Cyber Security Incident Management

Leading your organization on the worst day

Incident Commander

Gerry Johansen
Principal
IR Proactive

@irproactive

10+ Years of Incident Response, Digital Forensics and Threat Intelligence

BS – Justice and Law Admin, MA– Information Assurance, GCTI, GCFA, GNFA, GRID, CISSP Detective / Task Force Agent (FBI)

Digital Forensics and Incident Response, 3rd Edition

Rapid City, South Dakota

Incident Management and Command Overview

Is this your Incident Management process?

Why discuss Incident Management?

- Often overlooked for the more fun and technical Digital Forensics.
- Attackers are gaining speed: Initial infection to full impact is now measured in hours.
- Not a real call for full-time Incident Management personnel.
- Incident Management is not trained as often as some of the other topics related to DFIR.
- Proper coordination between teams is critical to incident resolution.
- There are a variety of processes that are more tailored to natural/man made events and not cyber: FEMA ICS.

What is Incident Management?

- Incident management incorporates the four P’s
  - Practices: How an organizations addresses key aspects of incident response
  - Processes: What approach, technical and non-technical is applied to incidents.
  - Procedures: How are those processes worked through.
  - Personnel: Who is responsible for the variety of actions taken throughout the lifecycle of an incident.

Who leads Incident Management?

- Leading the Incident Management process is the **Incident Commander**.
- The Incident Commander or IC is someone with a broad base of security and incident management knowledge
- The key attributes needed are Calm, Cool and Collected.
- This is a position that is assigned as a full-time role or assumed by someone within the organization to take on during an incident.
- Responsible for ensuring that everyone is kept well informed and that key decisions are made in a timely fashion (breaking up Analysis Paralysis).
- Makes available all the necessary resources.

