
GUARDSIGHT
https://www.guardsight.com

GUARDSIGHT

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

VIRTUAL SECURITY OPERATIONS CENTER QUICK REACTION FORCE (VSOC QRF)

TABLE TOP EXERCISE (TTX)

vsoc@guardsight.com
844-482-7374

pool.sks-keyservers.net:
0x4D067DE9FB83E74B

TTX OBJECTIVE

ENSURE INCIDENT RESPONSE MISSION READINESS

Rewire For Speed
Embed Long Term DNA

TTX KEY RESULTS

1. DEFINE OPERATIONAL ROLES
2. DEFINE OPERATIONAL CHOREOGRAPHY
3. REVIEW CSIRT TACTICS, TECHNIQUES, PROCEDURES
4. REVIEW CRITICAL CONTAINMENT ASSETS
5. DISCUSS INCORPORATING IT SUPPORT TEAMS
6. DISCUSS PREPARING BUSINESS STAKEHOLDERS
7. DISCUSS FATIGUE MANAGEMENT
8. REHEARSE INITIAL RESPONSE TO ATTACK SCENARIO #1
9. IDENTIFY, REVIEW, & PLAN REMEDIATION OF TTX GAPS

TTX AGENDA

(~ 3 HOURS w/breaks)

1hr 10m

1. DEFINE OPERATIONAL ROLES: 15 min
2. DEFINE OPERATIONAL CHOREOGRAPHY: 20 min
3. REVIEW CSIRT TACTICS, TECHNIQUES, PROCEDURES: 20 min
4. REVIEW CRITICAL CONTAINMENT ASSETS: 15 min

30m

5. DISCUSS INCORPORATING IT SUPPORT TEAMS: 15 min
6. DISCUSS PREPARING BUSINESS STAKEHOLDER: 10 min
7. DISCUSS FATIGUE MANAGEMENT RULES: 5 min

