Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

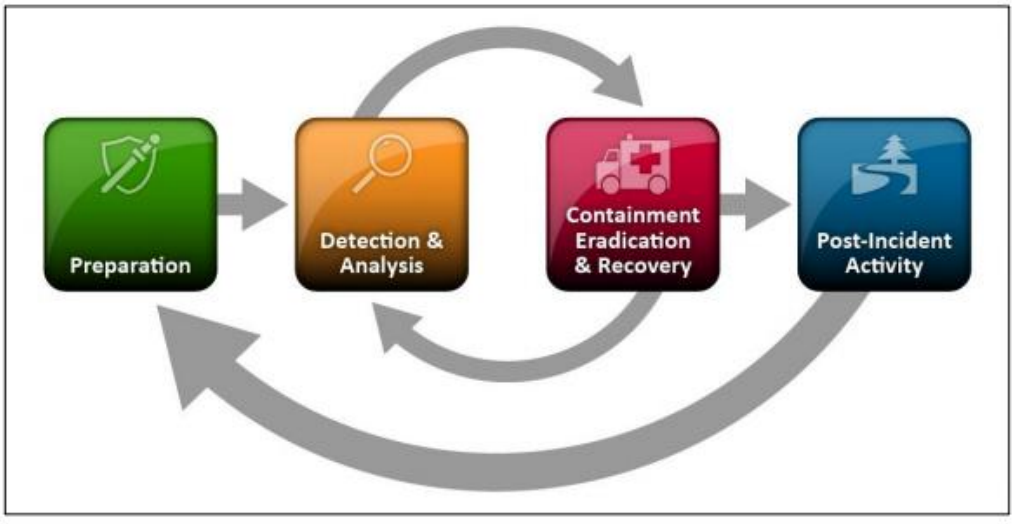
January 2014

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:

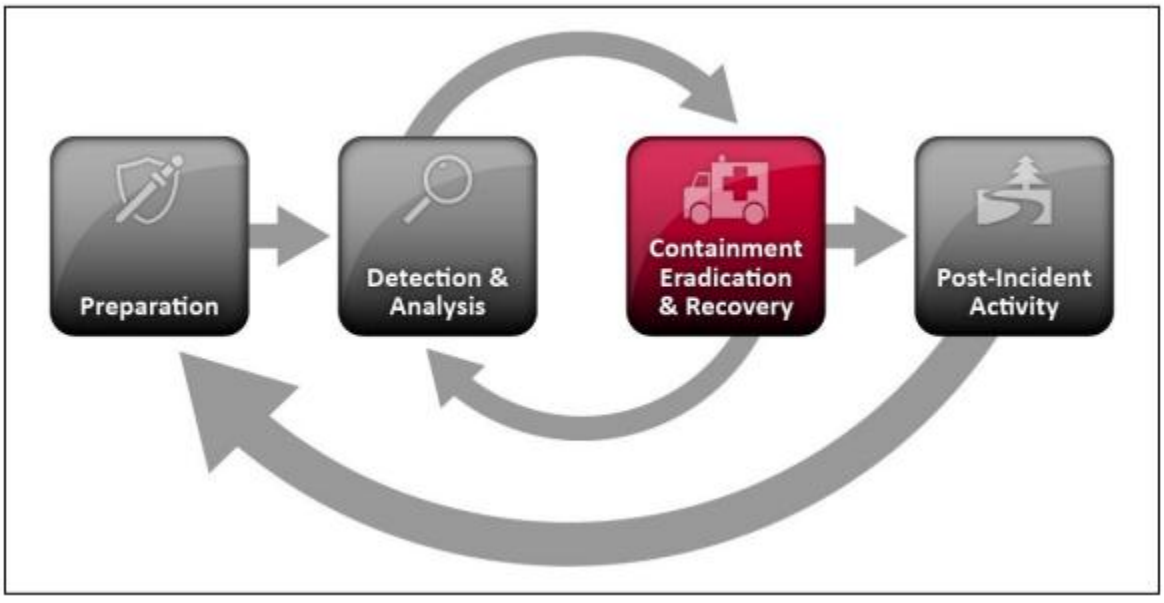
1. Modify the tabletop scenario as needed to conform to your environment.
2. Engage management.
3. Present scenario to the workgroup.
4. Discuss the process to address the scenario.
5. Document the response and findings for future reference



EXERCISE SCENARIO

- Numerous sensitive internal documents are found on the Internet. Thorough network checks review no evidence of a compromise, but it appears that the multi-function printer/copier is connected to an external facing IP. All documents found on the Internet are known to have been printed or copied on this machine.

- The machine was not originally connected to the Internet. It is now connected to the Internet through a Cat5 cable.



ITEMS TO DISCUSS

- How do you respond?
  - Who would you inform of this incident?

- How can you determine the severity of the leak?
  - How do you find out who has access to the printer?
  - How do you check printer logs?
  - How do you find out what kind of information was processed by this printer?

- How can you assure it doesn't happen again?
  - Should you try to find out who was response for connecting the printer?
  - Do you document changes to your environment? Or outside vendor/repairman who enter your environment?

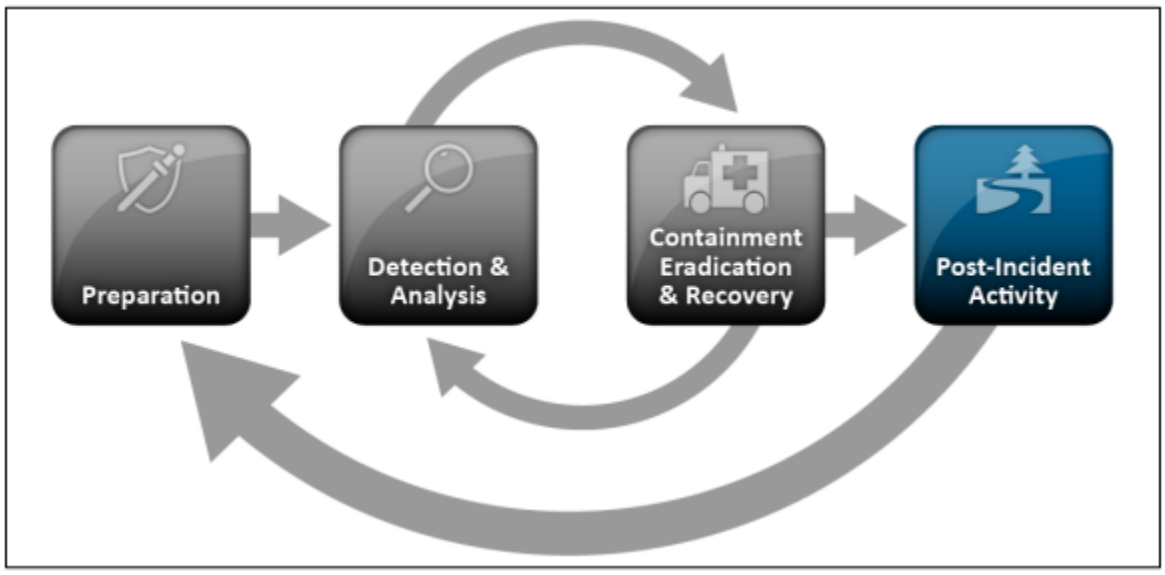
ITEMS TO REPORT

- 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:

http://sharepoint.dis.wa.gov/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.