uploads/2024/05/MITRE-ATTACK-Frequency-Analysis.xlsx

https://attack.mitre.org

When do losses occur?



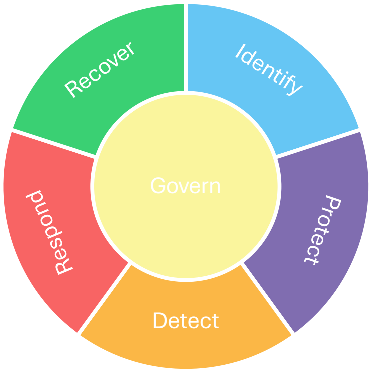
Hypothetical example based on Ponemon Study

What is an incident response plan?

The Standards

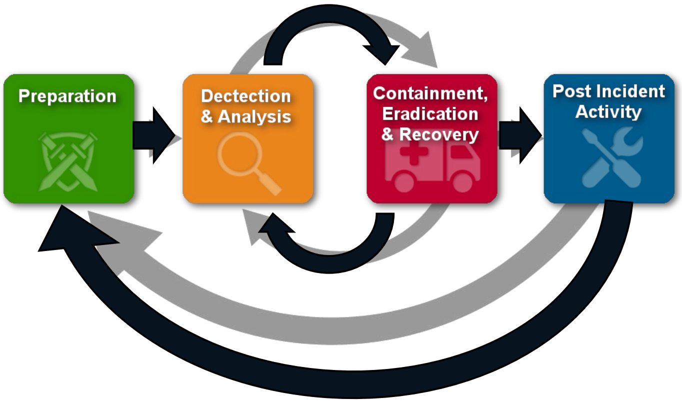
Cybersecurity Framework 2.0

For Industry,
Government, and
Organizations to Reduce.
Cybersecurity Risks

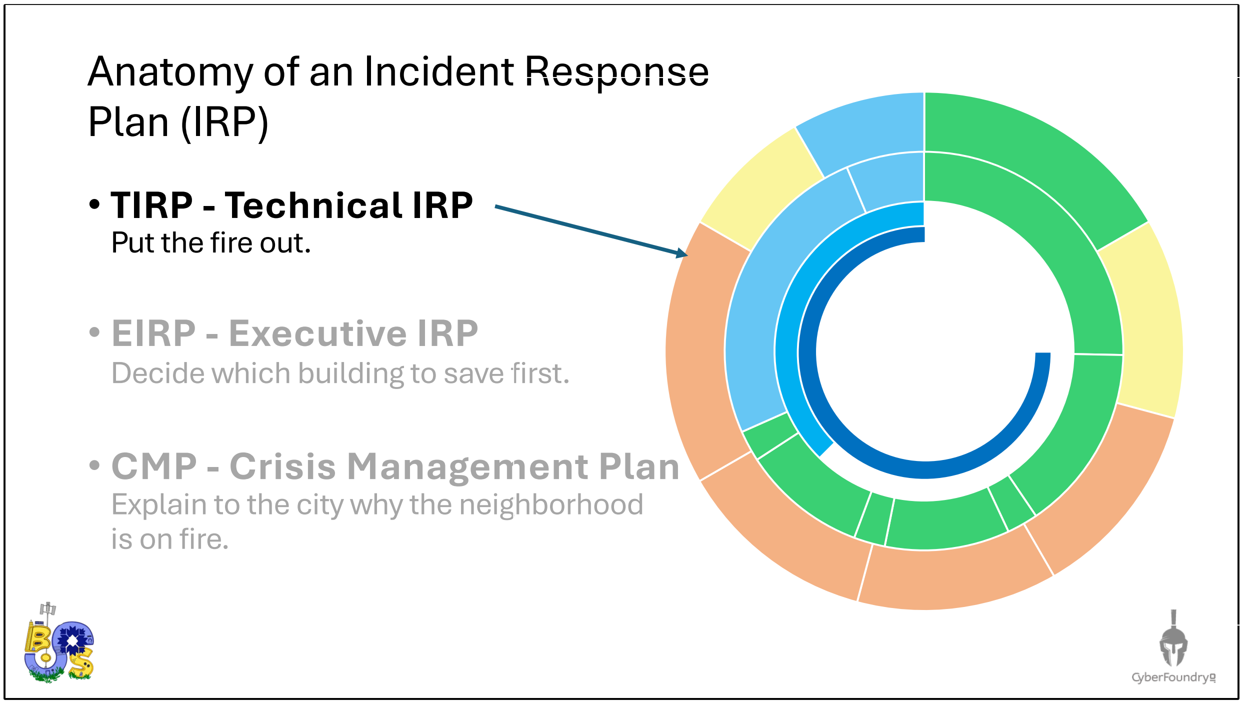


Computer Security Incident Handling Guide
NIST SP800-61r2

Industry Standard
Cyber Incident
Response Cycle



Cyber Foundry Incident Response Plan



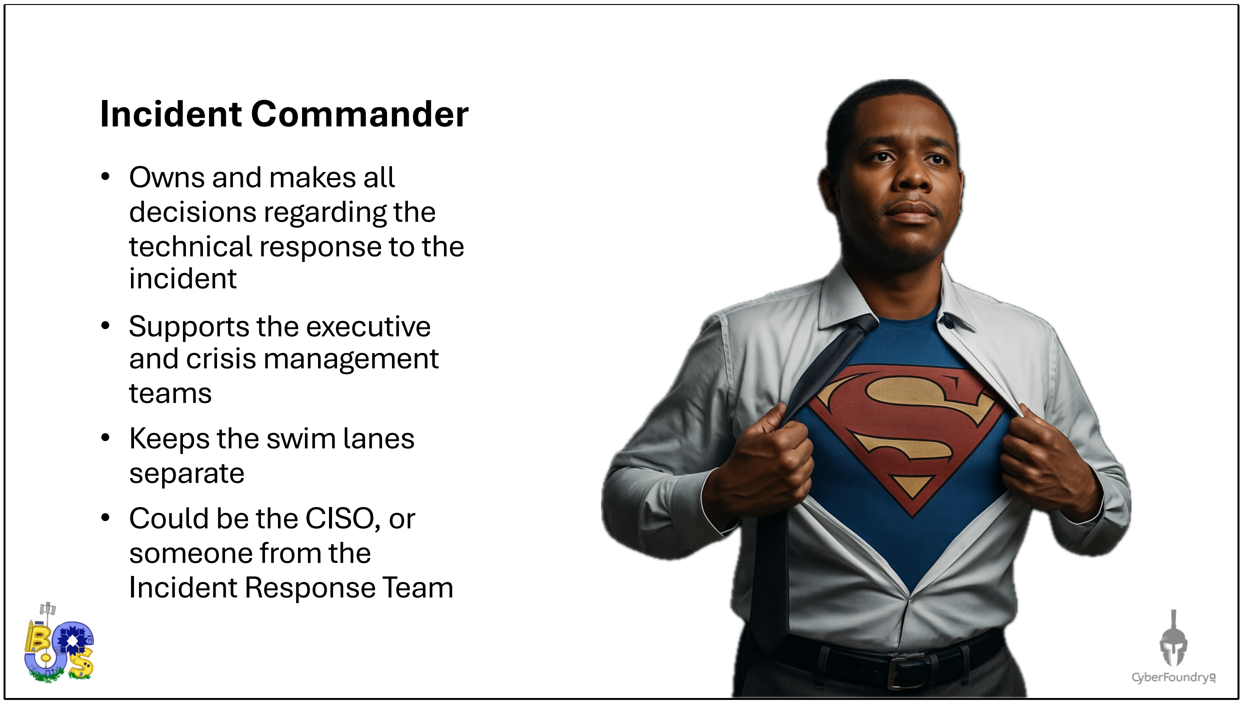
Anatomy of an Incident Response Plan (IRP)

- **TIRP - Technical IRP**
  Put the fire out.

- **EIRP - Executive IRP**
  Decide which building to save first.

- **CMP - Crisis Management Plan**
  Explain to the city why the neighborhood is on fire.

The Characters



Incident Commander

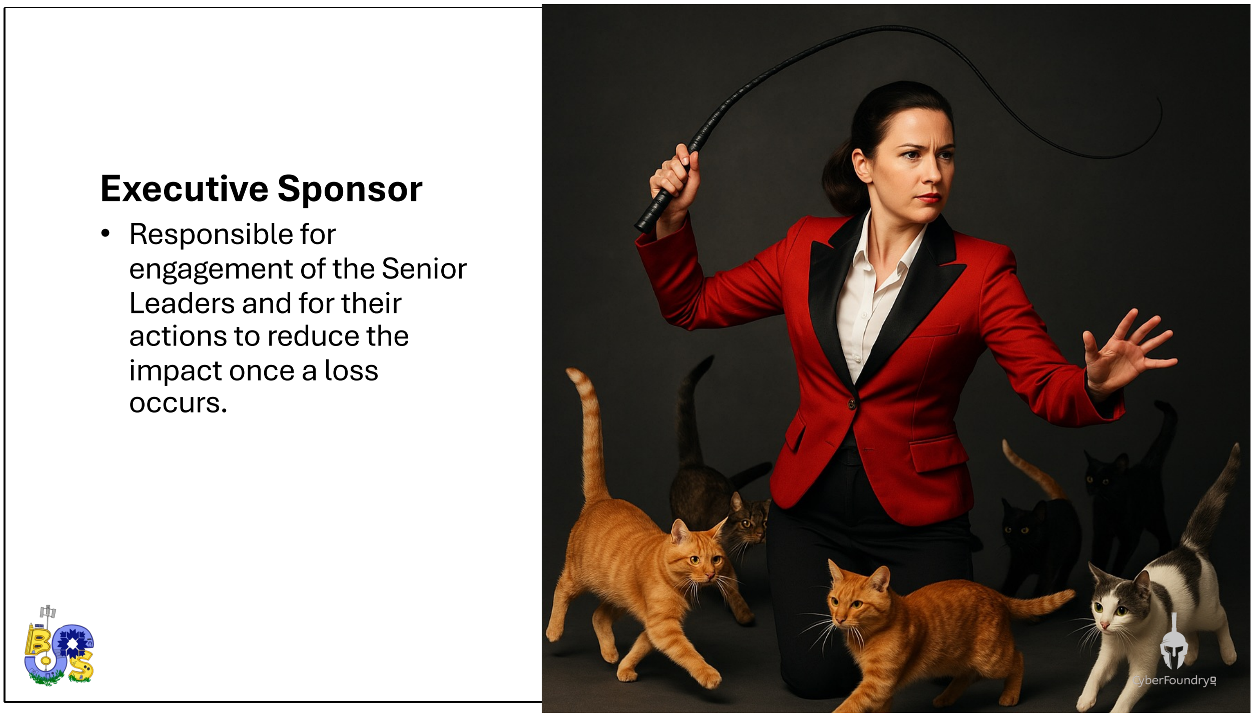
- Owns and makes all decisions regarding the technical response to the incident
- Supports the executive and crisis management teams
- Keeps the swim lanes separate
- Could be the CISO, or someone from the Incident Response Team

Incident Response Team (IRT) / SOC

- Leads the implementation of the technical incident response plan steps under leadership of the incident commander.
- Collaborates with the other teams to execute and validate changes in the environment.

IT / Business Support

- Leads changes to the IT environment necessary to contain, eradicate and recover from an incident.
- Closest to the business impact and the users.

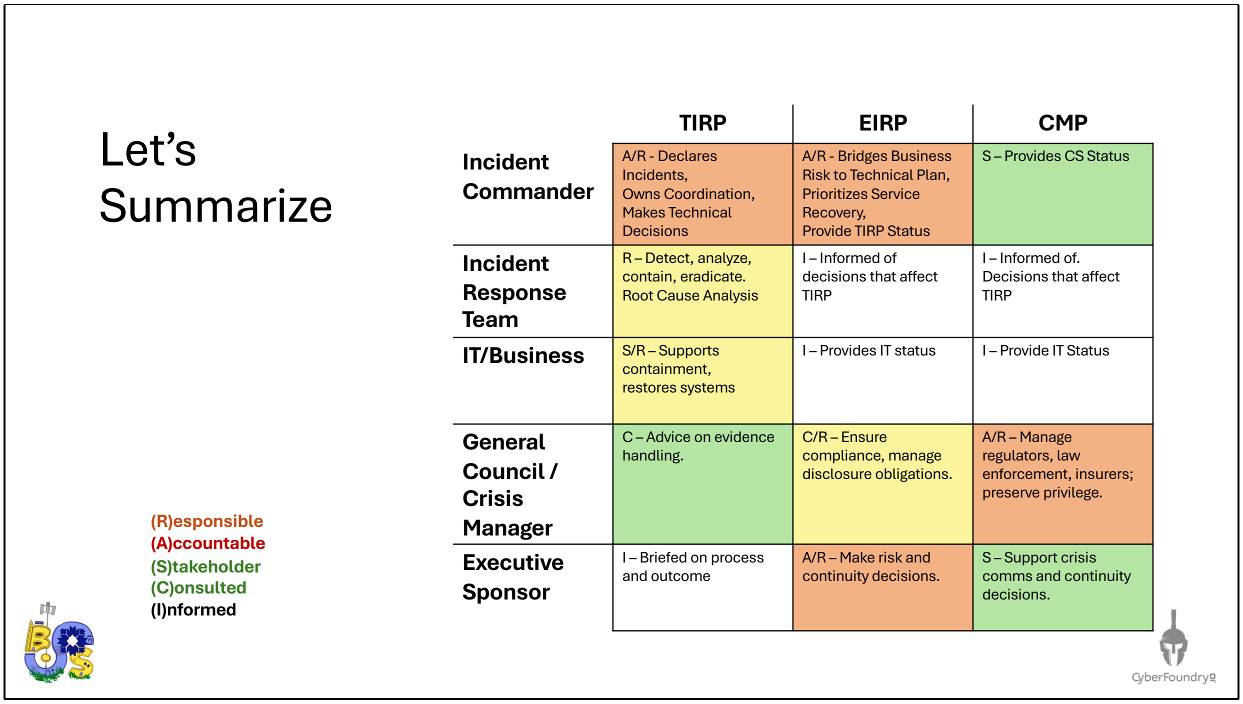


Executive Sponsor

- Responsible for engagement of the Senior Leaders and for their actions to reduce the impact once a loss occurs.

General Council Crisis Manager

- Responsible for maintaining attorney client privilege over all evidence.
- Responsible for communicating with regulators, law enforcement, insurers, investors and the media.
- Enforce separation of duties.



Let’s Summarize

	TIRP	EIRP	CMP
Incident Commander	A/R - Declares Incidents, Owns Coordination, Makes Technical Decisions	A/R - Bridges Business Risk to Technical Plan, Prioritizes Service Recovery, Provide TIRP Status	S – Provides CS Status
Incident Response Team	R – Detect, analyze, contain, eradicate. Root Cause Analysis	I – Informed of decisions that affect TIRP	I – Informed of. Decisions that affect TIRP
IT/Business	S/R – Supports containment, restores systems	I – Provides IT status	I – Provide IT Status
General Council / Crisis Manager	C – Advice on evidence handling.	C/R – Ensure compliance, manage disclosure obligations.	A/R – Manage regulators, law enforcement, insurers; preserve privilege.
Executive Sponsor	I – Briefed on process and outcome	A/R – Make risk and continuity decisions.	S – Support crisis comms and continuity decisions.

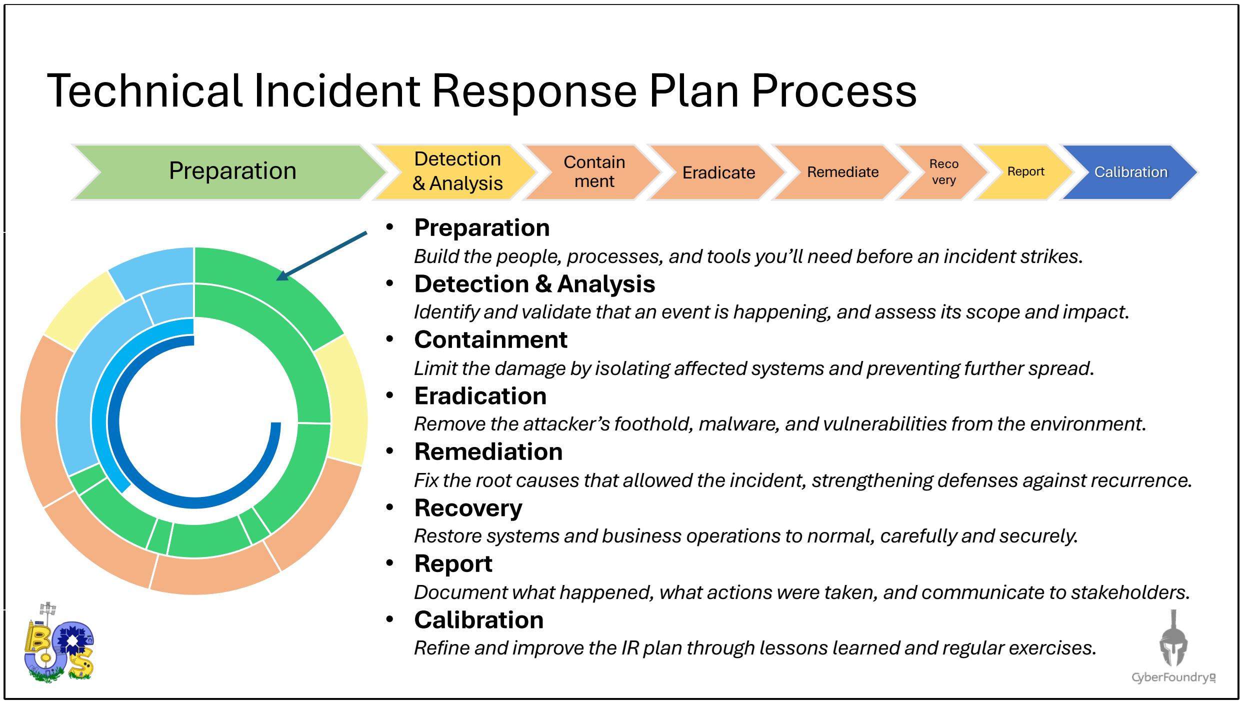
(R)esponsible
(A)ccountable
(S)takeholder
(C)onsulted
(I)nformed

CyberFoundry

Technical Incident Response Plan

Objectives

- Rapid Detection & Assessment
- Effective Containment & Mitigation
- Eradication & Recovery
- Learning & Improvement
- Impact Reduction



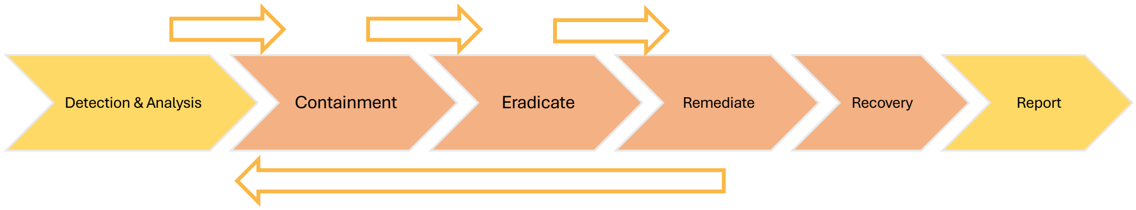
Technical Incident Response Plan Process

Preparation | Detection & Analysis | Contain ment | Eradicate | Remediate | Reco very | Report | Calibration

- **Preparation**
  Build the people, processes, and tools you'll need before an incident strikes.
- **Detection & Analysis**
  Identify and validate that an event is happening, and assess its scope and impact.
- **Containment**
  Limit the damage by isolating affected systems and preventing further spread.
- **Eradication**
  Remove the attacker's foothold, malware, and vulnerabilities from the environment.
- **Remediation**
  Fix the root causes that allowed the incident, strengthening defenses against recurrence.
- **Recovery**
  Restore systems and business operations to normal, carefully and securely.
- **Report**
  Document what happened, what actions were taken, and communicate to stakeholders.
- **Calibration**
  Refine and improve the IR plan through lessons learned and regular exercises.

CyberFoundry

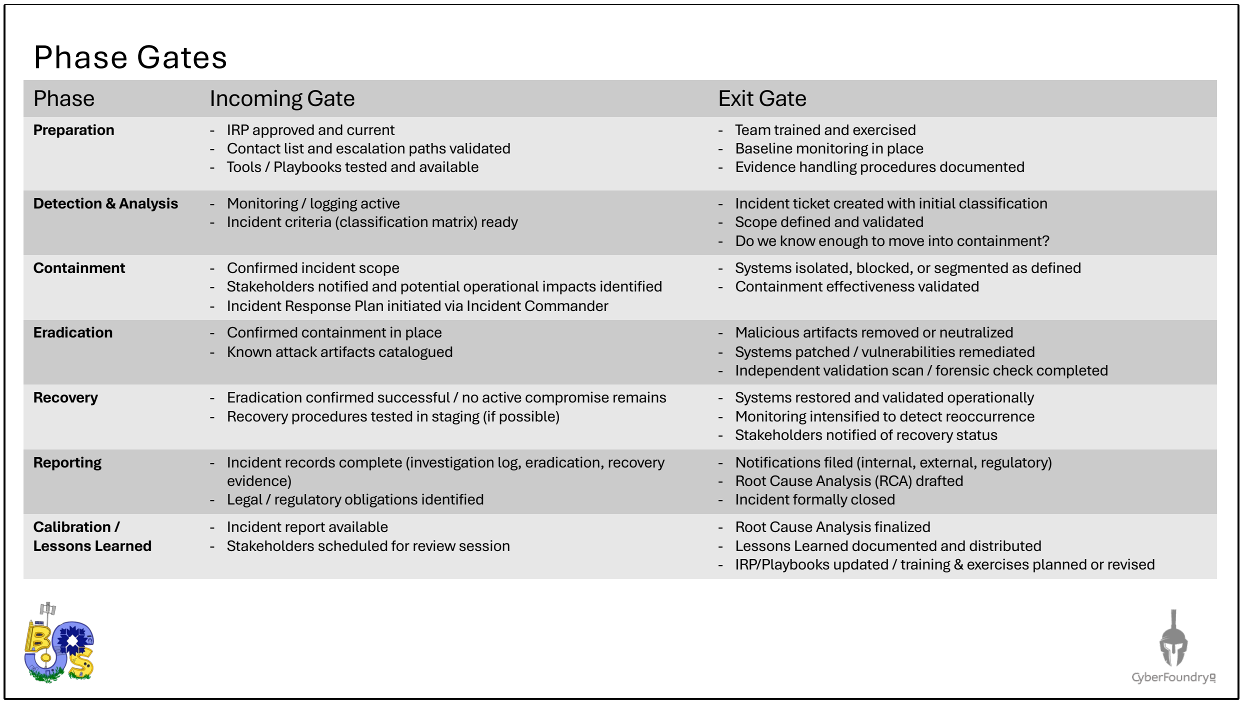
Gates & Continuous Validation



Every Phase has an Entry set of Actions and an Exit set of Criteria.
If these Gates are found to not have been completed, then action must go back to the previous phase.

Examples:

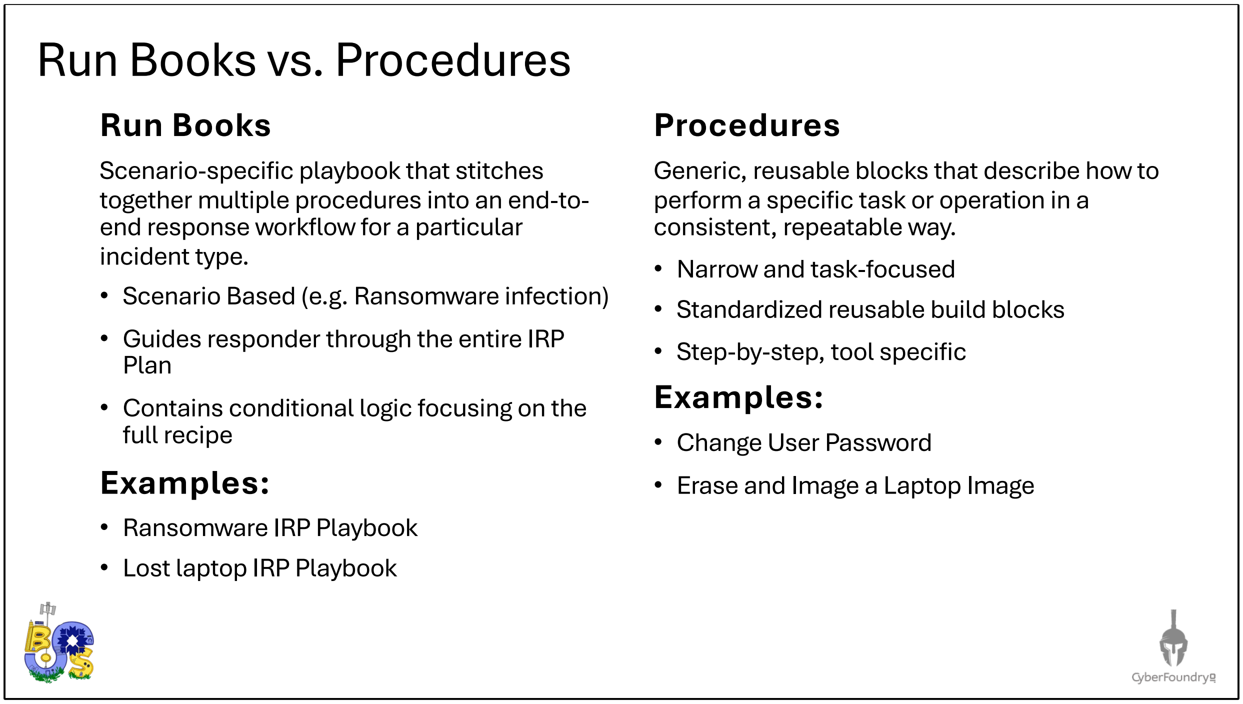
- The Detection & Analysis phase indicated an incomplete scope which was later detected during Eradication.
- The Eradication phase missed an impacted system which was later detected during Recovery.
- An Indicator of Compromise (IOC) was identified in the Containment phase but not acted on.
  This was detected when writing up the final report.



Phase Gates

Phase	Incoming Gate	Exit Gate
Preparation	- IRP approved and current - Contact list and escalation paths validated - Tools / Playbooks tested and available	- Team trained and exercised - Baseline monitoring in place - Evidence handling procedures documented
Detection & Analysis	- Monitoring / logging active - Incident criteria (classification matrix) ready	- Incident ticket created with initial classification - Scope defined and validated - Do we know enough to move into containment?
Containment	- Confirmed incident scope - Stakeholders notified and potential operational impacts identified - Incident Response Plan initiated via Incident Commander	- Systems isolated, blocked, or segmented as defined - Containment effectiveness validated
Eradication	- Confirmed containment in place - Known attack artifacts catalogued	- Malicious artifacts removed or neutralized - Systems patched / vulnerabilities remediated - Independent validation scan / forensic check completed
Recovery	- Eradication confirmed successful / no active compromise remains - Recovery procedures tested in staging (if possible)	- Systems restored and validated operationally - Monitoring intensified to detect reoccurrence - Stakeholders notified of recovery status
Reporting	- Incident records complete (investigation log, eradication, recovery evidence) - Legal / regulatory obligations identified	- Notifications filed (internal, external, regulatory) - Root Cause Analysis (RCA) drafted - Incident formally closed
Calibration / Lessons Learned	- Incident report available - Stakeholders scheduled for review session	- Root Cause Analysis finalized - Lessons Learned documented and distributed - IRP/Playbooks updated / training & exercises planned or revised

CyberFoundry



Run Books vs. Procedures

Run Books

Scenario-specific playbook that stitches together multiple procedures into an end-to-end response workflow for a particular incident type.

- Scenario Based (e.g. Ransomware infection)
- Guides responder through the entire IRP Plan
- Contains conditional logic focusing on the full recipe

Examples:

- Ransomware IRP Playbook
- Lost laptop IRP Playbook

Procedures

Generic, reusable blocks that describe how to perform a specific task or operation in a consistent, repeatable way.