1hr 5m

8. REHEARSE INITIAL RESPONSE TO ATTACK SCENARIO #1: 45 min
9. IDENTIFY, REVIEW, & PLAN REMEDIATION OF TTX GAPS: 20 min

- LOCATION
- FACILITATOR
- MINUTES
- PARTICIPANTS
- Q&A PROTOCOL
- ETIQUETTE
- BREAKS
- SUSTENANCE

TTX GUIDING RESOURCES

TACTICAL CYBERSECURITY INCIDENT RESPONSE PLAN

https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan

AFTER ACTION REPORT TEMPLATE

https://github.com/guardsight/gsvsoc_mission-model

INCIDENT RESPONSE PLAYBOOK BATTLE CARDS

https://github.com/guardsight/gsvsoc_cirt-playbook-battle-cards

W-0028

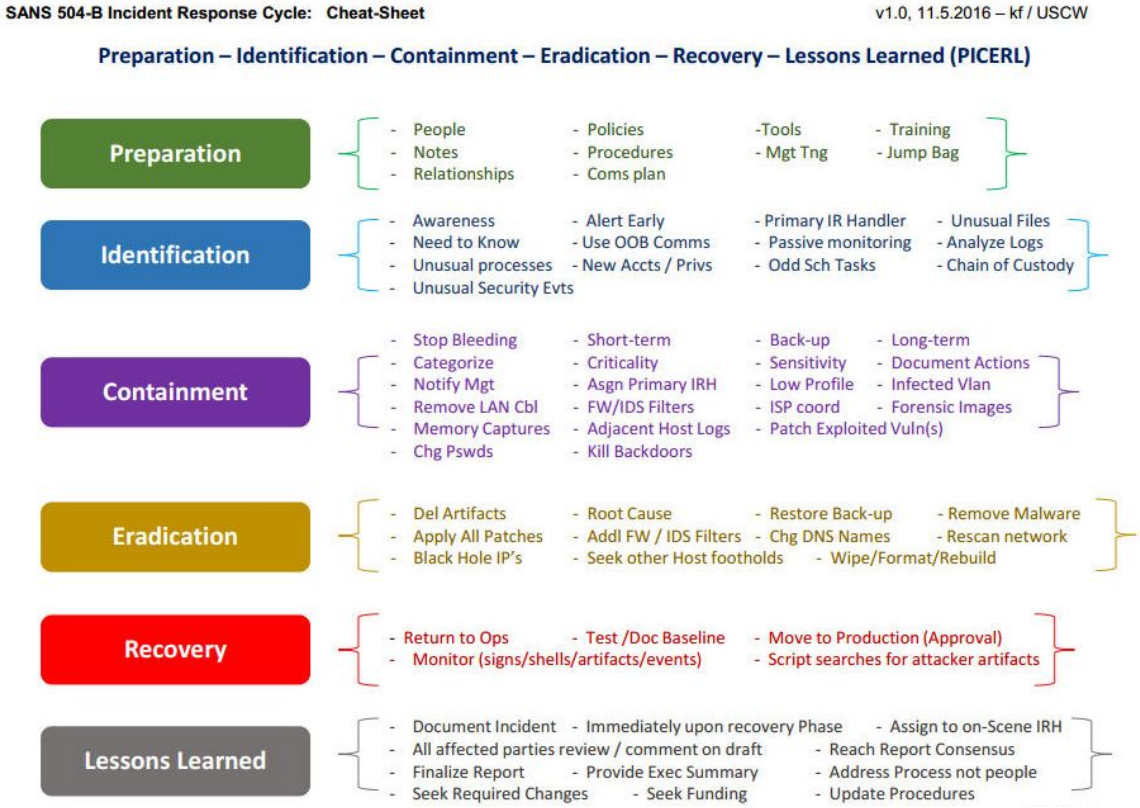
Instruction:W-0028 - How-To Conduct Information Security Incident Response Activities

EXPERIENCE!

