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

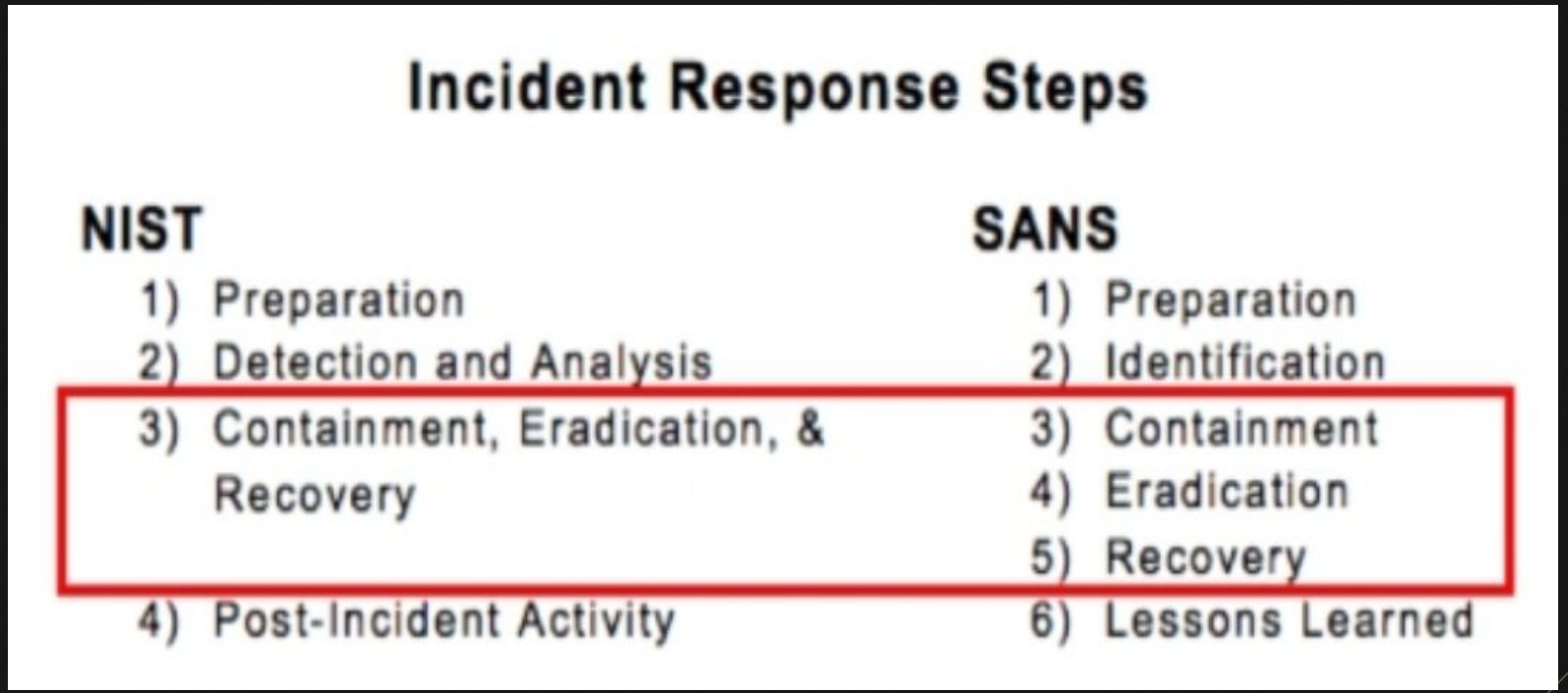
Incident response is a plan for responding to a cybersecurity incident methodically.

