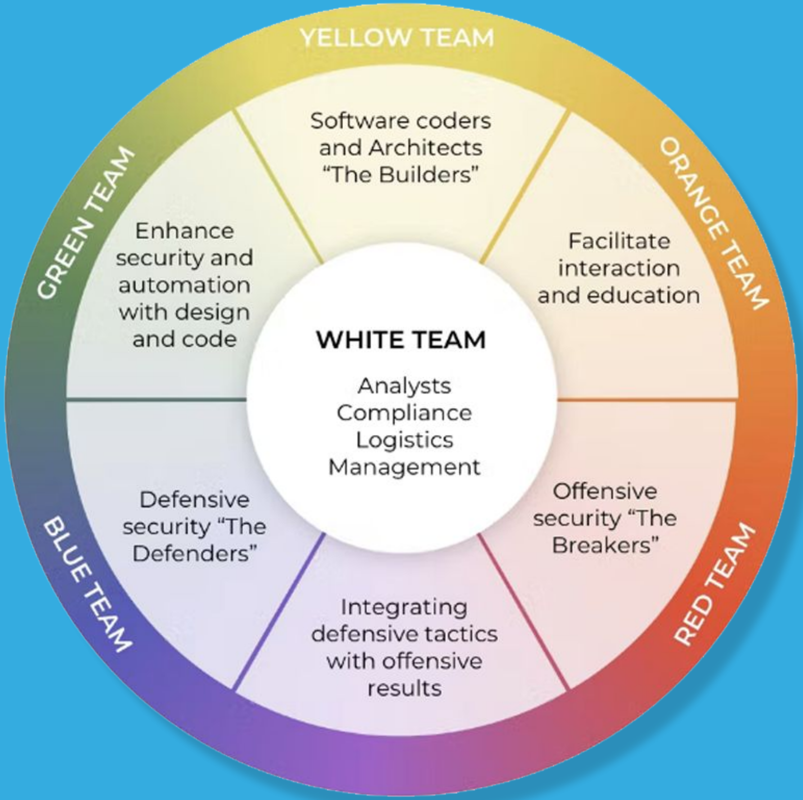
BLUE TEAMS

Deel 3

PXL DIGITAL



YELLOW TEAM

Software coders and Architects "The Builders"

ORANGE TEAM

Facilitate interaction and education

RED TEAM

Offensive security "The Breakers"

Integrating defensive tactics with offensive results

BLUE TEAM

Defensive security "The Defenders"