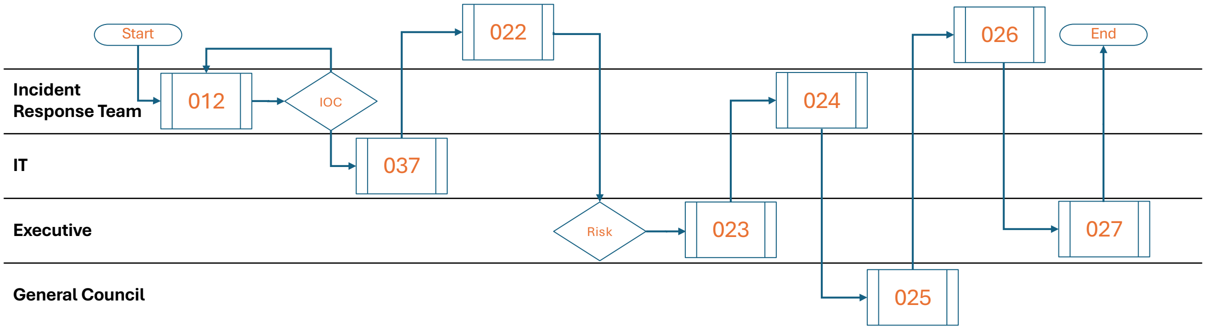
- Narrow and task-focused
- Standardized reusable build blocks
- Step-by-step, tool specific

Examples:

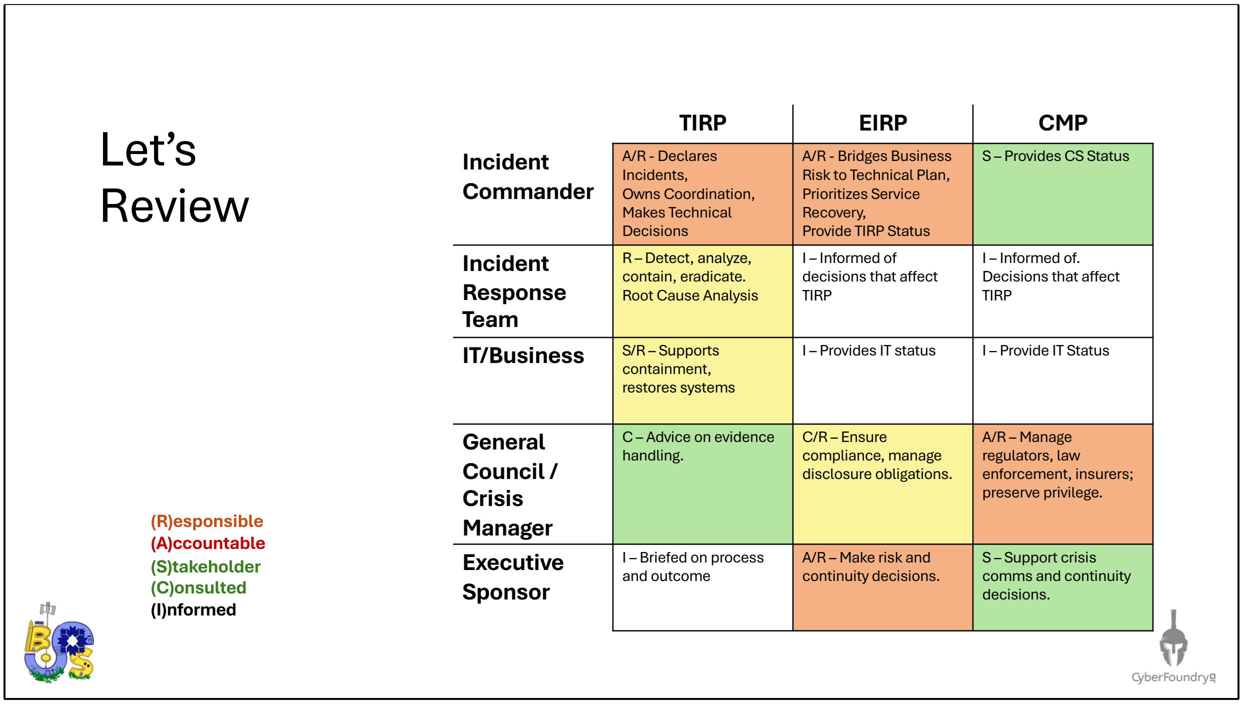
- Change User Password
- Erase and Image a Laptop Image

CyberFoundry

Run Books vs. Procedures Example



CyberFoundry

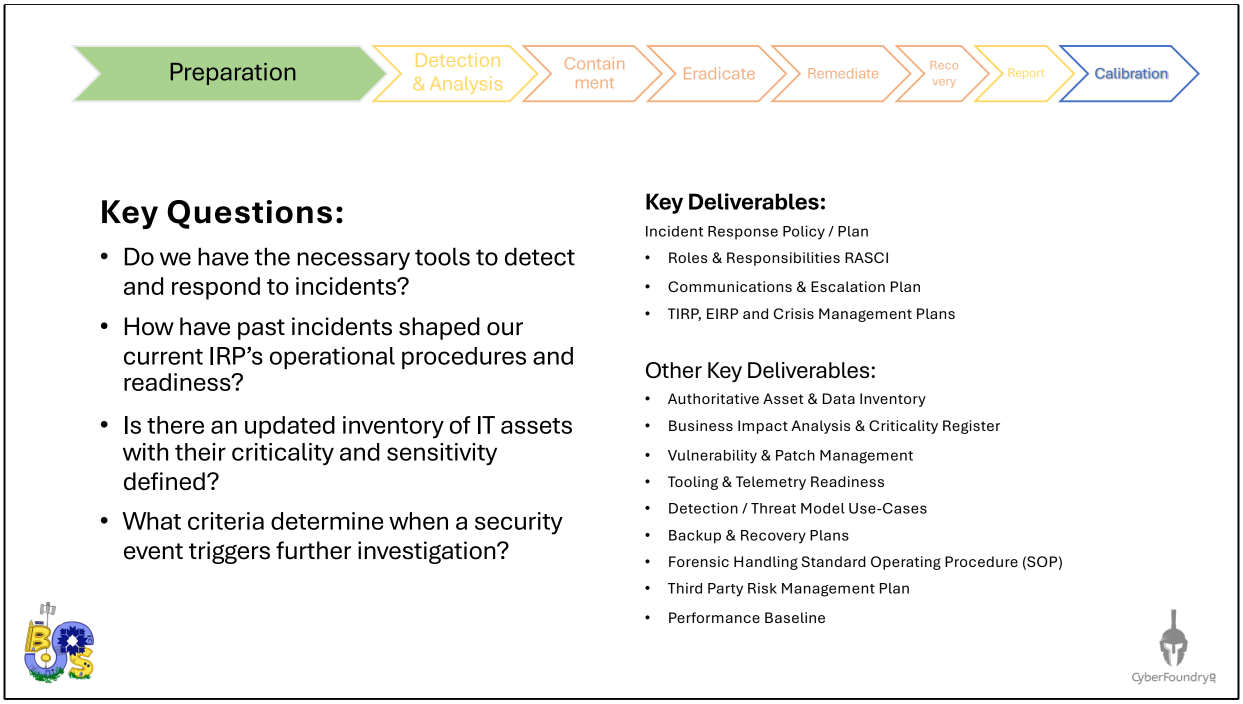


Let's Review

	TIRP	EIRP	CMP
Incident Commander	A/R - Declares Incidents, Owns Coordination, Makes Technical Decisions	A/R - Bridges Business Risk to Technical Plan, Prioritizes Service Recovery, Provide TIRP Status	S – Provides CS Status
Incident Response Team	R – Detect, analyze, contain, eradicate. Root Cause Analysis	I – Informed of decisions that affect TIRP	I – Informed of. Decisions that affect TIRP
IT/Business	S/R – Supports containment, restores systems	I – Provides IT status	I – Provide IT Status
General Council / Crisis Manager	C – Advice on evidence handling.	C/R – Ensure compliance, manage disclosure obligations.	A/R – Manage regulators, law enforcement, insurers; preserve privilege.
Executive Sponsor	I – Briefed on process and outcome	A/R – Make risk and continuity decisions.	S – Support crisis comms and continuity decisions.

(R)esponsible
(A)ccountable
(S)takeholder
(C)onsulted
(I)nformed

CyberFoundry



Preparation | Detection & Analysis | Containment | Eradicate | Remediate | Recovery | Report | Calibration

Key Questions:

- Do we have the necessary tools to detect and respond to incidents?
- How have past incidents shaped our current IRP's operational procedures and readiness?
- Is there an updated inventory of IT assets with their criticality and sensitivity defined?
- What criteria determine when a security event triggers further investigation?

Key Deliverables:

Incident Response Policy / Plan

- Roles & Responsibilities RASCI
- Communications & Escalation Plan
- TIRP, EIRP and Crisis Management Plans

Other Key Deliverables:

- Authoritative Asset & Data Inventory
- Business Impact Analysis & Criticality Register
- Vulnerability & Patch Management
- Tooling & Telemetry Readiness
- Detection / Threat Model Use-Cases
- Backup & Recovery Plans
- Forensic Handling Standard Operating Procedure (SOP)
- Third Party Risk Management Plan
- Performance Baseline

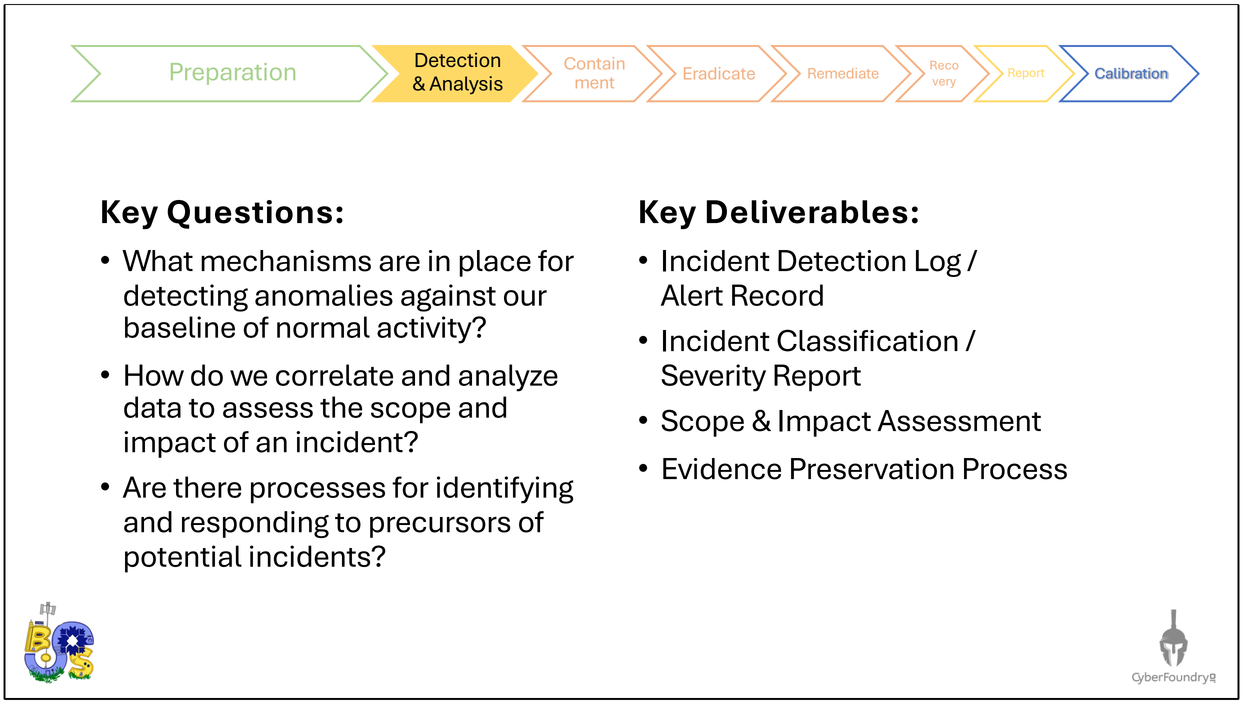
CyberFoundry

Preparation

Technical responders should ensure the organization has both the tools and processes necessary to detect and respond to incidents effectively. Preparation requires making deliberate investments not only in detection and response capabilities, but also in the supporting infrastructure and procedures that will be used throughout the incident response lifecycle. A complete IRP should document these capabilities and translate them into operational procedures that can be executed under pressure. Your role in the EIRP preparation phase is to register risks appropriate to your environment, prioritize investments that close identified gaps, and ensure the IRP can be executed efficiently. Insights from past incidents and lessons learned from tabletop exercises provide critical feedback in assessing readiness and strengthening future preparation.

- Compiling an inventory of IT assets, their importance, and sensitivity. (asset management - inventory)
- Establishing a baseline of normal activity for monitoring purposes. (behavioral analysis)
- Determining which security events warrant further investigation. (risk management - sensitivity analysis)

- Creating detailed response steps for common types of incidents. (policy & procedure - playbooks)



Preparation | Detection & Analysis | Containment | Eradicate | Remediate | Recovery | Report | Calibration

Key Questions:

- What mechanisms are in place for detecting anomalies against our baseline of normal activity?
- How do we correlate and analyze data to assess the scope and impact of an incident?
- Are there processes for identifying and responding to precursors of potential incidents?

Key Deliverables:

- Incident Detection Log / Alert Record
- Incident Classification / Severity Report
- Scope & Impact Assessment
- Evidence Preservation Process

Detection & Analysis

During the detection and analysis phase, technical responders must ensure that the organization has the visibility and processes required to distinguish normal activity from anomalous behavior. This phase depends on both the quality of monitoring investments and the discipline of correlating and triaging alerts to assess their scope, impact, and severity. A mature IRP provides the playbooks and criteria necessary to validate potential incidents, escalate them appropriately, and preserve the evidence required for further response. Your role is to ensure that the TIRP defines how anomalies are detected, how data is analyzed and enriched, and how escalation thresholds are applied consistently. The accuracy and timeliness of detection are often shaped by lessons learned in prior incidents and table-top exercises, which provide critical insight into both detection gaps and opportunities for improved analysis.

Detection Coverage & Sources

What event sources feed into our monitoring (EDR, SIEM, IDS, vulnerability scans, logs), and how do we validate their completeness?
Do we have visibility across endpoints, networks, cloud, SaaS, and third-party integrations?

Triage & Prioritization

How do we validate whether a detected anomaly is a false positive or true incident?

What criteria (e.g., criticality of systems, data sensitivity, threat intelligence context) drive incident severity classification?

How quickly must triage be completed, and who is authorized to make that call?

Correlation & Enrichment

How do we integrate external threat intelligence (IOCs, TTPs) into analysis?

Do we enrich events with context (asset ownership, business criticality, ATT&CK mappings) before escalation?

How do we ensure correlations don't over- or under-scope the incident?

Notification & Escalation

What is the defined threshold for escalating a "security event" into a declared "incident"?

Who must be notified once an incident is confirmed (internal RASCI chain, regulators, insurance, law enforcement)?

Tooling & Automation

Are our detection systems tuned (rules, models, signatures) to reduce alert fatigue?

What automated playbooks (n8n, SOAR, MCP workflows) are in place to assist triage?

Evidence Handling

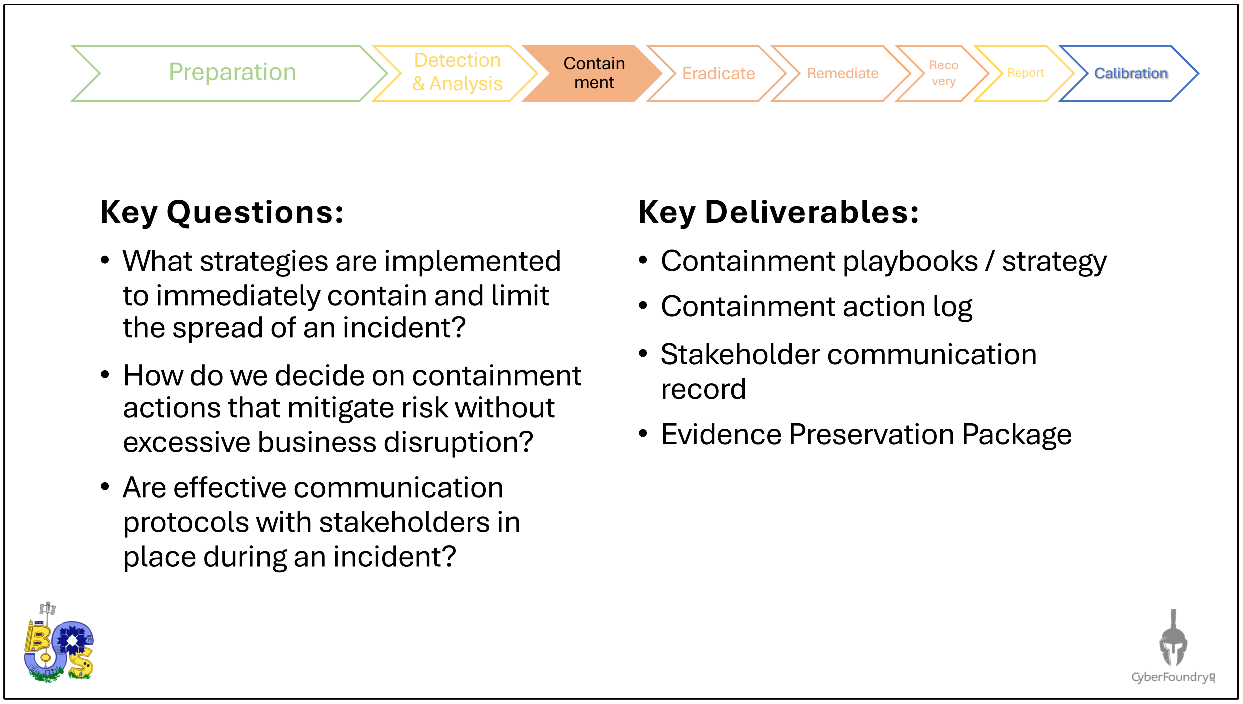
How is forensic evidence (logs, memory, disk images) collected, preserved, and protected for later analysis or legal action?

How do we avoid contaminating evidence while still responding quickly?

Continuous Improvement

How do we measure mean time to detect (MTTD) and mean time to analyze (MTTA)?

Are lessons from prior incidents feeding back into tuning detection and analysis processes?



Preparation
Detection & Analysis
Contain ment
Eradicate
Remediate
Reco very
Report
Calibration

Key Questions:

- What strategies are implemented to immediately contain and limit the spread of an incident?
- How do we decide on containment actions that mitigate risk without excessive business disruption?
- Are effective communication protocols with stakeholders in place during an incident?

Key Deliverables:

- Containment playbooks / strategy
- Containment action log
- Stakeholder communication record
- Evidence Preservation Package

Containment

During the containment phase, technical responders must act decisively to prevent further damage while preserving the integrity of systems and evidence. This requires having pre-defined strategies that balance the urgency of isolating affected assets with the need to minimize unnecessary business disruption. Effective containment is not only about executing technical measures, but also about ensuring clear communication with stakeholders so that decisions are understood, authorized, and documented. The deliverables from this phase — including playbooks, action logs, communication records, and preserved evidence — demonstrate that containment actions were deliberate, proportionate, and traceable. Lessons learned here feed directly into refining both tactical playbooks and long-term containment strategies for future incidents.

What strategies are prepared to immediately contain and limit the spread of an incident?
Deliverable: Containment Playbooks / Strategy Matrix
Pre-approved short-term and long-term containment options for different incident types (e.g., isolate host, disable account, block traffic). Ensures

responders act quickly and consistently under pressure.

How do we decide on containment actions that mitigate risk without excessive business disruption?
Deliverable: Containment Decision Log
A documented record of containment options considered, decisions taken, and the rationale for each. Demonstrates that actions balanced business impact against risk reduction.

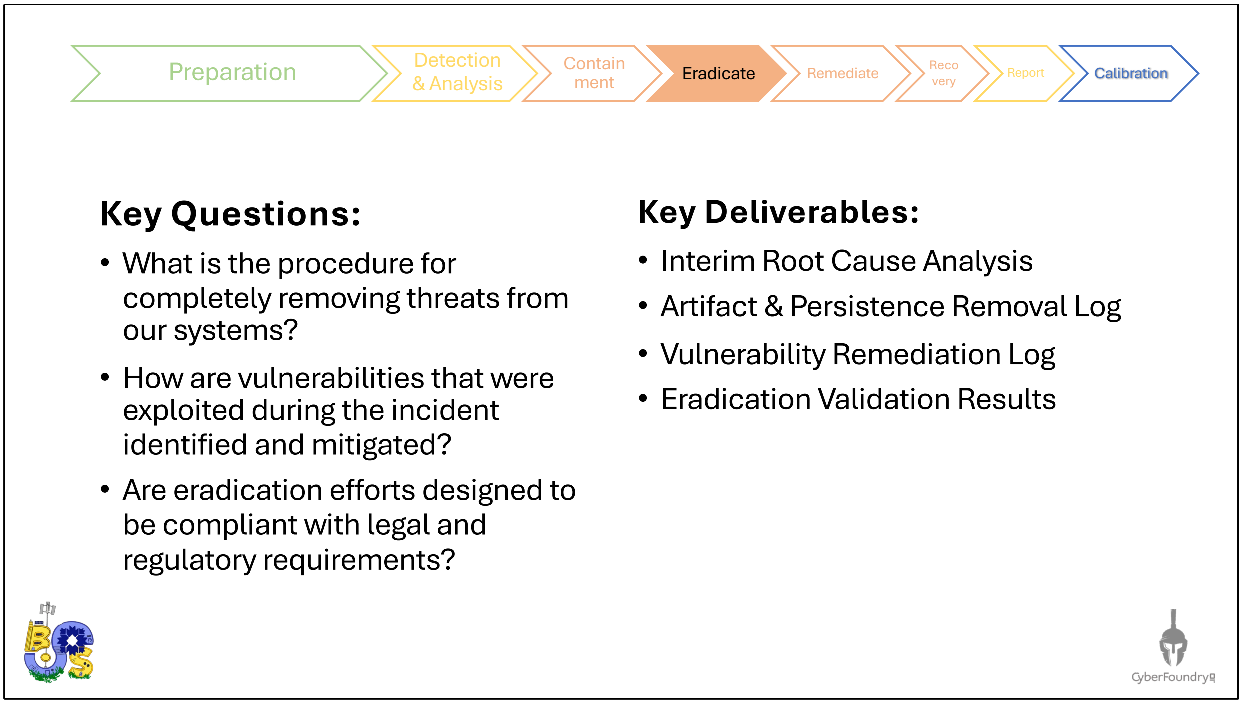
Are effective communication protocols with stakeholders in place during an incident?
Deliverable: Stakeholder Communication Record
Documented timeline of who was notified, when, and through what channel (executives, legal, regulators, vendors). Proves that escalation and communications were performed according to plan.

Who has the authority to approve and execute containment actions?
Deliverable: Containment Authority Register
A record of the individuals/roles authorized to approve specific containment steps. Ensures decisions are properly governed and traceable.

How do we preserve forensic evidence while executing containment?
Deliverable: Evidence Preservation Checklist
Checklist confirming logs, disk images, and volatile memory were captured before systems were isolated, wiped, or otherwise modified. Maintains evidentiary integrity for later analysis.

What isolation methods are available and have they been applied effectively?
Deliverable: Isolation Action Report
Detailed record of the technical containment measures executed (host isolation, network segmentation, account disables). Includes timestamps and verification of effectiveness.

What indicators confirm that containment was successful?
Deliverable: Containment Effectiveness Report
Evidence from monitoring and validation that the incident's spread has been stopped. Demonstrates that containment achieved its intended effect.



Preparation | Detection & Analysis | Contain ment | Eradicate | Remediate | Reco very | Report | Calibration

Key Questions:

- What is the procedure for completely removing threats from our systems?
- How are vulnerabilities that were exploited during the incident identified and mitigated?
- Are eradication efforts designed to be compliant with legal and regulatory requirements?

Key Deliverables:

- Interim Root Cause Analysis
- Artifact & Persistence Removal Log
- Vulnerability Remediation Log
- Eradication Validation Results

CyberFoundry

Eradication

In the eradication phase, the technical team shifts from containing the incident to removing the underlying cause and eliminating any malicious artifacts. While much of this work is highly technical, it should also result in an eradication strategy that informs the decisions you will make in the remediation phase. For example, the recommendation may be to act conservatively by decommissioning or rebuilding compromised assets to ensure the integrity of core services. These decisions often involve trade-offs: aggressive eradication may speed recovery but limit the ability to retain evidence or perform forensic analysis that could strengthen the root cause investigation. Business leadership should weigh these considerations carefully, as the pace and scope of eradication directly affect resilience against both the current threat and future incidents. In addition, this is the point at which legal and compliance obligations should be revisited—breach notification, regulatory reporting, or contractual requirements may require steps beyond the technical team’s scope and must be factored into the eradication plan.

What is the confirmed root cause of the incident?
Deliverable: Root Cause Analysis Report (Interim)

A preliminary report documenting the attack vector, exploited vulnerability, or misconfiguration. Links evidence to the identified root cause to guide remediation.

What malicious artifacts, persistence mechanisms, or unauthorized accounts must be removed?
Deliverable: Artifact & Persistence Removal Log
A detailed log of eradication actions — malware deletion, registry key cleanup, rogue account disablement, token/session revocation. Ensures each removal is verified and traceable.

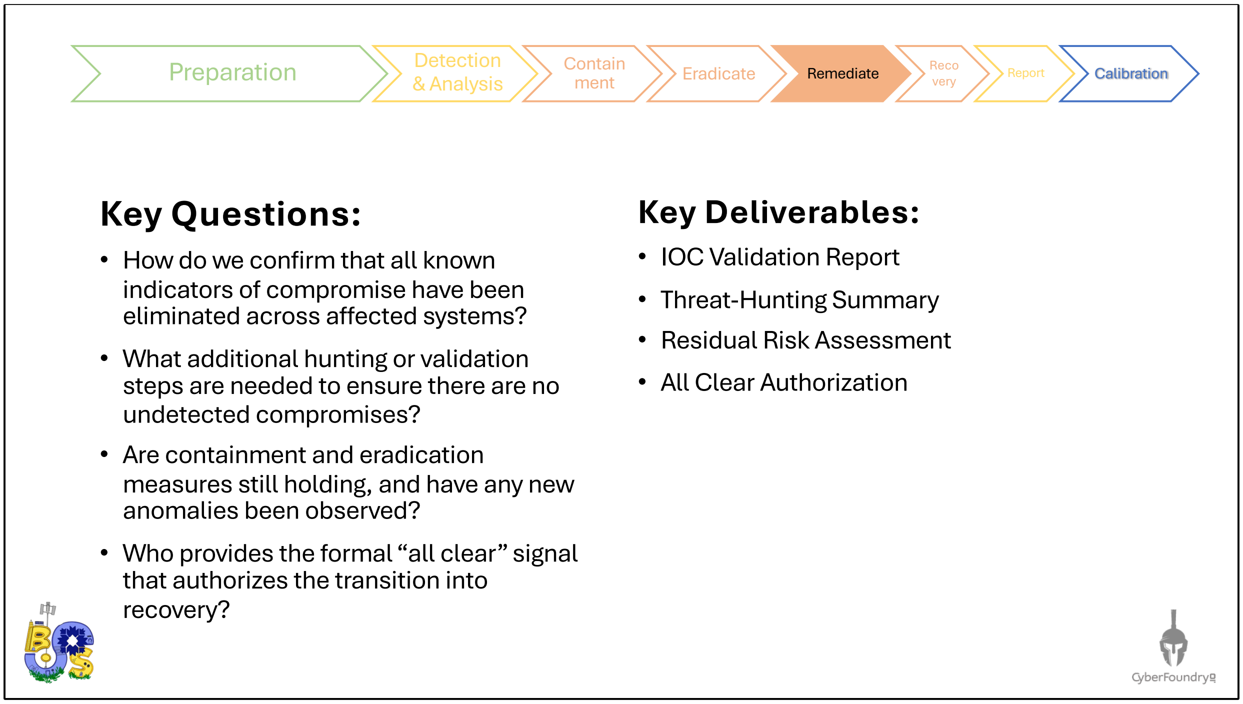
Have all affected systems been identified, remediated, and cleaned?
Deliverable: System Remediation Checklist
A system-by-system record confirming that each impacted host or service has been examined and cleaned. Prevents overlooked compromised assets.

How are vulnerabilities or misconfigurations that enabled the incident being corrected?
Deliverable: Vulnerability Remediation Report
Documentation of patches, config changes, or other corrective actions applied during eradication. Provides evidence that weaknesses have been addressed.

What forensic evidence must be preserved before eradication actions are taken?
Deliverable: Forensic Evidence Collection Record
A record showing that logs, images, and other artifacts were preserved before systems were wiped, rebuilt, or modified. Maintains chain of custody for legal and investigative use.

What criteria will confirm that eradication is successful?
Deliverable: Eradication Validation Results
Evidence from re-scans, system health checks, and monitoring that confirm artifacts and attacker presence have been removed. Provides measurable "done" criteria.

How do we validate eradication across hybrid environments (on-prem, cloud, SaaS)?
Deliverable: Environment Validation Report
A consolidated report confirming that eradication activities were applied consistently across all environments. Reduces risk of residual compromise in less visible domains.



Preparation | Detection & Analysis | Contain ment | Eradicate | Remediate | Reco very | Report | Calibration

Key Questions:

- How do we confirm that all known indicators of compromise have been eliminated across affected systems?
- What additional hunting or validation steps are needed to ensure there are no undetected compromises?
- Are containment and eradication measures still holding, and have any new anomalies been observed?
- Who provides the formal "all clear" signal that authorizes the transition into recovery?

Key Deliverables:

- IOC Validation Report
- Threat-Hunting Summary
- Residual Risk Assessment
- All Clear Authorization

CyberFoundry

Remediation

In the remediation phase, the technical team's responsibility is to confirm that the incident has been fully neutralized before normal operations resume. Unlike eradication, which removes known artifacts and vulnerabilities, remediation focuses on validating that there are no lingering indicators of compromise (IOCs), no persistence mechanisms left behind, and no missed systems still under threat. This is a phase of verification and assurance: the team must re-scan the environment, correlate logs across sources, and hunt proactively for evidence of additional attacker activity. It is critical to recognize that incidents often unfold in layers — what first appears as a single compromised endpoint may later reveal lateral movement, privilege escalation, or secondary persistence. Remediation is therefore the checkpoint where the organization pauses to ensure that containment and eradication were comprehensive. Only when the technical team can signal "all clear" — backed by evidence that no active threat remains — should the organization transition into recovery. This makes remediation not just a technical milestone, but a critical governance step, ensuring business leaders understand residual risk before restoration begins.

