

INCIDENT RESPONSE 9-LINE

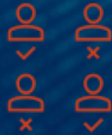
A tool for rapid incident escalation



INCIDENT RESPONSE – A LITTLE HUMOR



INCIDENT RESPONSE CHALLENGES



Various Teams from Security Operations, Incident Response, Security Management and third-party providers are needed for proper response.



Logs roll over quickly and evidence is at risk of destruction.



The stress of an incident often creates communication gaps during critical steps such as incident escalation

INCIDENT RESPONSE QUESTIONS

*What kind of incident
is it?*


How bad?

How many systems?

Are we blocking them?

MEDEVAC 9-LINE

- *High stress situations impact ability to communicate effectively*
- *Standard across all units*
- *Captures the necessary information to prepare various teams*
- *Trainable and repeatable process for everyone*

MEDEVAC REQUEST FORM		GTA 08-01-004
LINE	ITEM	EVACUATION REQUEST MESSAGE
1	Location of Pickup Site.	
2	Radio Frequ., Call Sign, & Suffix.	
3	No. of Patients by Precedence.	
4	Special Equipment Required.	
5	Number of Patients by Type.	
6	Security of Pickup Site (Wartime).	
6	Number and Type of Wound, Injury, or Illness (Peacetime).	
7	Method of Marking Pickup Site.	
8	Patient Nationality and Status.	
9	NBC Contamination (Wartime).	
9	Terrain Description (Peacetime).	

This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside U.S. Government agencies for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to Commander USATSC, ATTN: GTA Program Manager ATIC-ITST-T, Fort Eustis, VA 23064-5166. DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of document.

AUG 2002 (This supersedes GTA 08-01-004 MAY 1997)

DISTRIBUTION: US ARMY TRAINING SUPPORT CENTERS (TSCs)
HEADQUARTERS, DEPARTMENT OF THE ARMY,
ATTN: ATIC-ITST-T, GTA Program, Fort Eustis, VA 23604-5166

INCIDENT RESPONSE 9-LINE

1. DATE AND TIME OF DETECTION



- *First line is the simple one, Date and Time of the incident detection or declaration.*
- *Standardize the Date and Time format and zone: UTC vs. Local (UTC is preferable)*

2. REPORTING PERSON



- *Tie into the Incident Response Plan – SOC Manager, SOC Personnel, Security Analyst*
- *Everyone should be able to execute the Nine-Line escalation*
- *Included contact information:*
 - *Mobile and/or Desk Number*
 - *Email*
 - *IM*

3. INCIDENT TYPE



Incident Classification Criteria from Incident Response Plan

- ☐ *Ransomware*
- ☐ *Malware Infection*
- ☐ *Ongoing Compromise*
- ☐ *Data Exfiltration*
- ☐ *Command and Control*
- ☐ *Denial of Service*
- ☐ *Other*

4. INCIDENT SEVERITY



Incident Severity Criteria from Incident Response Plan

Severity Rating	Description
<i>Emergency</i>	<i>An Emergency priority incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.</i>
<i>Severe</i>	<i>A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>
<i>High</i>	<i>A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
<i>Medium</i>	<i>A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
<i>Low</i>	<i>A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>

5. NUMBER OF SYSTEMS IMPACTED



- *Define the number and OS of impacted systems*
- *Locations if geographically diverse*
- *Prepares Incident Responders:*
 - ✓ *Assists with identifying scope*
 - ✓ *Potential evidence sources*
 - ✓ *Containment*

6. PATIENT ZERO IDENTIFIED



- *This may not be possible during the initial reporting but in some circumstances be possible*
 - *Yes (Confirmed)*
 - *Yes (Unconfirmed)*
 - *No*

7. TACTICS IDENTIFIED



- *MITRE ATT&CK Framework*
- *Focus on those that are confirmed or that there is sufficient evidence*
- *Focus on brevity and focus on TTPs that can be acted on*
- *Ex.: “Adversary is using Cobalt Strike for C2 to an external system over HTTPS”*

8. INDICATORS OF COMPROMISE



- *What we have identified thus far*
- *Bias toward IOCs that can be immediately acted upon such as a Domain or URL*

9. ACTIONS TAKEN



- *What has the first team that touched this done? Evidence acquisition?
Containment?*
- *Tie back to Incident Response Plan and Playbooks*

9-LINE SAMPLES

ANALOG

Incident Response 9-Line

Code Name: **Atomic Squirrel**

1. Incident Detection Data and Time ☒ UTC ☐ Local
20210713T14:32

2. Reporting Person
Name: **John Smith** IM: **Jsmith**
Phone #: **989-321-9751** Email: **j.smith@yourcorp.com**

3. Incident Type
☒ Ransomware ☐ Malware Infection ☐ Data Exfiltration
☐ Command and Control ☐ Denial of Service ☐ Other: _____

4. Incident Severity
☒ EMERGENCY
☐ SEVERE
☐ HIGH
☐ MEDIUM
☐ LOW

5. Number of Systems Impacted:
Of Systems: **130+** Location(s): **Corp HQ** System(s): **WIN**

6. Patient Zero Identified ☐ Yes Confirmed ☒ Yes Suspected ☐ No
System Name: **Corp-Acct-015**

7. Tactics Identified:
- Lateral Movement via SMB
- C2

8. IOCs
- badurl.com - malware.exe
- 9.238.205.61

9. Actions Taken:
- FW Containment
- Disable SMB

DIGITAL

EMERGENCY Incident Escalation - Message (HTML)

File Message Insert Options Format Text Review Help Tell me what you want to do

Attach File Attach Item Assign Policy Dictate Sensitivity Switch Background Insights View Templates

Clipboard Basic Text Names Include Tags Voice Sensitivity Dark Mode My Templates

The following recipient is outside your organization: **cairt@evilcorp.com**

To: **cairt@evilcorp.com**

Cc:

Subject: EMERGENCY Incident Escalation

This is an incident escalation.

Incident Response 9-Line

Code Name: AtomicSquirrel

1. Incident Detection Data and Time ☒ UTC ☐ Local
20210713T14:32

2. Reporting Person
Name: John Smith IM: jsmith
Phone #: 989-321-9751 Email: j.smith@yourcorp.com

3. Incident Type
☒ Ransomware ☐ Malware Infection ☐ Data Exfiltration
☐ Command and Control ☐ Denial of Service ☐ Other: _____

4. Incident Severity
☒ EMERGENCY
☐ SEVERE
☐ HIGH
☐ MEDIUM
☐ LOW

5. Number of Systems Impacted:
Of Systems: **130+**
Location(s): **Corporate HQ, NYC**



Gerry Johansen

CISSP, GCTI, GRID, GNFA, GCFA

Gerry.johansen@optiv.com