PICERL

- PREPARATION
- IDENTIFICATION
- CONTAINMENT
- ERADICATION
- RECOVERY
- LESSONS/OFI

TTX GUIDING RESOURCES

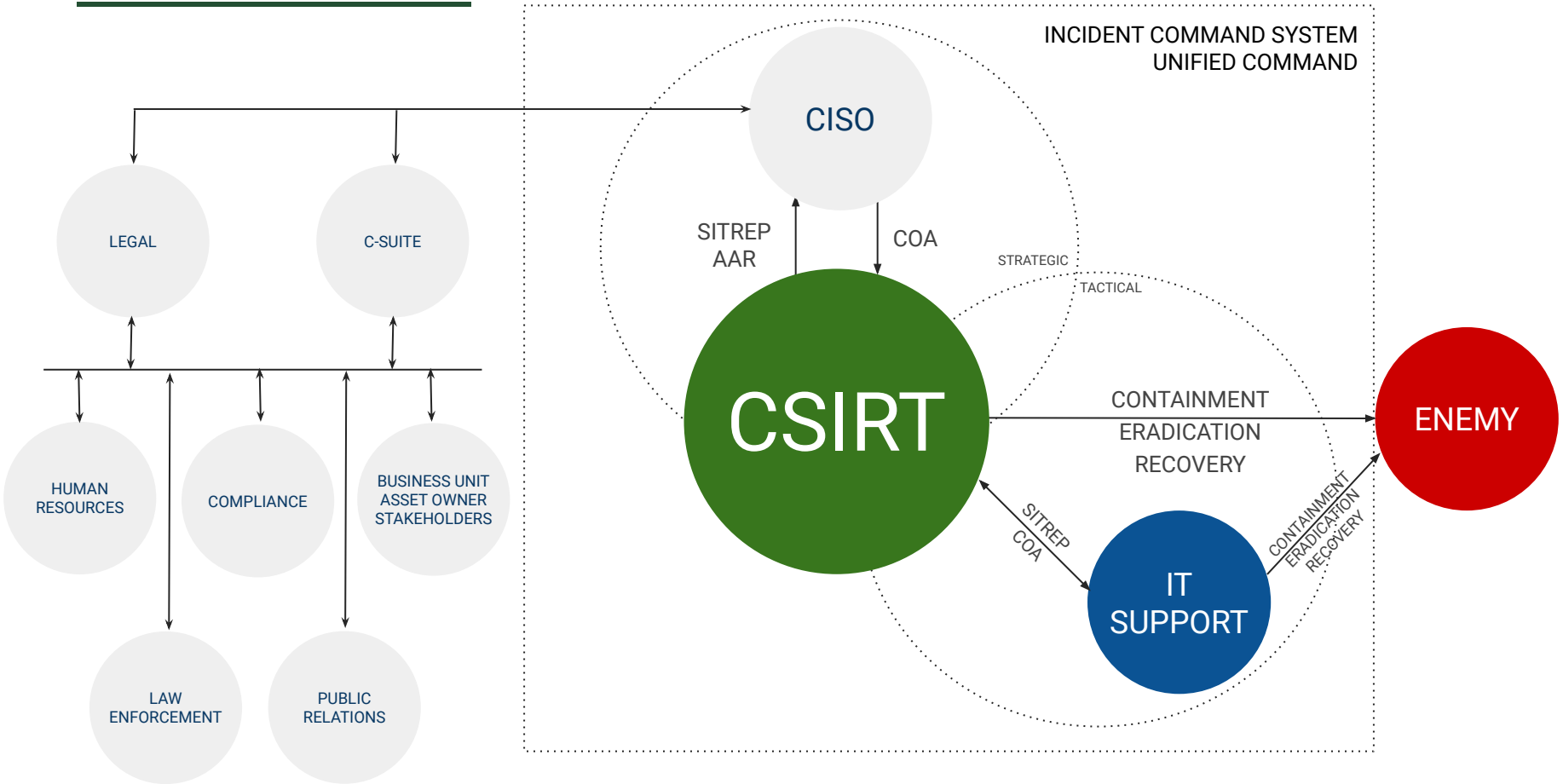


GUARDSIGHT

CSIRT MISSION PRIORITY #1

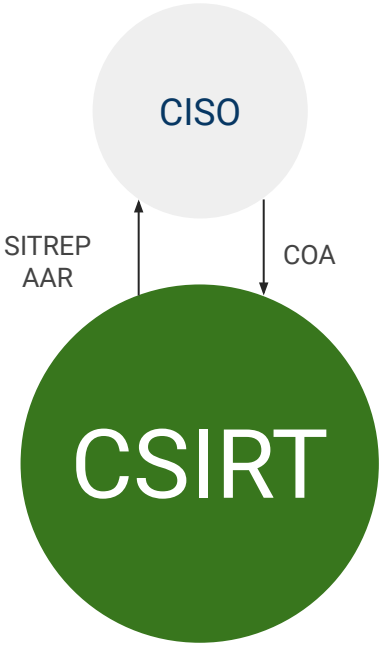
CONTAIN THE THREAT

OPERATIONAL ROLES



GUARDSIGHT

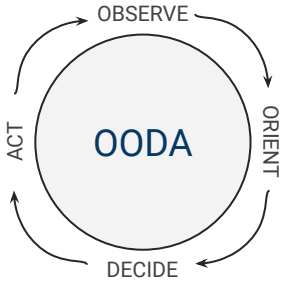
OPERATIONAL ROLES



COMMAND RANK

01 **INCIDENT COMMANDER**
Mission Captain

1. Tactical Authority
2. Resource allocation
3. CISO Comms & Briefings
4. COA Planning & Delegation
5. SITREP Cadence & Approval
6. AAR Custodian & Dissemination



02 **SCRIBE**
Mission Support

1. AAR Journal Entries
2. Command Center Initiation
3. Evidence Locker Custodian
4. COA Coordination & Feedback
5. SITREP Comms & Dissemination

03 **QRF PERSONNEL**
First Responder

1. Impact Assessment & Severity Rating
2. Containment COA Guidance
3. Timelines Corroboration
4. Kill Chain Analysis & Forensics
5. OFI Suggestions

04 **VSOC & IT SUPPORT**
COA Execution

1. SITREP Feedback
2. Asset Owner Support
3. Flank Observation (“watch the wire!”)
4. OFI Suggestions

GUARDSIGHT

OPERATIONAL CHOREOGRAPHY

GET IN THE CYBER FIGHT!