Incident Commander Information Coordination

Incident Commander Information Coordination

Regulator Reporting

Forensic Analysis Update

Analysis Tasking

Executive Briefings

Eradication and Recovery Tasking

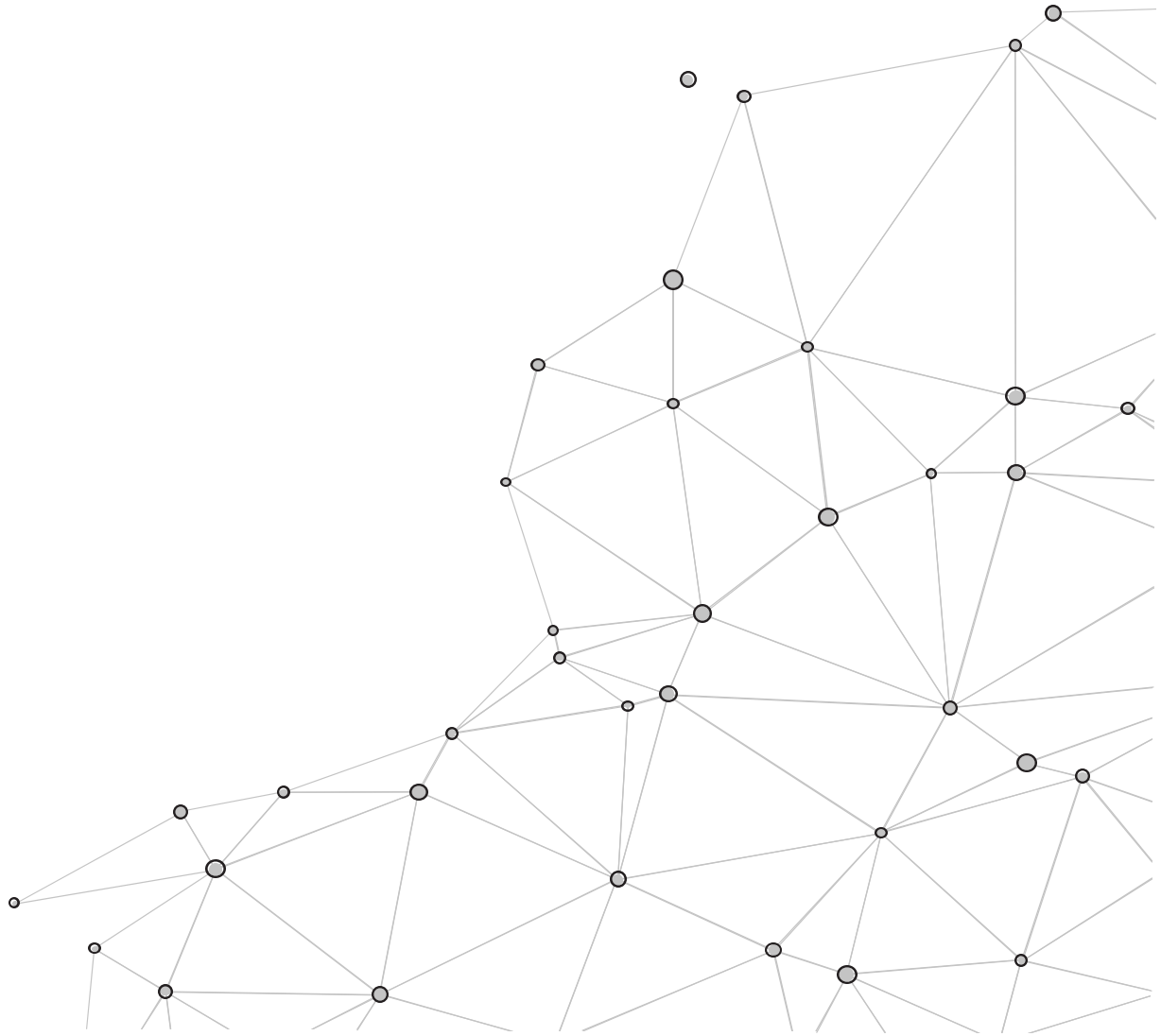
Incident Command Leading Procedures

Incident Command Leading Procedures (ICLPs)

- An overall Incident Management process that ties in various procedures through the entire incident lifecycle.
- Based on the US Army's Troop Leading Procedures.
- Scalable based on the size of the organization and the resources that are available.
- Flows from one step to the next with inputs and outputs.
- Goes deeper than some other processes such as the NIST SP800-61r2.

Incident Command Leading Procedures

1. Receive the Incident Escalation
2. Activate the CSIRT
3. Perform Initial Analysis
4. Deploy Containment Measures
5. Update Objectives
6. Perform Secondary Analysis
7. Execute Eradication and Recovery Plans
8. Close out incident



Malicious Activity has been detected!!!