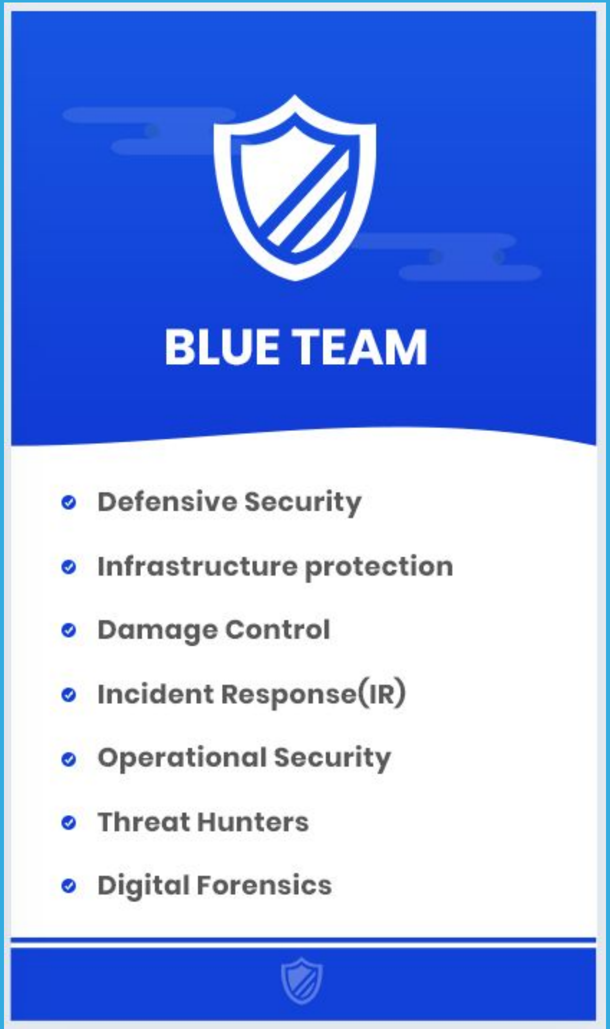
GREEN TEAM

Enhance security and automation with design and code

WHITE TEAM

Analysts
Compliance
Logistics
Management

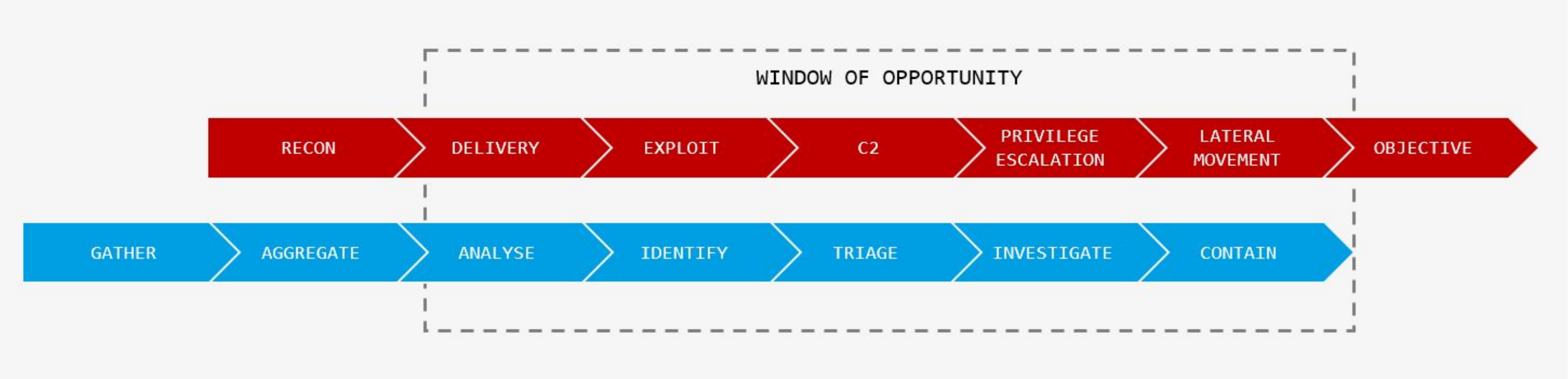
PXL DIGITAL



BLUE TEAM

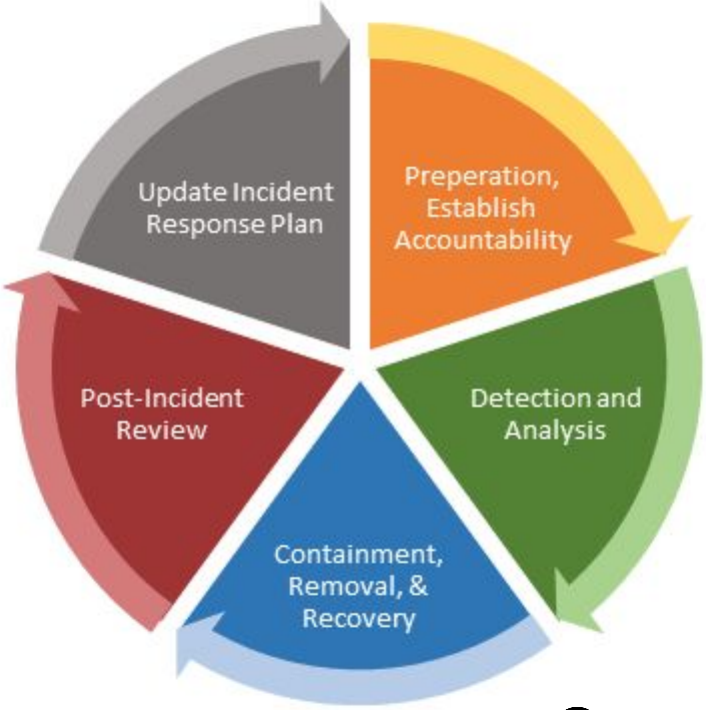
- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

