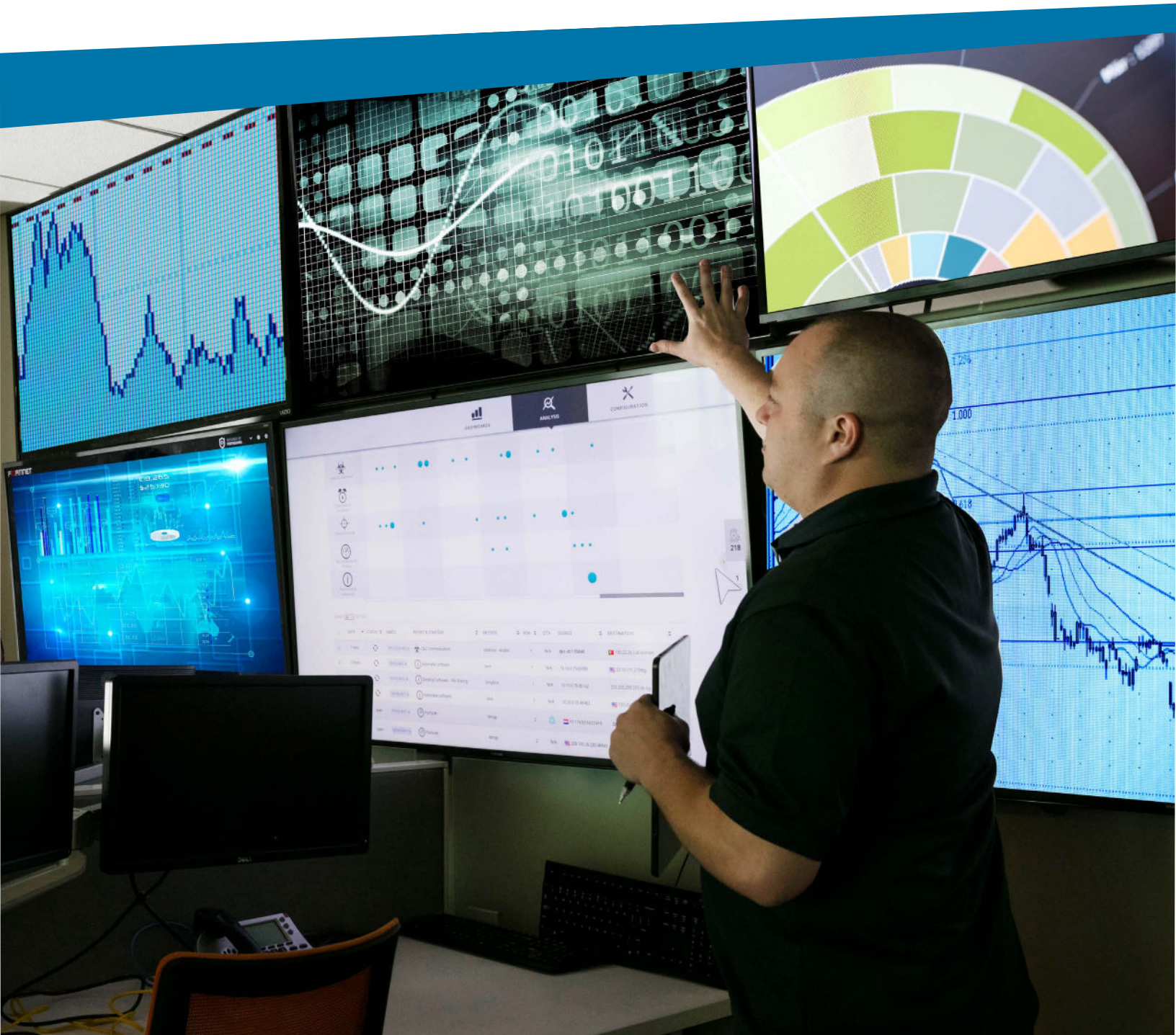
DATAPRISE

Dataprise Defense Tabletop Exercise Guide:

Security Intrusion



Introduction

Today's threat landscape continues to evolve, with cybercriminals executing complex, sophisticated, and targeted attacks against organizations of all sizes. Organizations need to have a cybersecurity program in place that effectively identifies, mitigates, and remediates threats from an increasingly dangerous and widespread threat landscape.

This exercise is designed to spark discussion within your IT department on your organizational preparedness for a cyberattack in the highlighted scenario and provide tangible guidance on areas to improve.