Receive Escalation

Process Input

- Incident Declaration/Escalation from SOC or other source

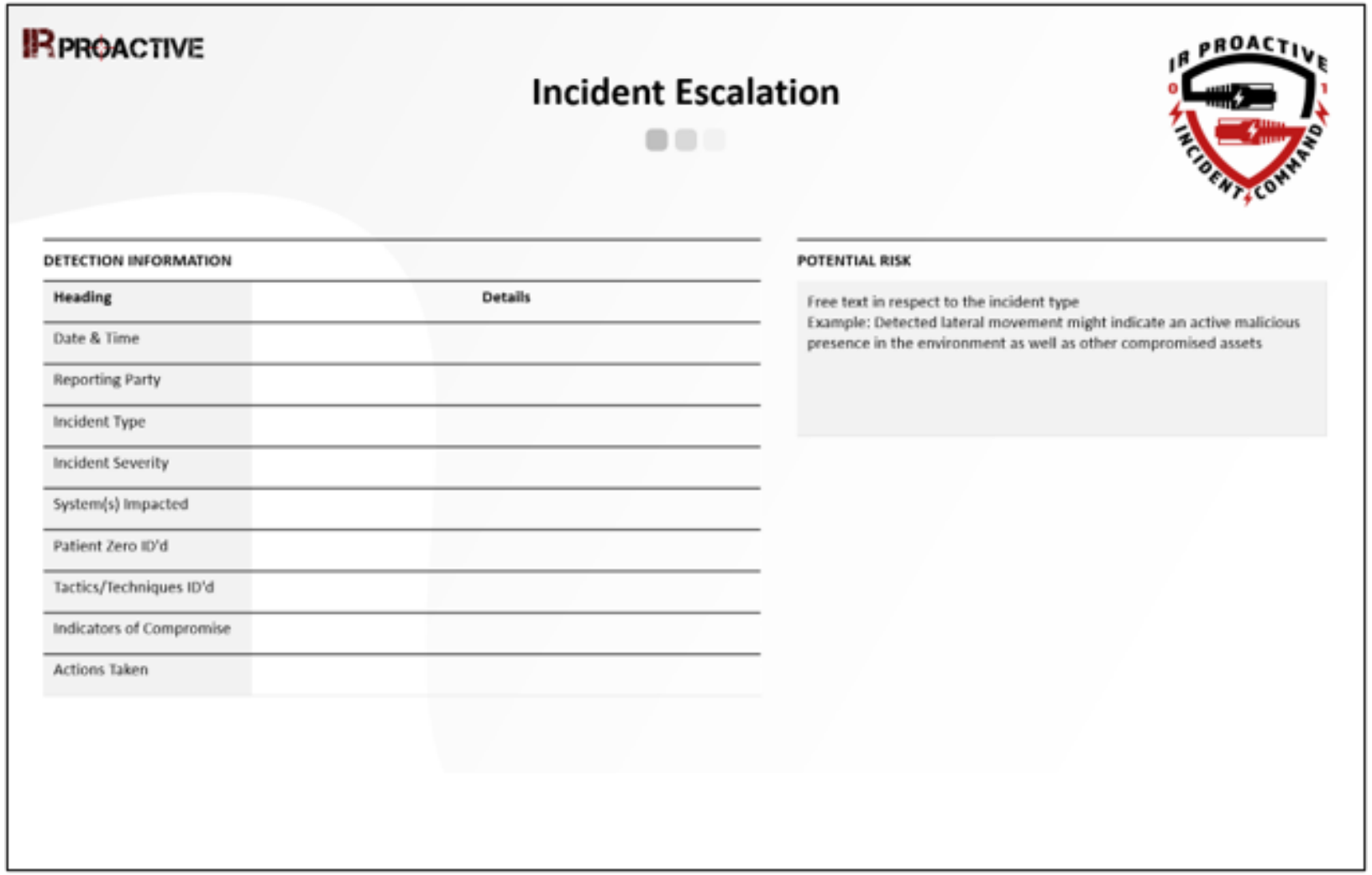
Significant Actions

- Gather pertinent details from SOC and other analysts
- Verify if an incident escalation is warranted

Process Output

- Incident Briefing: This can be a written or oral briefing that is prepared for the next stage of the ICLPs.

Incident Escalation Briefing



IR PROACTIVE

Incident Escalation

IR PROACTIVE INCIDENT COMMAND

DETECTION INFORMATION

Heading	Details
Date & Time	
Reporting Party	
Incident Type	
Incident Severity	
System(s) Impacted	
Patient Zero ID'd	
Tactics/Techniques ID'd	
Indicators of Compromise	
Actions Taken	

POTENTIAL RISK

Free text in respect to the incident type
Example: Detected lateral movement might indicate an active malicious presence in the environment as well as other compromised assets

Activate the CSIRT

Process Input

- Incident Briefing

Significant Actions

- Start building the Common Operational Picture for the CSIRT
- Identify any specific resources and personnel outside the core CSIRT
- Identify potential sources for Situational Awareness
- Task out personnel for evidence acquisition and analysis

Process Output

- Initial Analysis Tasking

Initial Analysis

1-4 Hours

Process Input

- Initial Analysis Tasking

Significant Actions

- Acquire key evidence artifacts
- Rapid analysis

Process Output

- Actionable IOCs

Initial Analysis

- A comprehensive analysis of all available evidence is not necessary.
- Focus on key evidence items to identify the following:
  - **Initial Access**: The key here is to identify how the threat actor was able to gain access: Software vulnerability, open remote access, phishing email.
  - **Execution**: We do not need a detailed malware analysis, but rather an understanding of what combination of malicious scripts, code, and LOLBINS have executed.
  - **Lateral Movement**: Threat actors almost universally move from system to system. Identify what software, ports and protocols are in use.
  - **Command and Control**: Cobalt Strike or other similar C2 frameworks are used. Identify URLs or IP addresses.

