PXL DIGITAL

Blue Teams

INFOSEC WHEEL

@aprilwright
@proxyblue

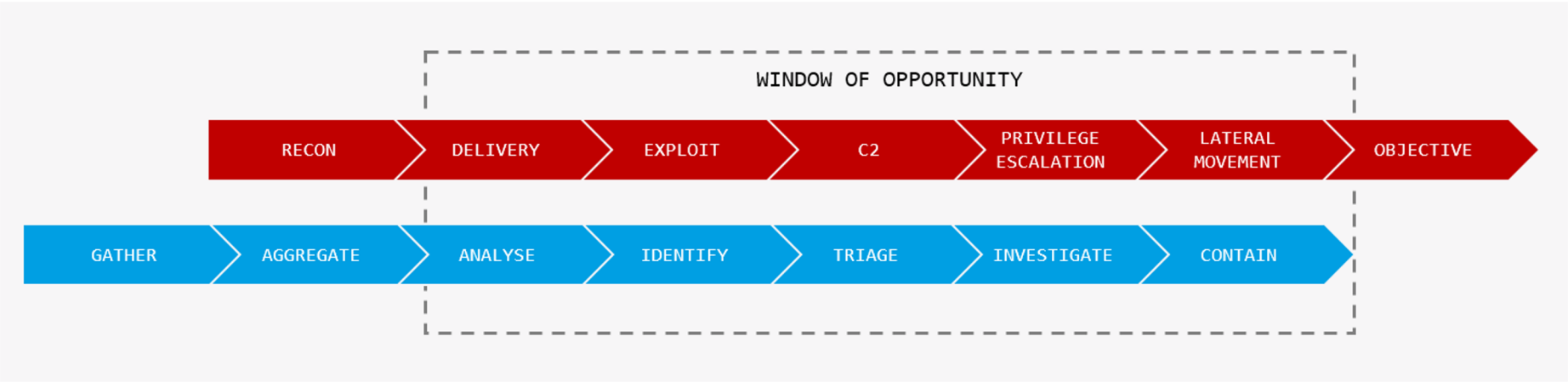
PXL DIGITAL

PXL DIGITAL

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

Blue team Incident workflow



The 5 phases in the incident response plan

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, Recovery
4. Post-Incident Review
5. Update the plan !

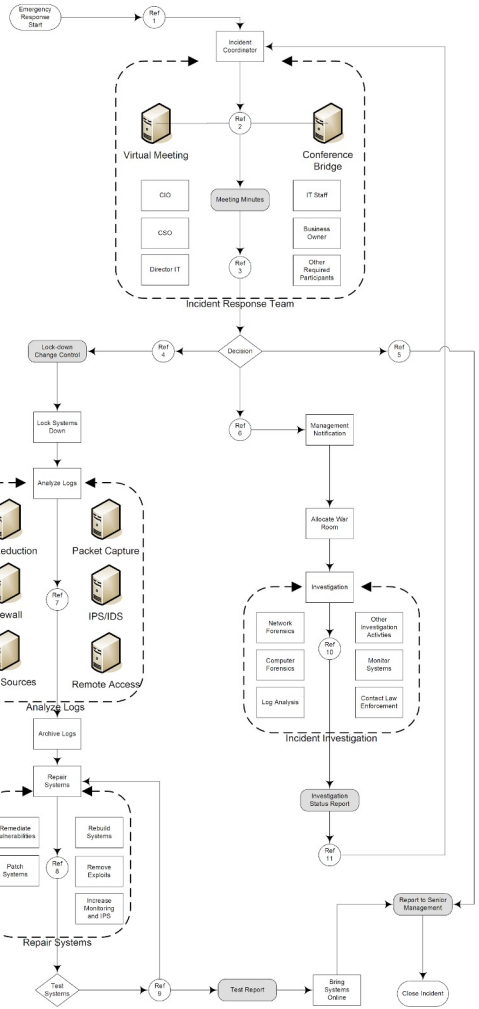
Phase 3: Containment, Eradication & Recovery