How do we confirm that all known indicators of compromise (IOCs) have

been eliminated across affected systems?
Deliverable: IOC Validation Report
A structured report of re-scans, forensic checks, and cross-tool validation confirming no known IOCs remain. Demonstrates eradication was complete and validated.

What additional hunting or validation steps are needed to detect hidden persistence or lateral movement?
Deliverable: Threat Hunting Log
Documentation of proactive hunts for residual attacker presence — including lateral movement checks, credential use review, beaconing analysis, and persistence mechanism sweeps. Provides assurance that the environment was fully checked for hidden compromise.

Have containment controls remained effective, and have any new anomalies emerged since eradication?
Deliverable: Containment Control Verification Report
A record confirming that isolation measures, account disables, or network blocks remain in place and effective. Ensures attackers did not bypass containment while remediation was underway.

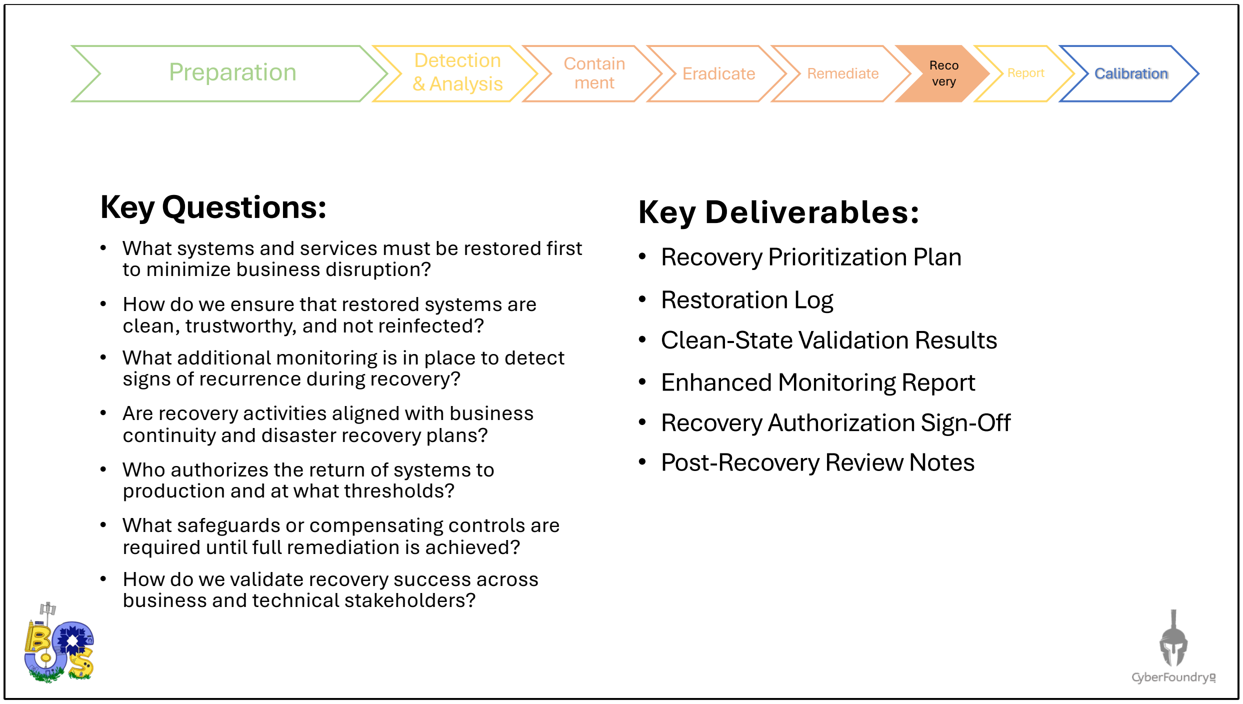
Have all vulnerabilities, misconfigurations, and exploited weaknesses been remediated?
Deliverable: Vulnerability & Misconfiguration Remediation Report
Evidence that patches, configuration changes, and credential resets have been applied across all affected systems. Links remediation actions back to identified CVEs or findings for traceability.

Have we preserved the necessary forensic evidence before further cleanup actions?
Deliverable: Forensic Evidence Preservation Checklist
A verified checklist confirming logs, images, and memory captures have been collected and secured before any additional cleanup. Protects against evidence loss for root cause or legal review.

What residual risks remain if some fixes cannot be applied immediately?
Deliverable: Residual Risk Statement
A concise summary of any remaining risks, deferred fixes, or compensating controls. Provides leadership with transparency on what remains unresolved.

Who has the authority to declare "all clear" and allow transition to recovery?
Deliverable: All Clear Authorization

Formal sign-off from the incident commander, CISO, or designated authority that remediation is complete. Serves as the official checkpoint allowing the organization to enter Recovery.



Preparation → Detection & Analysis → Containment → Eradicate → Remediate → Recovery → Report → Calibration

Key Questions:

- What systems and services must be restored first to minimize business disruption?
- How do we ensure that restored systems are clean, trustworthy, and not reinfected?
- What additional monitoring is in place to detect signs of recurrence during recovery?
- Are recovery activities aligned with business continuity and disaster recovery plans?
- Who authorizes the return of systems to production and at what thresholds?
- What safeguards or compensating controls are required until full remediation is achieved?
- How do we validate recovery success across business and technical stakeholders?

Key Deliverables:

- Recovery Prioritization Plan
- Restoration Log
- Clean-State Validation Results
- Enhanced Monitoring Report
- Recovery Authorization Sign-Off
- Post-Recovery Review Notes

CyberFoundry

Recovery

In the recovery phase, the organization transitions from containment and remediation into restoring systems and business services to their normal operational state. Recovery closely aligns with business continuity and disaster recovery (BCP/DR) processes, but with the added discipline of continuous monitoring to ensure that the incident has truly been resolved. If prior phases were executed effectively, recovery should be a controlled and deliberate process: rebuilding or restoring from clean backups, reintroducing systems into production, and validating functionality against business priorities. From an executive perspective, the critical decision is prioritization — determining which services must be restored first to minimize business impact, based on the organization's BIA and continuity planning. The technical IRP team must also remain alert for signs that the incident was not fully addressed, looping back into remediation if new indicators emerge. Recovery concludes with a post-recovery validation, ensuring both technical soundness and business readiness before declaring the incident fully closed.

What systems and services must be restored first to minimize business disruption?

Deliverable: Recovery Prioritization Plan
A documented plan that identifies which systems, applications, and services are restored first, mapped directly to the Business Impact Analysis (BIA). Ensures restoration efforts align with critical business needs and continuity planning.

How do we ensure that restored systems are clean, trustworthy, and not reinfected?
Deliverable: Clean-State Validation Results
Evidence such as forensic scans, malware checks, and configuration verifications proving that restored systems are free from compromise. Provides assurance that recovery sources (backups, rebuilds) are safe.

What additional monitoring is in place to detect signs of recurrence during recovery?
Deliverable: Enhanced Monitoring Report
A record of temporary, heightened monitoring (e.g., SIEM alerts, endpoint detections, anomaly tracking) applied during the recovery period. Demonstrates vigilance against recurrence while systems come back online.

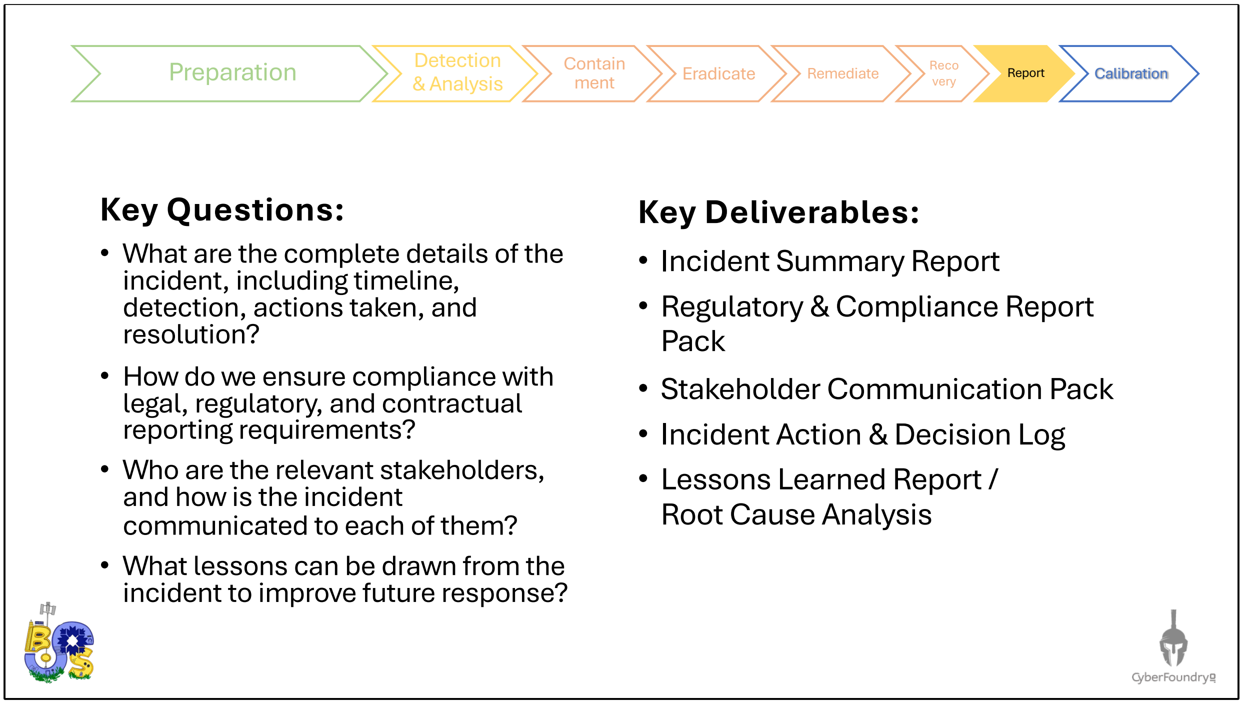
Are recovery activities aligned with business continuity and disaster recovery (BCP/DR) plans?
Deliverable: Restoration Log
A detailed log of systems restored, data recovered, and services reintroduced. Tracks timing, responsible personnel, and outcomes, ensuring activities were performed in accordance with BCP/DR processes.

Who authorizes the return of systems to production and at what thresholds?
Deliverable: Recovery Authorization Sign-Off
Formal approval by the incident commander or business owner that systems are ready for production. Creates a governance checkpoint showing recovery decisions were deliberate and risk-informed.

What safeguards or compensating controls are required until full remediation is achieved?
Deliverable: Temporary Controls Register
Document listing compensating controls (e.g., firewall blocks, restricted accounts, enhanced logging) that must remain in place during recovery. Ensures leadership is aware of residual risks.

How do we validate recovery success across business and technical stakeholders?
Deliverable: Post-Recovery Review Notes

A short, structured set of findings summarizing whether recovery was complete and effective. Includes feedback from business owners, executives, and technical staff, preparing inputs for the later Calibration phase.



Key Questions:

- What are the complete details of the incident, including timeline, detection, actions taken, and resolution?
- How do we ensure compliance with legal, regulatory, and contractual reporting requirements?
- Who are the relevant stakeholders, and how is the incident communicated to each of them?
- What lessons can be drawn from the incident to improve future response?

Key Deliverables:

- Incident Summary Report
- Regulatory & Compliance Report Pack
- Stakeholder Communication Pack
- Incident Action & Decision Log
- Lessons Learned Report / Root Cause Analysis

Report

The reporting phase ensures that the incident is fully documented, communicated, and aligned with compliance obligations. This is more than just paperwork — it creates the authoritative record of what happened, how the organization responded, and what lessons were derived. A strong report provides transparency for executives, regulators, insurers, and other stakeholders while preserving the organization's credibility. From a technical perspective, the report consolidates logs, actions, and decisions into a single incident record. From a business perspective, it fulfills contractual, legal, or regulatory reporting requirements. The incident report also serves as a learning tool, feeding into the calibration phase by identifying gaps and opportunities for improvement. Above all, reporting formalizes closure: the incident is captured, analyzed, and communicated so the organization can move forward with trust.

What are the complete details of the incident, including timeline, detection, actions taken, and resolution?

Deliverable: Incident Summary Report

A comprehensive, chronological account of the incident from detection through recovery. Includes key decisions, escalation points, and closure status.

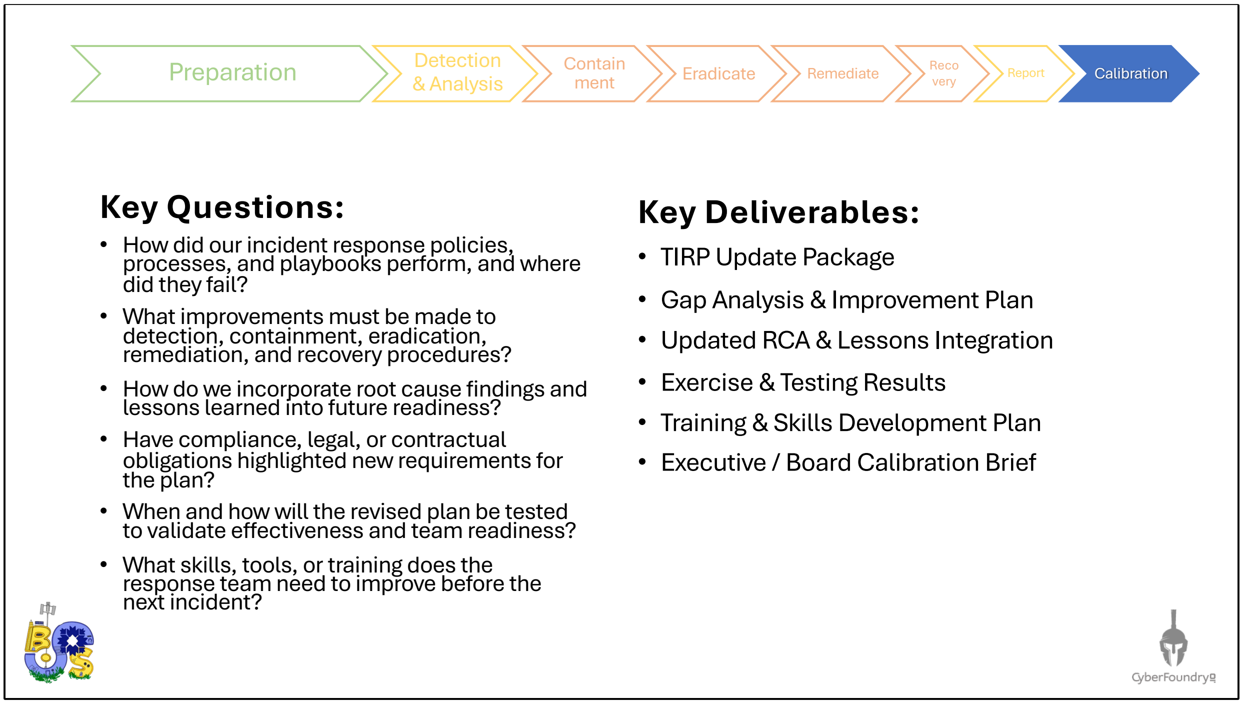
How do we ensure that reporting requirements for compliance, regulatory, contractual, or legal obligations are met?
Deliverable: Regulatory & Compliance Report Pack
Formal submissions tailored to each applicable regime (e.g., SEC, GDPR, HIPAA, DoD/CUI). Includes deadlines met, forms submitted, and counsel sign-off.

Who are the relevant stakeholders, and how is the incident communicated to each of them?
Deliverable: Stakeholder Communication Package
Tailored reports or notifications for executives, boards, customers, insurers, and partners. Ensures each group receives the right level of detail and assurance.

How do we capture and preserve evidence of decisions and actions for future reference or litigation?
Deliverable: Incident Action & Decision Log
Consolidated record of technical and business actions taken, including authorizations. Serves as an evidentiary-quality audit trail.

What lessons can be drawn from the incident to improve future response?
Deliverable: Lessons Learned Report
Structured documentation of strengths, weaknesses, and recommendations. Provides direct input into the calibration phase and continuous improvement cycle.

How do we ensure the final report is consistent, accessible, and retained appropriately?
Deliverable: Finalized Incident Report Repository Entry
The authoritative version of the incident report, reviewed and approved, stored securely in the organization's knowledge base or compliance archive.



Preparation | Detection & Analysis | Contain ment | Eradicate | Remediate | Reco very | Report | Calibration

Key Questions:

- How did our incident response policies, processes, and playbooks perform, and where did they fail?
- What improvements must be made to detection, containment, eradication, remediation, and recovery procedures?
- How do we incorporate root cause findings and lessons learned into future readiness?
- Have compliance, legal, or contractual obligations highlighted new requirements for the plan?
- When and how will the revised plan be tested to validate effectiveness and team readiness?
- What skills, tools, or training does the response team need to improve before the next incident?

Key Deliverables:

- TIRP Update Package
- Gap Analysis & Improvement Plan
- Updated RCA & Lessons Integration
- Exercise & Testing Results
- Training & Skills Development Plan
- Executive / Board Calibration Brief

Calibration

The calibration phase ensures that the organization learns from the incident and continuously improves its response posture. This is not just a lessons-learned discussion, but a deliberate process of reviewing what worked, what failed, and how policies, procedures, and technologies must be updated to reflect evolving threats and organizational priorities. Calibration incorporates findings from the report phase — including root cause analysis, action logs, and lessons learned — and translates them into concrete updates to the incident response plan, escalation thresholds, playbooks, and training. It also involves exercising the revised plan through tabletops or simulations to validate improvements. At its core, calibration ensures that the organization emerges from an incident stronger, with a response capability that adapts to both internal change and the external threat landscape.

How did our incident response policies, processes, and playbooks perform, and where did they fail?

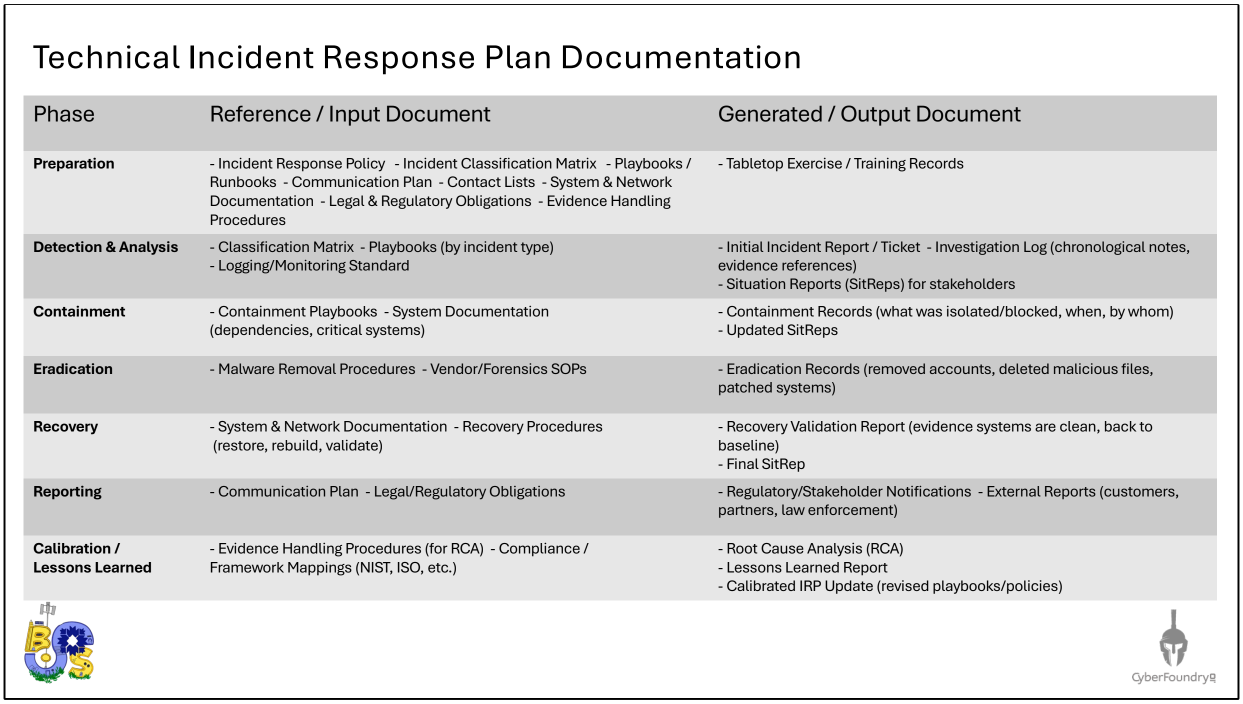
Deliverable: Gap Analysis & Improvement Plan — Documents strengths, weaknesses, and prioritized fixes to strengthen the program.

What improvements must be made to detection, containment, eradication, remediation, and recovery procedures?
Deliverable: IRP/TIRP Update Package — Revised playbooks, thresholds, and workflows updated to reflect lessons learned.

How do we incorporate root cause findings and lessons learned into future readiness?
Deliverable: Updated RCA & Lessons Integration Report — Ensures technical and business insights are formally embedded into policies and controls.

When and how will the revised plan be tested for effectiveness and team readiness?
Deliverable: Exercise & Testing Results — Records of tabletop drills, red-team exercises, or simulations validating improvements.

What skills, training, or tools does the team need to improve before the next incident?
Deliverable: Training & Skills Development Plan — Roadmap for certifications, exercises, and tooling enhancements to boost response maturity.



Technical Incident Response Plan Documentation

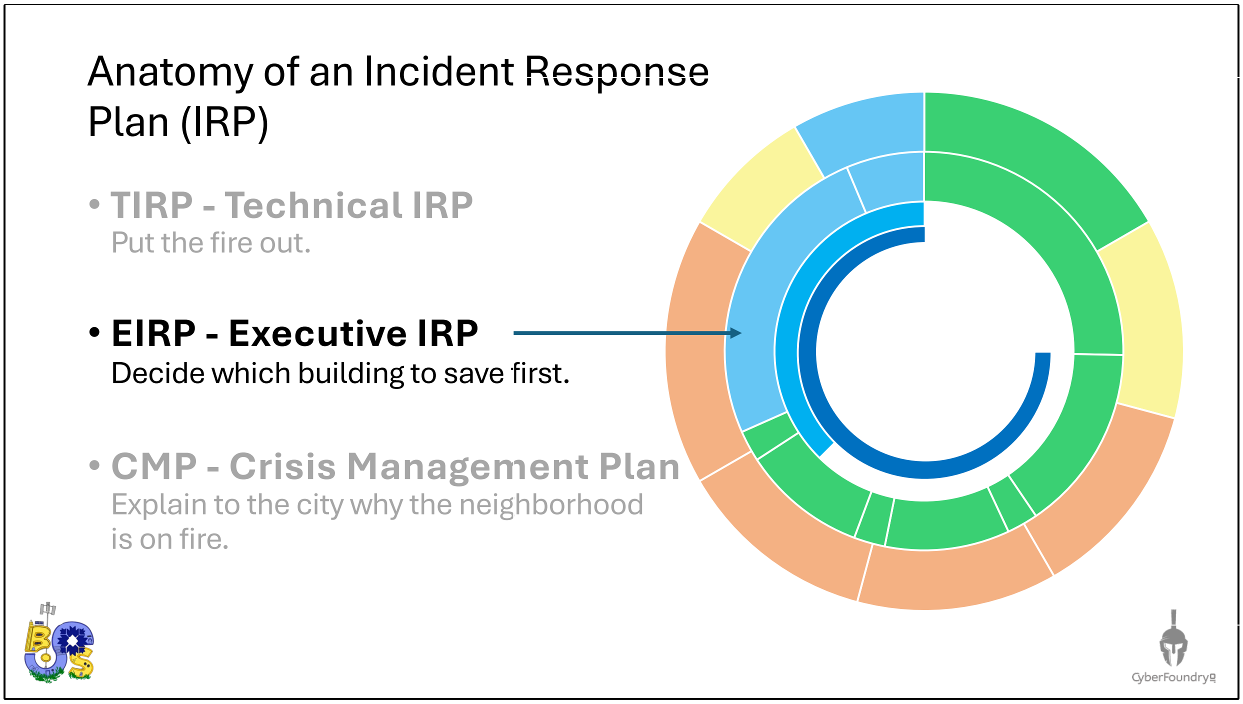
Phase	Reference / Input Document	Generated / Output Document
Preparation	- Incident Response Policy - Incident Classification Matrix - Playbooks / Runbooks - Communication Plan - Contact Lists - System & Network Documentation - Legal & Regulatory Obligations - Evidence Handling Procedures	- Tabletop Exercise / Training Records
Detection & Analysis	- Classification Matrix - Playbooks (by incident type) - Logging/Monitoring Standard	- Initial Incident Report / Ticket - Investigation Log (chronological notes, evidence references) - Situation Reports (SitReps) for stakeholders
Containment	- Containment Playbooks - System Documentation (dependencies, critical systems)	- Containment Records (what was isolated/blocked, when, by whom) - Updated SitReps
Eradication	- Malware Removal Procedures - Vendor/Forensics SOPs	- Eradication Records (removed accounts, deleted malicious files, patched systems)
Recovery	- System & Network Documentation - Recovery Procedures (restore, rebuild, validate)	- Recovery Validation Report (evidence systems are clean, back to baseline) - Final SitRep
Reporting	- Communication Plan - Legal/Regulatory Obligations	- Regulatory/Stakeholder Notifications - External Reports (customers, partners, law enforcement)
Calibration / Lessons Learned	- Evidence Handling Procedures (for RCA) - Compliance / Framework Mappings (NIST, ISO, etc.)	- Root Cause Analysis (RCA) - Lessons Learned Report - Calibrated IRP Update (revised playbooks/policies)

CyberFoundry

Executive Incident Response Plan

Objectives

- Reduce the material impact to the business from a cybersecurity incident
- Inform the business, stakeholders and officials



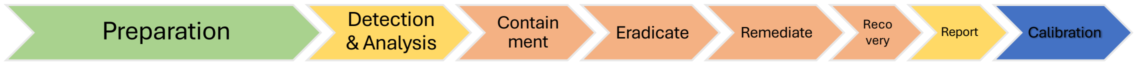
Anatomy of an Incident Response Plan (IRP)

- **TIRP - Technical IRP**
  Put the fire out.

- **EIRP - Executive IRP**
  Decide which building to save first.

- **CMP - Crisis Management Plan**
  Explain to the city why the neighborhood is on fire.

