

Gov-X Innovation Challenge 2021

# Incident Response 101

## Samantha Rule

CISO



# Samantha Rule

Head of Information and Cybersecurity and IT Risk

## Background:

MSc, BCom(Hons) IS, CISSP®, CCSP, CDPSE, CISA is currently the Head of Information and Cybersecurity and IT Risk at Ninety One. Has over 22 years IT sector experience with more than 17 years of those specializing in information security and digital forensics both in South Africa, Europe, APAC and the US.

# Agenda

- What is Incident Response
- Why is Incident Response important
- Phases of Incident Response
- Q&A

“ There are only **two types** of **companies**: those that **have been** hacked, and those that **will be.** ”

Robert Mueller – FBI Director 2012



**1.**

# **What is Incident Response**



**Incident response** is a **plan** for responding to a cybersecurity incident methodically.



**2.**

**Why is Incident Response  
important?**



# To avoid the chicken run



**Whenever there's a Security  
Incident**

**3.**

# Incident Response Phases



# Incident Response Planning

## Incident Response Steps

### NIST

- 1) Preparation
- 2) Detection and Analysis
- 3) Containment, Eradication, & Recovery
- 4) Post-Incident Activity

### SANS

- 1) Preparation
- 2) Identification
- 3) Containment
- 4) Eradication
- 5) Recovery
- 6) Lessons Learned

# Incident Response Phases



# Preparation Phase

1. Establishment CSIRT/IR team
2. Conduct criticality assessment
3. Carry out cyber security incident threat analysis
4. Consider implications
5. Create appropriate control environment
6. Review state of readiness

# Incident Reponse Teams

1. Security Operations Centre (SOC)
  2. Computer Incident Response Team (CSIRT)
- 

# Preparation cont.

## People

Who's in charge around here ?

- Technical lead
- Senior

Major Business stakeholders

- Crisis Management Team

## Communication

Internal Communication

- Constant communication between local and remote support
- "War Room" - Center of operations
- Update meetings

External Communication

- Media Liaisons

# Identification Phase

1. Identify the Cyber Security Incident
  2. What happened?
  3. Which systems are affected
  4. What data is impacted
- 

# Containment Phase

1. Limit and contain the impact of the incident
  2. Monitor, isolate or shutdown affected systems
- 

# Eradication Phase

1. Cleanup continues
2. Remove the threat
3. Patch vulnerabilities

# Recovery Phase

1. Rebuilding systems
2. Restoring data
3. Restoring systems
4. System validation

# Lessons Learned Phase

1. Carry out post incident review
  2. Lessons learnt
  3. Update any key information, processes, controls
  4. Perform trend analysis
- 

# Incident Response Phases

Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)

## Preparation

- People
- Notes
- Relationships
- Policies
- Procedures
- Coms plan
- Tools
- Mgt Tng
- Training
- Jump Bag

## Identification

- Awareness
- Need to Know
- Unusual processes
- Unusual Security Evt's
- Alert Early
- Use OOB Comms
- New Accts / Privs
- Primary IR Handler
- Passive monitoring
- Odd Sch Tasks
- Unusual Files
- Analyze Logs
- Chain of Custody

## Containment

- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds
- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors
- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)
- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

## Eradication

- Del Artifacts
- Apply All Patches
- Black Hole IP's
- Root Cause
- Addl FW / IDS Filters
- Seek other Host footholds
- Restore Back-up
- Chg DNS Names
- Wipe/Format/Rebuild
- Remove Malware
- Rescan network

## Recovery

- Return to Ops
- Monitor (signs/shells/artifacts/events)
- Test /Doc Baseline
- Move to Production (Approval)
- Script searches for attacker artifacts

## Lessons Learned

- Document Incident
- All affected parties review / comment on draft
- Finalize Report
- Seek Required Changes
- Immediately upon recovery Phase
- Provide Exec Summary
- Seek Funding
- Assign to on-Scene IRH
- Reach Report Consensus
- Address Process not people
- Update Procedures