Protect the Present

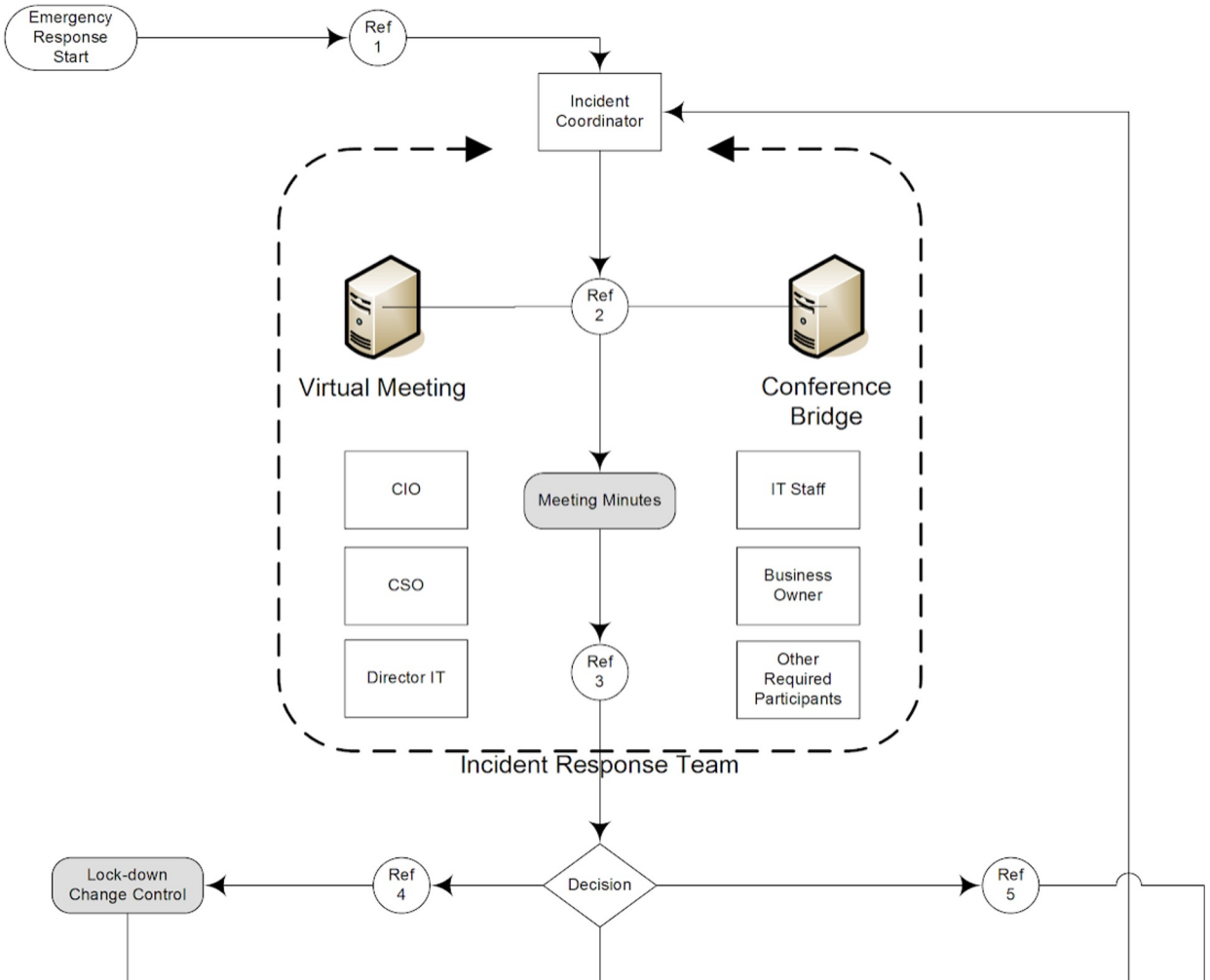
- Lock down systems
- Analyze logs
- Archive logs
- Repair/Rebuild systems
- Test Systems
- (repeat if needed)

