
Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

January 2015



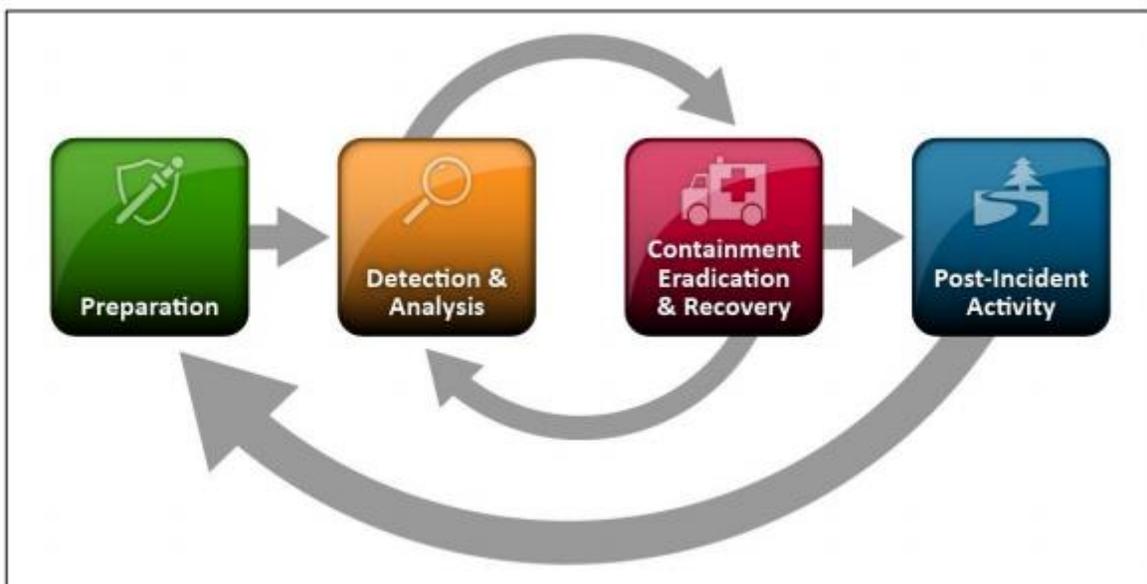
Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington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

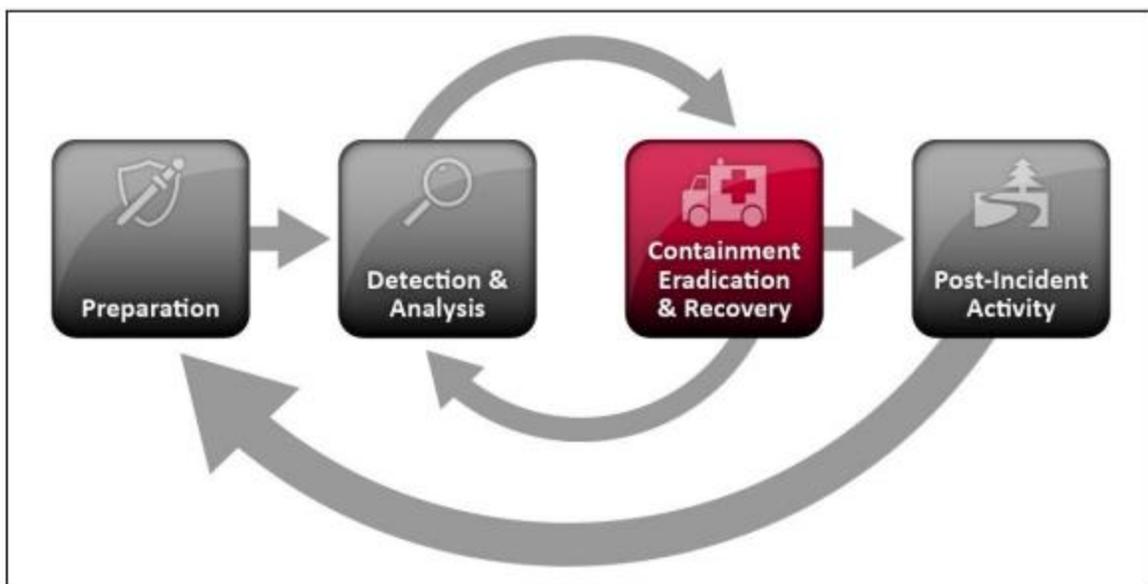
1. Modify the tabletop scenario as needed to conform to your environment.
2. Engage management.
3. Present scenario to the workgroup.
4. Discuss the process to address the scenario.
5. Document the response and findings for future reference

