
Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

September 2015



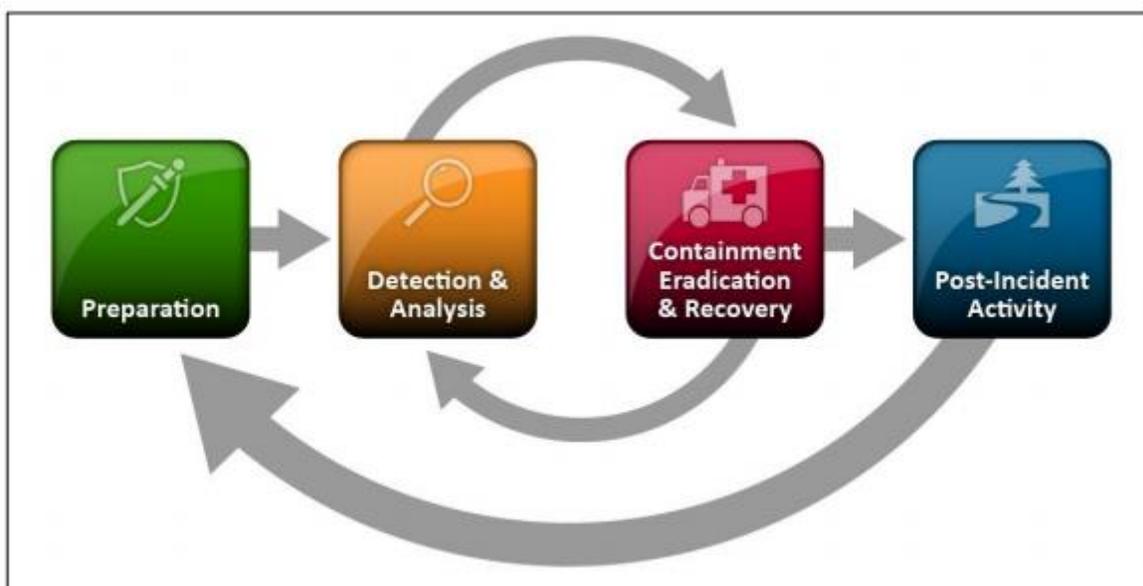
Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring,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

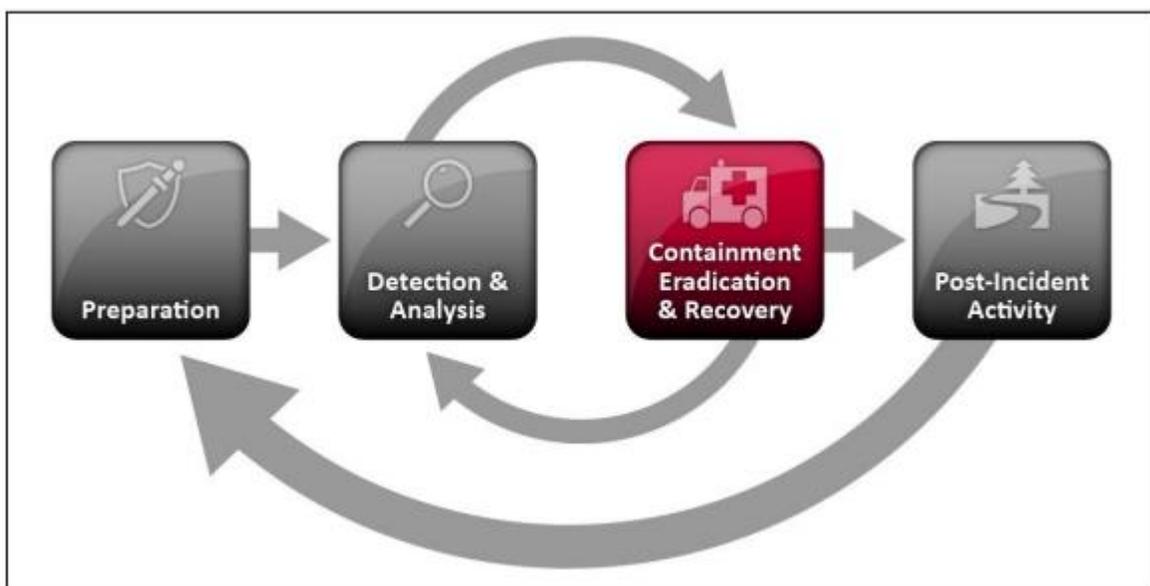
Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.