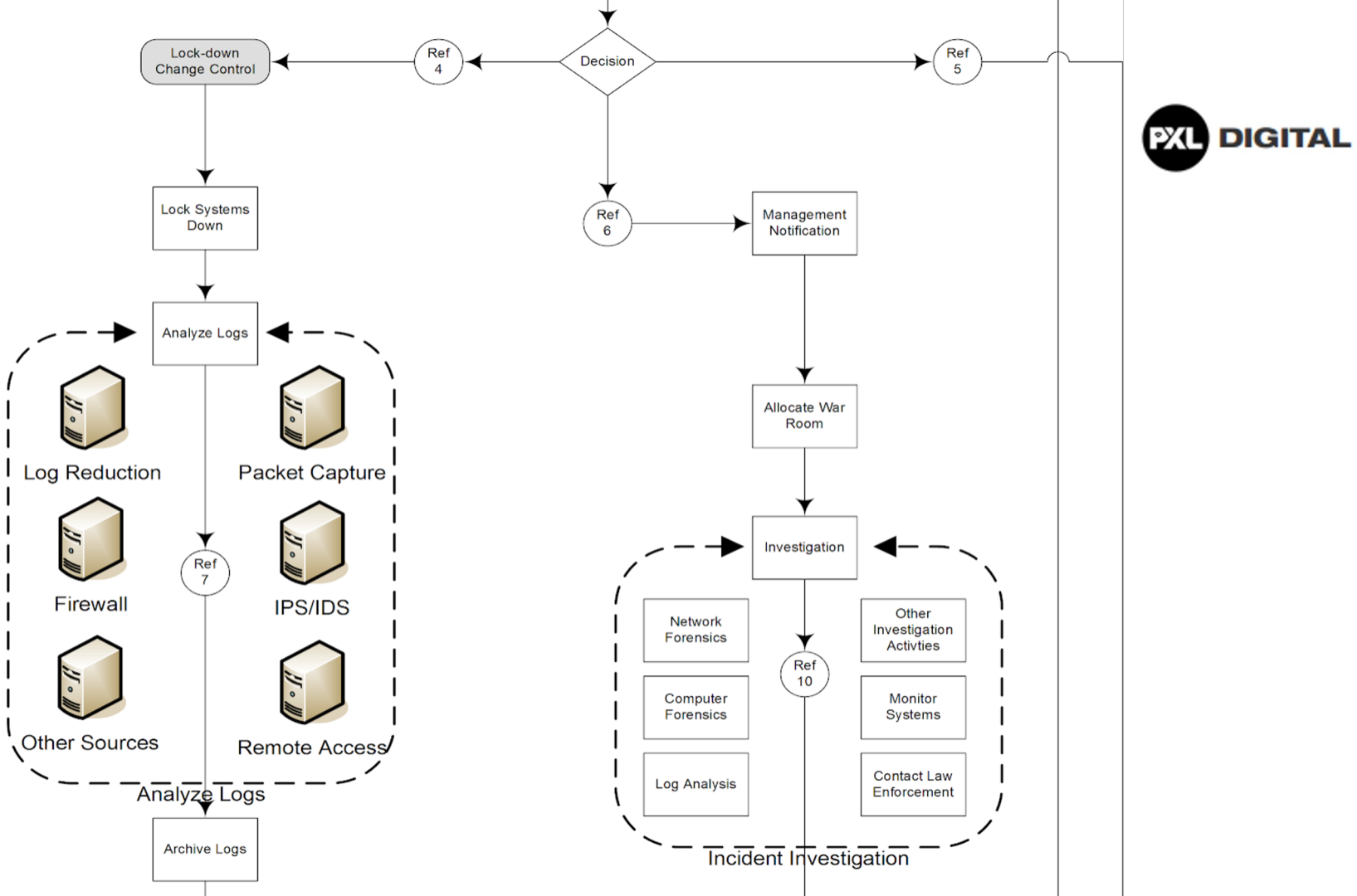
Recovered

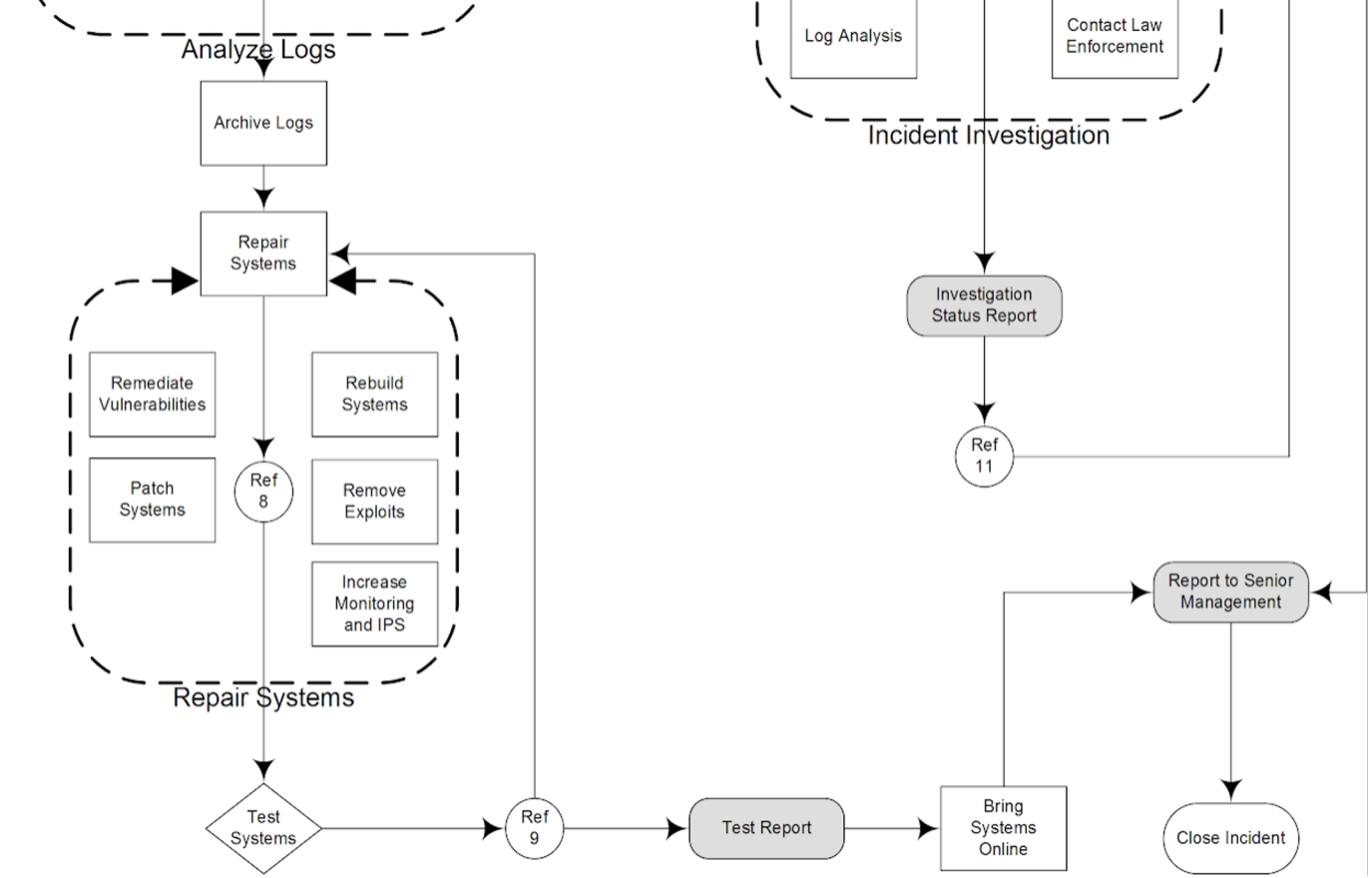
Emergency response detail



Emergency response detail




Lock-down Change Control
Ref 4
Decision
Ref 5
Lock Systems Down
Ref 6
Management Notification
Analyze Logs
Allocate War Room
Log Reduction
Packet Capture
Investigation
Ref 7
Firewall
IPS/IDS
Network Forensics
Other Investigation Activties
Ref 10
Computer Forensics
Monitor Systems
Other Sources
Remote Access
Log Analysis
Contact Law Enforcement
Analyze Logs
Incident Investigation
Archive Logs


Analyze Logs
Archive Logs
Repair Systems
Remediate Vulnerabilities
Rebuild Systems
Patch Systems
Ref 8
Remove Exploits
Increase Monitoring and IPS
Repair Systems
Test Systems
Ref 9
Test Report
Bring Systems Online
Report to Senior Management
Close Incident
Log Analysis
Contact Law Enforcement
Incident Investigation
Investigation Status Report
Ref 11