Technical Incident Response Plan



Preparation

Detection & Analysis

Containment

Eradicate

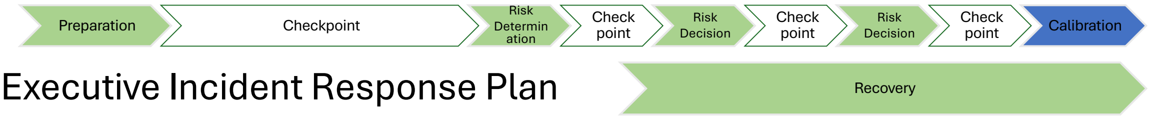
Remediate

Recovery

Report

Calibration

Executive Incident Response Plan



Preparation

Checkpoint

Risk Determination

Checkpoint

Risk Decision

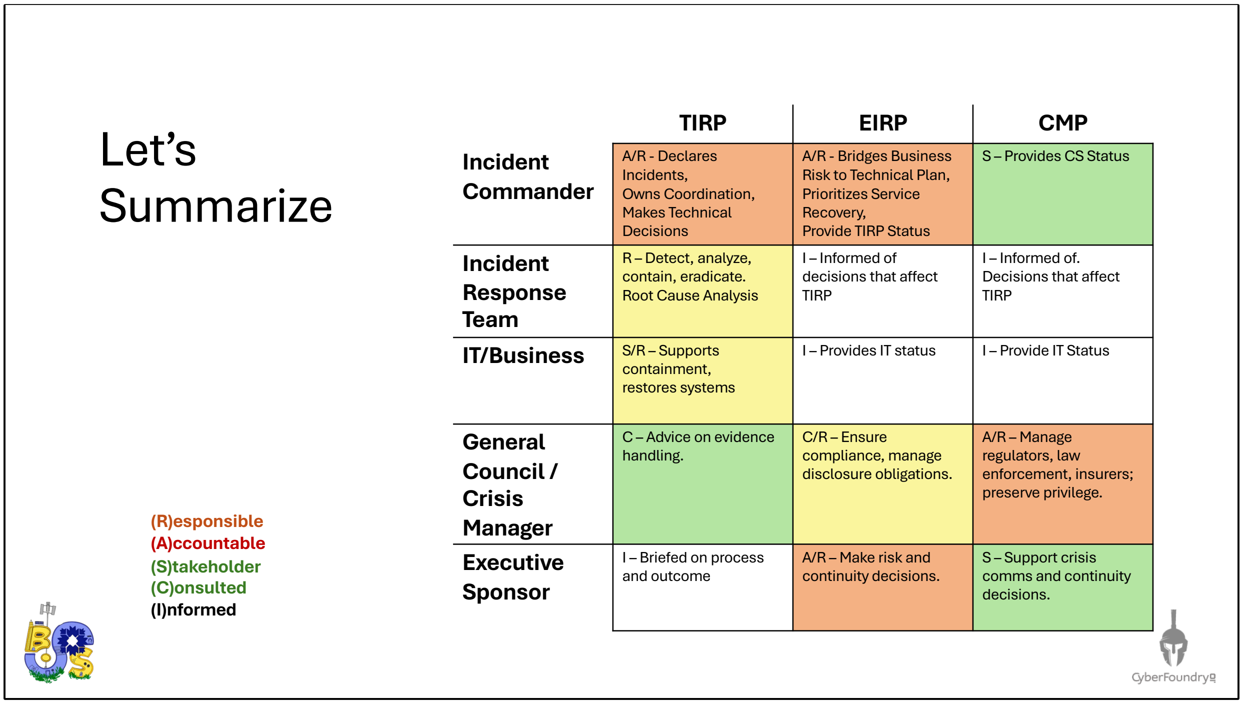
Checkpoint

Risk Decision

Checkpoint

Calibration

Recovery

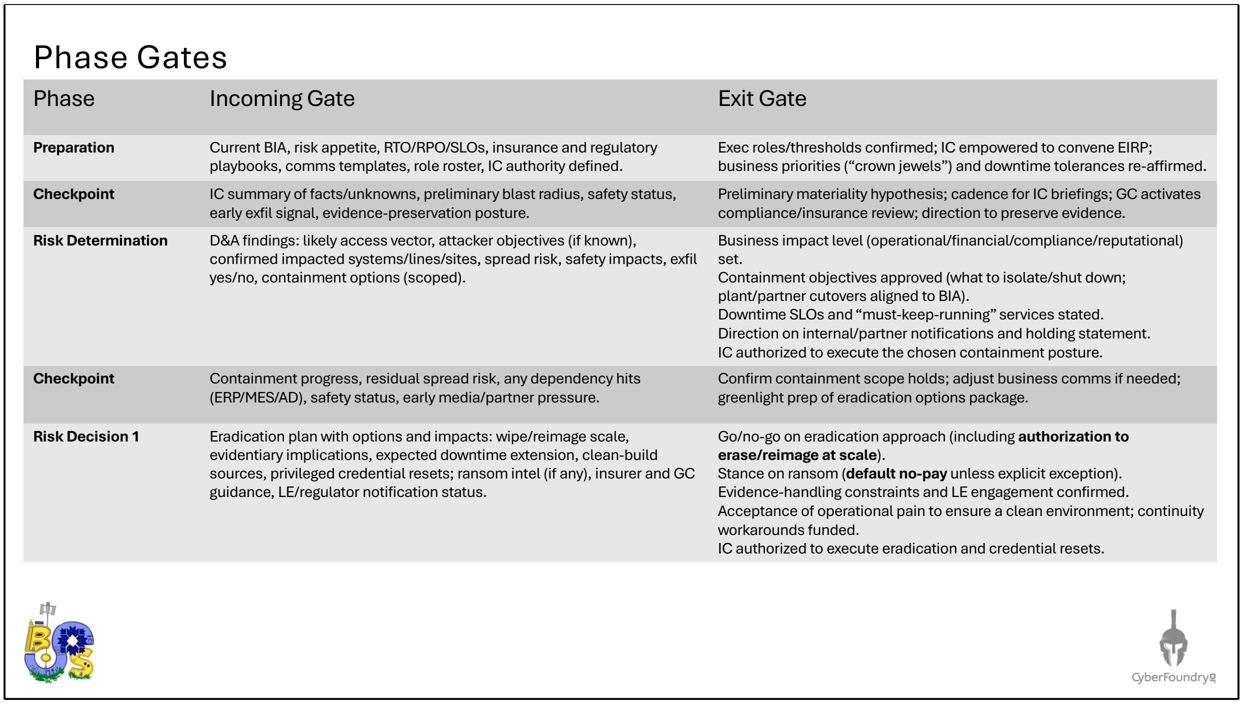


Let’s Summarize

	TIRP	EIRP	CMP
Incident Commander	A/R - Declares Incidents, Owns Coordination, Makes Technical Decisions	A/R - Bridges Business Risk to Technical Plan, Prioritizes Service Recovery, Provide TIRP Status	S – Provides CS Status
Incident Response Team	R – Detect, analyze, contain, eradicate. Root Cause Analysis	I – Informed of decisions that affect TIRP	I – Informed of. Decisions that affect TIRP
IT/Business	S/R – Supports containment, restores systems	I – Provides IT status	I – Provide IT Status
General Council / Crisis Manager	C – Advice on evidence handling.	C/R – Ensure compliance, manage disclosure obligations.	A/R – Manage regulators, law enforcement, insurers; preserve privilege.
Executive Sponsor	I – Briefed on process and outcome	A/R – Make risk and continuity decisions.	S – Support crisis comms and continuity decisions.

(R)esponsible
(A)ccountable
(S)takeholder
(C)onsulted
(I)nformed

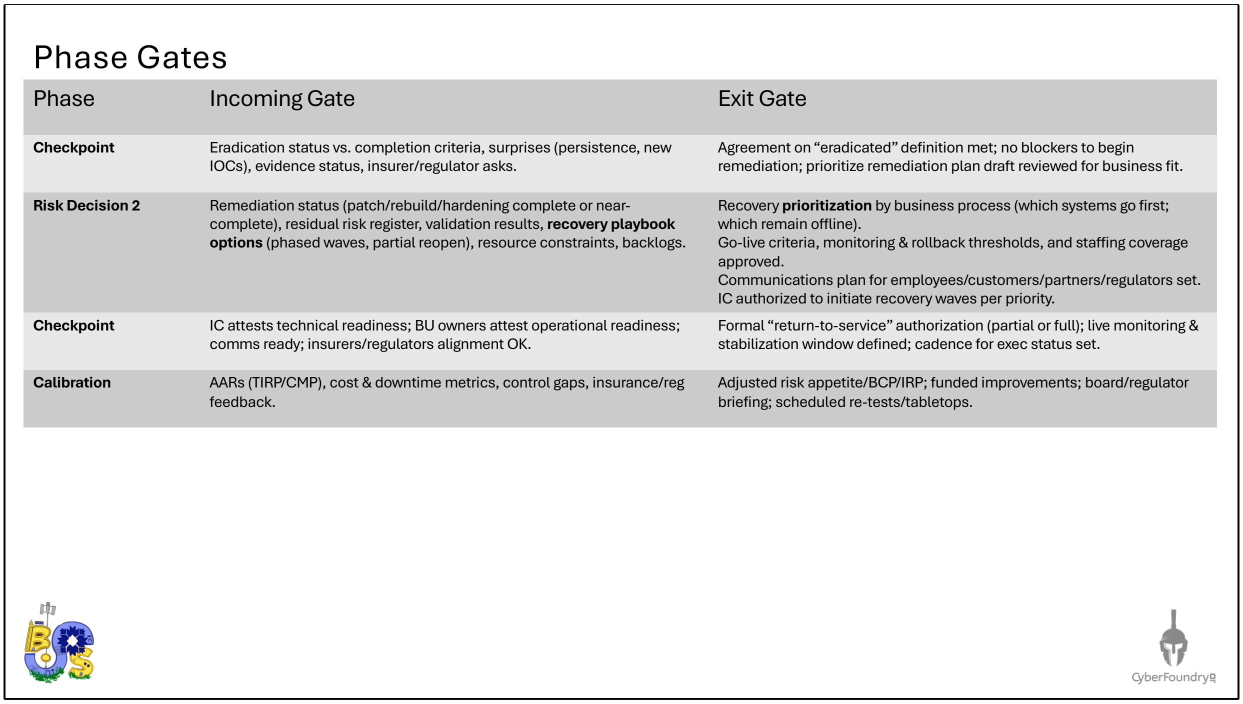
CyberFoundry



Phase Gates

Phase	Incoming Gate	Exit Gate
Preparation	Current BIA, risk appetite, RTO/RPO/SLOs, insurance and regulatory playbooks, comms templates, role roster, IC authority defined.	Exec roles/thresholds confirmed; IC empowered to convene EIRP; business priorities (“crown jewels”) and downtime tolerances re-affirmed.
Checkpoint	IC summary of facts/unknowns, preliminary blast radius, safety status, early exfil signal, evidence-preservation posture.	Preliminary materiality hypothesis; cadence for IC briefings; GC activates compliance/insurance review; direction to preserve evidence.
Risk Determination	D&A findings: likely access vector, attacker objectives (if known), confirmed impacted systems/lines/sites, spread risk, safety impacts, exfil yes/no, containment options (scoped).	Business impact level (operational/financial/compliance/reputational) set. Containment objectives approved (what to isolate/shut down; plant/partner cutovers aligned to BIA). Downtime SLOs and “must-keep-running” services stated. Direction on internal/partner notifications and holding statement. IC authorized to execute the chosen containment posture.
Checkpoint	Containment progress, residual spread risk, any dependency hits (ERP/MES/AD), safety status, early media/partner pressure.	Confirm containment scope holds; adjust business comms if needed; greenlight prep of eradication options package.
Risk Decision 1	Eradication plan with options and impacts: wipe/reimage scale, evidentiary implications, expected downtime extension, clean-build sources, privileged credential resets; ransom intel (if any), insurer and GC guidance, LE/regulator notification status.	Go/no-go on eradication approach (including **authorization to erase/reimage at scale**). Stance on ransom (**default no-pay** unless explicit exception). Evidence-handling constraints and LE engagement confirmed. Acceptance of operational pain to ensure a clean environment; continuity workarounds funded. IC authorized to execute eradication and credential resets.

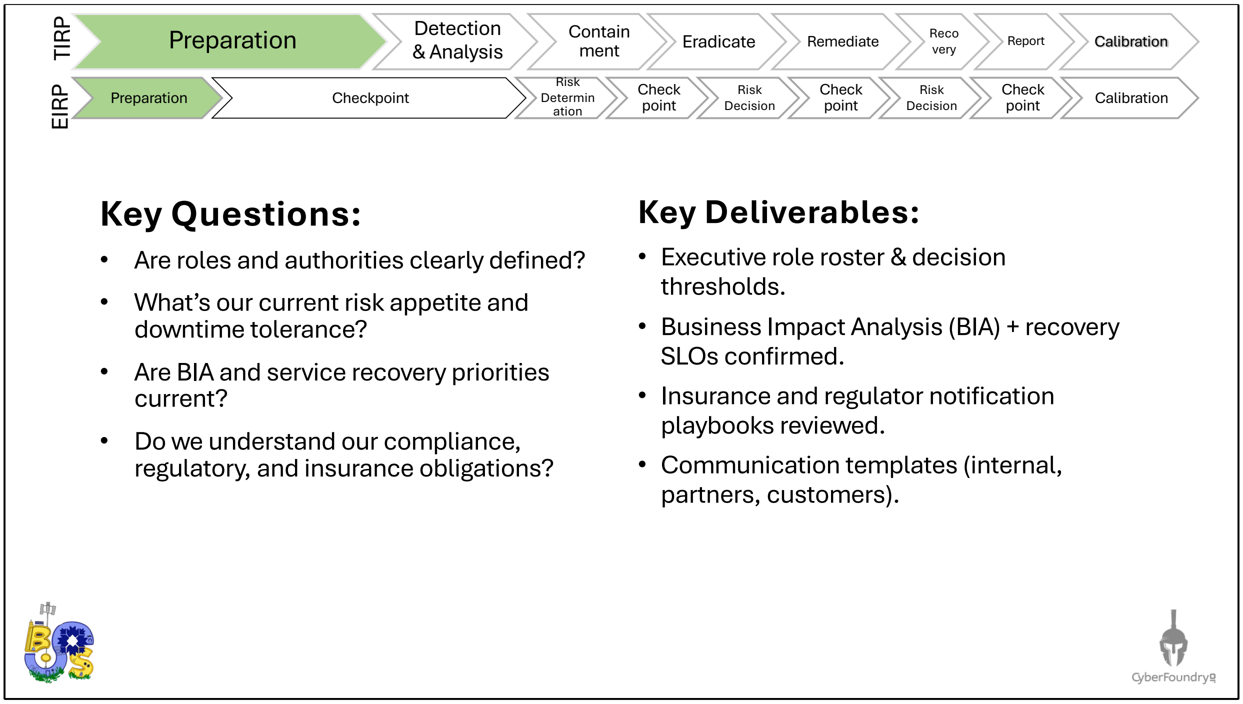
CyberFoundry



Phase Gates

Phase	Incoming Gate	Exit Gate
Checkpoint	Eradication status vs. completion criteria, surprises (persistence, new IOCs), evidence status, insurer/regulator asks.	Agreement on “eradicated” definition met; no blockers to begin remediation; prioritize remediation plan draft reviewed for business fit.
Risk Decision 2	Remediation status (patch/rebuild/hardening complete or near-complete), residual risk register, validation results, **recovery playbook options** (phased waves, partial reopen), resource constraints, backlogs.	Recovery **prioritization** by business process (which systems go first; which remain offline). Go-live criteria, monitoring & rollback thresholds, and staffing coverage approved. Communications plan for employees/customers/partners/regulators set. IC authorized to initiate recovery waves per priority.
Checkpoint	IC attests technical readiness; BU owners attest operational readiness; comms ready; insurers/regulators alignment OK.	Formal “return-to-service” authorization (partial or full); live monitoring & stabilization window defined; cadence for exec status set.
Calibration	AARs (TIRP/CMP), cost & downtime metrics, control gaps, insurance/reg feedback.	Adjusted risk appetite/BCP/IRP; funded improvements; board/regulator briefing; scheduled re-tests/tabletops.

CyberFoundry



TIRP: Preparation › Detection & Analysis › Contain ment › Eradicate › Remediate › Reco very › Report › Calibration

EIRP: Preparation › Checkpoint › Risk Determin ation › Check point › Risk Decision › Check point › Risk Decision › Check point › Calibration

Key Questions:

- Are roles and authorities clearly defined?
- What's our current risk appetite and downtime tolerance?
- Are BIA and service recovery priorities current?
- Do we understand our compliance, regulatory, and insurance obligations?

Key Deliverables:

- Executive role roster & decision thresholds.
- Business Impact Analysis (BIA) + recovery SLOs confirmed.
- Insurance and regulator notification playbooks reviewed.
- Communication templates (internal, partners, customers).

CyberFoundry

Before an incident ever happens, the Executive IRP has to be set up to succeed. The Preparation phase is about removing ambiguity and making sure executives know their role in a crisis.

The first question we ask is: *who has the authority to make which decisions?* We don't want to figure that out in the middle of a ransomware outbreak. That's why the RASCI model matters — the Incident Commander knows exactly who to escalate to, and executives know what calls land on their desk.

The second piece is *our business priorities*. We need to know which functions are mission critical, and in what order. That comes from a current Business Impact Analysis. For example, is keeping ERP online more important than email? How much downtime can each tolerate? Those recovery objectives — RTOs and RPOs — are what guide containment and recovery decisions later.

Third, we check our **external obligations**. That means compliance and legal reporting, insurance requirements, and third-party obligations. The General Counsel, Risk, and Communications teams all weigh in here, and we prepare notification templates so we aren't drafting from scratch under pressure.

Finally, we set the **briefing cadence**. One of the hidden purposes of the EIRP is keeping the CEO and the Board properly informed while shielding the SOC from constant executive interruptions. That only works if we've already defined how information flows: how often the IC briefs the EIRP, and how often the EIRP briefs the CEO and Board.

The outcome of this phase is clarity: executives understand their role, our risk tolerance is documented, our communication and compliance playbooks are ready, and the IC has authority to act. That's the foundation that makes the rest of the IRP run smoothly."

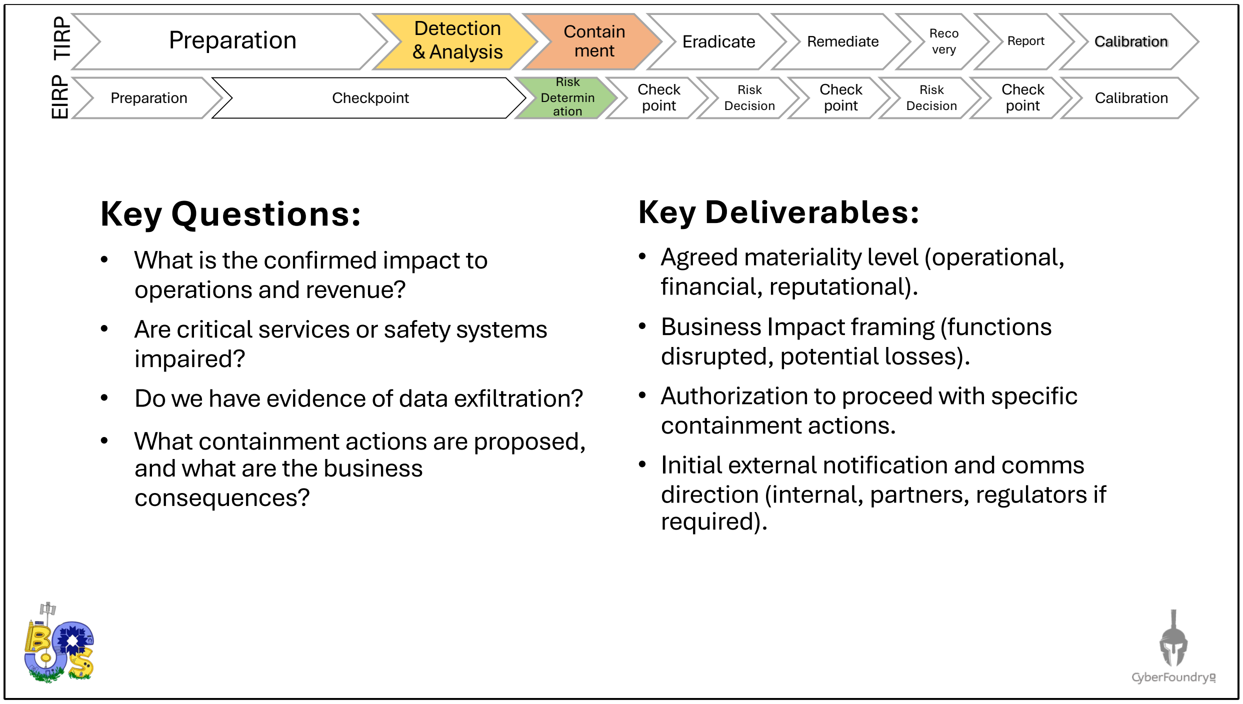
"Who has the authority to make risk calls?"
Answered by executive sponsor, GC, and COO.
Output: RASCI matrix validated, delegation documented; IC knows when to escalate and to whom.

"What are our crown jewels and recovery priorities?"
Answered by BU leaders against the BIA.
Output: Tiered recovery priority list (e.g., ERP > MES > email), codified as executive guidance.

"What's our tolerance for downtime and data loss?"
Answered via exec alignment on RTO (recovery time objective) / RPO (recovery point objective).
Output: Service-level objectives (SLOs) expressed in hours/days, to guide TIRP containment/recovery.

"What external obligations must we plan for?"
Answered by GC (regulatory reporting), risk/insurance (policy triggers), comms (partners/customers).
Output: Notification matrix (who, when, how), staged templates prepared.

"How do we keep the CEO and Board engaged without disrupting?"
Answered by exec sponsor and GC.
Output: Defined briefing cadence (e.g., IC → EIRP q2h, EIRP → CEO/Board daily).



Key Questions:

- What is the confirmed impact to operations and revenue?
- Are critical services or safety systems impaired?
- Do we have evidence of data exfiltration?
- What containment actions are proposed, and what are the business consequences?

Key Deliverables:

- Agreed materiality level (operational, financial, reputational).
- Business Impact framing (functions disrupted, potential losses).
- Authorization to proceed with specific containment actions.
- Initial external notification and comms direction (internal, partners, regulators if required).

Once the technical team finishes their initial Detection and Analysis, the EIRP convenes for the first big decision point: Risk Determination.

At this stage, the Incident Commander brings forward the facts: which systems are down, whether safety is at risk, and whether there are signs of data leaving the network. Executives don't debate malware signatures — they decide what the business impact actually is.

The key questions are: *what's broken, what's the scale of the loss, and what happens if we contain in this way versus that way?* For example, if we shut down the plant floor we may lose two days of production, but if we don't, the ransomware could jump into ERP and take the whole company down.

This is also where compliance starts to come into play. If there are indicators of exfiltration, the General Counsel begins preparing for potential breach notifications.

The deliverables are simple: executives set the materiality level, they approve the containment strategy, and they authorize the Incident Commander to move forward. And critically, they start shaping communications — what do we tell employees, partners, regulators, or the press at this stage.

In short: the Risk Determination gate reframes the incident as a business loss, and gives the technical team the mandate to contain, even if that means downtime. The Incident Commander ensures both sides are aligned before Containment begins."

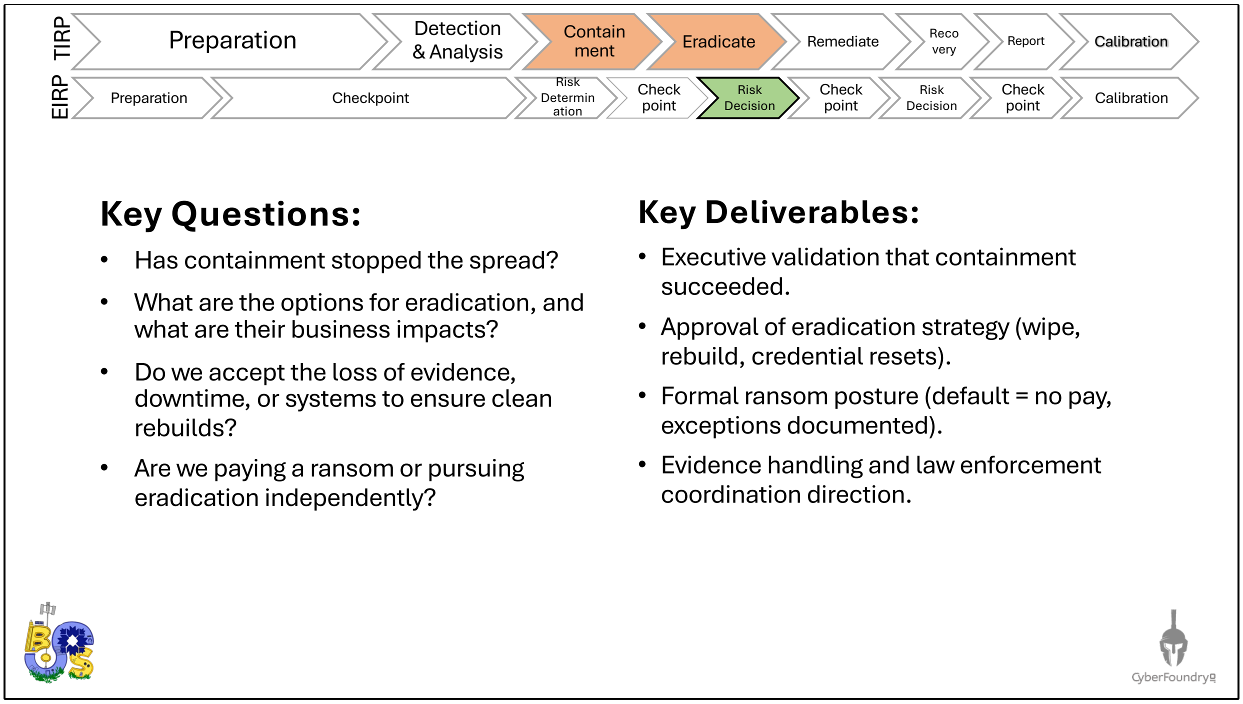
"What has actually been impacted?"
Answer: SOC/IRT confirms affected systems, business units add operational context.
Output: Map of impacted business processes vs. IT/OT assets.

"What's the scale of loss if this continues?"
Answer: BU leaders quantify downtime impact ($/day, safety, compliance).
Output: Materiality rating (low/medium/high/critical) anchored in $ and operational terms.

"Has data left the environment?"
Answer: Forensics team provides exfil indicators, GC advises on legal thresholds.
Output: Compliance risk posture (notification triggers Y/N).

"What containment options exist, and what's the business cost?"
Answer: TIRP presents options (network isolation, plant shutdown, partner disconnects). Executives weigh against BIA and customer obligations.
Output: Approved containment strategy + explicit tolerances (e.g., accept 2-day outage to prevent spread).

"Who needs to know now?"
Answer: GC, Comms, Insurance confirm who must be notified (regulators, partners, customers, law enforcement).
Output: Notification/communications plan activated at the appropriate level.



TIRP: Preparation | Detection & Analysis | Containment | Eradicate | Remediate | Recovery | Report | Calibration

EIRP: Preparation | Checkpoint | Risk Determination | Checkpoint | Risk Decision | Checkpoint | Risk Decision | Checkpoint | Calibration

Key Questions:

- Has containment stopped the spread?
- What are the options for eradication, and what are their business impacts?
- Do we accept the loss of evidence, downtime, or systems to ensure clean rebuilds?
- Are we paying a ransom or pursuing eradication independently?

Key Deliverables:

- Executive validation that containment succeeded.
- Approval of eradication strategy (wipe, rebuild, credential resets).
- Formal ransom posture (default = no pay, exceptions documented).
- Evidence handling and law enforcement coordination direction.

At this checkpoint, the technical team has contained the outbreak. Now the executive question becomes: do we authorize eradication?

Eradication almost always means more pain in the short term. Systems will be wiped, OT controllers may need to be reimaged, domain credentials reset. This is the moment where executives accept that it may get worse before it gets better — but only by taking the hit now can we ensure a clean recovery.

The Incident Commander presents options, each with tradeoffs. Business leaders weigh what downtime or data loss the company can tolerate. Legal and compliance confirm that evidence has been preserved, and that law enforcement and insurers are aligned.

The big decision here is also the ransom. The EIRP is where the company formally declares its posture: we will not pay, and we will accept the consequences of rebuilding ourselves. That decision has to be explicit, documented, and owned at the executive level.

The deliverables are clear: validate containment, authorize eradication, set the ransom posture, and ensure evidence handling is defensible. Once those are in place, the IC has the mandate to move the TIRP into full eradication.

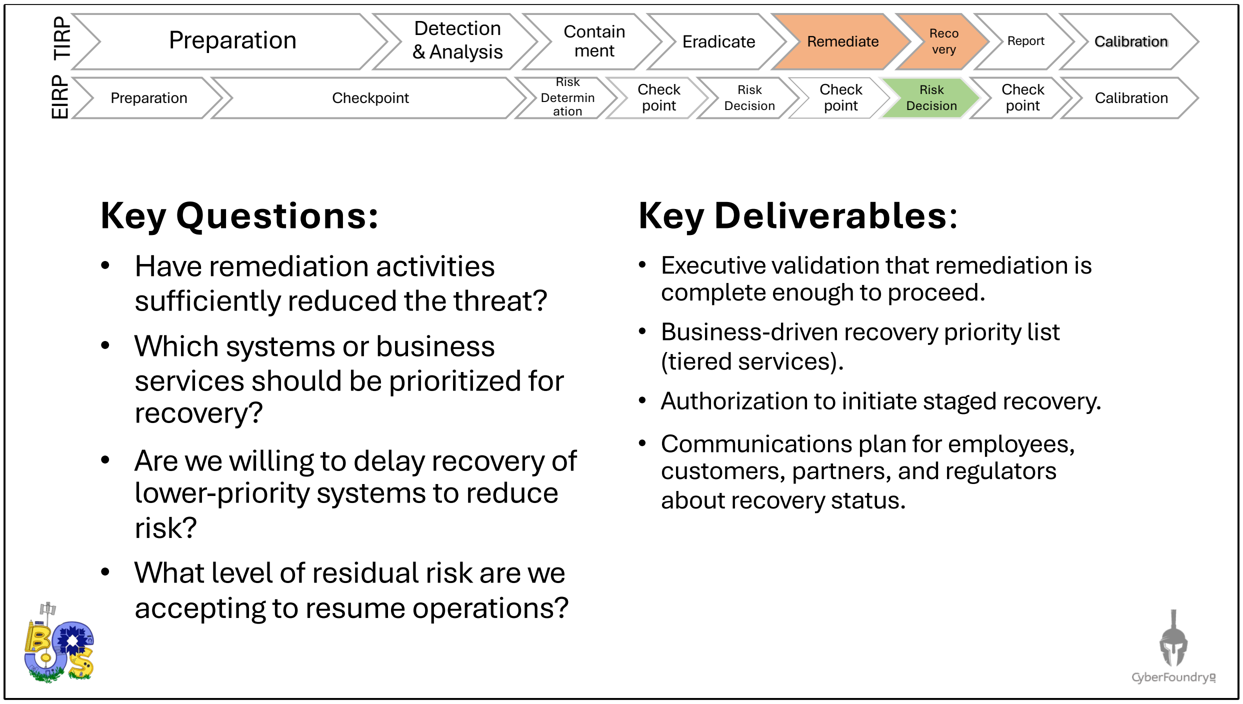
“Has containment held, or is the threat still spreading?”
Answer: TIRP reports on network isolation, infection metrics, and stabilization.
Output: Executives confident the ‘bleeding’ is stopped before destruction begins.

“What are our eradication options, and what do they cost the business?”
Answer: Technical team presents eradication plans (wipe all impacted hosts, reimage OT controllers, reset domain credentials). BU leaders quantify downtime impact.
Output: Approved eradication path, with explicit business acceptance of downtime and system loss.

