Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

July 2014

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

1. Modify the tabletop scenario as needed to conform to your environment.

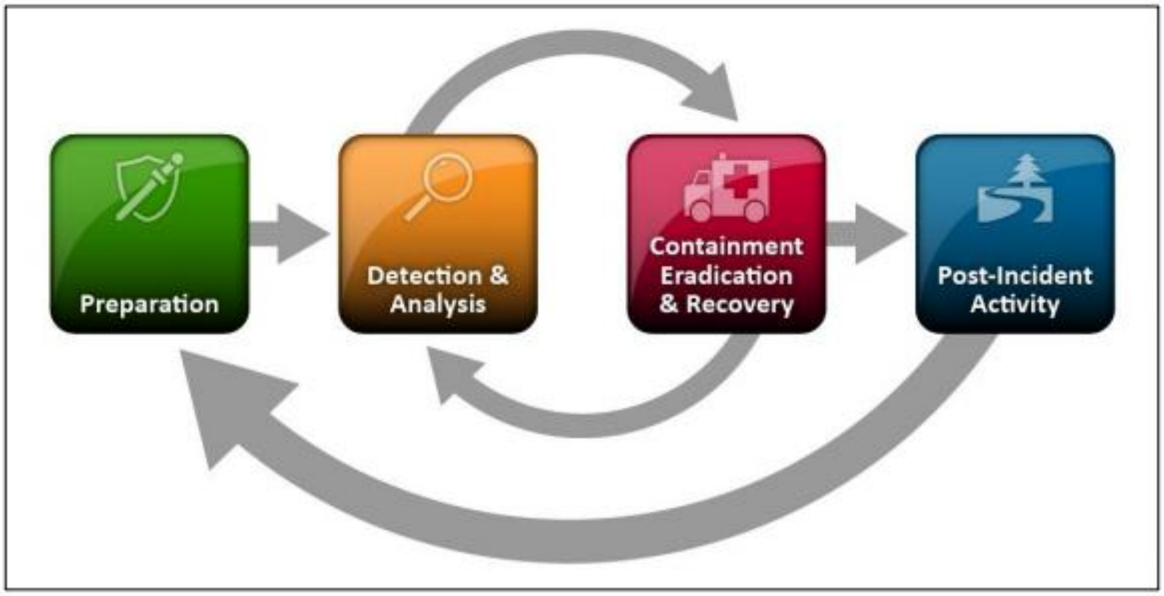
2. Engage management.

3. Present scenario to the workgroup.

4. Discuss the process to address the scenario.

5. Document the response and findings for future reference

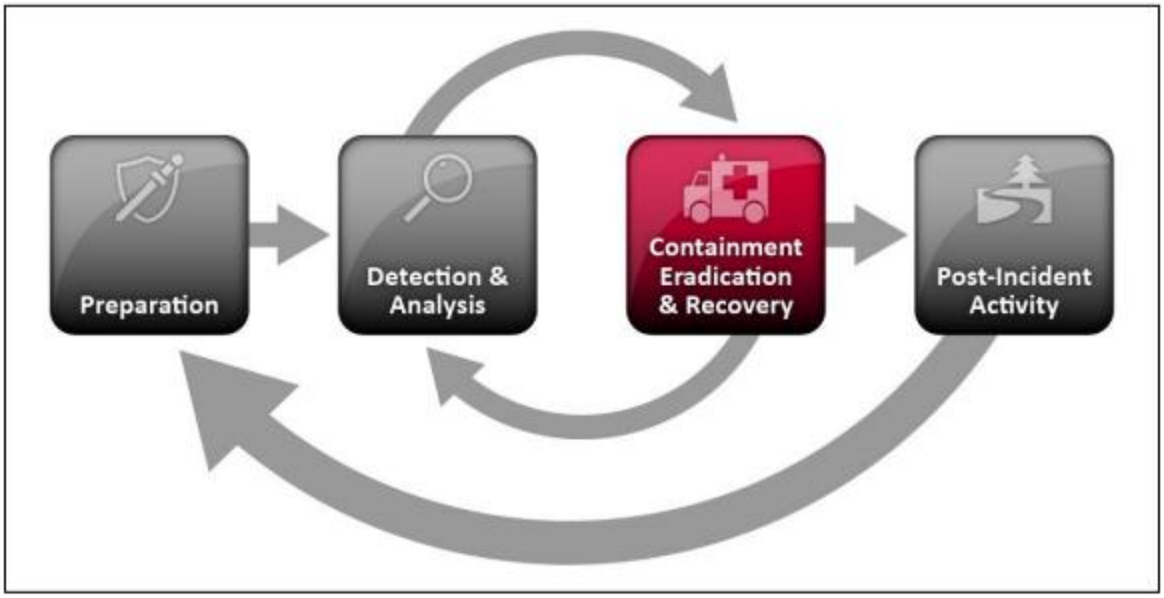
Note: A member of the CTS Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the CTS Service Desk at 360-753-2454.