EXERCISE SCENARIO

A review of network logs show RDP (Remote Desktop Protocol) activity on a server between midnight and 5:00am. The server in question runs a critical line of business application which is used by hundreds of users daily as part of their job needs. Further analysis show these connections are from countries that your agency doesn't do business with and not one of your systems administrators. Your logs show these connections have been occurring for at least the past 90 days (which is as far as your logs go back).

How do you respond?

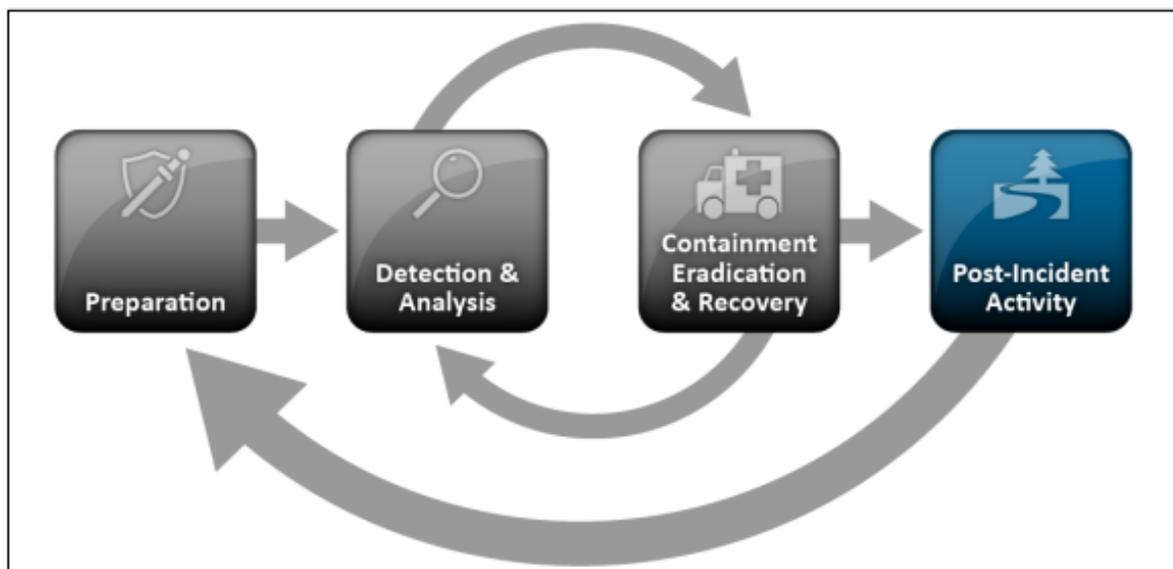


ITEMS TO DISCUSS

- Who can login to your servers as an administrator?
- Who would have legitimate cause for accessing this server (not the application) after hours?
- When do you disconnect the server from the network? What evidence do you have to find before taking this action?
- Do you know which servers you own that would require sending a notification of a breach? (Example: HIPAA, PCI, IRS, or OCIO Standards)
- How would you determine the method the attackers used to access the server in the first place so you can prevent the attackers from doing it in the future?
- What is your process to quickly clean/wipe and then restore servers back to operational status?

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 State Office of Cyber Security SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

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

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

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

The State Office of Cyber Security, 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 (DHS) 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 State Office of Cyber Security 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 State Office of Cyber Security SOC is to provide centralized information sharing, monitoring, and analysis of Washington State's 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