Initial Analysis

- From a tooling perspective, use tools that allow for remote evidence collection, scaling and hunting:
  - Remote collection tools such as EDR platforms or dedicated DFIR tools such as Velociraptor.
  - Digital forensic analysts may need to scale across multiple systems. Scripts or bulk collection and analysis.
  - Hunting for other associated indicators across multiple systems in the enterprise.
- Again, the goal here is to find indicators that can be leveraged for containment.

Deploy Containment

4-8 hours

Process Input

- Actionable IOCs

Significant Actions

- Determine if IOCs are sufficient to implement containment
- Develop a containment plan: Network, Credential, Host, Cloud
- Communicate to stakeholders the potential impact

Process Output

- Containment Confirmation

Update Incident Objs.

Process Input

- Updated analysis tasking

Significant Actions

- Update the analysis tasking with new IOCs, TTPs, Threat Intelligence
- Identify additional evidence sources
- Communicate to CSIRT members

Process Output

- Secondary Analysis Tasking

Secondary Analysis

Process Input

- Secondary Analysis Tasking

Significant Actions

- Conduct more detailed analysis of compromised systems
- Evidence acquisition and analysis
- Incorporate threat intelligence

Process Output

- Secondary analysis findings or Root Cause Analysis TTPs and IOCs

Secondary Analysis

- More wide reaching & comprehensive analysis.
- Add additional evidence and form a Root Cause.
- Focus on Post-exploitation:
  - **Persistence**: Identify mechanisms that threat actors use to maintain control over compromised systems.
  - **Credential Access**: What credentials were compromised.
  - **Exfiltration**: Were the threat actors able to acquire and exfil data.
  - **Impact:** What was the overall impact to the organization.

Eradication & Recovery

24-72 Hours

Process Input

- Secondary analysis findings or Root Cause Analysis TTPs and IOCs

Significant Actions

- Bring systems back up and running to pre-incident state
- Restore from backups (Execute Business Continuity/Disaster Recovery)
- Restore from known good image
- Enhanced monitoring

