Water Information Sharing and Analysis Center

DHS Hunt and Incident Response Team
September 12, 2018

Presenter

- Brian Draper, DHS NCCIC HIRT

Slides and recording will be posted by Thursday.

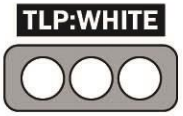
National Cybersecurity & Communications Integration Center (NCCIC)

HUNT AND INCIDENT RESPONSE TEAM (HIRT)

Brian Draper
Sr. Incident Response Analyst
NCCIC Hunt and Incident Response Team (HIRT)

Homeland Security

DISCLAIMER



DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this report or otherwise.

This document is distributed as TLP:WHITE: Subject to standard copyright rules.

TLP: WHITE information my be distributed without restriction.

For more information on the Traffic Light Protocol, see:

https://www.us-cert.gov/tlp.

Agenda

1. HIRT Overview
2. HIRT Service Offerings
3. Proactive Hunt vs. Incident Response
4. Incident Response Lifecycle
5. Prioritizing Incidents
6. Engagement Types
7. Engagement Workflow
8. How to Contact HIRT








Hunt & Incident Response Team (HIRT)

The National Cybersecurity Communications and Integration Center (NCCIC) Hunt and Incident Response Team (HIRT) provides expert intrusion analysis and mitigation guidance to clients who lack the in-house capability or require additional assistance with responding to a cyber incident.

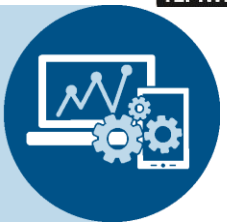
HIRT's clients include:

- Federal departments and agencies
- State, Local, Tribal and Territorial (SLTT) governments
- Private Sector (Industry & Critical Infrastructure)
- Academia
- International Organizations

Uniquely positioned to provide comprehensive analysis

- Classified and unclassified tactics, techniques and procedures (tips)
- Public and private sector partners
- Established relationships with Law Enforcement, Intelligence Community and International Partners

HIRT Service Offerings



✓ Incident Triage	✓ Hunt Analysis
✓ Network Topology Review	✓ Mitigation
✓ Infrastructure Configuration Review	✓ Malware Analysis
✓ Log Analysis	✓ Digital Media Analysis
✓ Incident Specific Risk Overview	✓ Control System Incident Analysis