BLUE TEAM - Incident workflow



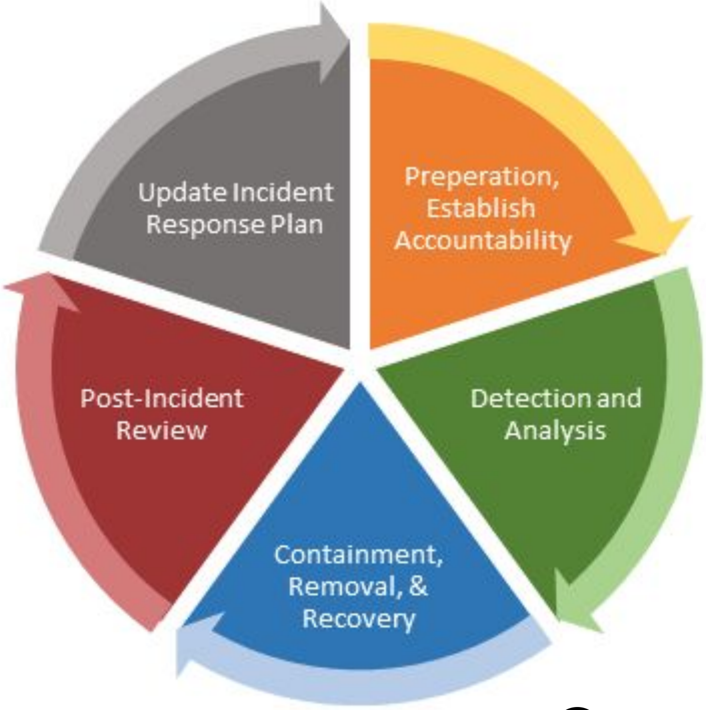
THE INCIDENT RESPONSE PLAN

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


Preperation, Establish Accountability
Detection and Analysis
Containment, Removal, & Recovery
Post-Incident Review
Update Incident Response Plan

THE INCIDENT RESPONSE PLAN

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


Update Incident Response Plan
Preperation, Establish Accountability
Detection and Analysis
Containment, Removal, & Recovery
Post-Incident Review