Getting Started

How To Use This Exercise

Tabletop exercises are designed to help organizations walk through potential cyber risk scenarios, evaluate cybersecurity posture, and identify potential gaps.

This exercise is meant to be a constructive and convenient tool that can be completed within 30 minutes. We recommend the below tips to provide the most value to your organization:

1. Involve all relevant IT stakeholders
2. Tailor the scenario to best match your environment
3. Determine a single facilitator for the exercise
4. Encourage discussion about how your organization would handle the scenario
5. Document your responses to the key questions
6. Develop a plan to close any gaps identified during the exercise

Copyright 2021 © Dataprise.

Scenario Set-Up:

Your IT department has received numerous complaints from employees that their machines are running slow and are facing difficulties when trying to access the network. Your Systems Administrator takes a closer look at your network logs and discovers that there is an unauthorized intruder in your IT environment.

Questions to Discuss

1. What do you do first?

2. How do you determine the impact of the intruder?

3. What do you have in place to contain the intruder?

4. Can the intruder access your critical data?

5. Who do you notify about the incident?

6. What steps will you take to reduce risk in the future?

Copyright 2021 © Dataprise.

Review

How did you do?

Below are some critical components that cybersecurity experts recommend should be included as part of your cybersecurity program.

1. What do you do first?

Recommendations:

The first step your organization should take is to review your Incident Response Plan (IRP), which should be accurate and up-to-date. If you do not have an IRP or your IRP is out of date, ideal first steps (aligned with NIST's Incident Handling Guide) include:

- **Preparation:**
  - Identify communication and coordination mechanisms and involved parties
  - Determine and access hardware, software, and resources needed for incident analysis and mitigation
  - Ensure you have visibility into the necessary systems

- **Detection & Analysis:**
  - Perform initial analysis and validation for the incident and its indicators to determine incident's scope, such as what systems are affected, who or what originated the incident, and how the incident is occurring
  - Document every step taken from the time the incident was detected to its final resolution
  - Prioritize the handling of the incident by relevant factors such as functional and information impact

2. How do you determine the impact of the intruder?

Recommendations:

Your organization needs tools in place that provide the monitoring, data collection, and visibility needed to determine what has happened in your environment and what data the intruder may have had access to.

Data collected by anti-virus and anti-spam software, third-party monitoring services, operating system and network device logs, network flow, and Security Information and Event Management (SIEM) products can provide insight into the attack vector the intruder used and potential impact.

3. What do you have in place to contain the intruder?

Recommendations:

Your organization needs to develop a strategy for containing any intruders in your environment. This strategy should be determined by factors such as potential damage, service availability, and strategy effectiveness. Once a strategy is determined, solutions such as next-gen endpoint detection and automated incident response should be in place to help assist with this.

Copyright 2021 © Dataprise.

4. Can the intruder access your critical data?

Recommendations:

The first step to determining if the intruder can get access to your critical data is defining what your organization considers to be critical data and who owns it. Understanding what your 'crown jewels' are is key to setting up security measures that protect and back-up this data.

Alongside measures such as 24x7x365 security monitoring and incident detection, validation, and reporting, data protection measures should include:

- Zero Trust Access
- Data Encryption
- Continuous Vulnerability Scanning

5. Who do you notify about the incident?

Recommendations:

Internally, you should identify the stakeholders that are impacted by the incident or may need to become involved, such as the legal team. Depending upon your industry and nature of the incident and data accessed, you may have requirements to report cybersecurity incidents to governing bodies and federal agencies. Review the compliance standards you are held to and have a communication plan in place.

6. What steps will you take to reduce risk in the future?

Recommendations:

With cybersecurity, it's not a matter of if you get attacked. It's a matter of when.

To effectively protect your organization, you need a cybersecurity program in place that provides real-time detection, validation, reporting, and response capabilities to protect your IT environment from end to end. Based on your answers above, determine if there are gaps in your current program and use that information to create an action plan to remediate.

About Dataprise

Founded in 1995, Dataprise is the leading strategic IT solution provider to midmarket IT leaders who believe technology should allow you to be the best at what you do. Dataprise's unbeatable IT solutions and services are tailored to the needs of strategic CIOs and provide best-in-class managed security, network, infrastructure, collaboration, mobility, and end-user solutions. Dataprise has offices across the United States to support our clients.

Have questions on how to enhance your cybersecurity?

Visit Us:

www.dataprise.com

Call Us at 1.888.519.8111

Copyright 2021 © Dataprise.