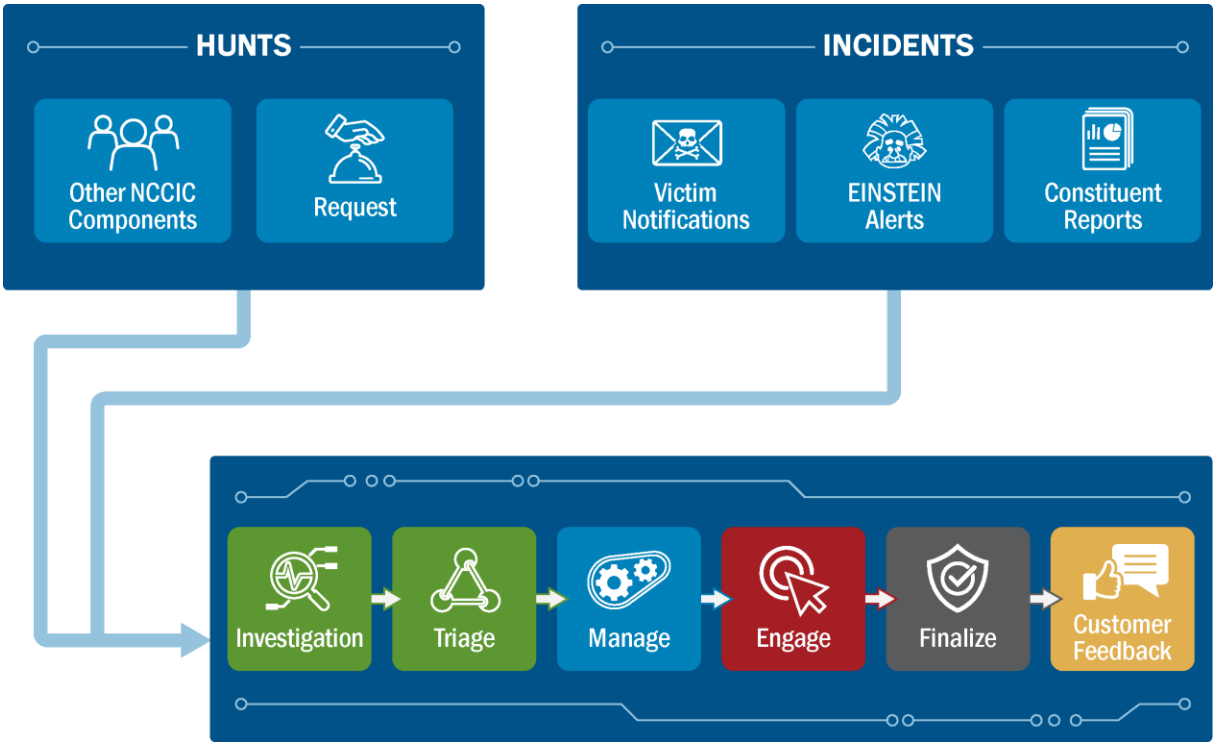
Proactive Hunt

Incident Response

- A search for malicious activity through the examination of a network environment for exploitation tools, tactics, procedures, and associated artifacts
- An asset owner-driven request
- Uses a risk review to scope the breadth of the Proactive Hunt
- If malicious activity is observed during a hunt, move to Incident Response

- HIRT takes action to respond to a reported incident and to address the increased risks generated by the incident
- Asset owners and trusted third parties report information to NCCIC.
  - Trusted reporters include FBI, Information Sharing and Analysis Centers (ISACs), and other government agencies
- Uses a risk review to scope the breadth of the Incident Response

HIRT Incident Response Lifecycle



NCISS Solution

NCCIC Cyber Incident Scoring System (NCISS)

Based on NIST 800-61 Revision 2

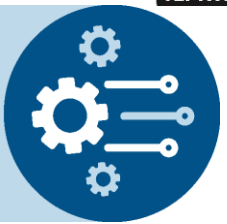
- Functional Impact
- Information Impact
- Recoverability
- Adds Actor Characterization
- Adds Observed Activity
- Adds Location of Observed Activity
- Adds Cross Sector Dependency
- Adds Potential Impact