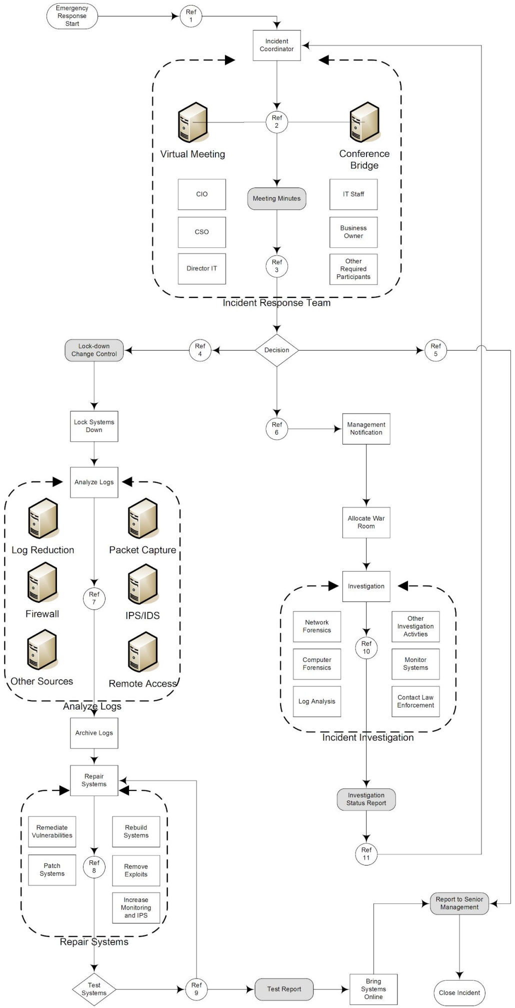
3 - CONTAINMENT, ERADICATION, RECOVERY

Protect the **Present**

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

Recovered

Emergency response detail



Emergency Response Start

Ref 1

Incident Coordinator

Ref 2

Virtual Meeting

Conference Bridge

Meeting Minutes

CIO

CSO

Director IT

IT Staff

Business Owner

Other Required Participants

Ref 3

Incident Response Team

Decision

Ref 4

Lock-down Change Control

Lock Systems Down

Analyze Logs

Log Reduction

Packet Capture

Firewall

IPS/IDS

Other Sources

Remote Access

