
Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

December 2015



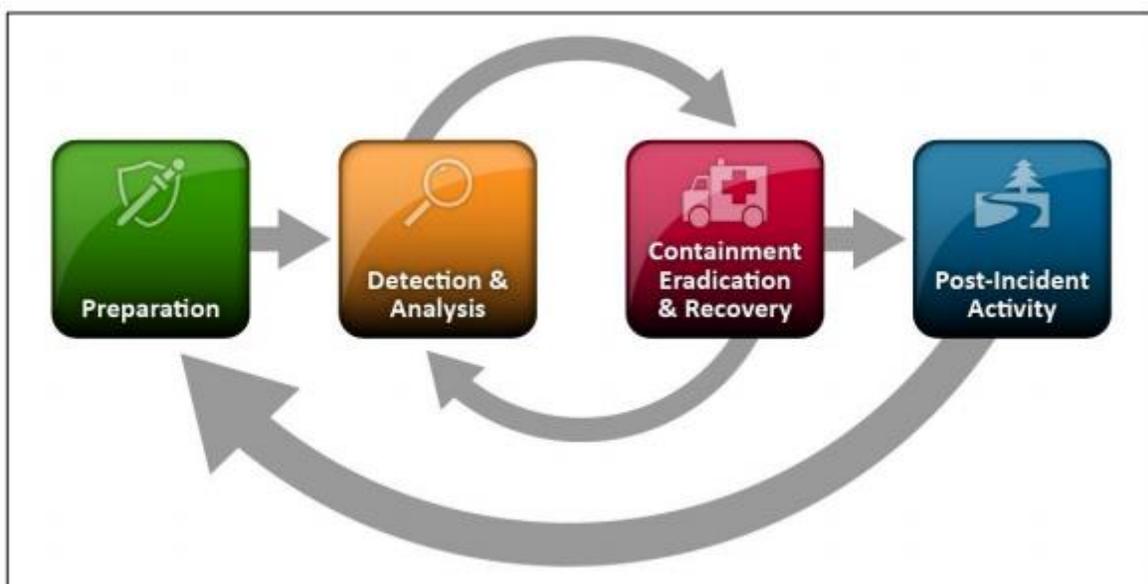
Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring,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

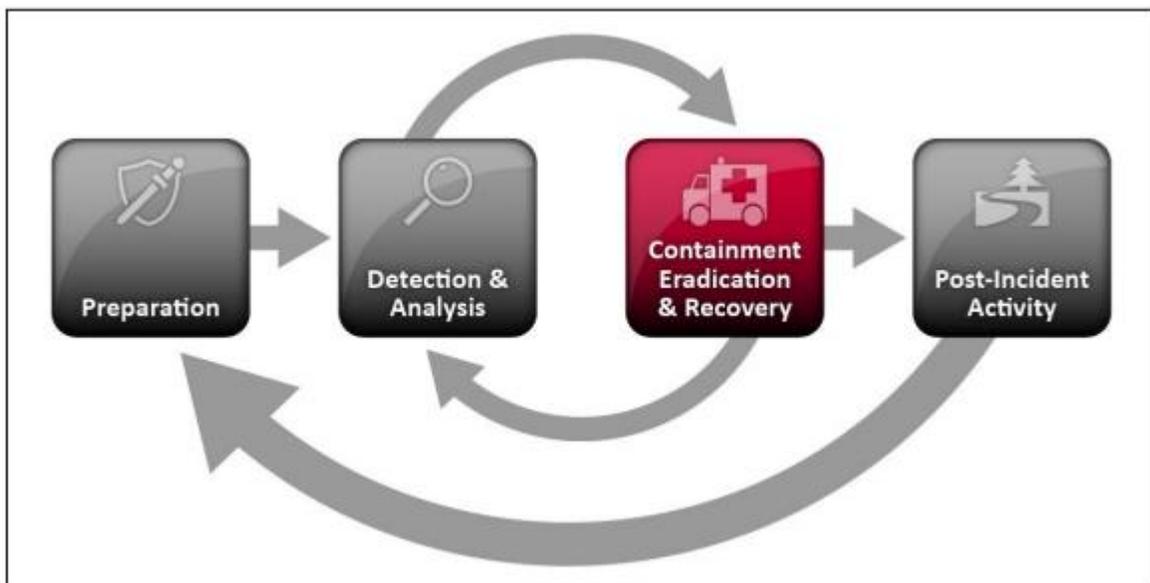
Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.