PXL DIGITAL

Phase 3: Containment, Eradication & Recovery

- Protect the future
  - Incident Investigation

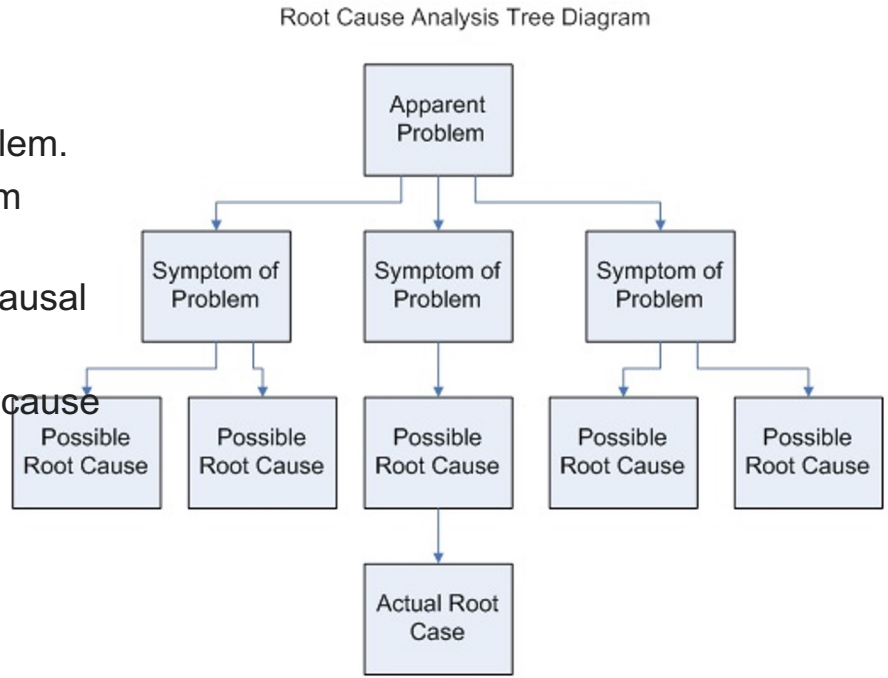
Get the facts!

- Network forensics
- Computer forensics
- Log analysis

Phase 3: Containment, Eradication & Recovery

- Protect the future
  - Root Cause Analysis

- **Identify** and describe clearly the fault/problem.
- Establish a **timeline** (history of events) from normal situation until the fault/problem.
- **Distinguish** between the root cause and causal factors (e.g., using event correlation).
- Establish a causal graph between the root cause and the fault/problem.



Phase 4 & 5: Post-Incident Review & update plan

Investigation status report

- Discusses by Incident Response Team
- When satisfied -> Send to management

- **When all is given the OK -> Incident closed**

Step 4 & 5: Post-Incident Review & update plan

- **Step 4 & 5 Post-Incident Review and update plan**
  - After-Action Meeting

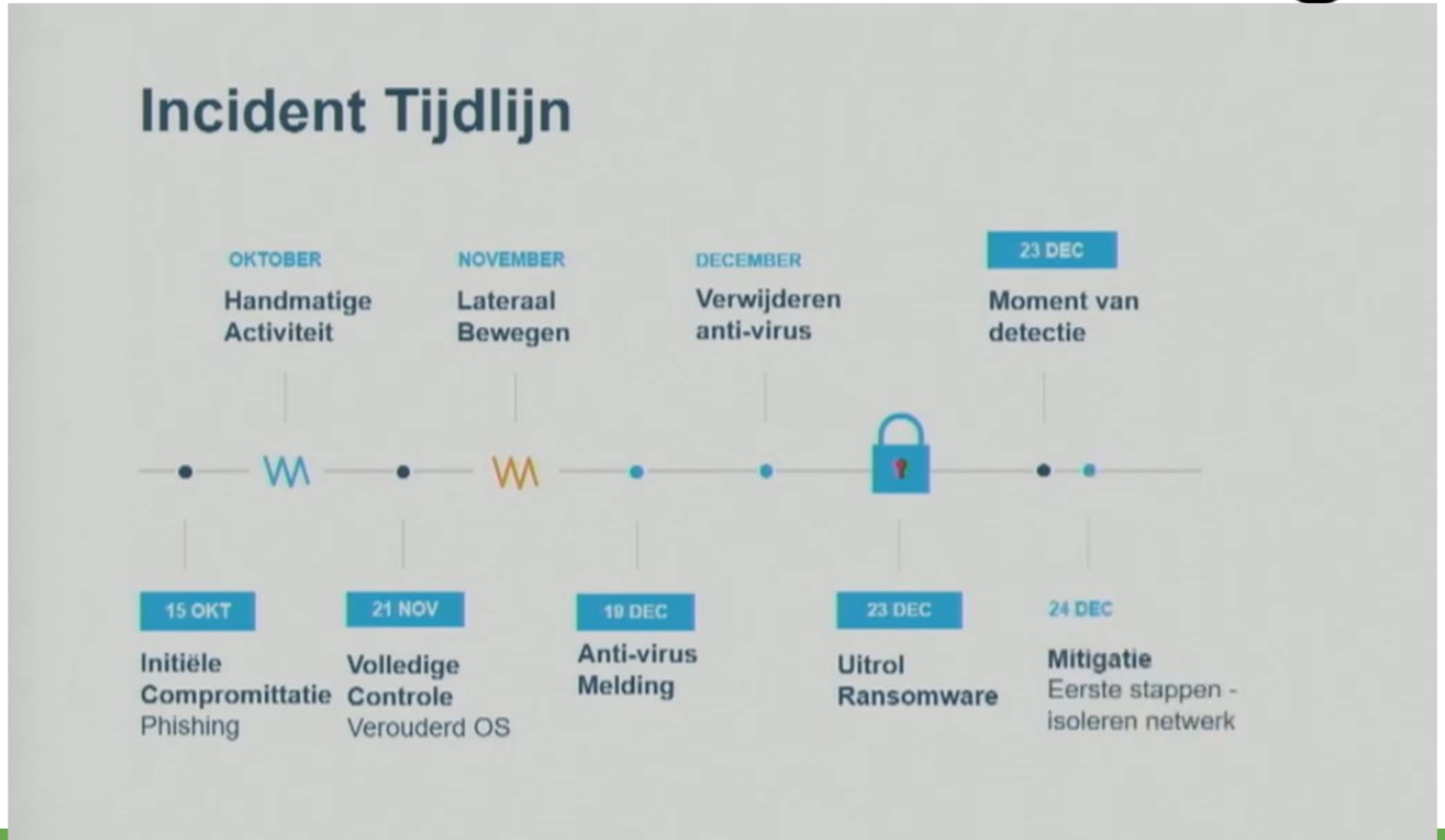
Hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.