Ref 7

Analyze Logs

Archive Logs

Repair Systems

Remediate Vulnerabilities

Patch Systems

Rebuild Systems

Remove Exploits

Increase Monitoring and IPS

Ref 8

Repair Systems

Test Systems

Ref 9

Test Report

Bring Systems Online

Ref 5

Ref 6

Management Notification

Allocate War Room

Investigation

Network Forensics

Computer Forensics

Log Analysis

Other Investigation Activties

Monitor Systems

Contact Law Enforcement

Ref 10

Incident Investigation

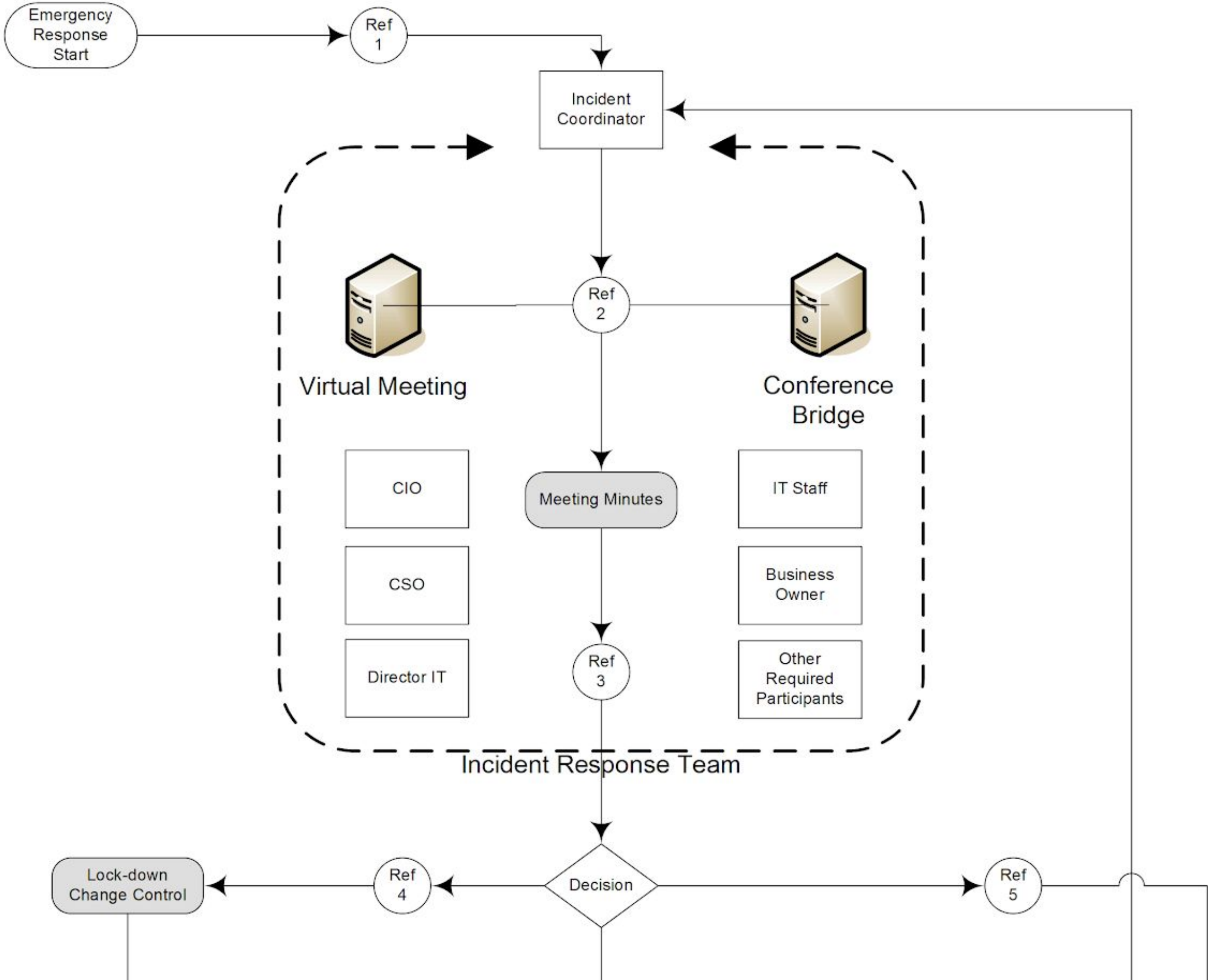
Investigation Status Report

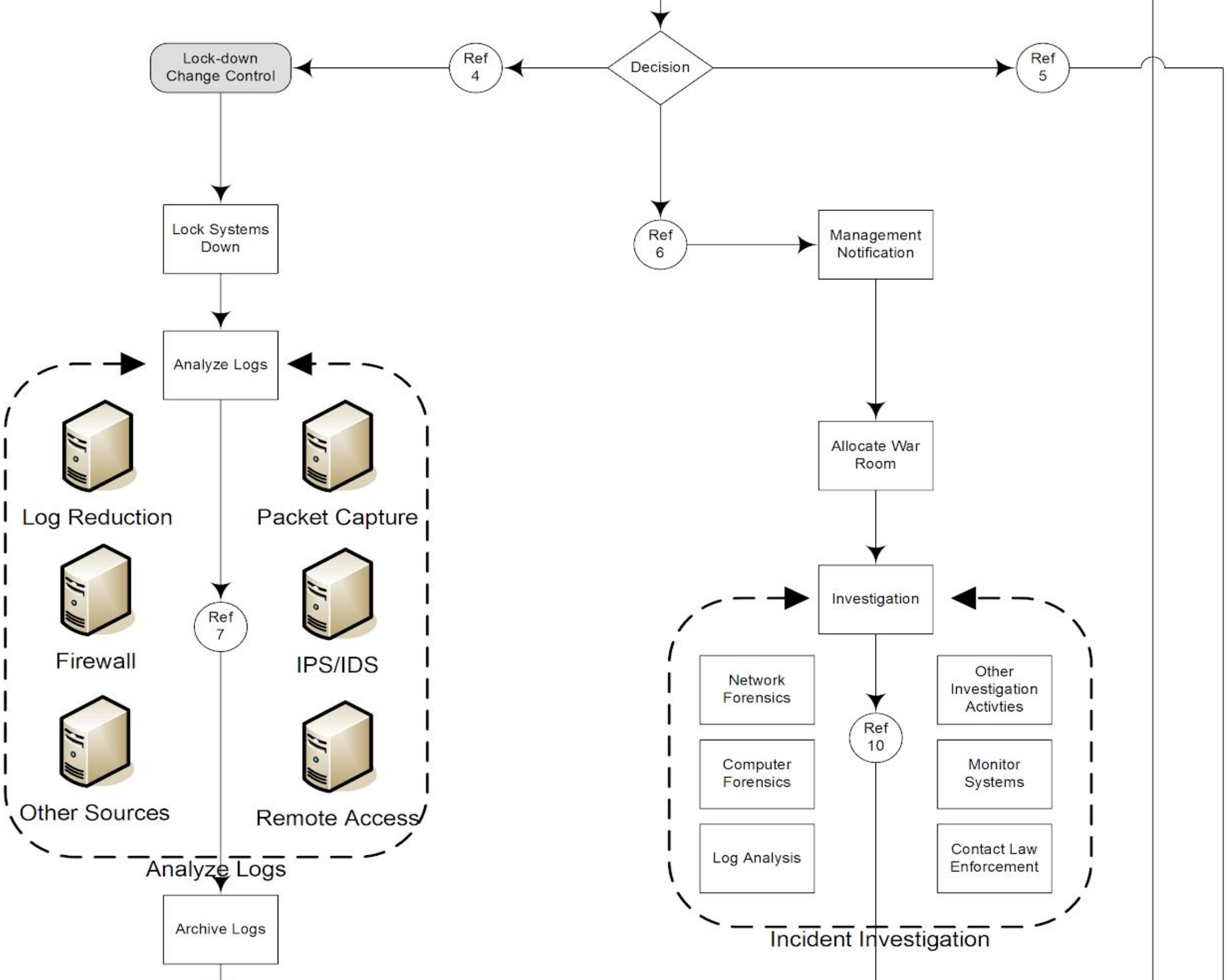
Ref 11