BREATHE -> OODA

REDUCE DWELL TIME -> CONTAIN THE THREAT

GENERAL ORDERS FOR INITIAL MISSION ENGAGEMENT

ROLE	PREPARE → IDENTIFY → CONTAIN → ERADICATE
QRF (First Responder)	1st 15 Minutes: Perform an impact assessment, communicate a severity rating to SECOPS, develop COA
INCIDENT COMMANDER (Mission Captain)	1st 20 Minutes: Comms with CISO, declare CSIRT mission, engage mission resources, review COA
SCRIBE (Mission Support)	1st 25 Minutes: Create AAR journal, establish command center, distribute SITREP
VSOC & IT SUPPORT (COA Execution)	1st 30 Minutes: Assign delegate(s) for command center participation, execute COA

GUARDSIGHT

OPERATIONAL CHOREOGRAPHY

GET IN THE CYBER FIGHT!

BREATHE -> OODA

REDUCE DWELL TIME -> CONTAIN THE THREAT

GENERAL ORDERS FOR STEADY STATE MISSION ENGAGEMENT

ROLE	CONTAIN →	ERADICATE →	RECOVER →	LESSONS/OFI
QRF (First Responder)	Develop & execute COA, kill chain analysis, submit evidence, populate AAR journal, attend OFI			
INCIDENT COMMANDER (Mission Captain)	Comms w/CISO, SITREP cadence, develop & review COA, allocate resources, populate & issue final AAR, attend OFI			
SCRIBE (Mission Support)	Distribute SITREP, maintain evidence locker, populate AAR journal, coordinate resources, attend OFI			
VSOC & IT SUPPORT (COA Execution)	Execute COA, submit evidence, populate AAR journal, attend OFI			

CSIRT TTP: QRF & FIRST RESPONDER ASSESSMENT RATING METHOD

GET IN THE CYBER FIGHT!

BREATHE -> OODA

REDUCE DWELL TIME -> CONTAIN THE THREAT

1. BREATHE
2. THINK "SMOOTH IS FAST"
3. INSPECT CHANGE LOGS TO DETERMINE IF ACTIVITY IS POSSIBLY THE RESULT OF AN AUTHORIZED CHANGE
4. REVIEW SYSTEM BASELINES TO DETERMINE IF ACTIVITY IS POSSIBLY THE RESULT OF EXPECTED BEHAVIOR
5. ASK ASSET OWNERS ABOUT OBSERVED INDICATORS OF COMPROMISE (IOC) AS A METHOD OF IOC COMMUNICATION
    a. USE TOP INDICATORS OF COMPROMISE (TOP-IOC)
    b. USE MITRE ATT&CK FRAMEWORK
6. ASK ASSET OWNERS "WAS THERE A LOSS OF DATA?"
7. ASK ASSET OWNERS "WAS RESTRICTED DATA AT RISK?"
8. ASSIGN AND COMMUNICATE A SEVERITY RATING TO SECOPS COMMAND USING 3-7 AS THE REASONING
    a. USE NCCIC CISS SEVERITY RATING MODEL

CSIRT TTP: CREATE AN AFTER ACTION REPORT (AAR) JOURNAL AT **_MISSION INITIATION_**

KEY BENEFITS OF ITERATIVE AAR JOURNALING

- **Better team communications**
- **Concurrent memorializing in real-time**
  Operational Transformation Algorithm (OTA)
- **Increased accuracy of observations**
- **Improved intra/inter knowledge transfers**
- **Fatigue management instrument**
- **High fidelity evidence recording**
- **Documented stream of intent**
- **Event posterity**

Total Impacted Assets:	0
Time To Respond:	0 Minutes
Total Dwell Time:	0 Days
Response Duration:	0 Hours
Weaponization:	Phishing / Malspam
Exploitation:	TrickBot / Emotet
Installation:	Ryuk / Powershell Empire
Data Compromise:	Negative
Date Legal Notified:	Not Required
Evidence Locker:	SEE NOTES

GUARDSIGHT

Incident Response After Action Report

Prepared For:

ACME Corp.