“Will eradication destroy evidence we might need for regulators or litigation?”
Answer: GC and IC confirm forensic captures completed; law enforcement stance provided.
Output: Written acknowledgement of evidence handling; GC preserved privilege.

“Are we considering ransom payment, or are we proceeding with eradication only?”
Answer: GC, insurer, and risk leaders weigh ransom posture; executives deliberate business impact.
Output: Documented **decision not to pay** (unless a pre-defined exception threshold is met), communicated to IC.

“What must we tell employees, partners, or customers before eradication begins?”
Answer: Comms and BU leaders provide messaging guidance.
Output: Updated comms plan aligned to eradication impacts.



TIRP: Preparation · Detection & Analysis · Contain ment · Eradicate · Remediate · Reco very · Report · Calibration

EIRP: Preparation · Checkpoint · Risk Determin ation · Check point · Risk Decision · Check point · Risk Decision · Check point · Calibration

Key Questions:

- Have remediation activities sufficiently reduced the threat?
- Which systems or business services should be prioritized for recovery?
- Are we willing to delay recovery of lower-priority systems to reduce risk?
- What level of residual risk are we accepting to resume operations?

Key Deliverables:

- Executive validation that remediation is complete enough to proceed.
- Business-driven recovery priority list (tiered services).
- Authorization to initiate staged recovery.
- Communications plan for employees, customers, partners, and regulators about recovery status.

This is the final executive gate before recovery begins. The technical team has remediated vulnerabilities, rebuilt systems, and confirmed security controls. Now the question is whether the business is ready to resume operations.

The Incident Commander brings remediation results, and executives evaluate them against business needs. This is where we set recovery priorities: which systems come back first, and which can wait. For example, ERP may be essential to resume production, while other internal systems can remain offline until risk is lower.

Executives must explicitly accept residual risk. No remediation is ever perfect, and this decision point is about balancing the need to restart operations with the risk of reintroducing the adversary or instability.

The deliverables are a prioritized recovery plan, authorization to begin staged recovery, and a clear communications strategy for employees, customers, partners, and regulators.

Once this decision is made, the Incident Commander has the mandate to move the TIRP into recovery, and the business begins its journey back to normal operations.

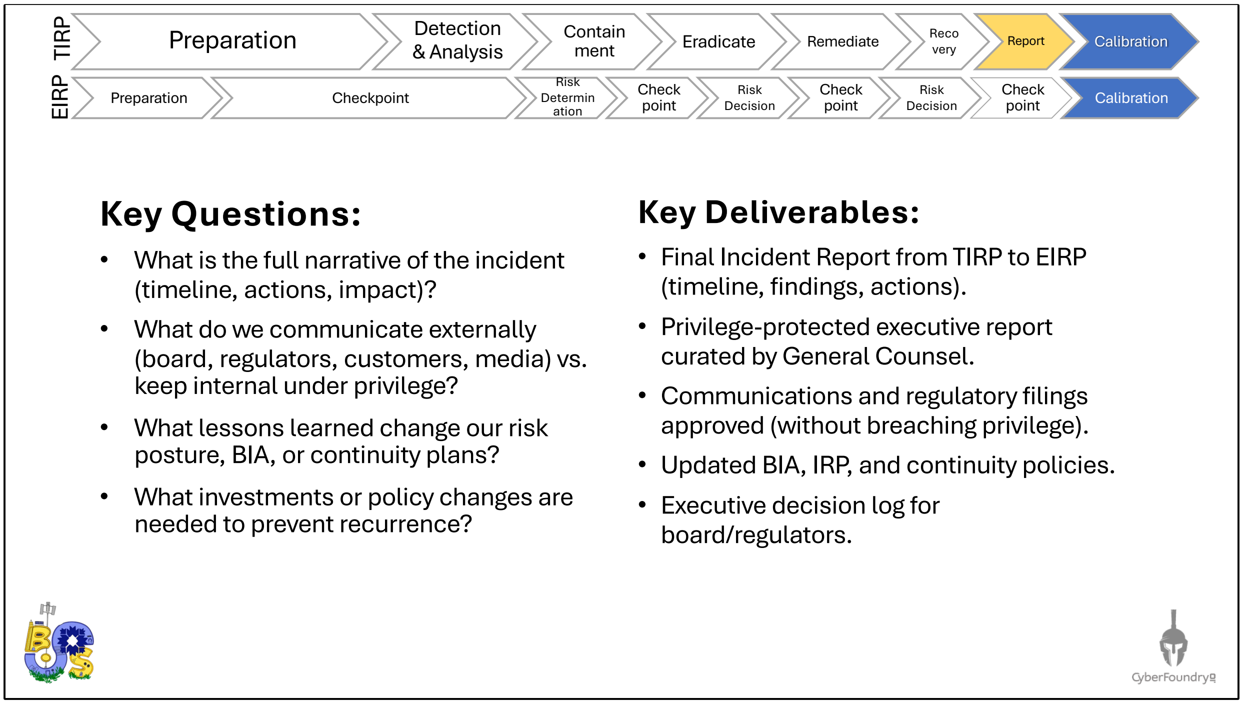
“Is remediation complete, and is the environment ready to recover?”
Answer: TIRP reports on patches, rebuilds, hardening, and validation testing.
Output: Execs confirm confidence in remediation, with GC noting any compliance caveats.

“Which systems must come back first to support the business?”
Answer: Business units provide recovery priority (e.g., ERP > MES > CRM > email).
Output: Tiered recovery plan, documented and approved by EIRP.

“Are we comfortable leaving some systems offline longer to reduce residual risk?”
Answer: TIRP identifies any “at-risk” systems, BU leaders weigh operational need vs. exposure.
Output: Decision to defer some recoveries; acceptance of continuity workarounds.

“What risk level are we accepting by resuming operations now?”
Answer: IC and risk team brief execs on residual risk register. Execs set tolerance.
Output: Documented executive acceptance of risk to resume business.

“What message do we send as systems come back online?”
Answer: Comms team drafts internal and external messaging; GC approves for compliance.
Output: Recovery communications package released at launch.



TIRP: Preparation → Detection & Analysis → Contain ment → Eradicate → Remediate → Reco very → Report → Calibration

EIRP: Preparation → Checkpoint → Risk Determin ation → Check point → Risk Decision → Check point → Risk Decision → Check point → Calibration

Key Questions:

- What is the full narrative of the incident (timeline, actions, impact)?
- What do we communicate externally (board, regulators, customers, media) vs. keep internal under privilege?
- What lessons learned change our risk posture, BIA, or continuity plans?
- What investments or policy changes are needed to prevent recurrence?

Key Deliverables:

- Final Incident Report from TIRP to EIRP (timeline, findings, actions).
- Privilege-protected executive report curated by General Counsel.
- Communications and regulatory filings approved (without breaching privilege).
- Updated BIA, IRP, and continuity policies.
- Executive decision log for board/regulators.

This is the last checkpoint of the incident, where the TIRP formally presents its report to the executive IRP. The job here is twofold: to capture what happened, and to calibrate the business for the future.

The technical team provides a detailed timeline of events, actions taken, and the outcomes. But before any of that information leaves this room, the General Counsel steps in. Their role is critical: to ensure that reports going outward don't waive attorney–client privilege, and that we aren't disclosing more than we are legally required to. Sometimes less is more.

From there, executives decide what lessons to capture. Did our risk appetite prove accurate? Do we need to update our Business Impact Analysis? Are new investments required in detection, backups, or compliance posture? These are the calibration points that strengthen us for the next incident.

The deliverables are clear: a final privileged report for leadership, curated external communications and filings, and an updated playbook that reflects what we've learned. This is where we demonstrate to the board, regulators, and our employees that we not only survived the incident but are stronger and better prepared because of it.

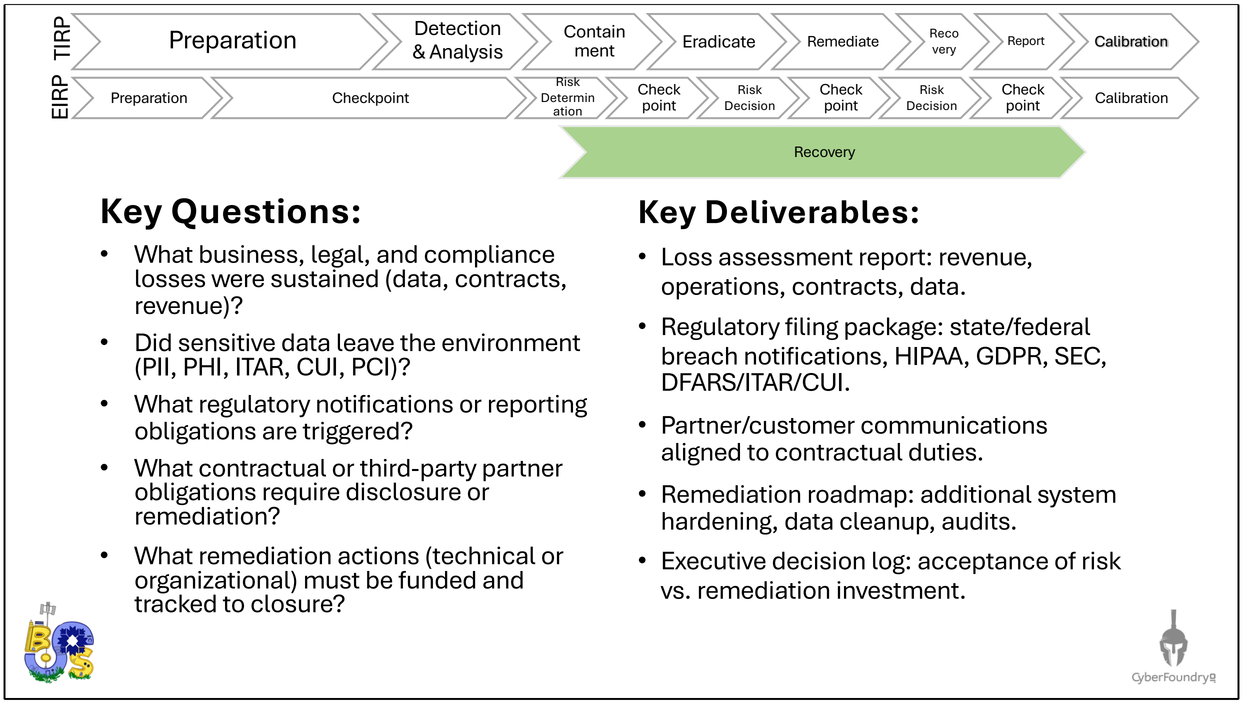
“What actually happened, from start to finish?”
Answer: TIRP presents a full timeline of detection, containment, eradication, and recovery.
Output: Factual record of the incident, handed to GC for legal review.

“What can safely be communicated outward?”
Answer: GC filters content through attorney–client privilege, removes sensitive detail, aligns with regulatory disclosure obligations.
Output: Two streams of reporting — privileged internal report vs. approved external disclosures.

“What lessons learned must be incorporated into our governance?”
Answer: BU leaders, IT, and IC highlight weaknesses (controls, processes, communication).
Output: List of required improvements, mapped to owners and deadlines.

“What is our new risk posture after this?”
Answer: Exec sponsor and risk/finance weigh cost of downtime vs. mitigation investments.
Output: Adjusted risk appetite statement, approved funding for improvements, updated continuity targets.

“How do we close the loop with the board and regulators?”
Answer: GC + Comms finalize formal filings, briefings, and reports.
Output: Finalized compliance communications plan; assurance that privileged and sensitive info remains protected.



TIRP: Preparation | Detection & Analysis | Contain ment | Eradicate | Remediate | Reco very | Report | Calibration

EIRP: Preparation | Checkpoint | Risk Determin ation | Check point | Risk Decision | Check point | Risk Decision | Check point | Calibration

Recovery

Key Questions:

- What business, legal, and compliance losses were sustained (data, contracts, revenue)?
- Did sensitive data leave the environment (PII, PHI, ITAR, CUI, PCI)?
- What regulatory notifications or reporting obligations are triggered?
- What contractual or third-party partner obligations require disclosure or remediation?
- What remediation actions (technical or organizational) must be funded and tracked to closure?

Key Deliverables:

- Loss assessment report: revenue, operations, contracts, data.
- Regulatory filing package: state/federal breach notifications, HIPAA, GDPR, SEC, DFARS/ITAR/CUI.
- Partner/customer communications aligned to contractual duties.
- Remediation roadmap: additional system hardening, data cleanup, audits.
- Executive decision log: acceptance of risk vs. remediation investment.

CyberFoundry

Even after operations are restored, the real work for executives often begins. Recovery in the EIRP sense is not just about turning the plant back on — it's about identifying and owning the losses, complying with regulatory obligations, and ensuring long-term remediation.

The first step is loss identification. We need a clear assessment of what was lost: production, revenue, customer orders, intellectual property. Just as important, did regulated data leave our environment — PII, PHI, PCI, ITAR, or CUI? Each of these triggers specific reporting duties.

The General Counsel leads here, translating forensic evidence into regulatory obligations. If PHI was lost, HIPAA requires patient notification within 60 days. If ITAR or CUI data was exposed, the DoD requires reporting within 72 hours. If the incident is material to our investors, the SEC requires disclosure in 4 business days. State AG laws and GDPR can be even tighter.

We also need to consider contractual obligations to customers, suppliers, and insurers. Some partners require notification within 24 hours. Cyber insurance often requires immediate engagement or claims may be denied.

From there, we shift to remediation. That means not just patching but cleaning up compromised accounts, re-baselining systems, tightening contracts, and in some cases funding new projects to ensure compliance. The EIRP owns approving those investments.

The deliverables here are a loss assessment, a regulatory and contractual reporting package, a communications plan, and a funded remediation roadmap. This closes the loop and positions the business not just to resume but to recover trust and compliance."

"What exactly did we lose?"
Answer: BU leaders + finance quantify lost production, missed shipments, revenue hits; IT/forensics confirm if regulated data was exfiltrated.
Output: Loss matrix (operational, financial, legal, reputational) validated at the exec level.

"Did regulated or sensitive data leave the environment?"
Answer: Forensics + SOC provide exfil evidence; GC confirms definitions (PII, PHI, PCI, ITAR, CUI).
Output: Data loss classification, tied directly to specific regulatory frameworks.

"Which regulatory regimes require reporting, and on what timeline?"
Answer: GC/Risk map data loss against obligations:
HIPAA breach notifications (60 days).
GDPR/UK DPA (72 hours).
SEC cyber incident disclosure (material within 4 business days).
State AG notification laws.
DoD DFARS/ITAR/CUI reporting to DIBNet/DC3 (72 hours).
Output: Regulatory reporting plan, deadlines tracked, owners assigned.

"Do we have third-party or customer disclosure requirements?"
Answer: BU + Legal review SLAs, supply chain contracts, cyber insurance conditions.
Output: Disclosure matrix, aligning customers/partners/insurers to obligations.

"What remediation actions must we take to restore compliance and resilience?"
Answer: IT/Business propose cleanup (credential resets, audit of privileged accounts, purge of compromised data sets, endpoint re-baselining).
Risk/Finance align budget.
Output: Post-incident remediation roadmap with clear funding and timelines.

“What narrative do we provide to stakeholders?”
Answer: Comms + GC draft messages; exec sponsor approves.
Output: Transparent but privilege-protected messaging for board, regulators, customers, employees.

What is a Tabletop Exercise

A Good Tabletop Exercise…

Step-by-Step simulation of a cybersecurity incident with technical and leadership staff.

Tests the plan, roles and decision-making process.

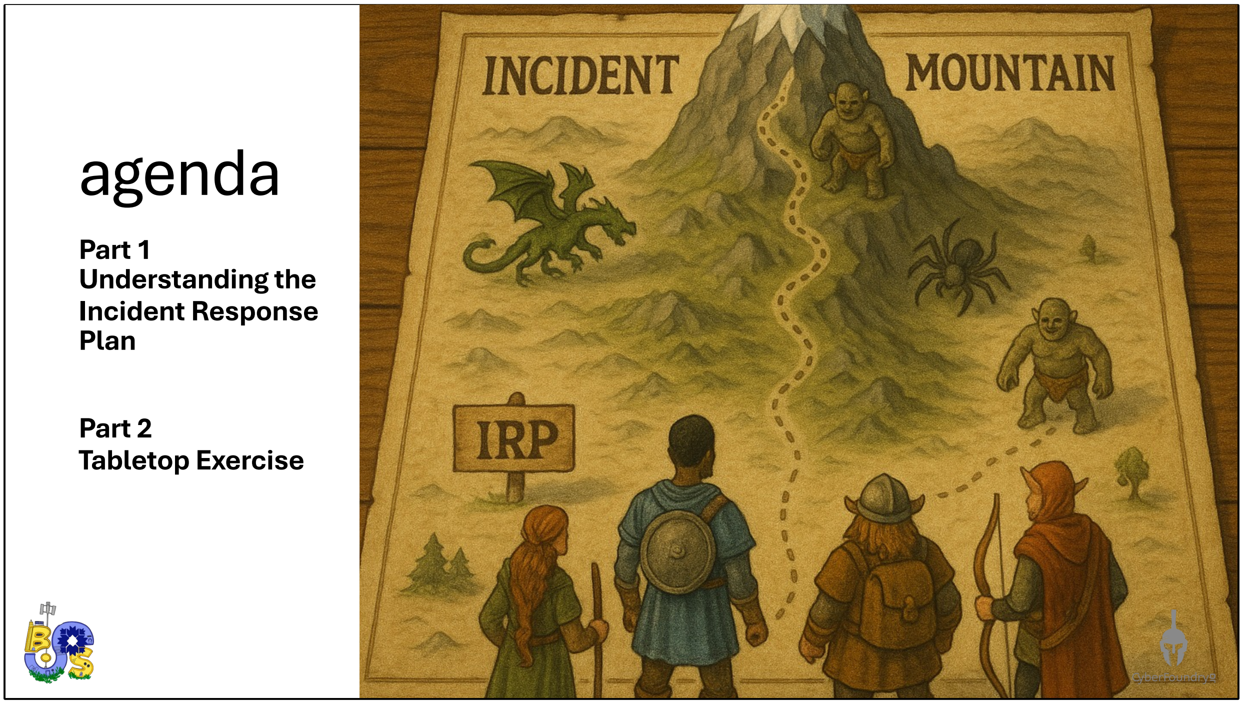
Identifies gaps in process, communication, and coordination before a real event occurs.

This is not a Threat Hunting Exercise

Tabletop Exercise

120 minutes at max.

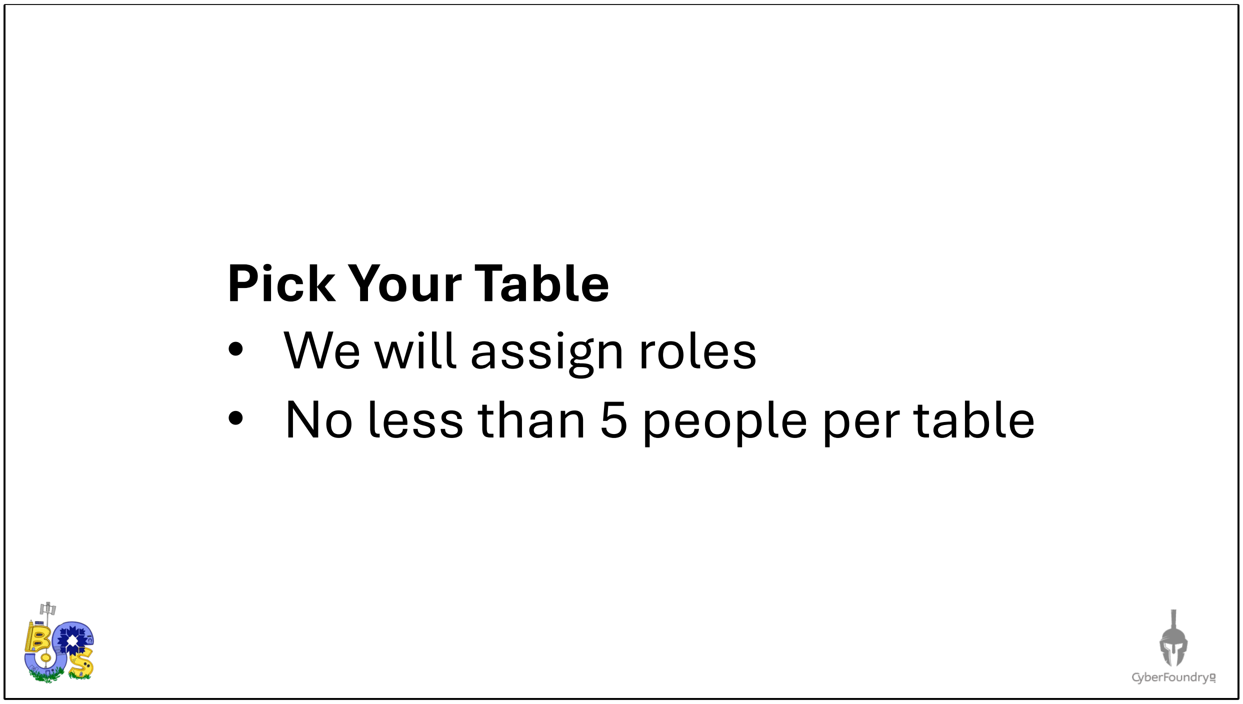
Lets break for Lunch and then do one.



agenda

Part 1
Understanding the Incident Response Plan

Part 2
Tabletop Exercise

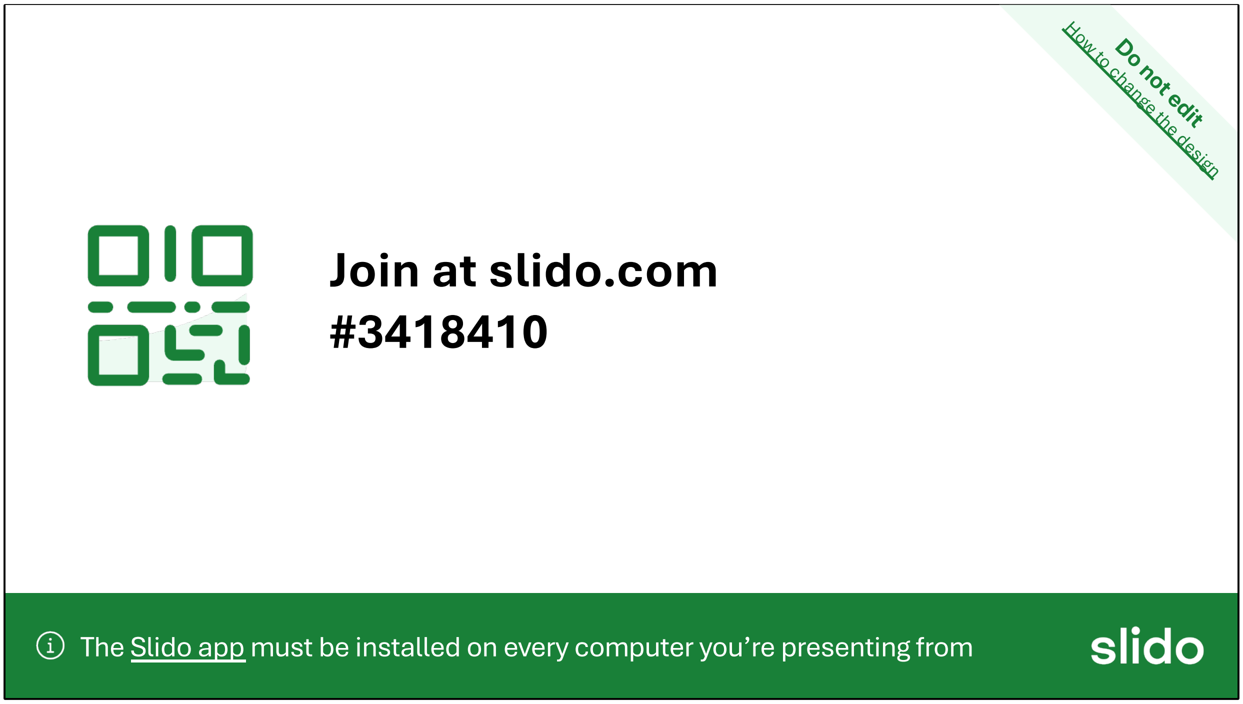


Pick Your Table

- We will assign roles
- No less than 5 people per table

Part 2

Tabletop Exercise



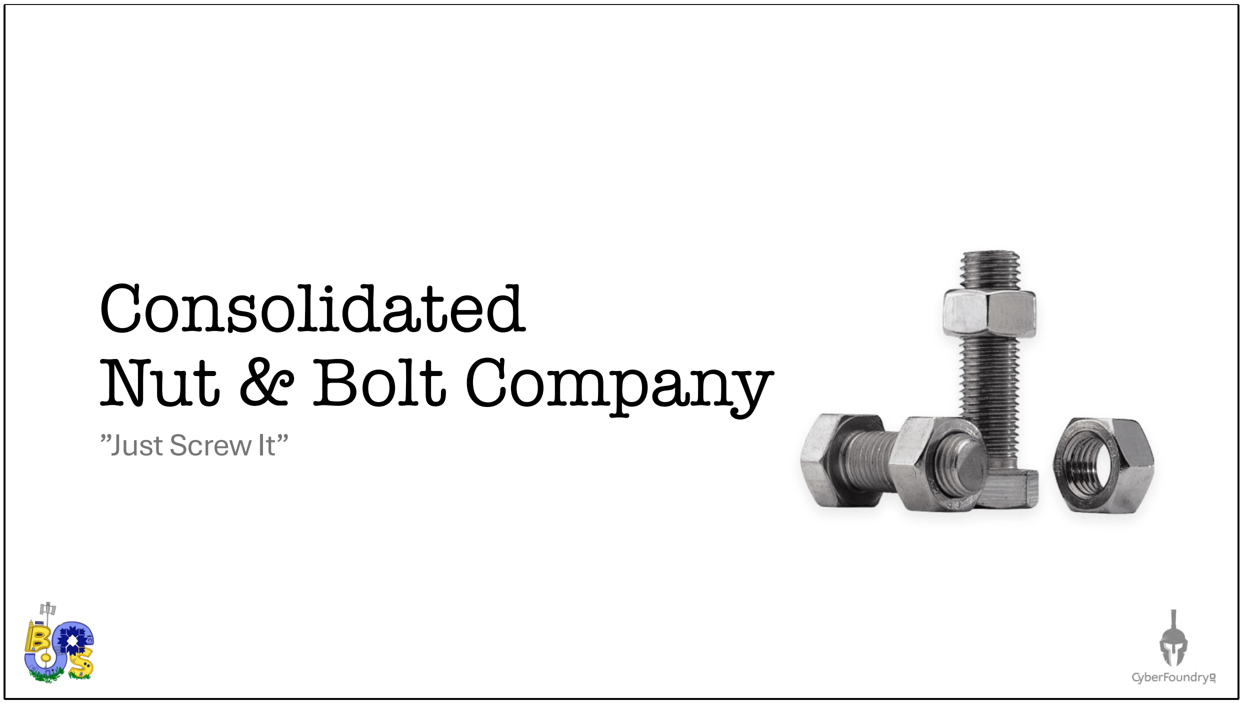
Do not edit

How to change the design

Join at slido.com
#3418410

ⓘ The Slido app must be installed on every computer you’re presenting from

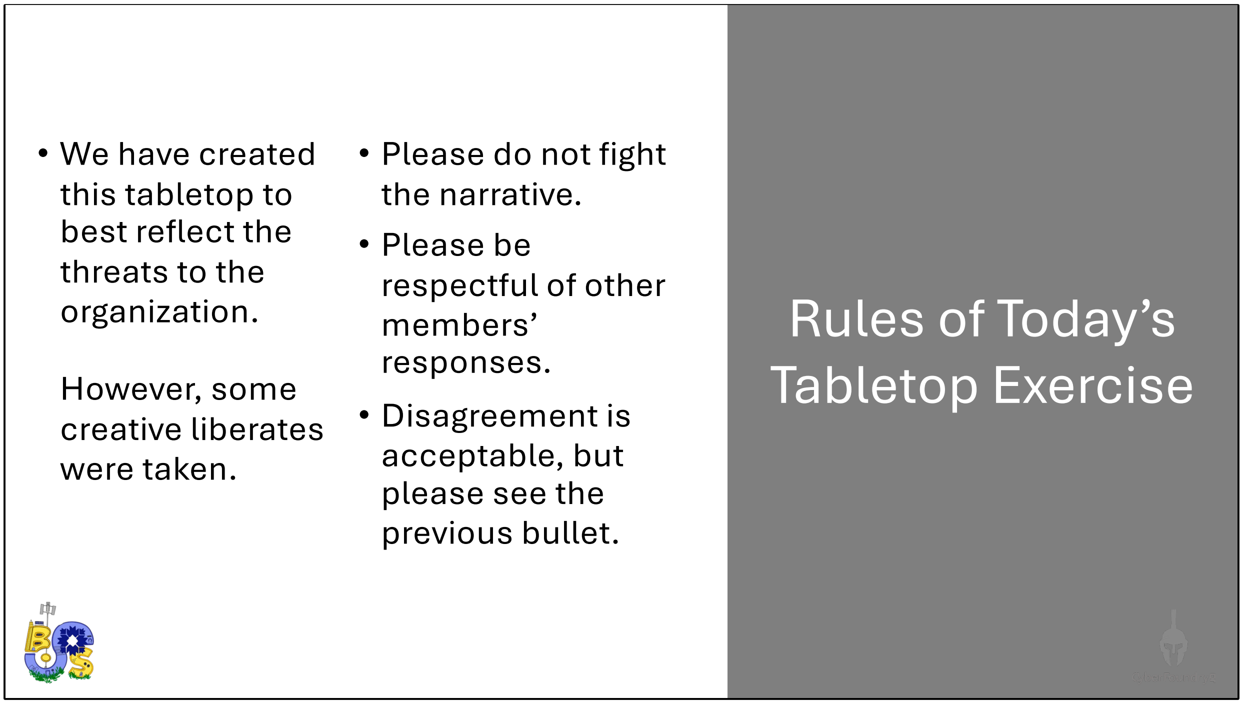
slido



Consolidated Nut & Bolt Company

"Just Screw It"

CyberFoundry

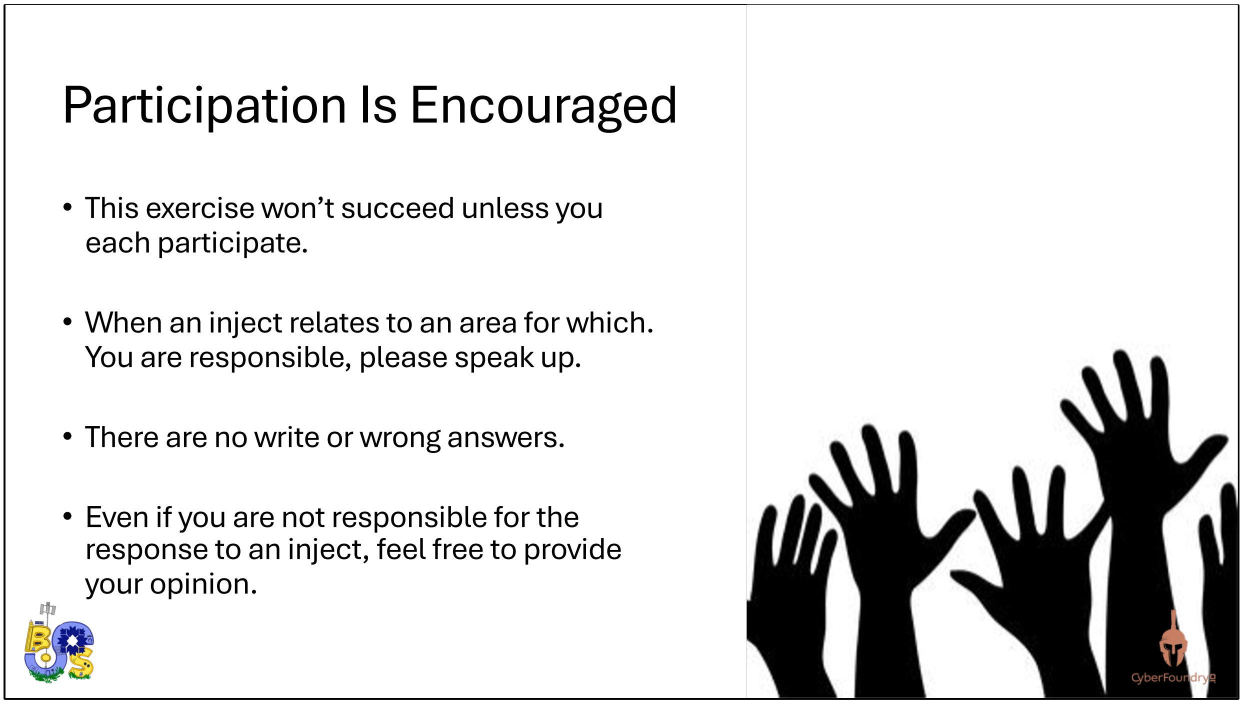


Rules of Today's Tabletop Exercise

- We have created this tabletop to best reflect the threats to the organization.