EXERCISE SCENARIO

Upon review of your logs, several of your organization’s internet facing assets are being scanned. After investigation, the scans are originating from what seems to be a legitimate private cyber security company.

The private company acknowledges the scans but refuses to disclose any information such as who ordered the scans due to a non-disclosure agreement (NDA). The scans from the same source continue to scan other external facing assets and the private company still refuses to disclose any information.

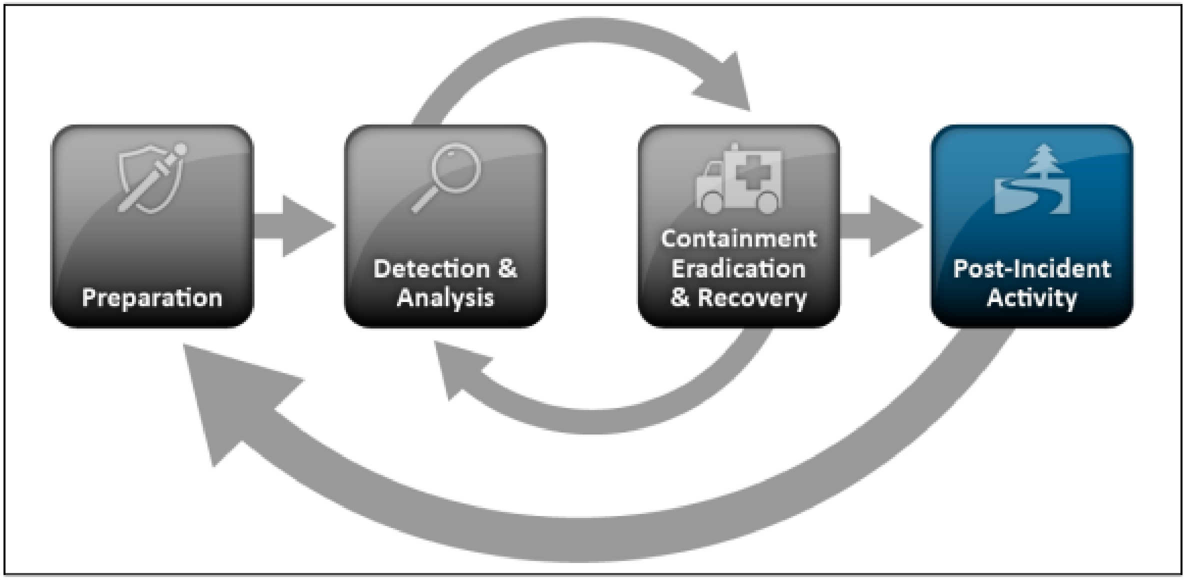


ITEMS TO DISCUSS

- What steps would you take to determine what actions have been taken by the external organization against the targeted assets?
- How would you verify that the private organization was authorized to do the scans?
- What tools and procedures does your organization have in place to detect and respond to this activity?
- What preventative/protective measures could you take to ensure that future scans are detected/prevented unless specifically authorized?
- Would you examine the targets of the scan? If so, what would you look for?

ITEMS TO REPORT

- Did communications flow as expected? If not, why?
- Were processes and procedures followed?
- Were there any surprises?
- How well did the exercise work for your organization?



CONTACT US

The CTS SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

Contact the CTS Service Desk to report a cyber-incident, or report cyber incidents online at:

https://sp.cts.wa.gov/ask/soc/default.aspx

To speak with a SOC analyst, call **360-407-8800**. For general questions, send us an email at soc@cts.wa.gov.

The CTS Security Operations Center (SOC) is an active member with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which has been designated by the US Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through this relationship, the CTS SOC is able to leverage resources available from MS-ISAC of malware analysis, reverse engineering, log analysis, and forensics analysis in a cyber incident.

The mission of the CTS SOC is to provide centralized information sharing, monitoring, and analysis of Washington State security posture. The promotion of cyber security education and awareness to end users is critical to maintenance of a strong security posture of the Washington State network.

Security Operations