Uses a weighted average (math) of the above criteria for a repeatable process

PRIORITY

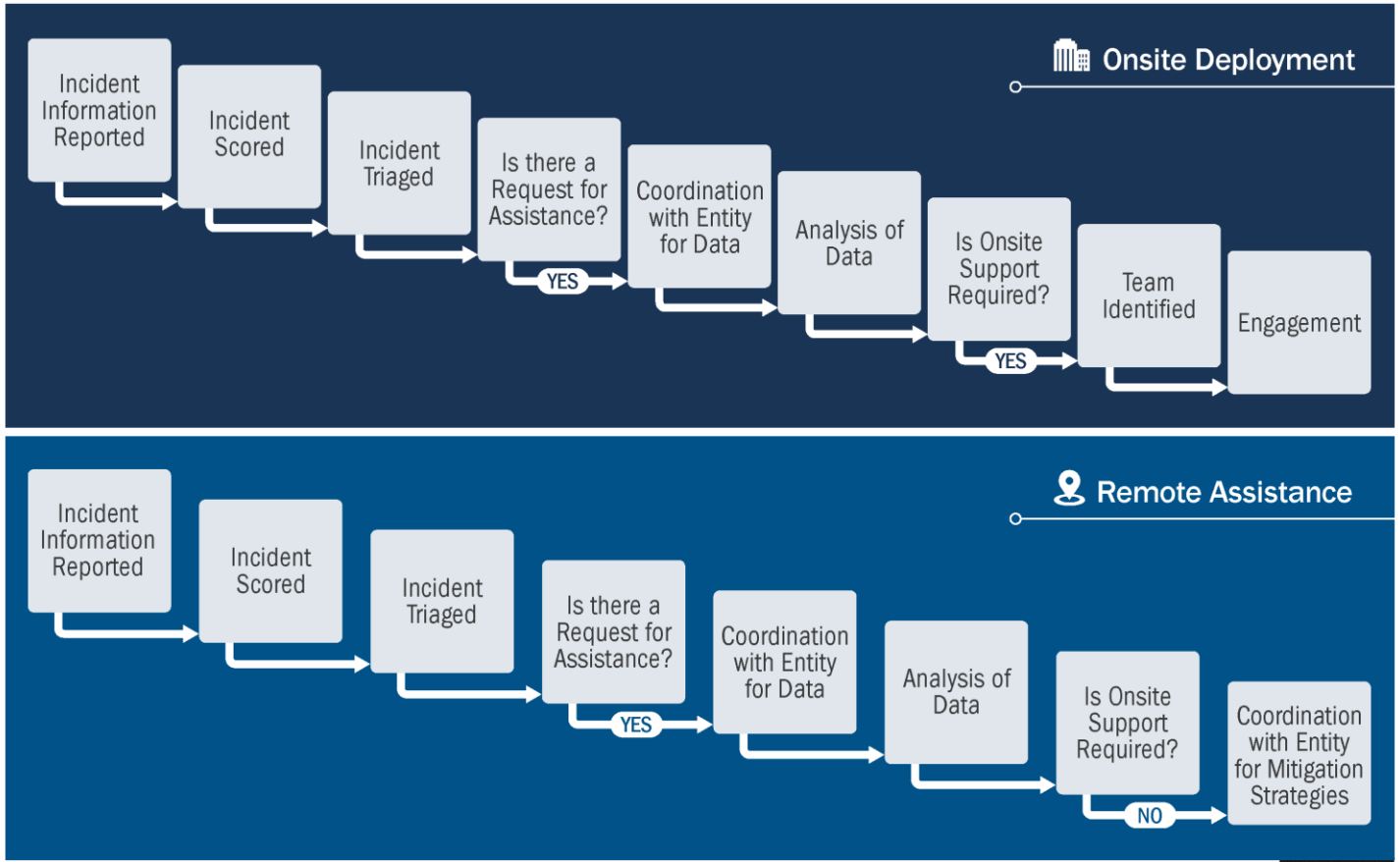
- Emergency
- Severe
- High
- Medium
- Low
- Baseline - Minimal
- Baseline - Negligible

Engagement Types



Remote Assistance	Providing assistance without being physically onsite
Advisory Deployment	Advising for mitigation onsite but technical analysis capabilities not deployed
Remote Deployment	Deploying Equipment, remotely conducting analysis
Onsite Deployment	Deployment of equipment and personal onsite to conduct technical analysis