Document Profile:

Mission Id:	MISSION-YYYYMMDD-1	MISSION IDENTIFIER
Revision Id:	1.1	CURRENT REVISION
Date:	2020-00-00	DATE OF LAST UPDATE
Rating:	SEVERE (NCCIC CISS)	WHAT'S THE SEVERITY?
COA Completion:	0/0 - n%	WHAT'S OUR PROGRESS?
Condition:	GUARDED (HSAS)	WHAT'S THE STATUS?
Authorized Distribution:	alice@acmecorp.com, bob@acmecorp.com	WHO'S IN THE KNOW?

CONFIDENTIAL//ATTORNEY-CLIENT PRIVILEGE//TLP:AMBER

This document is an after-action report that provides the details of an Information Security Incident signifying a violation of computer security policies, acceptable use policies, or standard security practices resulting in a compromise of this organization's assets.

This document is designated as Traffic Light Protocol (TLP): AMBER. Recipients may share TLP: AMBER information with members of their organization who need to know, and only widely as necessary to act on that information.

This document contains confidential and privileged material. Any interception, review, retransmission, dissemination or other use of or taking any action upon this information by persons or entities other than the intended recipient(s) is prohibited by law and may subject them to criminal or civil liability. This document contains material that may have been commissioned by counsel in anticipation of litigation. It should be treated as confidential to avoid waiver of the attorney/client privilege, the work-product privilege, or another applicable privilege. It was prepared for the sole use of the named recipient, and must not be relied upon by any third party.

This document is a deliverable that meets or exceeds a standard of reasonable cybersecurity practices.

CSIRT TTP: ISSUE CONSISTENT SITUATION REPORTS (SITREP) DURING THE MISSION

Subject: [acmecorp] | MISSION-19700101-1 | 0 | SIT SITREP IDENTIFIER

Update

===== As of: 1970-01-01 21:30 MT =====

COA progress: 12/31 - 38% WHAT'S OUR PROGRESS?

Threat actor fully contained as of 01-01 21:18 MT

Courses Of Action WHAT ARE OUR COA?

===== COA: Inventory =====
[acmecorp] Verify that shared drives were not impacted
[acmecorp] Verify servers were not impacted
[acmecorp] Verify backups were not impacted
[acmecorp] Verify VSS on assets were not impacted
[guardsight] Conduct initial forensics assessment
[guardsight] Reconstruct IOC for Timelines and Cyber Kill Chain
[guardsight] Examine external intelligence for IOC related to acmecorp
[guardsight] Generate list of known IOCs (SEE IOC)
[guardsight] Scan network for vulnerabilities

WHO OWNS THE COA?

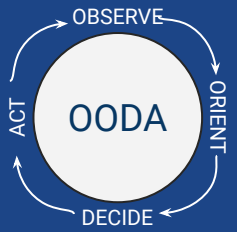
===== COA: Containment & Eradication ==== WHAT ARE OUR COA?
[guardsight] Terminate network activity for known compromised assets
[guardsight] Search the environment for IOCs
- Ransomware Notes
- Unusual file extensions
- Emails with executable attachments or links
- DNS Anomalies
- CPU Spikes
- Connection Anomalies
- Port Anomalies
- Atomic/IP IOCs
- Behavioral/C2 IOCs
- Computed IOCs
[guardsight] Add known IOC to watchlists
[acmecorp] Restore from backups
[acmecorp] Deploy GS provided hunter killer agent
[acmecorp] Re-image specific impacted assets
[acmecorp] Reset the krbtgt hash 2 times.
[acmecorp] Rebuild domain servers
[acmecorp] Implement Perimeter Enforcement
- biz@baz[.]com (Original Sender)
- 0.0.0.[.]0 - C2 Agent addr (0.0.0.0/22 - RIPE/DE)
- 0[.]0.0.0 - RAT access source addr (0.0.0.0/24 - REGRU-RU/RU)
[acmecorp] Patch asset vulnerabilities

Completed COAs WHAT COA ARE COMPLETED?