Process Output

- Confirm Eradication and Recovery

IR PROACTIVE

Close Out Incident

3-5 Days

Process Input

- Notes, Analysis Output, Collaboration Software Capture

Significant Actions

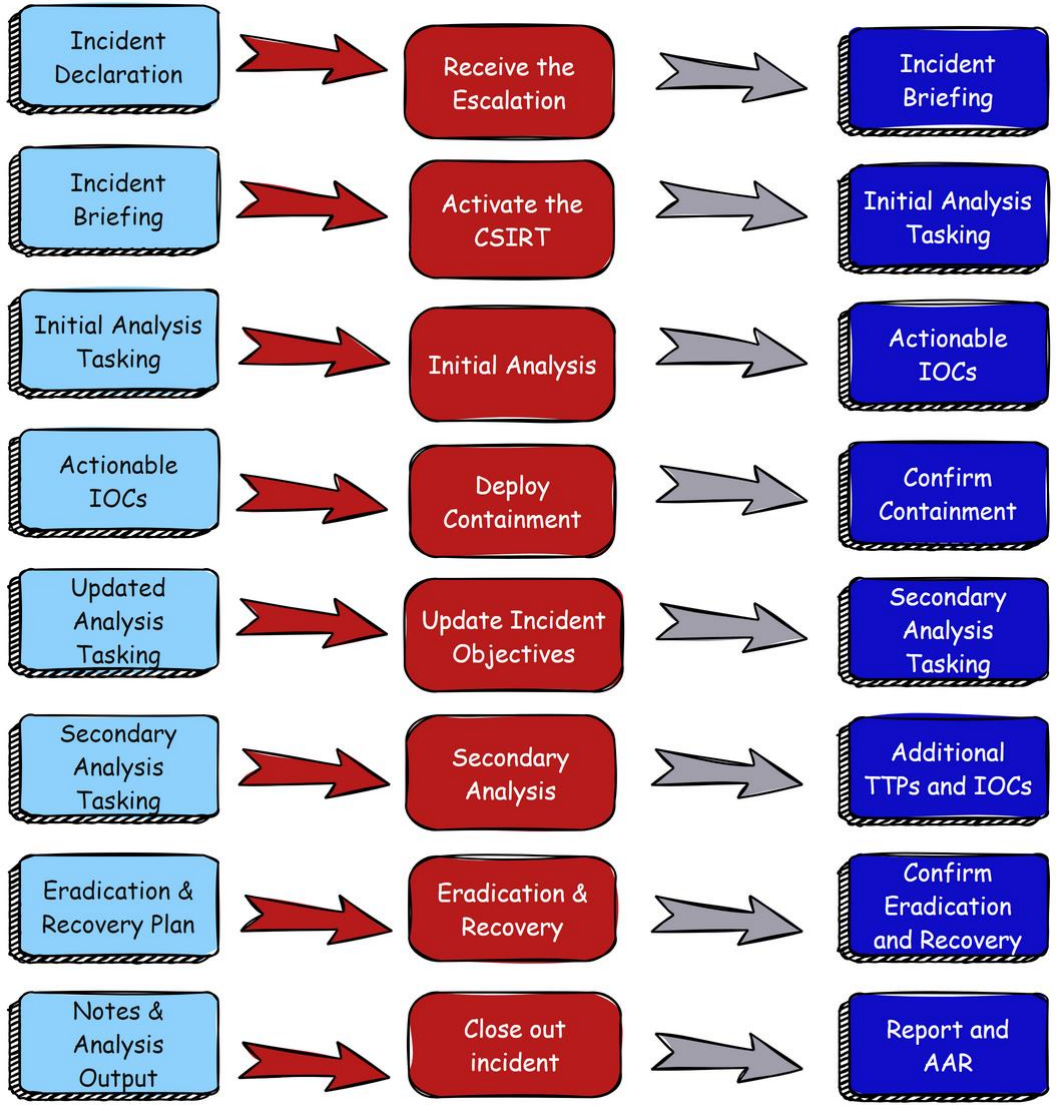
- Confirm with CSIRT that incident has concluded
- Conduct close-out briefing with all stakeholders
- Report or comprehensive out-brief
- After-Action Review with entire team

Process Output

- Report / Briefing docs
- Remediation & process improvement recommendations

Incident Command Leading Procedures

- The Incident Command Leading Procedures guides through the lifecycle of an incident.
- There are specific inputs and outputs for each phase.
- Often this moves from one to the other in a systematic fashion.



Communications

- Critical component of Incident Management and the Incident Commander role is addressing incident communications.
- Develop a Common Operational Picture: This is where everyone has a clear understanding of the overall incident along with their specific roles and tasks.
- Internal Communications: Communicate up and down – Network operations vs. Executives.
- The hard part is tailoring the message to the audience.
- External Communications: Customers, suppliers, regulators, social media.
- Regular cadence of communication during the incident.

Health and Welfare

- Incidents can have a stressful impact on everyone involved.
- There can be late nights or early mornings.
- Incidents can go on for days.
- Ensure you are working with the team to rotate people out, give them rest, get them fed.
- Ensure you have Incident Command backups to rotate in and out as well.
- Do not “Power through it”.
- Engage resources such as Employee Assistance Programs.
- Ensure that Incident Commanders have resources to ensure solid health and welfare.

Training and Exercises

- The larger the organization, the more resources and personnel are brought to bare.
- Exercises such as Breach and Attack Simulation, Purple Teaming and Table tops should include Incident Management components.
- Table-top Exercises are a necessity, not a nice to have.
- Incorporate various real-world scenarios.
- Focus on three key areas:
  - ✓ Technical: How do various individuals carry out tasks: Evidence Acquisition, Network Containment.
  - ✓ Intra-Team: How do you coordinate with your own team: Task division, reporting, communications.
  - ✓ Inter-Team: How does your team coordinate with the larger organization: Passing IOCs to network ops for blocking, disabling credentials.

IR PROACTIVE™

Email

gjohansen@irproactive.com

Our Address

Rapid City, SD

Thank You

For Your Time & Attention