2.
Why is Incident Response important?

To avoid the chicken run

3.
Incident Response Phases

Incident Response Planning



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

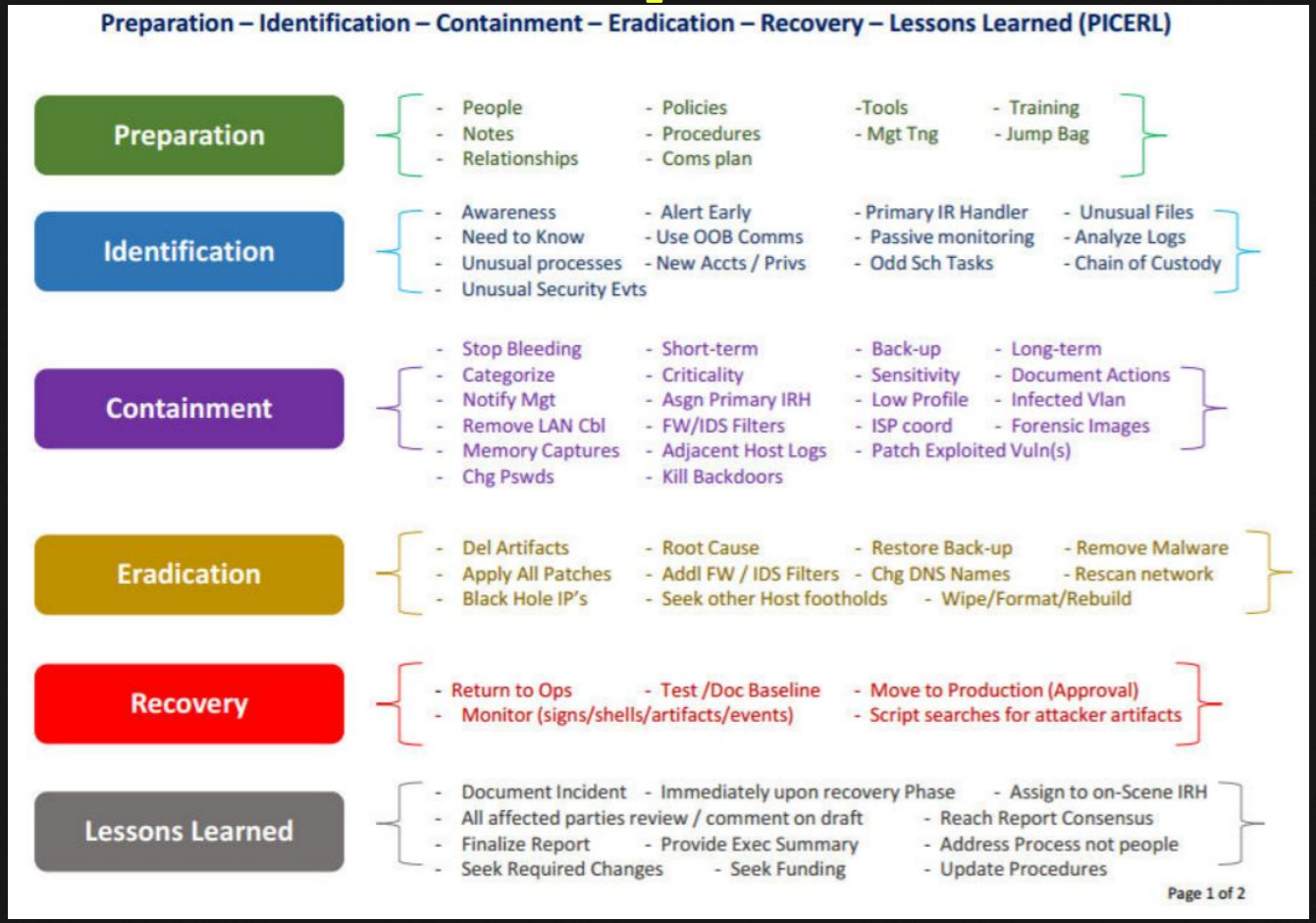
Recovery Phase

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

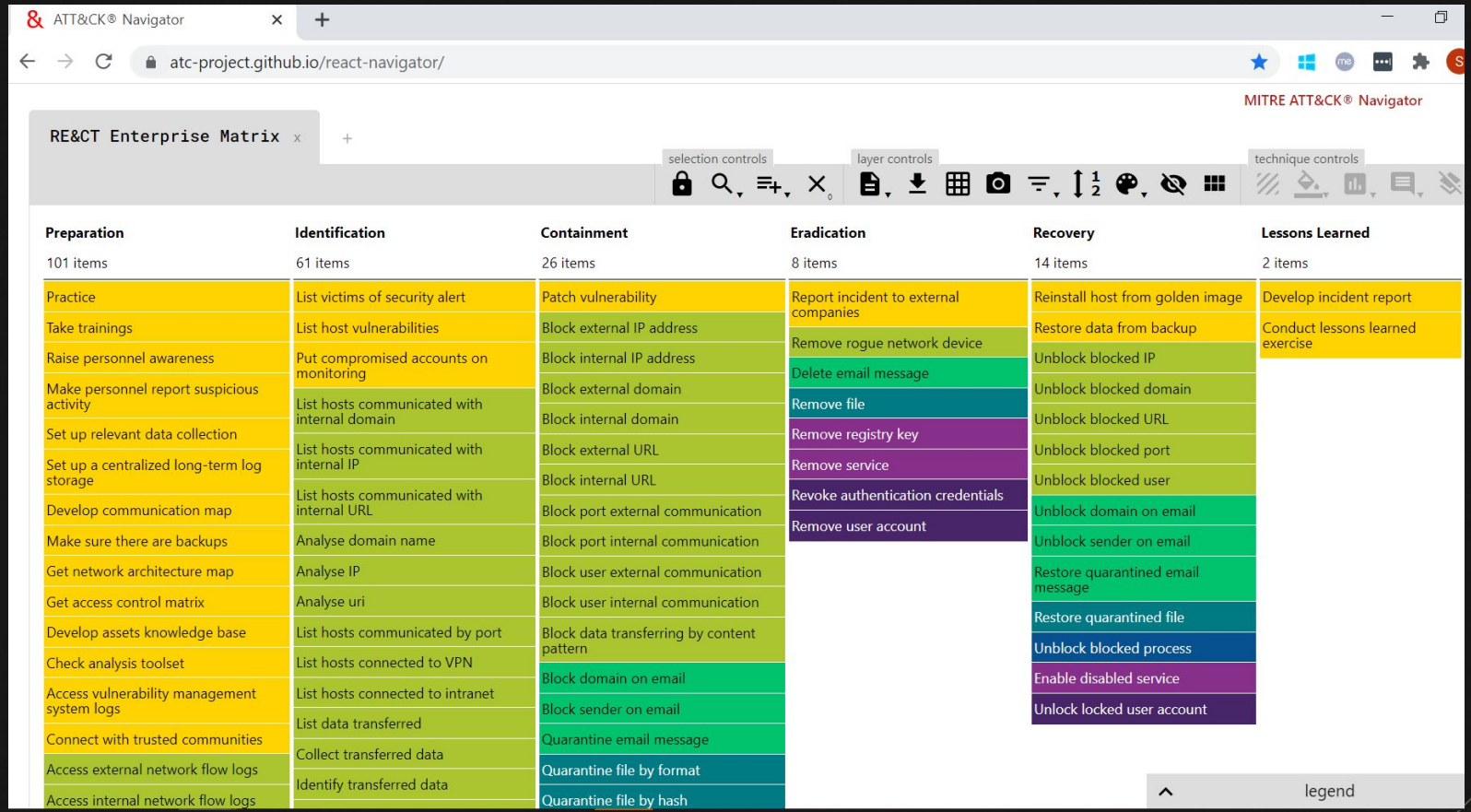
Lessons Learned Phase

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

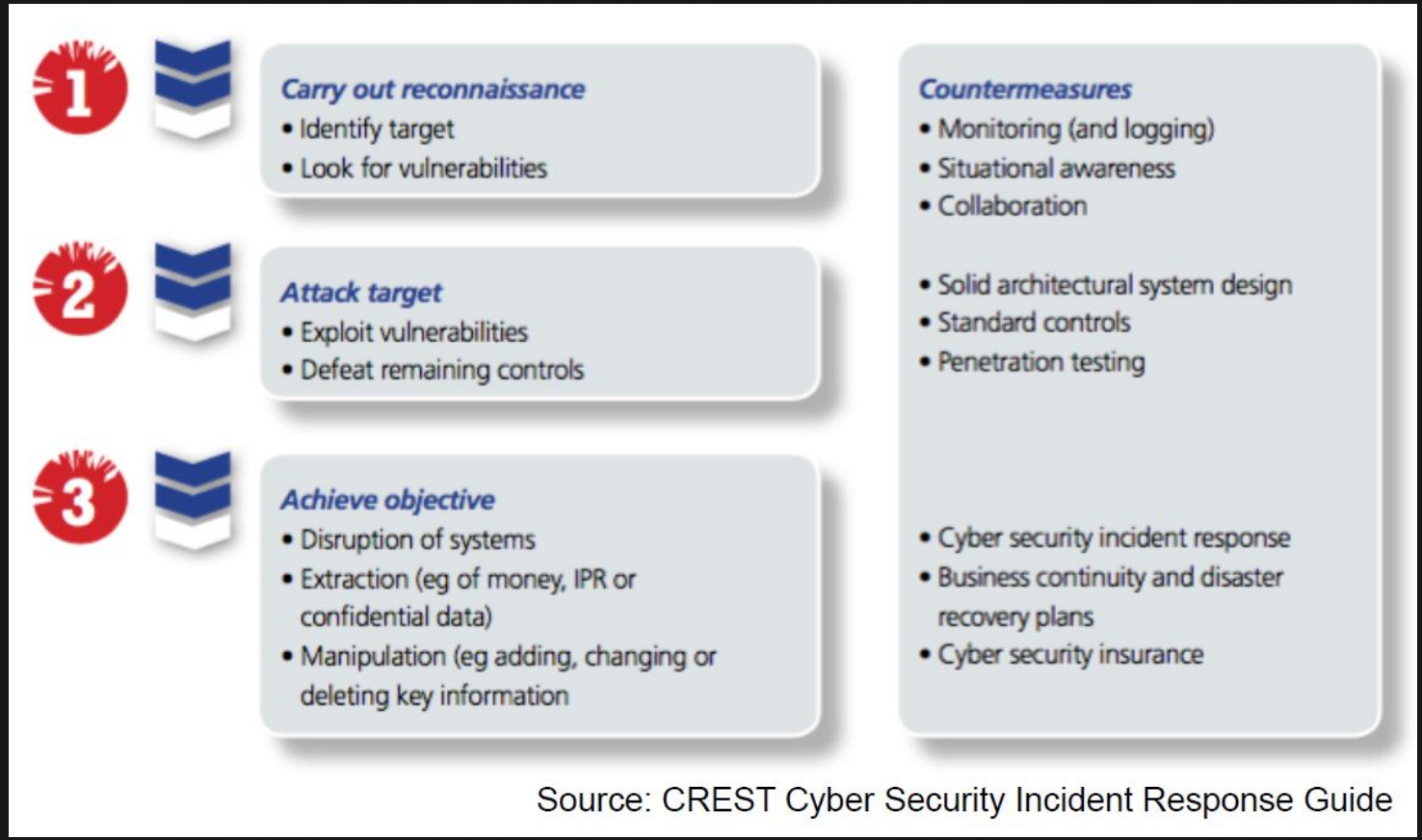
Incident Response Phases



RE&CT Matrix

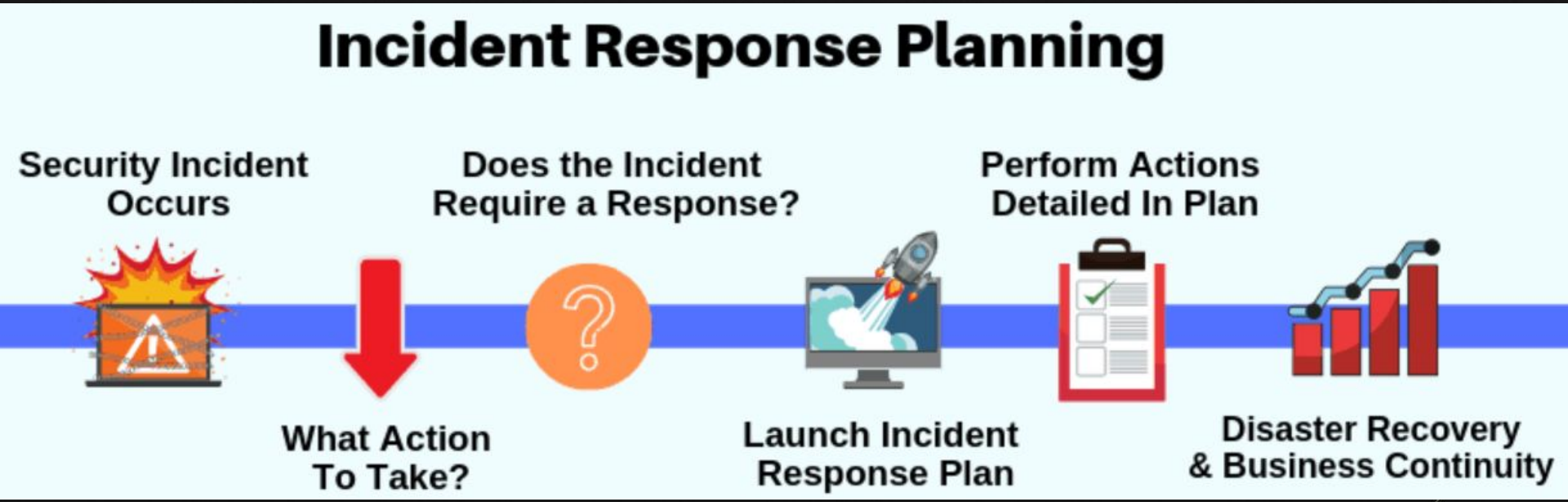

ATT&CK® Navigator
atc-project.github.io/react-navigator/
MITRE ATT&CK® Navigator
RE&CT Enterprise Matrix