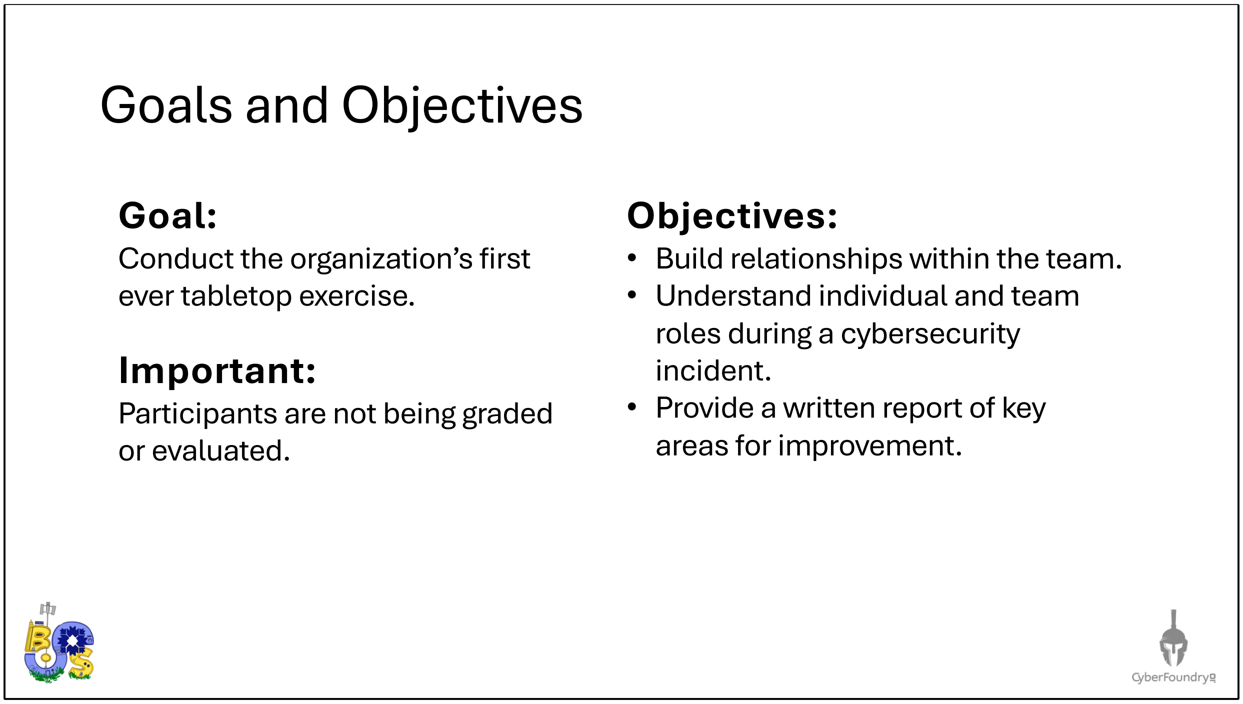
  However, some creative liberates were taken.

- Please do not fight the narrative.
- Please be respectful of other members' responses.
- Disagreement is acceptable, but please see the previous bullet.



Participation Is Encouraged

- This exercise won’t succeed unless you each participate.
- When an inject relates to an area for which. You are responsible, please speak up.
- There are no write or wrong answers.
- Even if you are not responsible for the response to an inject, feel free to provide your opinion.



Goals and Objectives

Goal:

Conduct the organization’s first ever tabletop exercise.

Important:

Participants are not being graded or evaluated.

Objectives:

- Build relationships within the team.
- Understand individual and team roles during a cybersecurity incident.
- Provide a written report of key areas for improvement.

CyberFoundry

Consolidated Nut & Bolt Company

“Just Screw It”

Founded in 1954 in Gary, Indiana — family-owned turned global supplier
Specializes in **industrial fasteners**: screws, bolts, washers, and custom fittings
Plants across the Midwest serving automotive, aerospace, and heavy manufacturing
Known for **reliability, volume production, and down-to-earth culture**

Current challenge: aging infrastructure and outdated OT systems leave operations **vulnerable to cyber disruption**

CyberFoundry

Choose Your Adventure

CISO Incident Commander

1 Person

SOC Incident Response Team

2+ People

Information Technology Tea

2+ People

Executive Sponsor

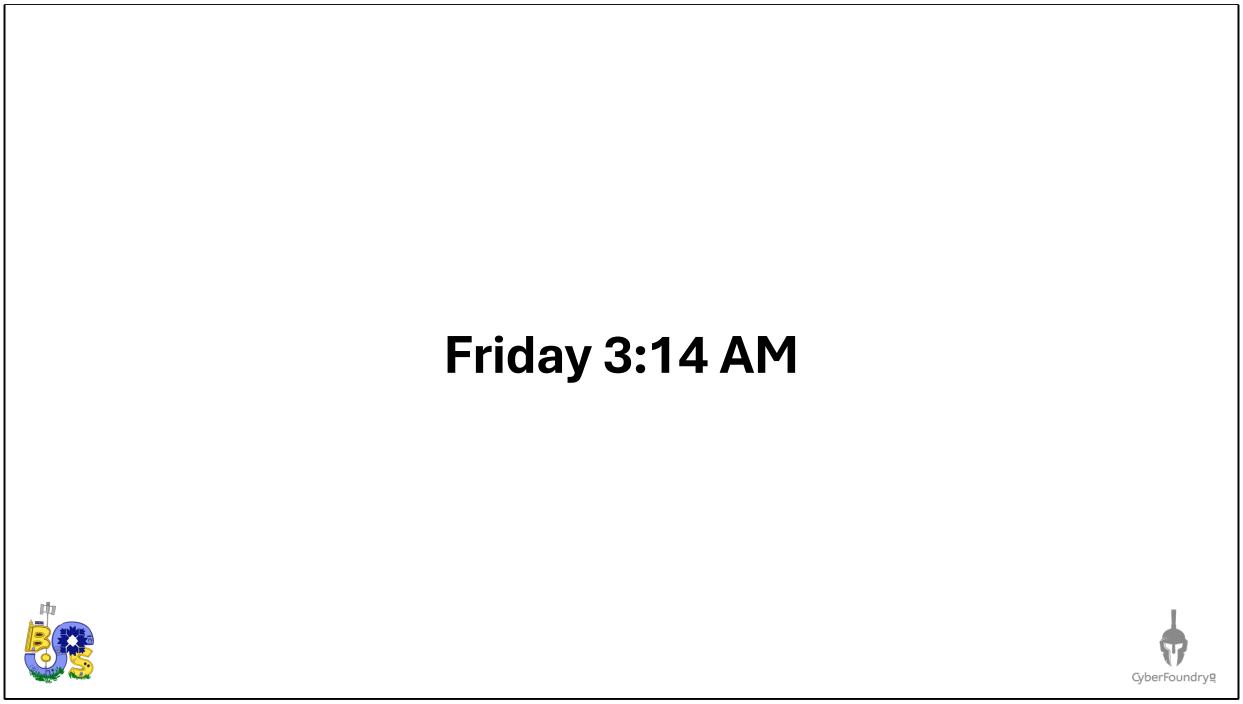
1 Person

General Council

1 Person

Reporting Out

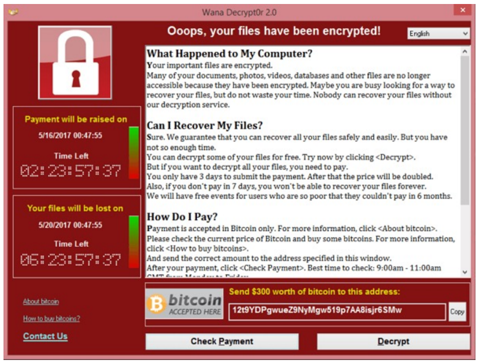
CyberFoundry



Friday 3:14 AM

TIRP

Preparation | **Detection & Analysis** | Contain | Eradicate | Remediate | Recover | Report | Calibration



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

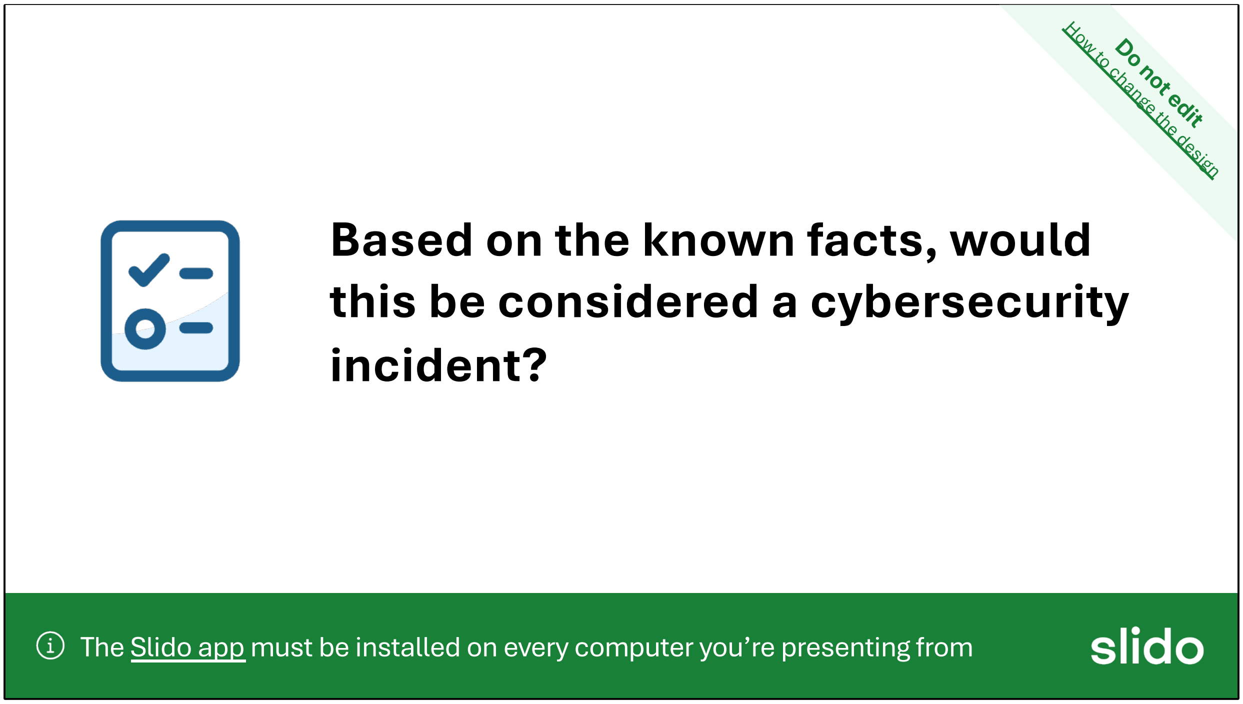
TIRP INJECT 1

Friday 3:14AM – IT Help Desk

Calls the CISO and says “The factory shut down about an hour ago. The computers all have this message on their screen. Something about being encrypted.

…so we called you. Can you fix it?”

CyberFoundry



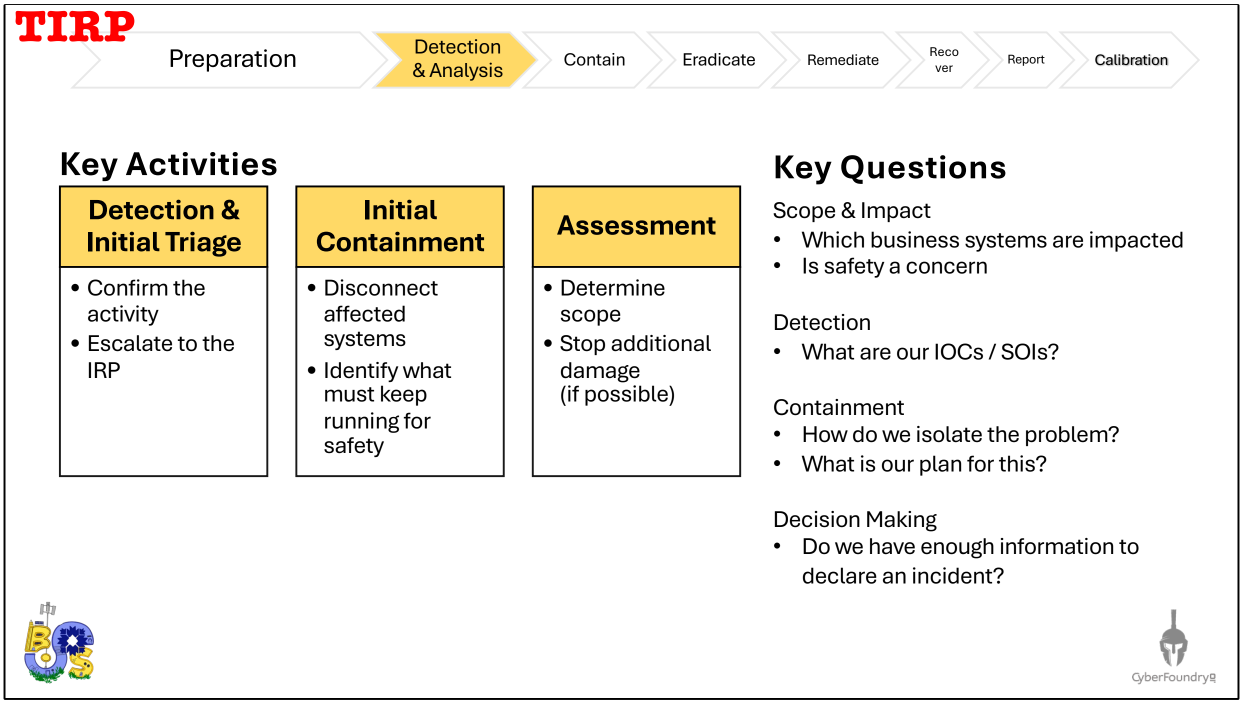
Do not edit

How to change the design

Based on the known facts, would this be considered a cybersecurity incident?

ⓘ The Slido app must be installed on every computer you're presenting from

slido



TIRP

Preparation → Detection & Analysis → Contain → Eradicate → Remediate → Recover → Report → Calibration

Key Activities

Detection & Initial Triage

- Confirm the activity
- Escalate to the IRP

Initial Containment

- Disconnect affected systems
- Identify what must keep running for safety

Assessment

- Determine scope
- Stop additional damage (if possible)

Key Questions

Scope & Impact

- Which business systems are impacted
- Is safety a concern

Detection

- What are our IOCs / SOIs?

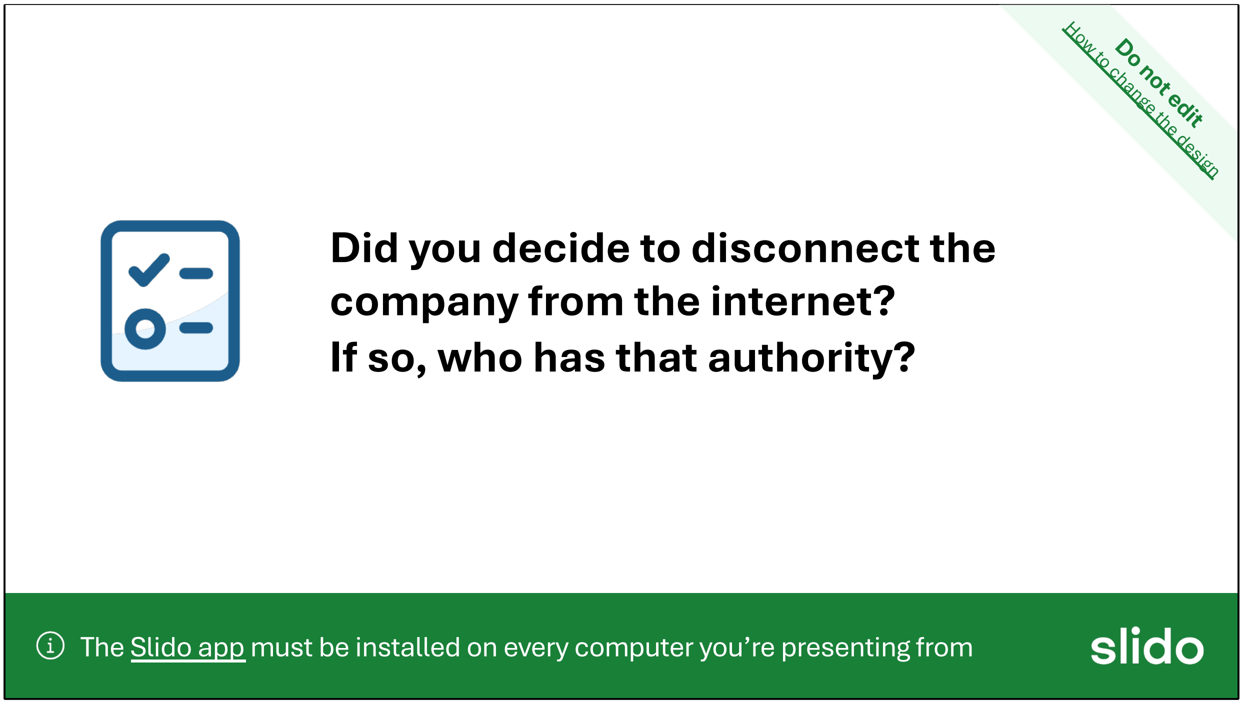
Containment

- How do we isolate the problem?
- What is our plan for this?

Decision Making

- Do we have enough information to declare an incident?

CyberFoundry



Do not edit

How to change the design

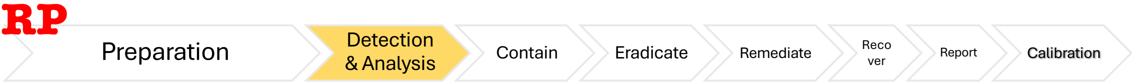
Did you decide to disconnect the company from the internet?
If so, who has that authority?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Friday 4:27 AM

TIRP



Preparation

Detection & Analysis

Contain

Eradicate

Remediate

Reco ver

Report

Calibration

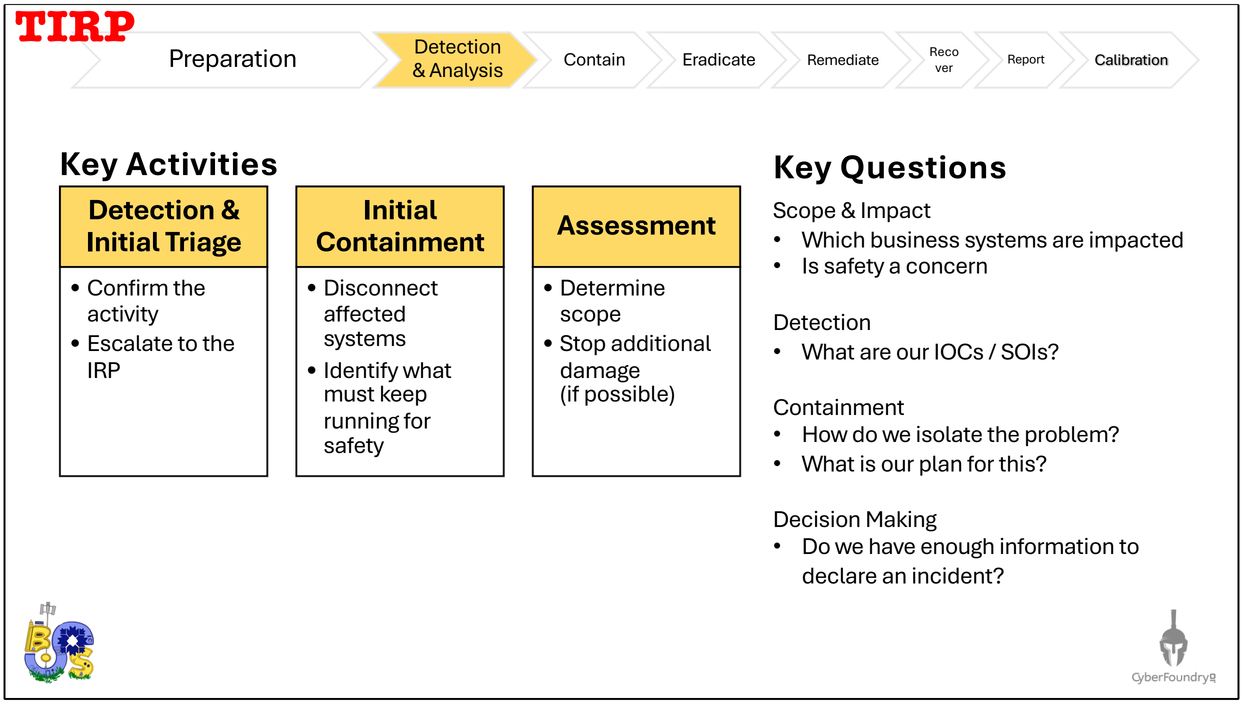
TIRP INJECT 2

Friday 4:27AM – War Room

IRT has identified the process that is running on the infected machines and why it wasn't detected earlier. They have what they believe to be an effective Indicator of Compromise (IOC) and have started scanning for it across the enterprise.

TOOLS:
EDR, SIEM

CyberFoundry



TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Reco ver | Report | Calibration

Key Activities

Detection & Initial Triage

- Confirm the activity
- Escalate to the IRP

Initial Containment

- Disconnect affected systems
- Identify what must keep running for safety

Assessment

- Determine scope
- Stop additional damage (if possible)

Key Questions

Scope & Impact

- Which business systems are impacted
- Is safety a concern

Detection

- What are our IOCs / SOIs?

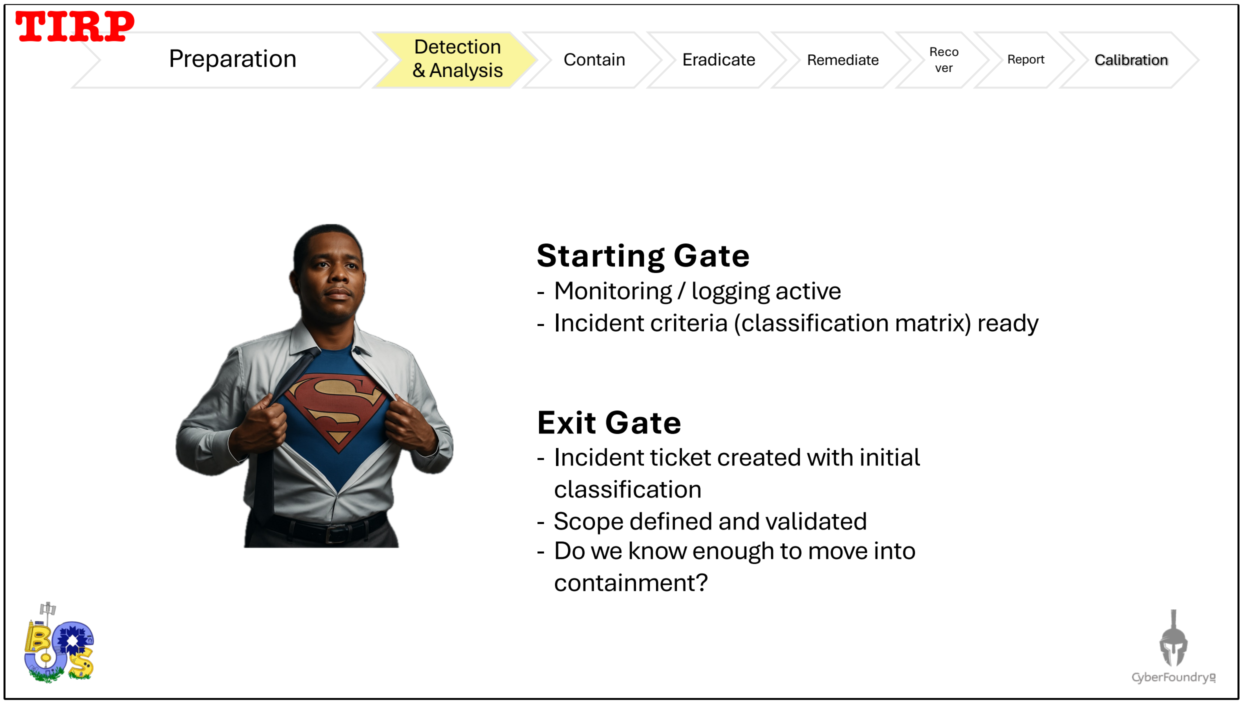
Containment

- How do we isolate the problem?
- What is our plan for this?

Decision Making

- Do we have enough information to declare an incident?