# RE&CT Matrix

ATT&CK® Navigator x +

atc-project.github.io/react-navigator/ MITRE ATT&CK® Navigator

RE&CT Enterprise Matrix x +

selection controls layer controls technique controls

Preparation	Identification	Containment	Eradication	Recovery	Lessons Learned
101 items	61 items	26 items	8 items	14 items	2 items
Practice	List victims of security alert	Patch vulnerability	Report incident to external companies	Reinstall host from golden image	Develop incident report
Take trainings	List host vulnerabilities	Block external IP address	Remove rogue network device	Restore data from backup	Conduct lessons learned exercise
Raise personnel awareness	Put compromised accounts on monitoring	Block internal IP address	Delete email message	Unblock blocked IP	
Make personnel report suspicious activity	List hosts communicated with internal domain	Block external domain	Remove file	Unblock blocked domain	
Set up relevant data collection	List hosts communicated with internal IP	Block internal domain	Remove registry key	Unblock blocked URL	
Set up a centralized long-term log storage	List hosts communicated with internal URL	Block external URL	Remove service	Unblock blocked port	
Develop communication map	List hosts communicated with internal URL	Block internal URL	Revoke authentication credentials	Unblock blocked user	
Make sure there are backups	Analyse domain name	Block port external communication	Remove user account	Unblock domain on email	
Get network architecture map	Analyse IP	Block port internal communication		Unblock sender on email	
Get access control matrix	Analyse uri	Block user external communication		Restore quarantined email message	
Develop assets knowledge base	List hosts communicated by port	Block user internal communication		Restore quarantined file	
Check analysis toolset	List hosts connected to VPN	Block data transferring by content pattern		Unblock blocked process	
Access vulnerability management system logs	List hosts connected to intranet	Block domain on email		Enable disabled service	
Connect with trusted communities	List data transferred	Block sender on email		Unlock locked user account	
Access external network flow logs	Collect transferred data	Quarantine email message			
Access internal network flow logs	Identify transferred data	Quarantine file by format			
		Quarantine file by hash			

^ legend

# Phases of a cyber security attack

1



## *Carry out reconnaissance*

- Identify target
- Look for vulnerabilities

2



## *Attack target*

- Exploit vulnerabilities
- Defeat remaining controls

3



## *Achieve objective*

- Disruption of systems
- Extraction (eg of money, IPR or confidential data)
- Manipulation (eg adding, changing or deleting key information)

## *Countermeasures*

- Monitoring (and logging)
- Situational awareness
- Collaboration
  
- Solid architectural system design
- Standard controls
- Penetration testing
  
- Cyber security incident response
- Business continuity and disaster recovery plans
- Cyber security insurance

Source: CREST Cyber Security Incident Response Guide

# Cyber Security Incidents

## Incident Response Planning



# Cyber Security Incidents

Examples of possible cyber security incidents	The sources of these signs include.....
<p>Precursors can include:</p> <ul style="list-style-type: none"><li>• Web server log entries that show the usage of a vulnerability scanner</li><li>• An announcement of a new exploit that targets a vulnerability of the organisation's mail server</li><li>• A threat from a group stating that the group will attack the organisation.</li></ul> <p>Indicators (there are many) can include:</p> <ul style="list-style-type: none"><li>• A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server</li><li>• Antivirus software alerts when it detects that a host is infected with malware.</li><li>• A system administrator sees a filename with unusual characters</li><li>• A host records an auditing configuration change in its log</li><li>• An application logs multiple failed login attempts from an unfamiliar remote system</li><li>• An email administrator sees a large number of bounced emails with suspicious content</li><li>• A network administrator notices an unusual deviation from typical network traffic flows.</li></ul>	<ul style="list-style-type: none"><li>• Security software (eg IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software, monitoring services (often provided by a third party))</li><li>• Logs (eg operating system logs, service and application logs, network device logs and network flows)</li><li>• Publicly available information (eg information on new exploits, information exchange groups, third party organisations, governments)</li><li>• People form within your organisation</li><li>• Third parties (eg customers, suppliers, IT providers, ISPs, partners; government bodies).</li></ul>

# Incident Response Summary

1. Identify suspected incident
2. Establish objectives of investigation and response
3. Analyse available information
4. Determine what actually happened
5. Identify the attack surface: DDoS, malware, system hack, session hijack, data corruption
6. Identify what internal assets have been compromised
7. Determine what information has been disclosed/deleted/corrupted
8. Find out who did it and why
9. Work out how attacker got initial entry
10. Determine potential impact
11. Conduct sufficient investigation to identify and prosecute perpetrators
12. Work through lessons learnt
13. Update any process documents or incident response plan



# THANK YOU!

Any questions?

You can find me at @secinfoopt &  
@cybersecgrit