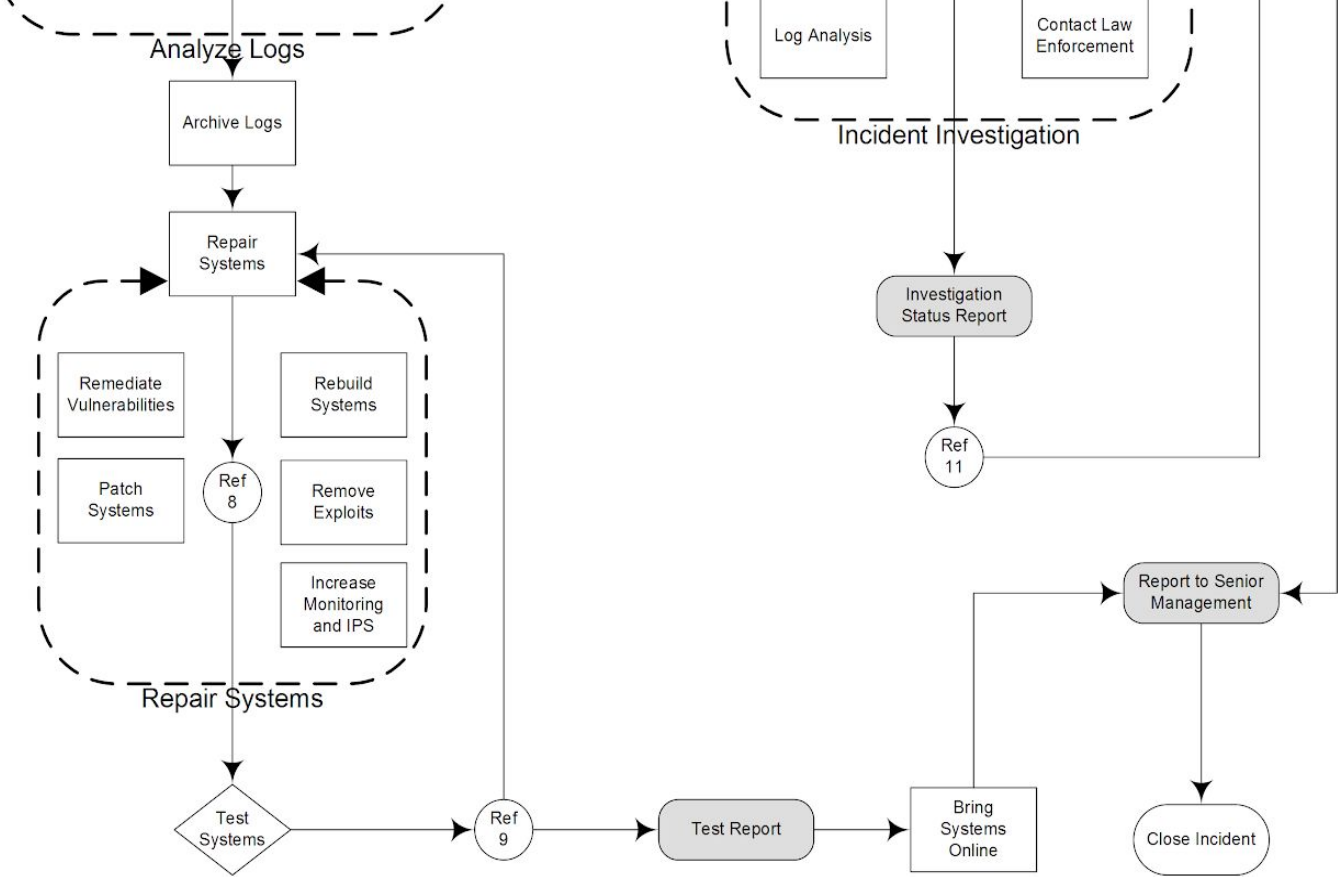
Report to Senior Management

Close Incident

Emergency response detail




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


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
Log Analysis
Contact Law Enforcement
Incident Investigation
Investigation Status Report
Ref 11
Report to Senior Management
Close Incident

PXL DIGITAL

3 - CONTAINMENT, ERADICATION, RECOVERY

Protect the **Future:** Incident Investigation - Get the facts

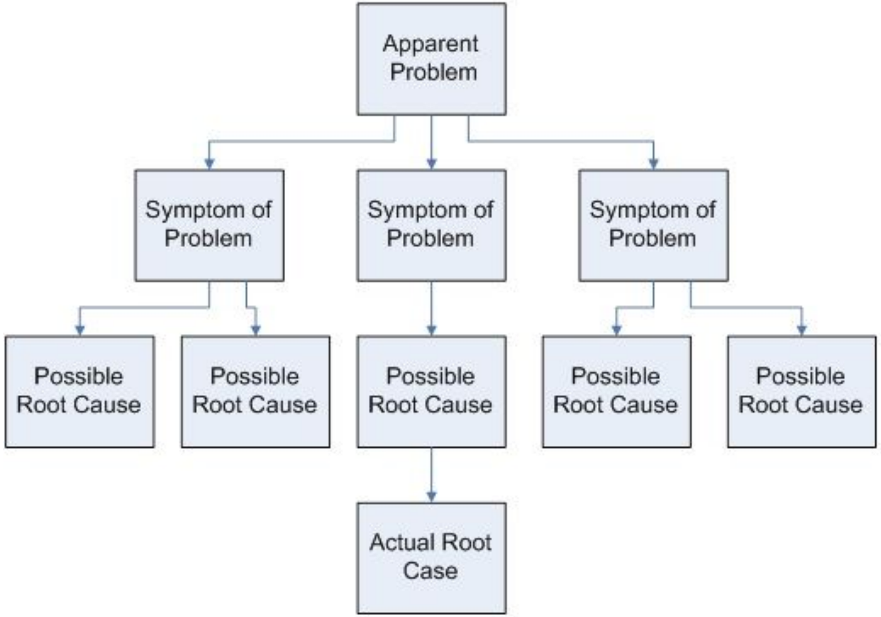
- Network Forensics
- Computer Forensics
- Log Analysis