[guardsight] Mission command center opened
[guardsight] Conduct forensic analysis of provided hardware
[guardsight] Investigate email logs for outbound emails
[guardsight] Obtain original inbound email headers

THINK OF COA AS "INVENTORY + 6-D's"

1. INVENTORY
2. DETECT
3. DENY
4. DISRUPT
5. DEGRADE
6. DECEIVE
7. DESTROY



GUARDSIGHT

CRITICAL CONTAINMENT ASSETS

CONCENTRIC -> ENCIRCLEMENT -> DEFENSE IN DEPTH -> CHOKE -> CONTAIN THE THREAT

CONTAINMENT ASSETS ARE THE CYBER WEAPONS/TOOLS USED TO FIGHT THE **ENEMY**. WHEN A CYBER ATTACK OCCURS, IT IS CRITICAL THAT THOSE ASSETS AND THEIR CAPABILITIES ARE KNOWN, AVAILABLE, AND FUNCTIONING PROPERLY (AT THE READY).

USE CONTAINMENT ASSETS TO REGAIN CONTROL OF THE IMPACTED ASSETS!

PRIOR TO AND DURING A CYBER FIGHT KNOW THE FOLLOWING ABOUT CONTAINMENT ASSETS:

1. LOCATION
    a. *Provides:* Proximity to Attacker, Relevance to Impacted Assets
2. NUMBER
    a. *Provides:* Enumeration, Coverage Strength
3. CAPABILITY
    a. *Provides:* Optics, Inventory, Detect, Deny, Disrupt, Degrade, Deceive, Destroy
4. OWNERS
    a. *Provides:* Authority, Team Proficiency, History of Cooperation
5. FRICTION
    a. *Provides:* Time to Implement, Business Impact, Collateral Damage Potential

INCORPORATING IT SUPPORT TEAMS

1. **CREATE VISIBILITY AND AWARENESS**
    a. **PRODUCE CSIRT MARKETING MATERIALS**
2. **MARKET TO IT SUPPORT TEAMS**
    a. **DISTRIBUTE CSIRT MARKETING MATERIALS**
3. **INVITE IT SUPPORT TEAMS TO COLLABORATE**
    a. **COMMUNICATE TIME, PLACE, & AGENDA**
4. **INVITE IT SUPPORT TEAMS TO PARTICIPATE IN A TTX**
    a. **DEFINE THEIR ROLE**
    b. **DEMONSTRATE THEIR CONTRIBUTIONS**

PREPARING BUSINESS STAKEHOLDERS

1. **CREATE VISIBILITY AND AWARENESS**
    a. **PRODUCE CSIRT MARKETING MATERIALS**
2. **MARKET TO STAKEHOLDERS**
    a. **DISTRIBUTE CSIRT MARKETING MATERIALS**
3. **INVITE STAKEHOLDERS TO COLLABORATE**
    a. **COMMUNICATE TIME, PLACE, & AGENDA**
4. **INVITE STAKEHOLDERS TO PARTICIPATE IN A TTX**
    a. **DEFINE THEIR ROLE**
    b. **DEMONSTRATE THEIR CONTRIBUTIONS**

FATIGUE MANAGEMENT

INCIDENT RESPONSE IS A HIGHLY DYNAMIC ECOSYSTEM THAT OFTEN CREATES EXCESS DEMAND ON HUMAN PHYSIOLOGY. IT IS UNREALISTIC TO THINK THAT HUMANS CAN MAINTAIN THE PACE OF PROLONGED IR AND SUSTAIN THE CRITICAL THINKING THAT A CSIRT MISSION DEMANDS.

MANAGE CSIRT TEAM FATIGUE TO MAINTAIN A HIGH LEVEL OF RESPONSE.