CyberFoundry



TIRP

Preparation → Detection & Analysis → Contain → Eradicate → Remediate → Reco ver → Report → Calibration

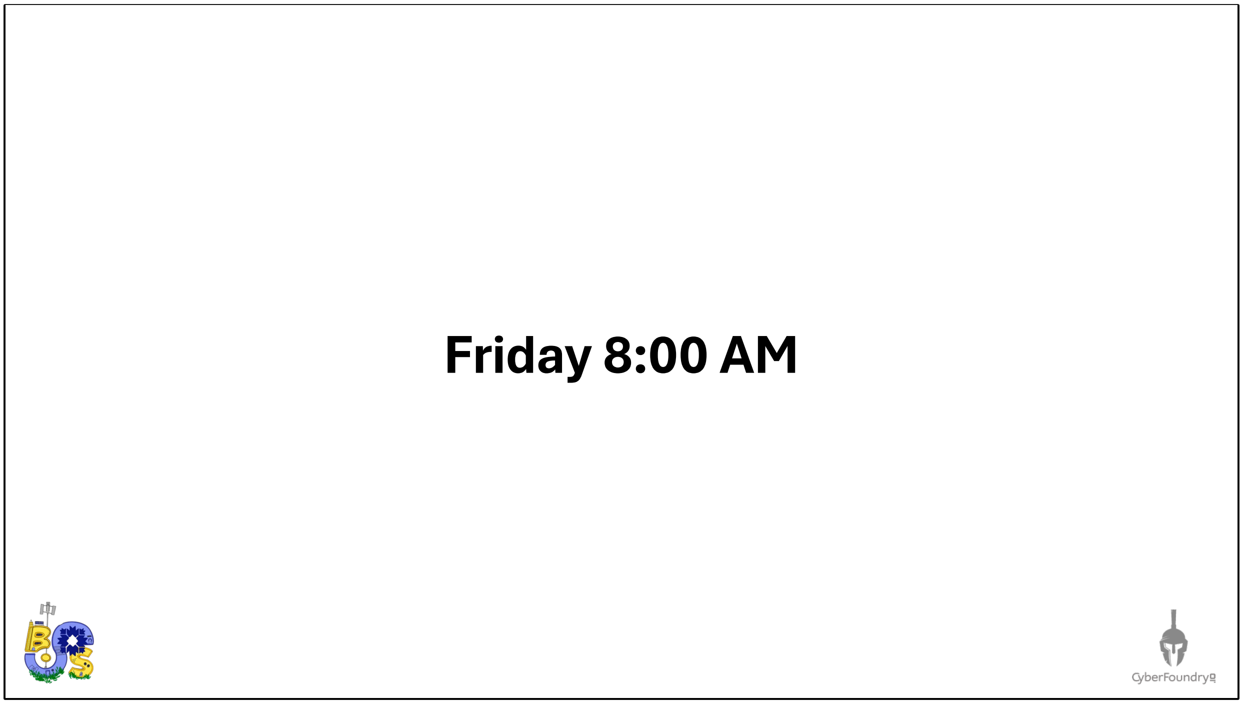
Starting Gate

- Monitoring / logging active
- Incident criteria (classification matrix) ready

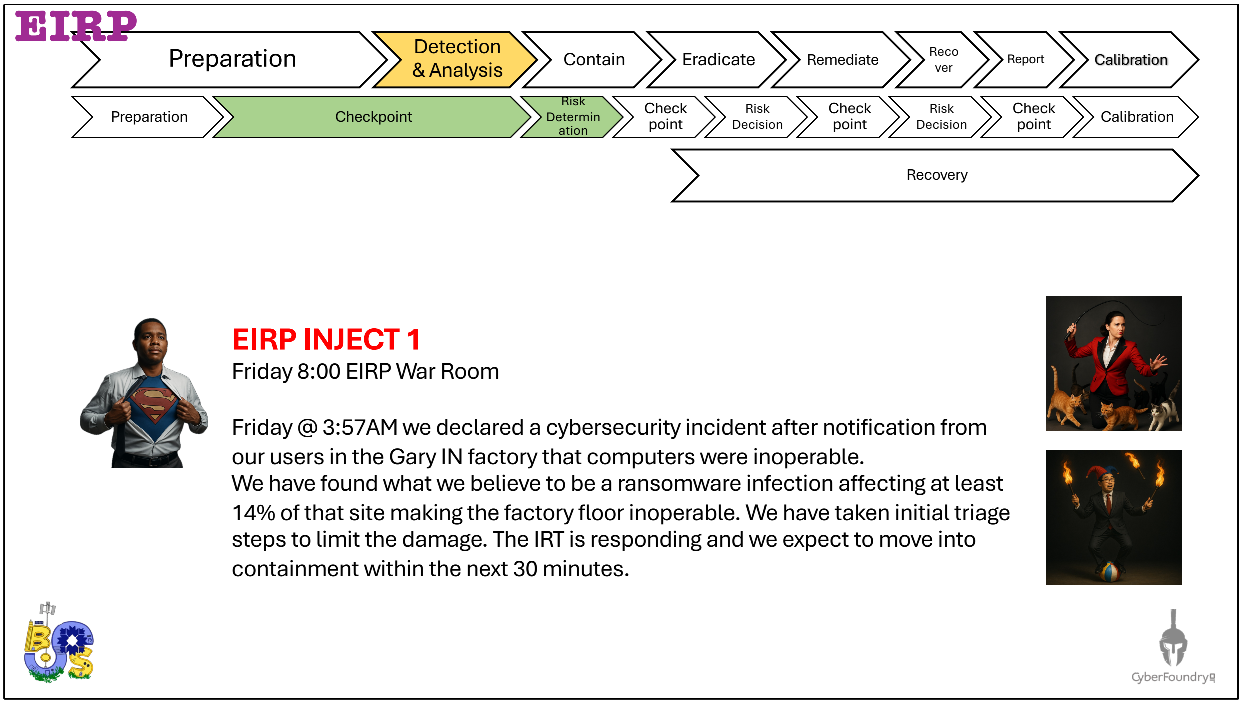
Exit Gate

- Incident ticket created with initial classification
- Scope defined and validated
- Do we know enough to move into containment?

CyberFoundry



Friday 8:00 AM



EIRP

Preparation → Detection & Analysis → Contain → Eradicate → Remediate → Reco ver → Report → Calibration

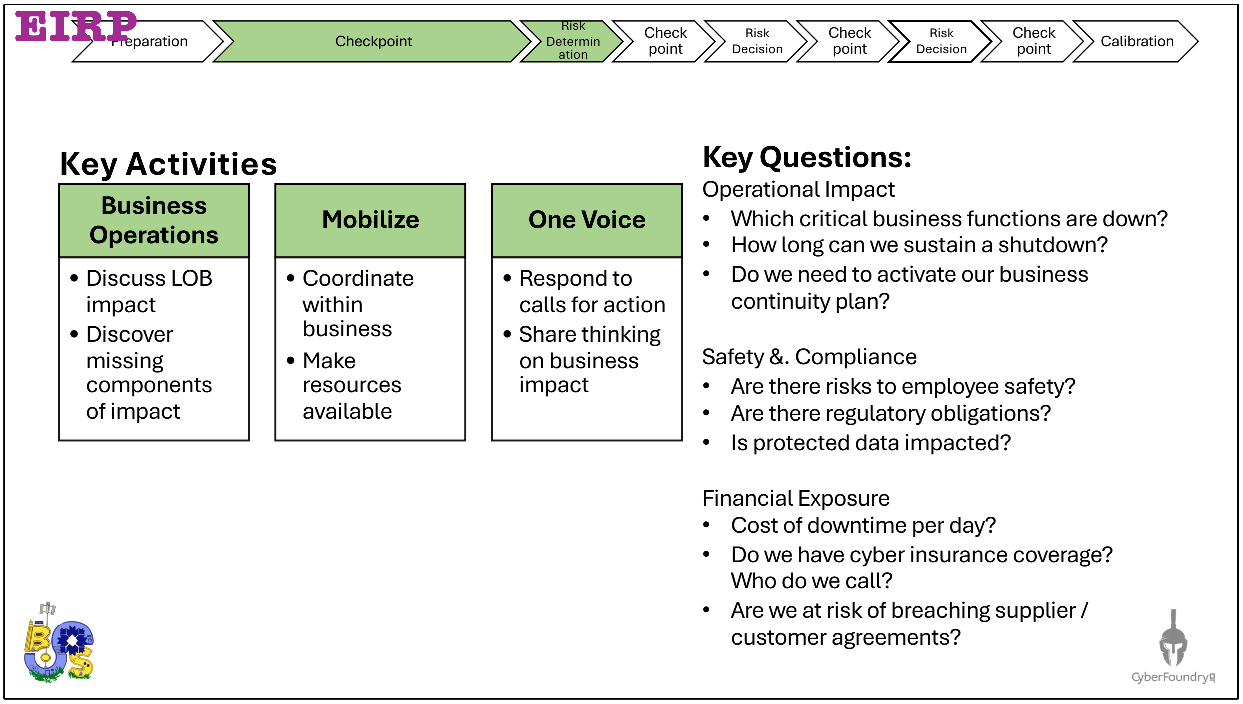
Preparation → Checkpoint → Risk Determin ation → Check point → Risk Decision → Check point → Risk Decision → Check point → Calibration

Recovery

EIRP INJECT 1

Friday 8:00 EIRP War Room

Friday @ 3:57AM we declared a cybersecurity incident after notification from our users in the Gary IN factory that computers were inoperable.
We have found what we believe to be a ransomware infection affecting at least 14% of that site making the factory floor inoperable. We have taken initial triage steps to limit the damage. The IRT is responding and we expect to move into containment within the next 30 minutes.


EIRP
Preparation
Checkpoint
Risk Determin ation
Check point
Risk Decision
Check point
Risk Decision
Check point
Calibration

Key Activities

Business Operations	Mobilize	One Voice
• Discuss LOB impact • Discover missing components of impact	• Coordinate within business • Make resources available	• Respond to calls for action • Share thinking on business impact

Key Questions:

Operational Impact

- Which critical business functions are down?
- How long can we sustain a shutdown?
- Do we need to activate our business continuity plan?

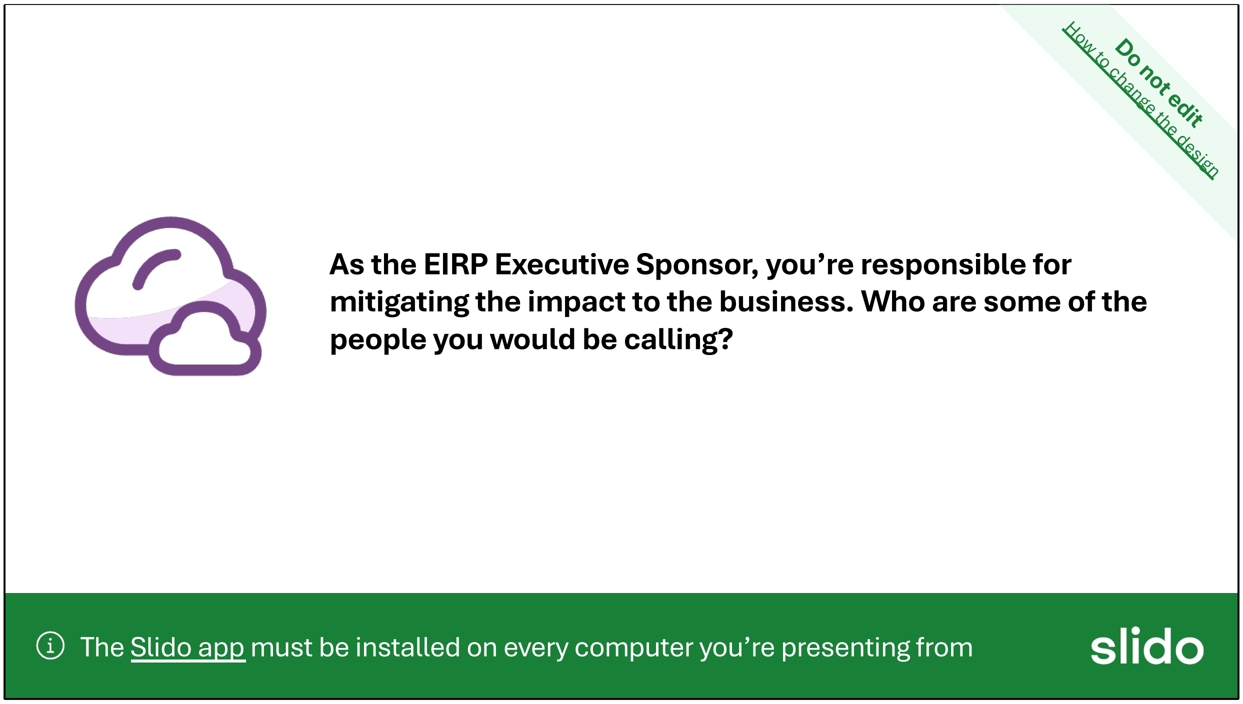
Safety &. Compliance

- Are there risks to employee safety?
- Are there regulatory obligations?
- Is protected data impacted?

Financial Exposure

- Cost of downtime per day?
- Do we have cyber insurance coverage? Who do we call?
- Are we at risk of breaching supplier / customer agreements?

CyberFoundry



Do not edit

How to change the design

As the EIRP Executive Sponsor, you're responsible for mitigating the impact to the business. Who are some of the people you would be calling?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

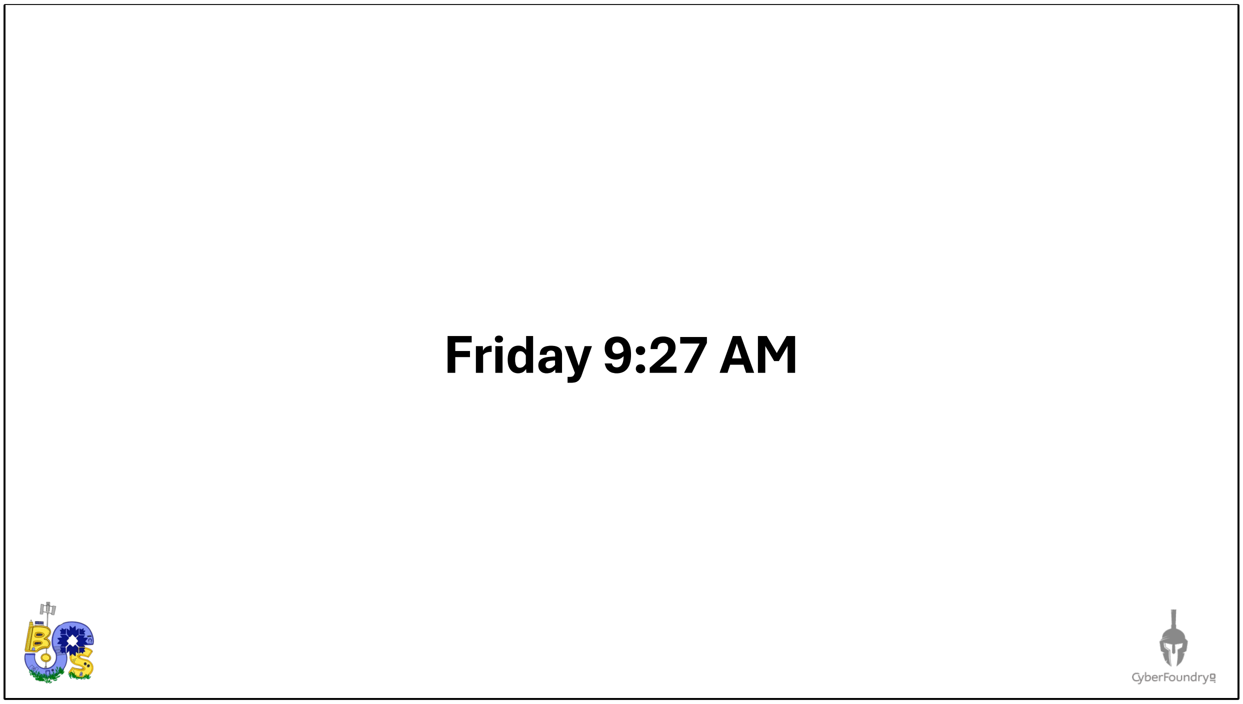
EIRP

Preparation > Checkpoint > Risk Determination > Check point > Risk Decision > Check point > Risk Decision > Check point > Calibration

Executive Sponsor

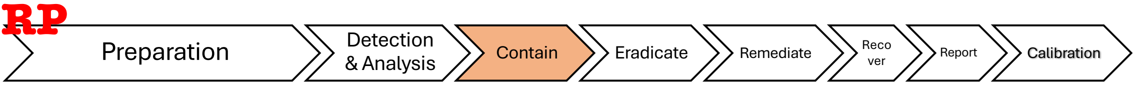
- Who did you call?
- What did you share?
- How does this impact your strategy?

CyberFoundry



Friday 9:27 AM

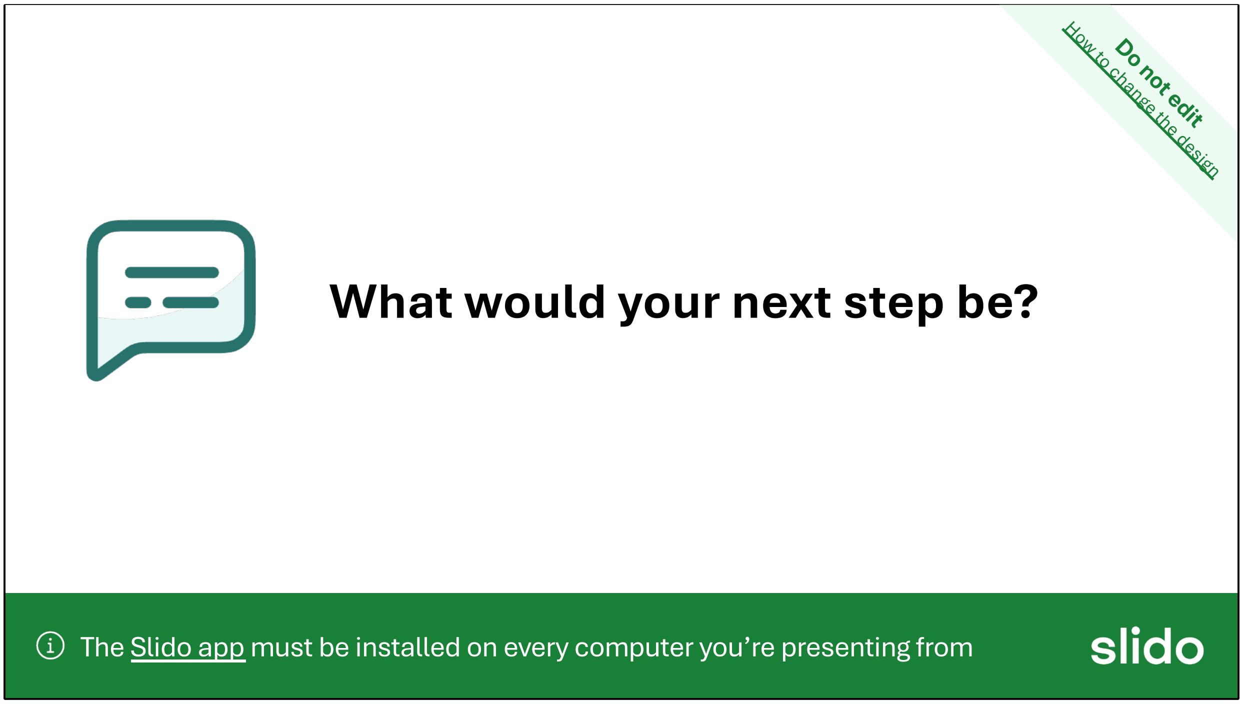
TIRP


Preparation
Detection & Analysis
Contain
Eradicate
Remediate
Reco ver
Report
Calibration

TIRP INJECT 3

Friday 9:27AM – War Room

The IRT reports that they are able to remove the malware now that their tools can see it, but the IT Help Desk keeps opening new tickets for infected machines.



Do not edit

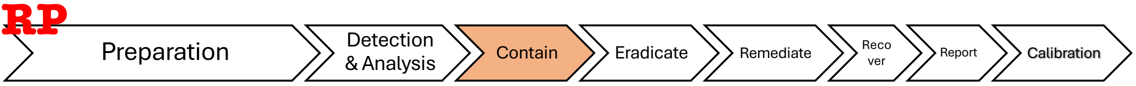
How to change the design

What would your next step be?

ⓘ The Slido app must be installed on every computer you're presenting from

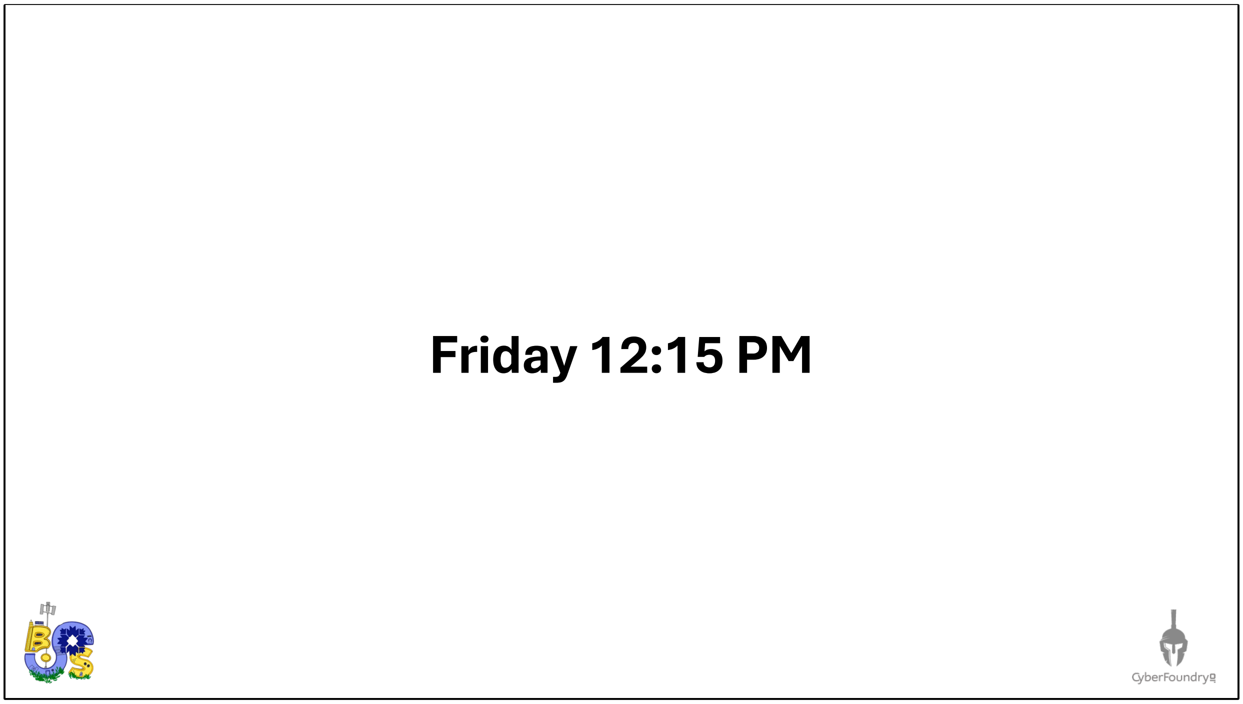
slido

TIRP

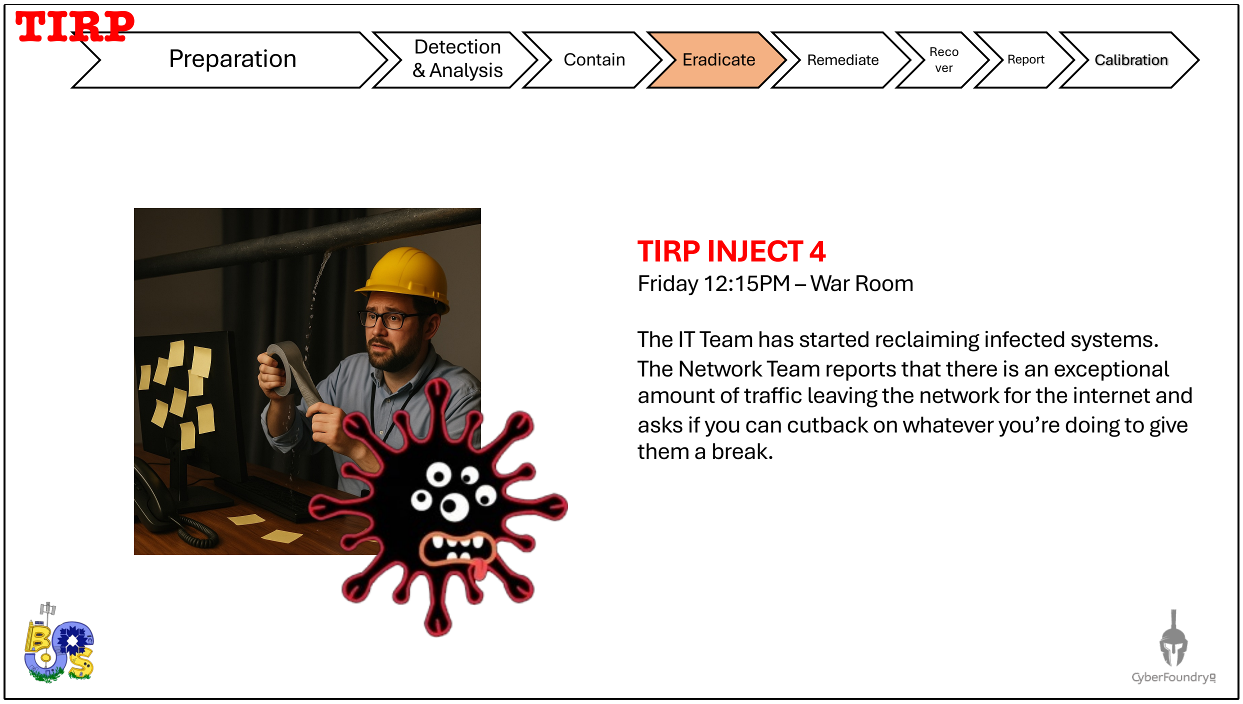

Preparation
Detection & Analysis
Contain
Eradicate
Remediate
Reco ver
Report
Calibration

How ya doing Incident Commander?

- Are you confident in your containment strategy?
- What did you communicate to your EIRP team?



Friday 12:15 PM



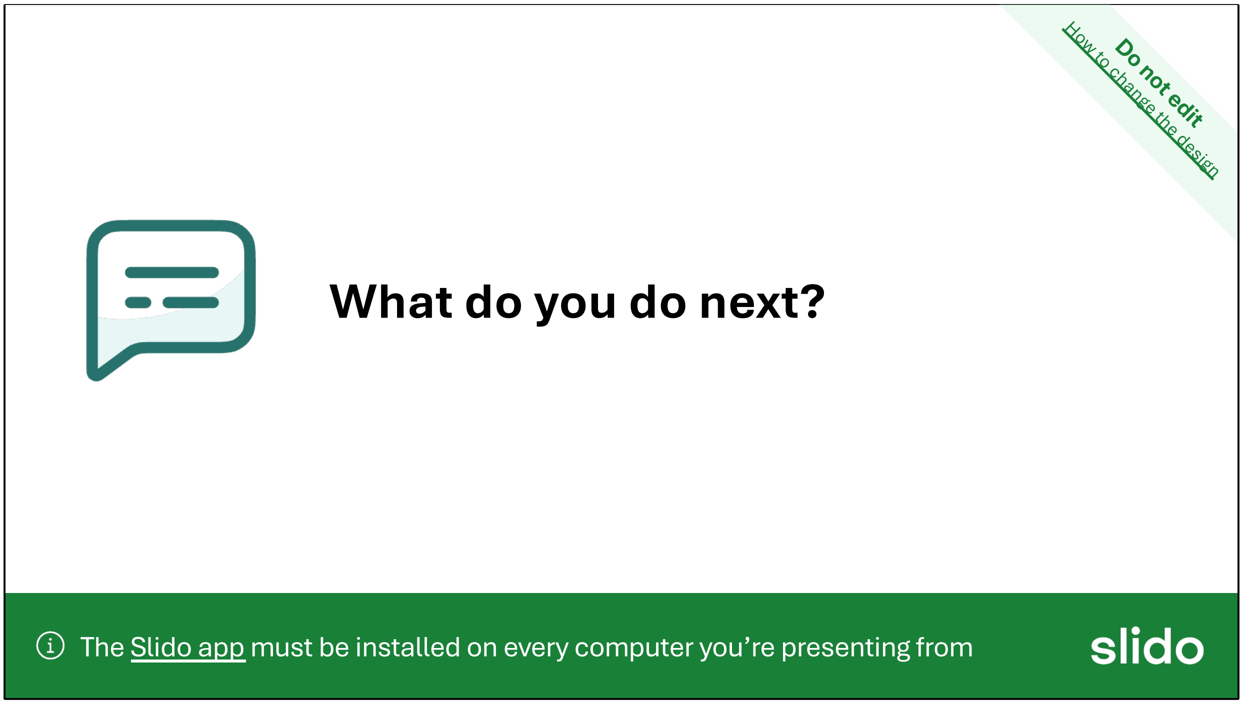
TIRP

Preparation → Detection & Analysis → Contain → Eradicate → Remediate → Reco ver → Report → Calibration

TIRP INJECT 4

Friday 12:15PM – War Room

The IT Team has started reclaiming infected systems. The Network Team reports that there is an exceptional amount of traffic leaving the network for the internet and asks if you can cutback on whatever you're doing to give them a break.