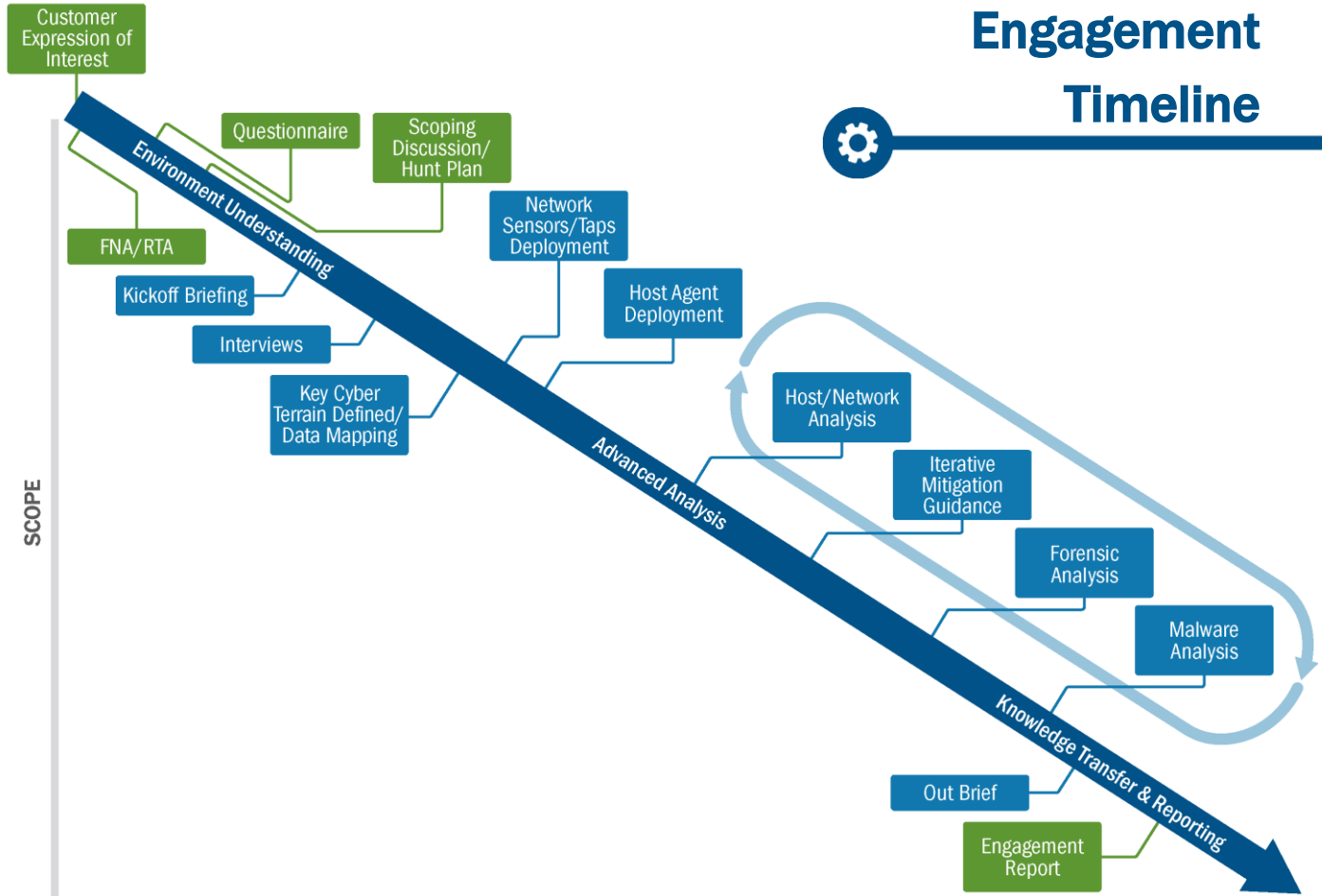
Incident Response Workflow



TLP:WHITE

Onsite Deployment Team Composition

Engagement Timeline



TLP:WHITE

How to Contact NCCIC for Hunt and Incident Response Services

OPERATIONS

Email: ncciccustomerservice@hq.dhs.gov

Phone: 888-282-0870

Homeland Security

Upcoming WaterISAC Events and Opportunities

- Monthly Water Sector Cyber Threat Web Briefing
  - Wednesday, September 26, 2018; 2:00 – 3:00 PM ET

Thank You

WaterISAC Contact Information:

1-866-H2O-ISAC

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

Paul Laporte
Member Relations Manager
laporte@waterisac.org

Chuck Egli
Lead Analyst
egli@waterisac.org

Jennifer Walker
Cybersecurity Risk Analyst
walker@waterisac.org