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.

Root Cause Analysis Tree Diagram



4 - POST-INCIDENT REVIEW

Investigation status report

- Discusses by Incident Response Team
- When satisfied -> Send to management
- **When all is given the OK -> Incident closed**

5 - UPDATE THE PLAN

AFTER-ACTION MEETING

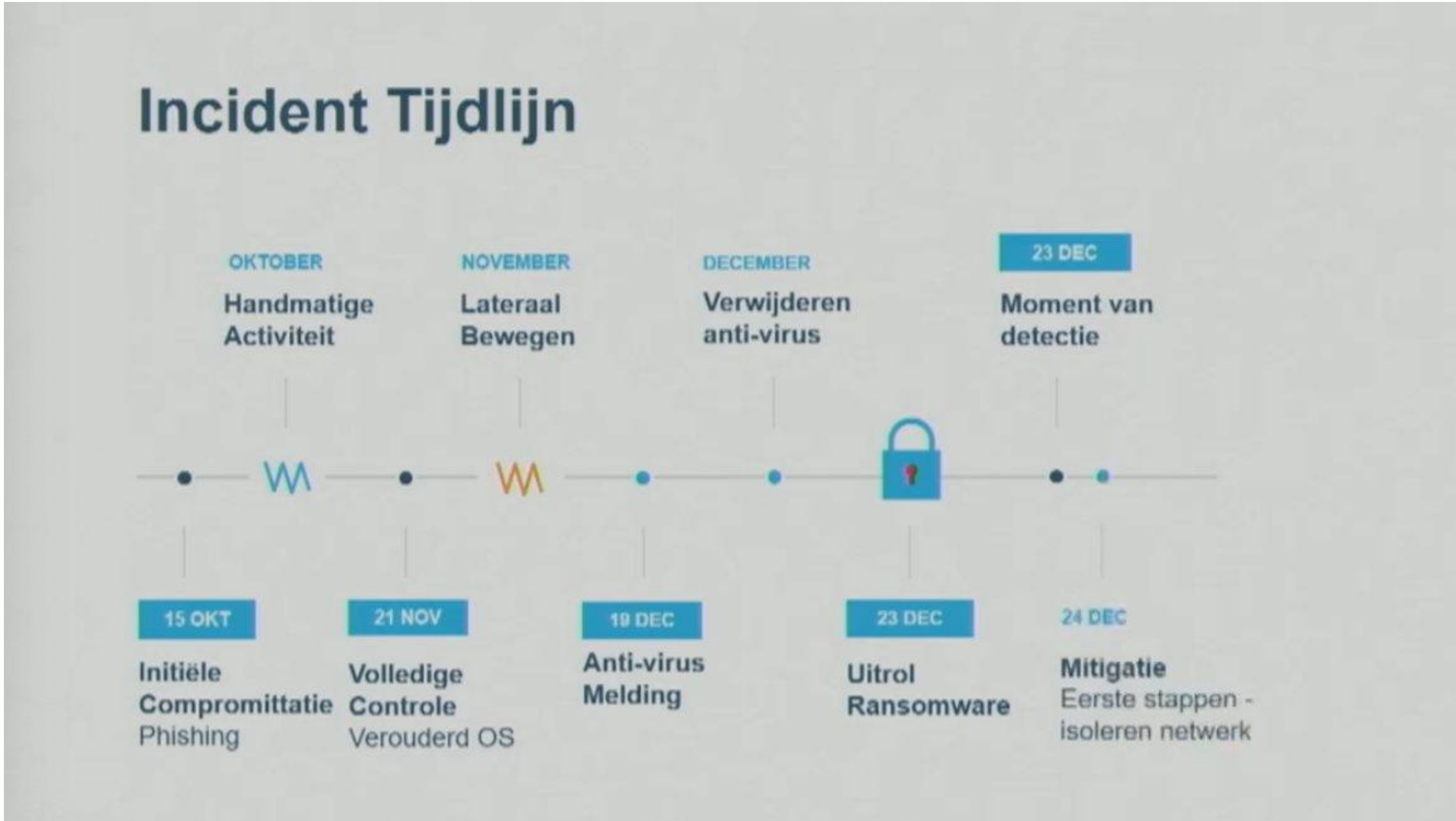
Hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.