1. **OODA IS YOUR FRIEND**
2. **DEFINE SHIFTS EARLY AND INFORM THE TEAMS PERFORMING COA**
3. **SITREPs ARE YOUR FRIEND**
4. **CSIRT TO FLOOD THE CISO ZONE WITH INFORMATION**
5. **MAINTAIN PHYSIOLOGY**

SCENARIO #1 EXERCISE

Attack	Ransomware
Alert Source	Business users working remote
Exercise Objective	1. Drill on initial phases of CSIRT engagement a. Validate the transition from Alert -> SITREP #1 b. Confirm establishment of infrastructure from Alert -> SITREP #1 c. Evaluate comms taxonomy between QRF -> IC -> CISO -> CISRT -> SITREP #1 to COA teams (*SECOPS receipt only for Scenario #1*) 2. Develop @Backlog of OFI
Capabilities Exercised	1. QRF impact assessment, severity rating and communication to SECOPS leadership (IC) 2. IC leadership comms and assignment 3. IC CSIRT resource preparation for possible MISSION 4. IC severity rating comms with CISO & authorization of MISSION 5. CSIRT assembly and MISSION engagement 6. QRF & IC initial containment COA definition 7. Command Center opening, AAR initiation, creation & distribution of SITREP #1 to COA teams (*SECOPS receipt only for Scenario #1*)
Scenario	<u>Day-1 @ 10:15 CT</u> Multiple users from a single business unit contacted the IT help desk reporting the inability to open files on at least one shared drive location. The IT help desk team contacted IT Administrators at 10:20 requesting they investigate. System administrators contacted SECOPS at 10:45 to convey a possible ransomware attack. SECOPS analysts review initial data and report it to QRF at 11:00. <u>Day-1 @ 11:00 CT</u> QRF is now engaged: what happens next?

SCENARIO #1 INITIAL COMMS HINTS FROM CSIRT -> CISO

QRF -> SECOPS -> CSIRT IC -> CISO -> CSIRT

1. Time now is 11:15 CT (24HR time)
2. QRF was engaged @ 11:00 CT today for a report of ransomware
3. SECOPS (we) has confirmed that several assets are negatively impacted and consistent with ransomware based on the following observations and data:
    a. Multiple user reports of impacted assets
        i. Majority of users reporting are affiliated with the accounting department
        ii. The help desk has a list of the usernames and times recorded - SECOPS has requested the IT Help Desk preserve this information
    b. TOP-IOC:
        i. Confirmation that the activity is NOT consistent with authorized changes
        ii. Confirmation that the activity is NOT consistent with system baselines
        iii. Confirmation of multiple files encrypted on accounting department file sharing system
        iv. Attack surface DOES exist - File shares
        v. Activity IS CONSISTENT with unusual lateral movement
        vi. Activity IS CONSISTENT with unusual egress network traffic
4. SECOPS has *SUFFICIENT* data/intel from threat detection assets to believe the attack is ongoing
    a. Egress traffic to a known bad IPV4 (RIPE/DE)
    b. Lateral source activity from a single IPV4 (RFC1918)
5. QRF has assessed the situation as *SEVERE* and SECOPS is recommending initiating a formal CSIRT MISSION
6. If the CSIRT MISSION is approved, expect SITREP #1 distribution at 11:25 CT with the following initial COA:
    a. [itsupport] Perimeter enforcement to arrest the egress network traffic to known bad IPV4
    b. [itsupport] Distribute a SECOPS provided EDR hunter/killer agent to source asset exhibiting lateral movement and other known impacted assets
    c. [secops] Terminate the threat at endpoints using EDR

SCENARIO #1 CONSIDERATIONS

1. Do IT Help Desk / IT Administrators know how to contact SECOPS?
2. Was a standard communication taxonomy, & severity rating used between QRF -> SECOPS -> CSIRT -> CISO?
3. Did essential personnel ONLY operate in the command center?
4. Was there a flow of communication established between the CSIRT <-> CISO <-> C-SUITE/LEGAL?
5. Were COA entries derived from a Playbook Battle Card (PBC)?
6. Did the CSIRT have a distribution list for SITREP #1?
7. Did SITREP #1 include command center info, COA progress, expected containment ETA, and next update?

<sidebar specific to ransomware>

If ransom needs to be paid (think extortion in addition to encryption), does the company have an external relationship with a legal/insurance firm experienced in ransomware negotiation? Does a Bitcoin facility exist?

GAPS / TEAM OFI (@Backlog)

1.