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

You've been receiving emails from concerned citizens that one of your websites has been periodically unavailable. In addition, you are informed that a known hacktivist has tweeted your website's address and #TangoDown with promises of additional attacks in upcoming days. How do you respond?



ITEMS TO DISCUSS

- How can you find out if your website is under DDoS attack?
- How can you find out the type of DDoS?
- What kind of logs do you have direct access to?
- What kind of logs can you get access to from third parties (hosting company)?
- What measures can you immediately put in place to reduce the impact?
- What measures can you put in place to mitigate future attacks?
- Who do you notify internally? Who do you notify externally?
- Who would you coordinate with to mitigate the attack?
- What mission essential function could be impacted by this attack?

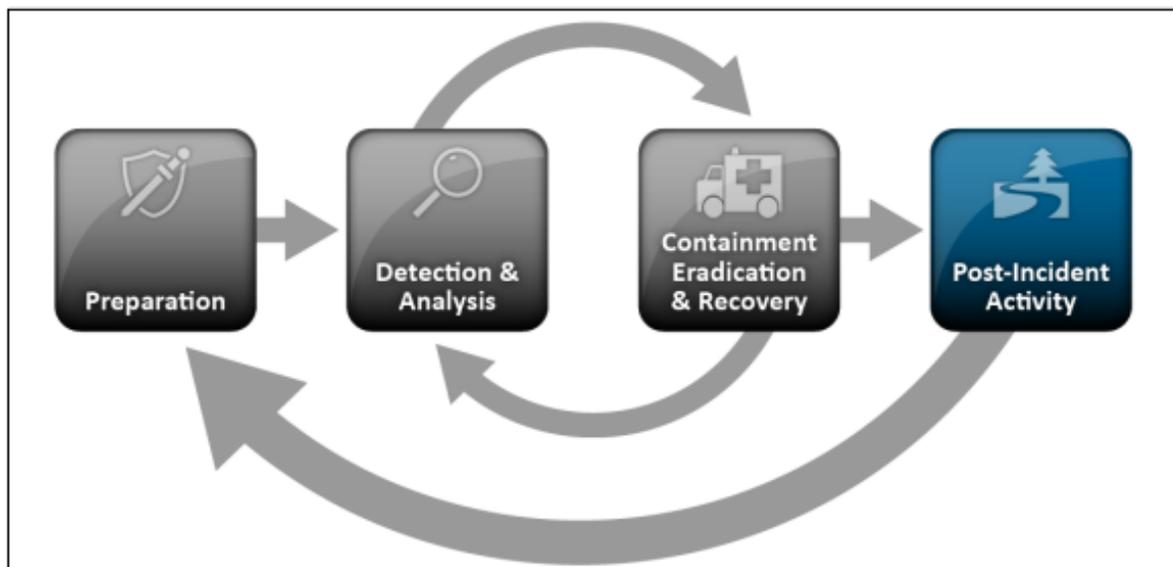
Inject

After putting in place an anti-DDoS measure, the attacker changes tactics from a simple UDP flood to a SSDP Reflection Attack.

- How do you respond to this change in tactic?

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.

To report a cyber-incident, contact the CTS Service Desk at (360) 753-2454 / 1-888-241-7597.

For general questions, send us an email at soc@cts.wa.gov.

For more information, visit our site at: <http://www.soc.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