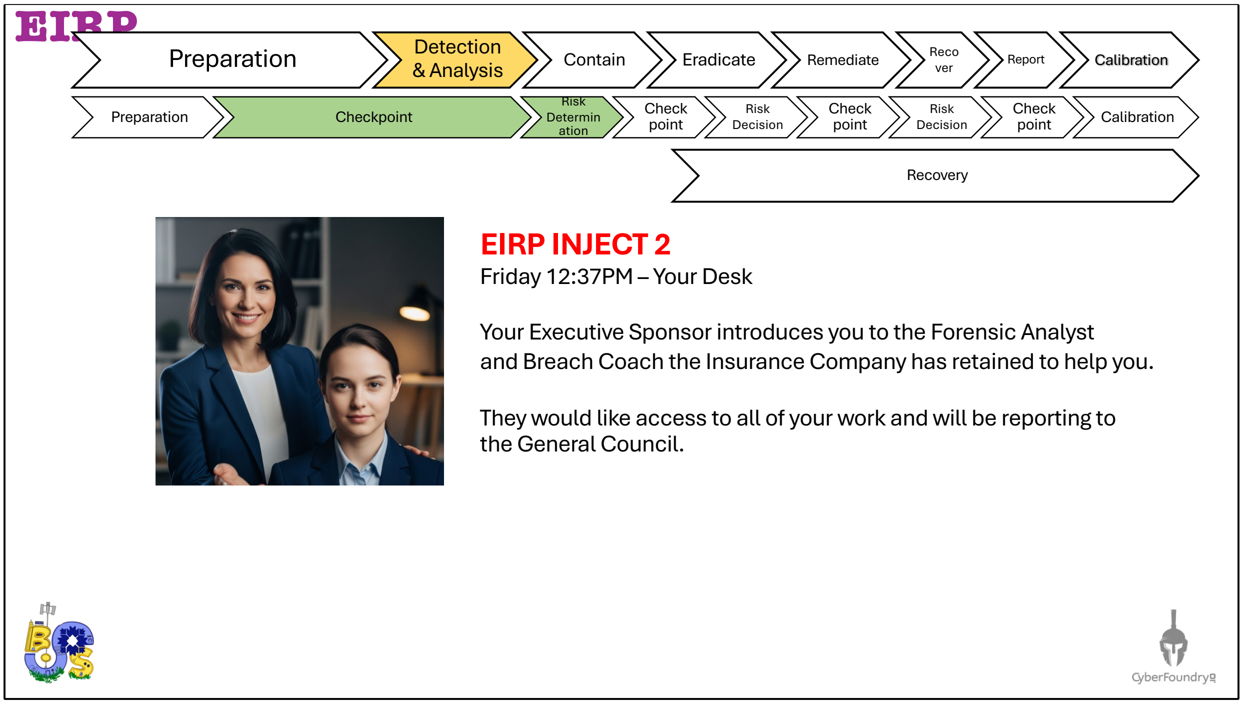


Do not edit

How to change the design

What do you do next?

The Slido app must be installed on every computer you're presenting from



EIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

Preparation | Checkpoint | Risk Determination | Check point | Risk Decision | Check point | Risk Decision | Check point | Calibration

Recovery

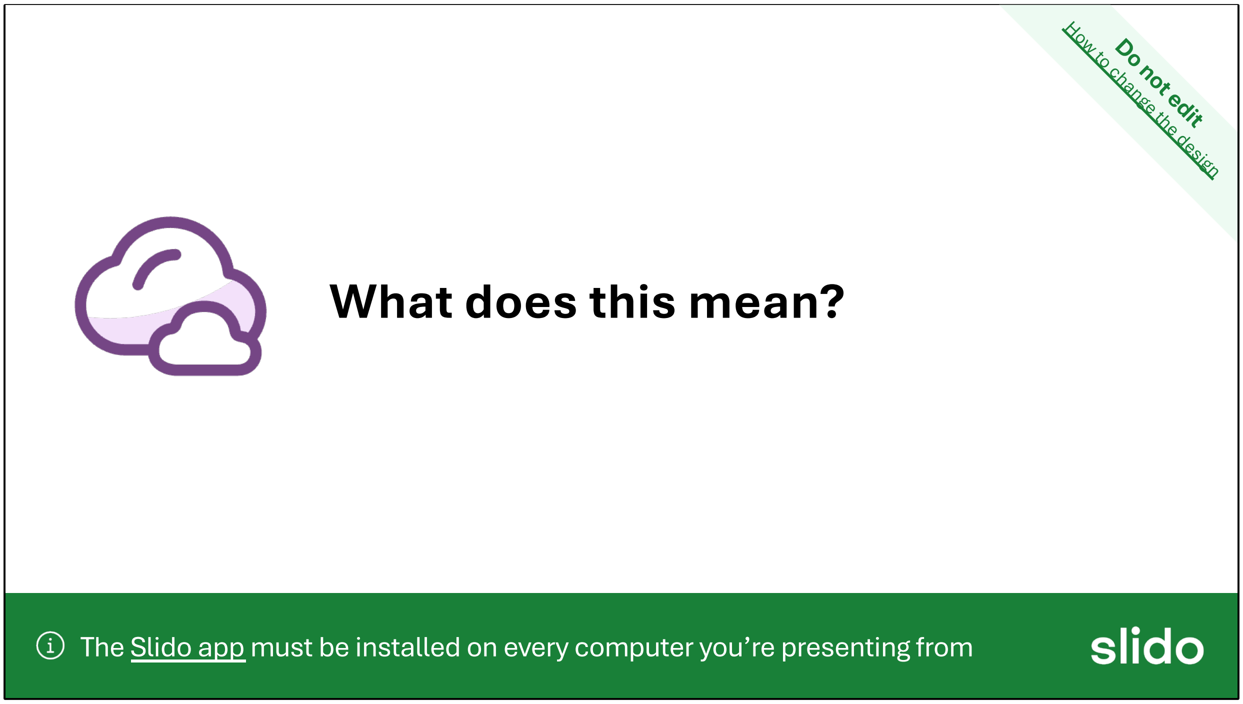
EIRP INJECT 2

Friday 12:37PM – Your Desk

Your Executive Sponsor introduces you to the Forensic Analyst and Breach Coach the Insurance Company has retained to help you.

They would like access to all of your work and will be reporting to the General Council.

CyberFoundry



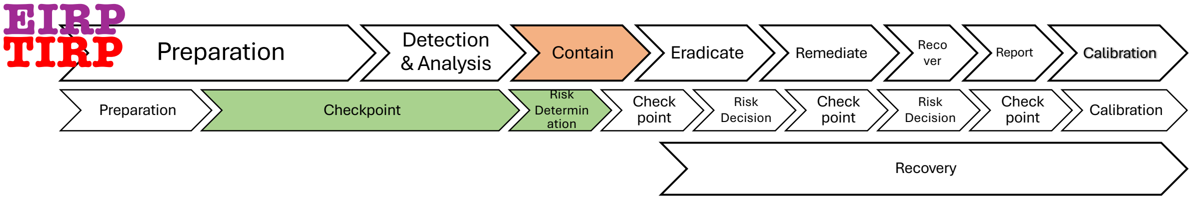
Do not edit

How to change the design

What does this mean?

ⓘ The Slido app must be installed on every computer you're presenting from

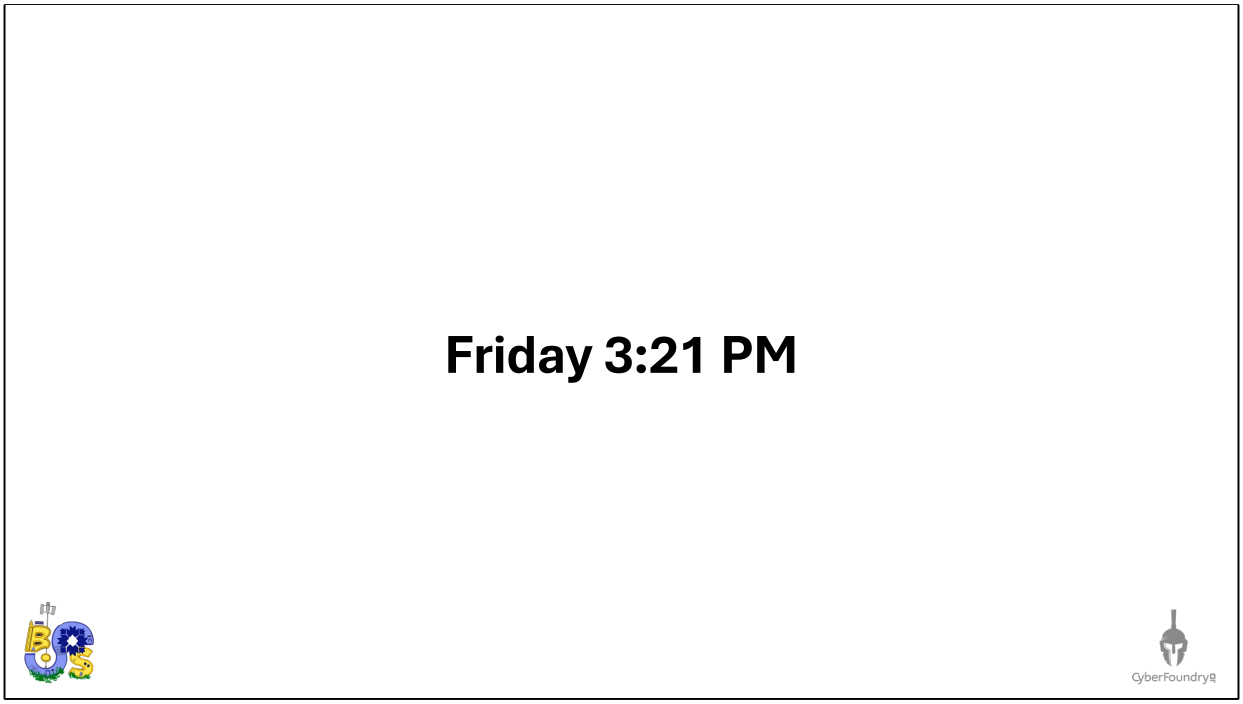
slido



How ya doing Incident Commander?

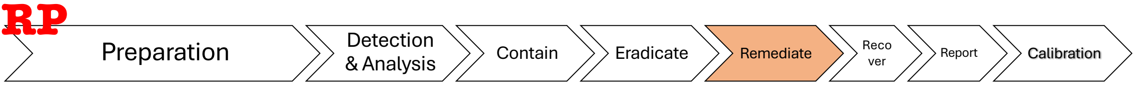
- Are you confident in your eradication strategy?
- What did you communicate to your EIRP team?
- How did you handle the Forensic Analyst from the Insurance Company?

CyberFoundry



Friday 3:21 PM

TIRP

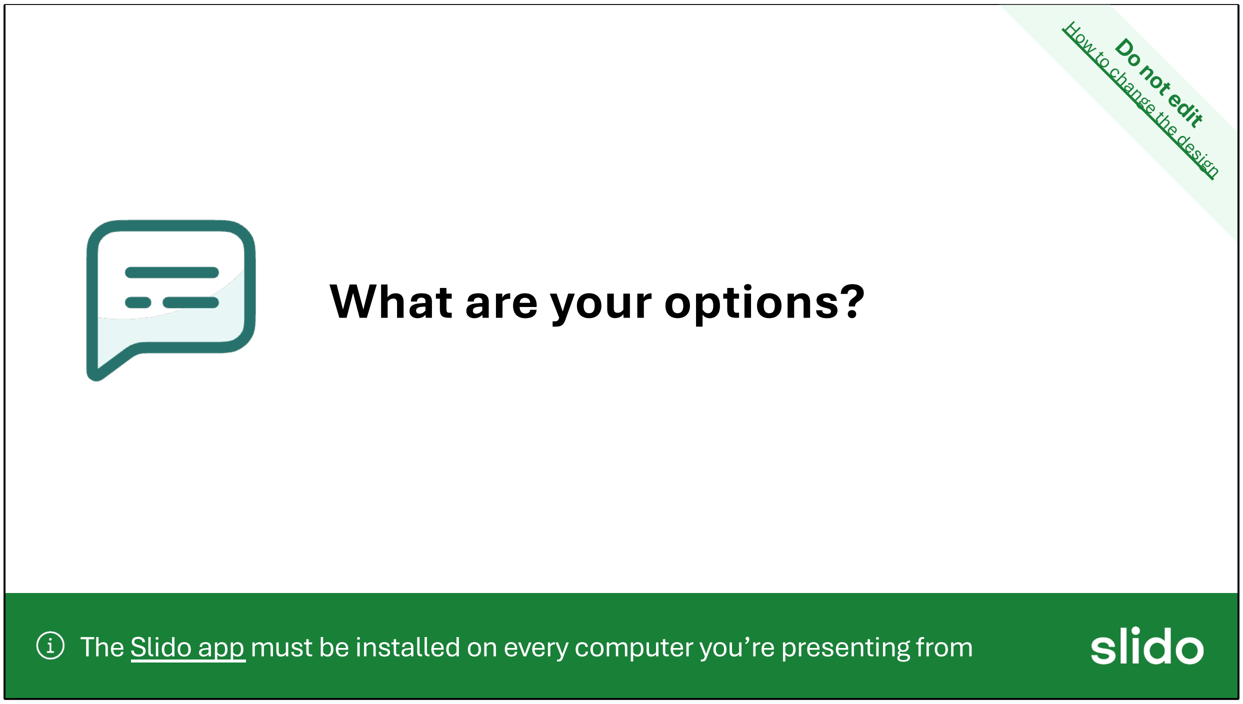


TIRP INJECT 5

Friday 3:21PM – War Room

The SOC found an outdated version of Java running on many of the infected machines and believe it may be the cause of the ransomware's spread across the environment. This is new information.

IT tells you that the specific version of Java they are using is a hard requirement for the ERP system and that updating it will break the business.



Do not edit

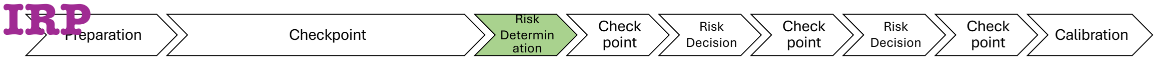
How to change the design

What are your options?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

EIRP



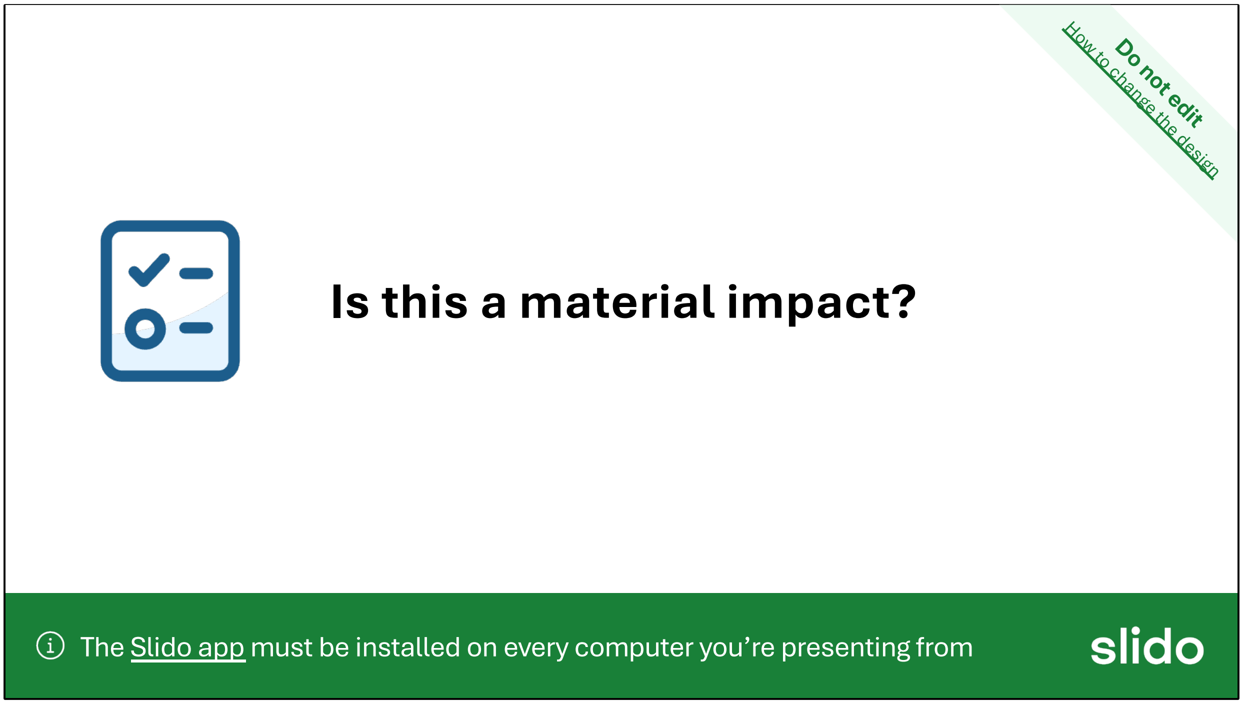
EIRP INJECT 3

Friday 4:12PM – Your Desk

Your General Council reminds you that the company has 48 hours to report any material losses to the SEC, and even less time to call your customer if there was a material breach of your protected information.

The network team analysis shows that significant information was exfiltrated over the last 48 hours.

CyberFoundry



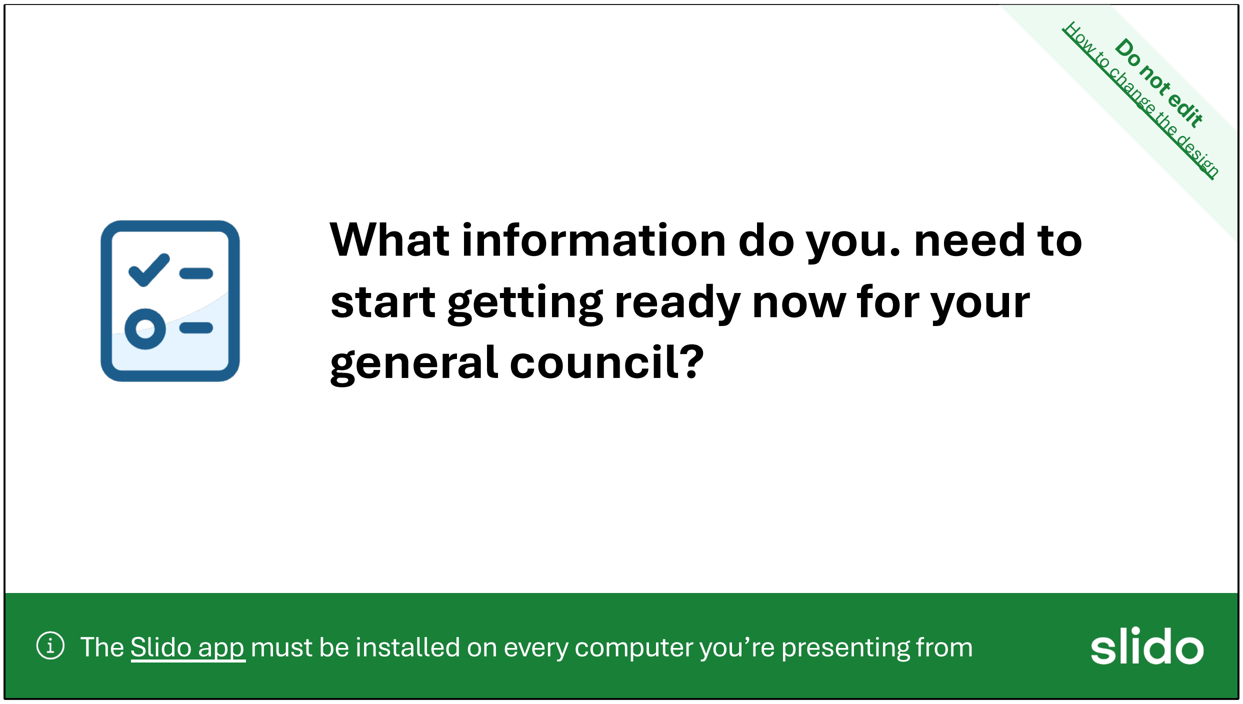
Do not edit

How to change the design

Is this a material impact?

ⓘ The Slido app must be installed on every computer you're presenting from

slido



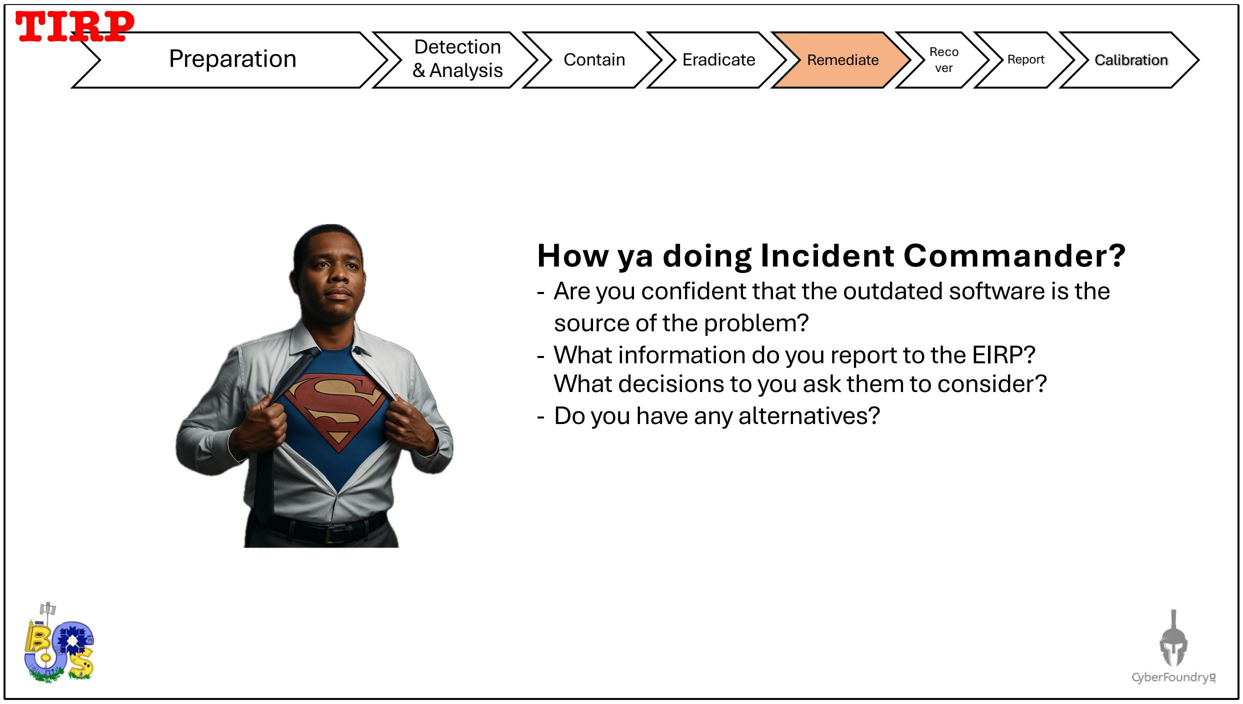
Do not edit

How to change the design

What information do you. need to start getting ready now for your general council?

ⓘ The Slido app must be installed on every computer you’re presenting from

slido



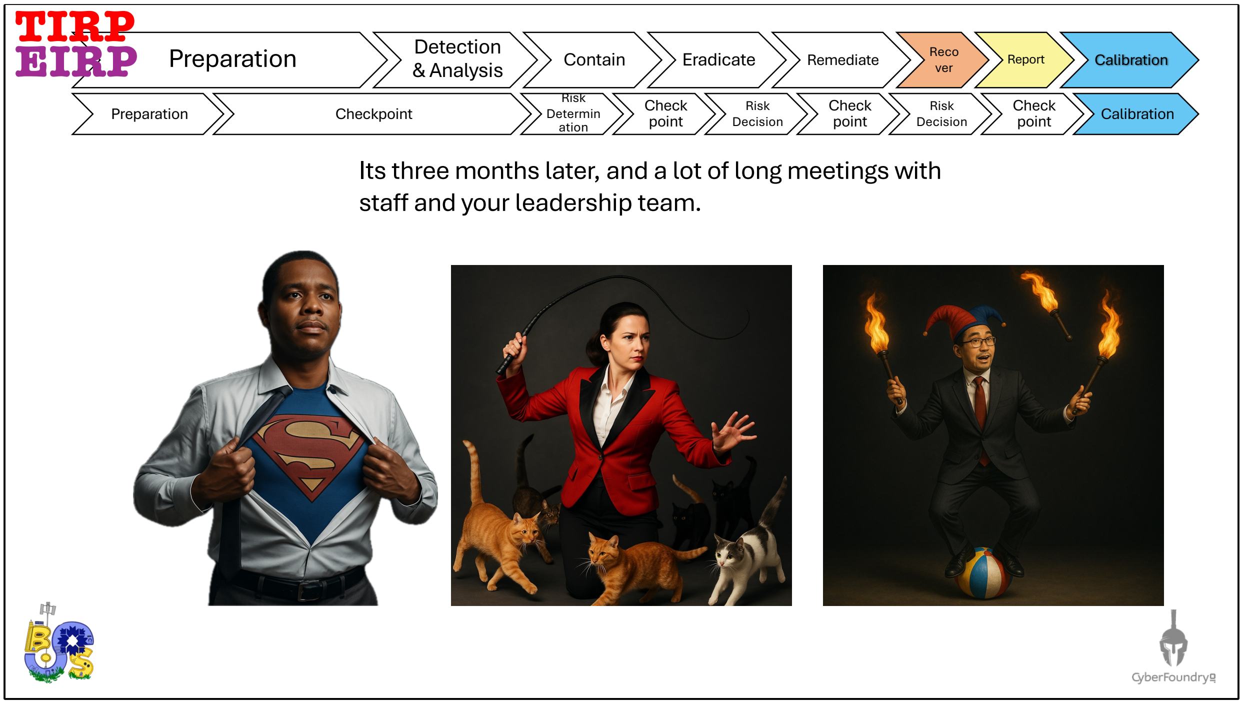
TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Reco ver | Report | Calibration

How ya doing Incident Commander?

- Are you confident that the outdated software is the source of the problem?
- What information do you report to the EIRP? What decisions to you ask them to consider?
- Do you have any alternatives?

CyberFoundry

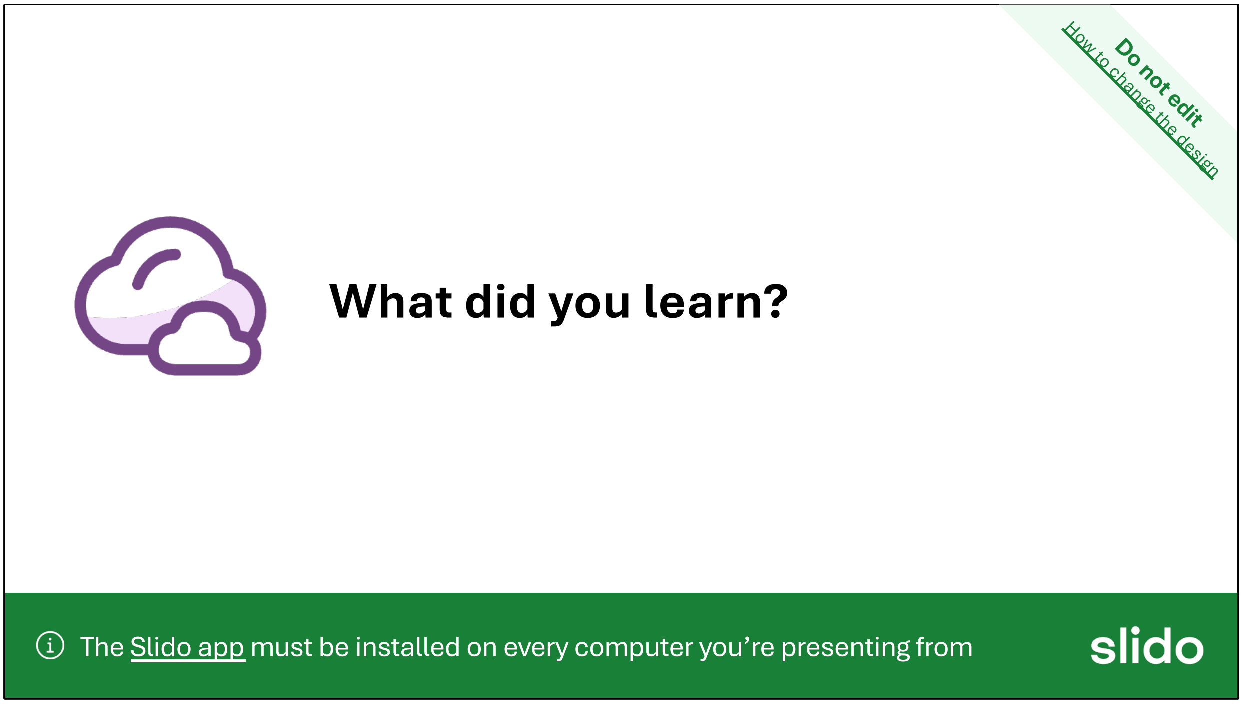


TIRP
EIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Reco ver | Report | Calibration

Preparation | Checkpoint | Risk Determin ation | Check point | Risk Decision | Check point | Risk Decision | Check point | Calibration

Its three months later, and a lot of long meetings with staff and your leadership team.



Do not edit

How to change the design

What did you learn?

ⓘ The Slido app must be installed on every computer you’re presenting from

Thank you for participating.

This story brought to you by CVE-2008-5353, CVE-2009-1103, CVE-2010-0840, CVE-2011-3544, CVE-2012-4681, CVE-2013-2465, CVE-2014-2490, CVE-2015-2590, CVE-2016-3427, CVE-2017-10086, CVE-2018-3183, CVE-2019-2698, CVE-2020-14664, CVE-2021-44228, CVE-2022-22965, CVE-2023-46606, CVE-2023-46364.

CyberFoundry

Let’s Do This Again…

We can deliver a tailored Incident Response Plan and Tabletop for your company.

CyberFoundry

https://www.cyberfoundry.io/bsides-resources/