selection controls
layer controls
technique controls
Preparation
101 items
Practice
Take trainings
Raise personnel awareness
Make personnel report suspicious activity
Set up relevant data collection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

Phases of a cyber security attack



Source: CREST Cyber Security Incident Response Guide

Cyber Security Incidents



Cyber Security Incidents

Examples of possible cyber security incidents	The sources of these signs include.....
Precursors can include: • Web server log entries that show the usage of a vulnerability scanner • An announcement of a new exploit that targets a vulnerability of the organisation's mail server • A threat from a group stating that the group will attack the organisation. Indicators (there are many) can include: • A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server • Antivirus software alerts when it detects that a host is infected with malware. • A system administrator sees a filename with unusual characters • A host records an auditing configuration change in its log • An application logs multiple failed login attempts from an unfamiliar remote system • An email administrator sees a large number of bounced emails with suspicious content • A network administrator notices an unusual deviation from typical network traffic flows.	• Security software (eg IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software, monitoring services (often provided by a third party) • Logs (eg operating system logs, service and application logs, network device logs and network flows) • Publicly available information (eg information on new exploits, information exchange groups, third party organisations, governments) • People form within your organisation • Third parties (eg customers, suppliers, IT providers, ISPs, partners; government bodies).

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 @secinfocpt &
@cybersecgrit