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



Incident Tijdlijn

15 OKT
Initiële Compromittatie
Phishing

OKTOBER
Handmatige Activiteit

21 NOV
Volledige Controle
Verouderd OS

NOVEMBER
Lateraal Bewegen

19 DEC
Anti-virus Melding

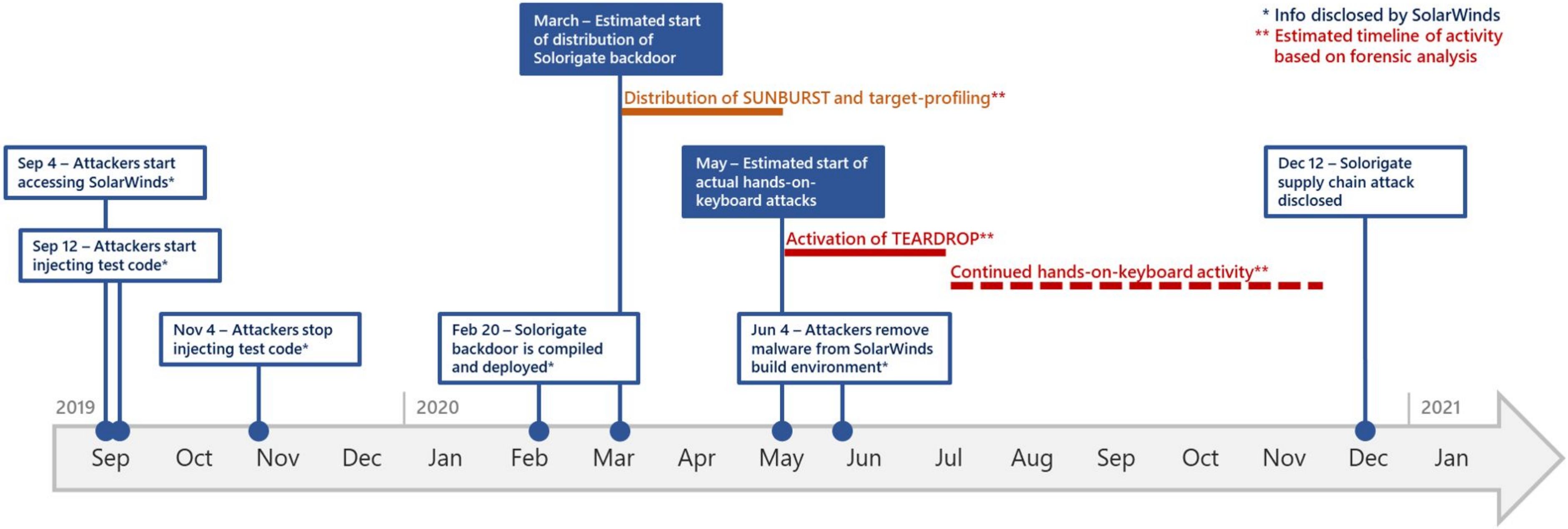
DECEMBER
Verwijderen anti-virus

23 DEC
Uitrol Ransomware

23 DEC
Moment van detectie

24 DEC
Mitigatie
Eerste stappen - isoleren netwerk

INCIDENT RESPONSE - EXAMPLE 2



* Info disclosed by SolarWinds

** Estimated timeline of activity based on forensic analysis

Sep 4 – Attackers start accessing SolarWinds*

Sep 12 – Attackers start injecting test code*

Nov 4 – Attackers stop injecting test code*

Feb 20 – Solorigate backdoor is compiled and deployed*

March – Estimated start of distribution of Solorigate backdoor

Distribution of SUNBURST and target-profiling**

May – Estimated start of actual hands-on-keyboard attacks

Activation of TEARDROP**

Continued hands-on-keyboard activity**

Jun 4 – Attackers remove malware from SolarWinds build environment*

Dec 12 – Solorigate supply chain attack disclosed

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

PLURALSIGHT VIDEOS

PLURALSIGHT

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