Determine what worked well in your response plan, and where there were some holes.

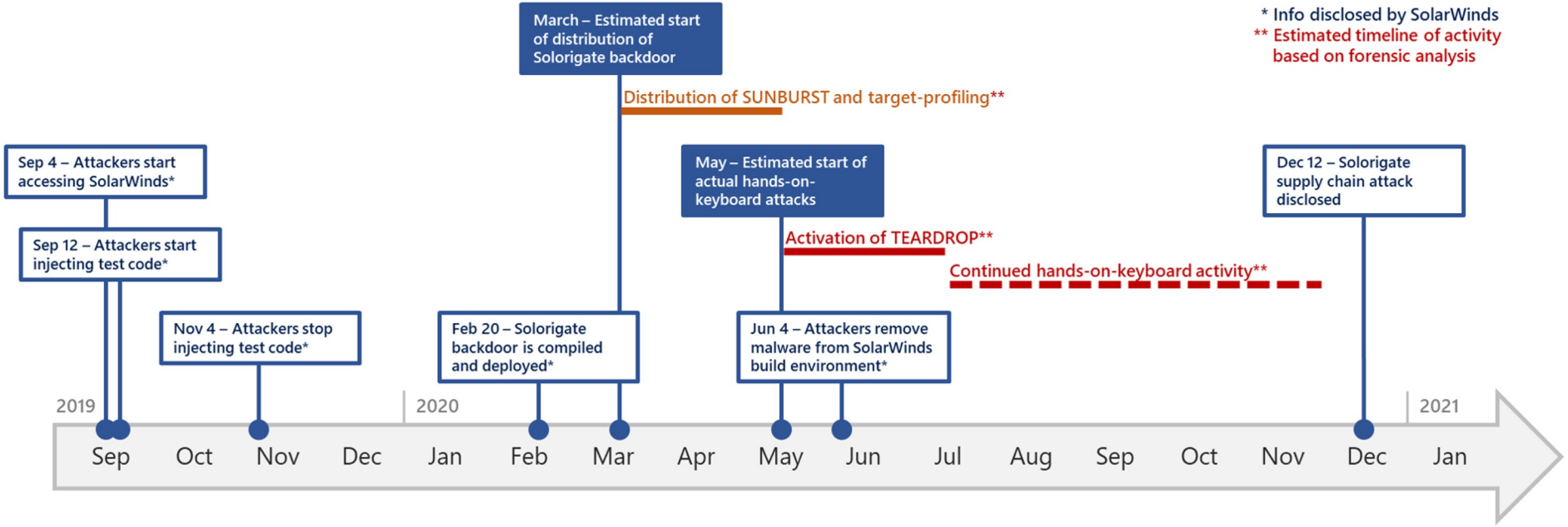
Questions to ask:

- What changes need to be made to the security?
- How should employee be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again

Incident Response - example



Solarwinds hack



Source: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Pluralsight video’s

PLURALSIGHT

PXL DIGITAL

Pluralsight video: link
Relevant : Digital Forensics: The Big Picture

Pluralsight video: link
Relevant : Digital Forensics: Getting Started with File Systems

Pluralsight video: link
Relevant : Getting Started with Memory Forensics Using Volatility

Pluralsight video: link
Relevant : Network Security Monitoring (NSM) with Security Onion