EXERCISE SCENARIO

While decorating for the holidays, you received an urgent message on your cellphone. This message states that based on open-source intelligence conducted by a federal partner, some users within your domain have been found in a recent credential dump posted on the JustPastelt.su site. This dump not only included usernames and email addresses, but also plaintext passwords. From quickly reading through the notification, you notice that there are in total 20 accounts from your organization and two of them are from network administrators.

How do you respond?

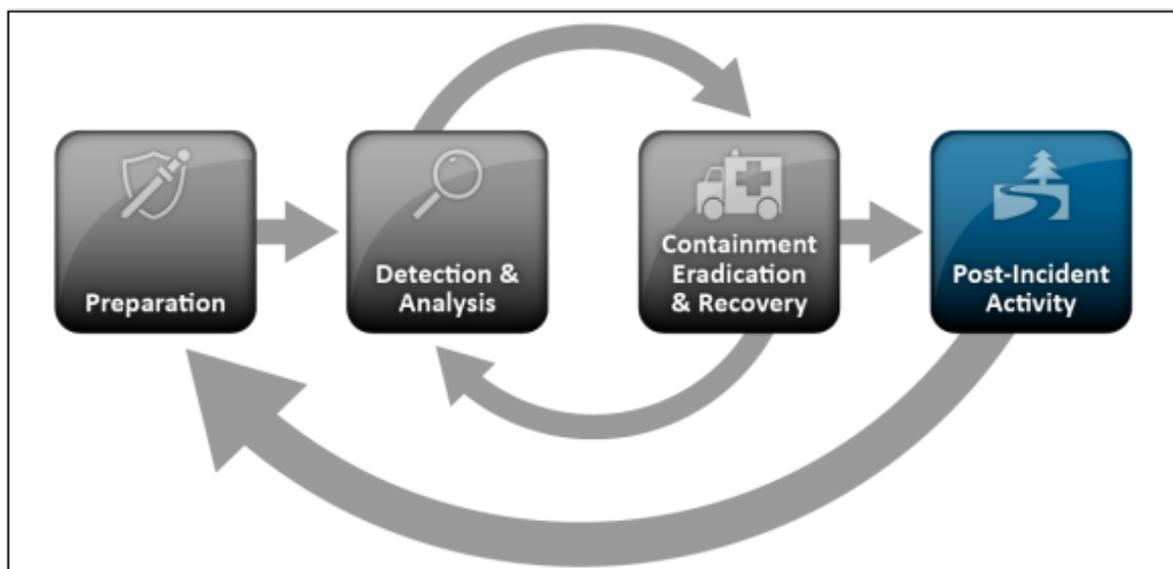


ITEMS TO DISCUSS

- How could you verify if the compromised accounts were valid?
- How is authentication and authorization done within your organization?
- How quickly could you revoke access to the compromised credentials?
- How many applications, internal and external, utilize this system or other system to manage users?
 - Which applications that your staff utilize are Internet facing?
 - Which applications are not hosted internally?
 - Which applications contain PII or other sensitive information?
- How can you verify that the compromised credentials were not used?
- How do you communicate to those users whose accounts were compromised?
- If attackers were able to use those compromised credentials, what could they access?
 - What would be the impact?
 - What about the administrator credentials?
- Does your organization have any policies regarding password use?
- Does your organization utilize multi-factor authentication?

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