ResearchSOC

researchsoc.iu.edu

Thank you for attending. Our webinar will begin shortly.

Building a Security Exercise Program

Josh Drake
Senior Security Analyst, Indiana University
Center for Applied Cybersecurity Research

ResearchSOC

Housekeeping

- All participants are on mute.
- Ask your questions via the Q&A feature.
- We will record this webinar and provide a link.
- Slides will also be made available.
- Tech troubles? Sign out and back in.

ResearchSOC

Building a Security Exercise Program

Josh Drake
Senior Security Analyst, Indiana University
Center for Applied Cybersecurity Research

ResearchSOC

What causes failure?

How can we improve our detection and response systems to address the issues most likely to cause loss of confidentiality, integrity or access to our data?

- **Missing Information**
- **Multiple concurrent problems**
- **Inability to Detect or Respond**
- **Incorrect Information**
- **Incomplete Information**

ResearchSOC

Any person can invent a security system so clever that she or he can't think of how to break it.

-Schneier’s Law

ResearchSOC

Imperfect Information

What “facts” do we know about our organization but haven’t **tested**?

How closely are our policies tied to the realities of our organization’s **operations**?

- New updates/controls
- Untested critical processes
- Logical or policy oversights
- Are policies focused on organizational goals?

ResearchSOC

What is a security exercise?

A **tool** to help us find and correct **errant assumptions** about our organization's security.

- Helps us to get better at dealing with things that (hopefully) rarely happen.
- Tells us if our policies are effective.
- Reveals the assumptions we have made that don't line up with reality.
- Creates elasticity in our thinking about how we respond to problems.

ResearchSOC

How do we find out?

Security Exercise *Programs*

A ***series*** of security exercises we run to continually ***improve*** our policies and processes and prepare our team for responding to real issues.

- It is ***iterative***
- It ***reinforces*** good behaviors
- It ***corrects*** bad behaviors
- ***Prepares*** for response stress
- Improves ***coordination***

ResearchSOC

Prerequisites

- What are you protecting and why?
  - Inventory
  - Priorities
- How are you going to achieve those goals?
  - Policies
  - Procedures
- Who will do what during and incident?
  - Defined responsibilities
  - Assigned to the role, not the individual

These can be simple documents, the important thing is that they exist as a starting point for iterating on your program.

“We will ensure data integrity while ensuring maximum availability for our researchers”

“During an incident the CISO will be authorized to…”

ResearchSOC

Poll: What's your experience with security exercises?

ResearchSOC

Elements of a successful program

- **Regularity**
  Exercises should be regular, repeatable, scalable and adaptable
- **Purpose and Focus**
  Exercises should have a clear focus that is tailored for your organization
- **Preparation**
  Exercises should be scheduled in advance, planned, and clearly communicated
- **Follow Through**
  Knowledge gained in exercises should be reviewed and applied regularly

Elements of a successful program

- **Regularity**
  Exercises should be regular, repeatable, scalable and adaptable
- **Purpose and Focus**
  Exercises should have a clear focus that is tailored for your organization
- **Preparation**
  Exercises should be scheduled in advance, planned, and clearly communicated
- **Follow Through**
  Knowledge gained in exercises should be reviewed and applied regularly

ResearchSOC

Elements of a successful program

- **Regularity**
  Exercises should be regular, repeatable, scalable and adaptable
- **Purpose and Focus**
  Exercises should have a clear focus that is tailored for your organization
- **Preparation**
  Exercises should be scheduled in advance, planned, and clearly communicated
- **Follow Through**
  Knowledge gained in exercises should be reviewed and applied regularly

ResearchSOC

Elements of a successful program

- **Regularity**
  Exercises should be regular, repeatable, scalable and adaptable
- **Purpose and Focus**
  Exercises should have a clear focus that is tailored for your organization
- **Preparation**
  Exercises should be scheduled in advance, planned, and clearly communicated
- **Follow Through**
  Knowledge gained in exercises should be reviewed and applied regularly

ResearchSOC

Elements of a successful program

- **Regularity**
  Exercises should be regular, repeatable, scalable and adaptable
- **Purpose and Focus**
  Exercises should have a clear focus that is tailored for your organization
- **Preparation**
  Exercises should be scheduled in advance, planned, and clearly communicated
- **Follow Through**
  Knowledge gained in exercises should be reviewed and applied regularly

ResearchSOC

Poll: What key elements of a security program do you have in place?

ResearchSOC

Types of Exercises

Tabletop Exercise

Real-time exercise where each organizational role walks through a hypothetical event together using the existing policies and procedures.

Evaluation Exercises

Exercises that explore, measure, or improve aspects of our documentation, inventory, resource availability and preparedness.

Live Exercises

Real-time exercise run in test or production environments to simulate potential security incidents.

ResearchSOC

Tabletop Exercises

Method

A moderator creates a scenario and runs the participants through it, much like a tabletop RPG. “What do you do?”

Requirements

- Moderator and a pre-written scenario
- Means of communicating in real time.
- Means of note taking and sharing at debrief
- Defined roles and responsibilities for participants

Use Case

- Early program
- Lack of Resources
- Testing Policies and Procedures

ResearchSOC

Evaluation Exercises

Method

Passive gathering of data about organization, documentation, infrastructure or policies.

Requirements

- At least one investigator
- Tools for gathering the type of data you are looking for: port scanner, software inventory tools, public IP addresses, etc

Use Cases

- Gathering Inventory
- Building Risk Assessment
- Verifying documentation

ResearchSOC

Live Exercises

Method

Real-time environment exercises on test or production hardware. Can be run as White team v Blue team or Red team v Blue team

Requirements

- Two teams of participants
- Production or test environment
- Defined expectations and boundaries
- Means of note taking and sharing at debrief

Use Cases

- Reinforcing human behavior
- Testing tools and software
- Evaluating hardware
- Finding wrong assumptions

ResearchSOC

Designing an Exercise

- Choose something to test that fits with the purpose/focus of your organization's security program
- Choose a type of exercise based on your resources and what you want to test
- Write an outline of the exercise (tabletop/live) or develop a methodology for evaluative exercises.

For tabletop scenarios decide how you will present information to the participants and get them thinking critically.

For live scenarios think about how you can focus the objectives around the systems and assumptions you want to test.

ResearchSOC

Running an Exercise

- Communicate the time and place of your exercise to participants (if any) ahead of time.
- Set a scope for the exercise, and define success/fail states to participants at the start.
- Provide Resources
- Take extensive notes during the exercise, ask participants to document their thoughts and reactions as well.
- Solicit feedback from participants
- Iterate on your execution- document successes and failures

ResearchSOC

Learning from an Exercise

- Conduct a debrief of the exercise as soon as possible in order to gather information as accurately as possible.
- Generate a report defining what was done, how and the outcomes of the exercise.
- Make recommendations to address failures or obstacles encountered while running the exercise

- **Revisit previous exercises to ensure issues are being addressed and documented.**
- **Repeat failed exercises after an interval to test effectiveness of changes.**

ResearchSOC

For More Information

List of example exercises

http://go.iu.edu/2heq

ResearchSOC

Poll: Which additional security exercise webinars might you attend?

ResearchSOC

Q & A

ResearchSOC

Connect with ResearchSOC

Visit the ResearchSOC website**:** https://researchsoc.iu.edu/

Subscribe to the ResearchSOC announcements list: https://researchsoc.iu.edu/contact/index.html

Read the ResearchSOC Blog: https://blogs.iu.edu/researchsoc/

Join our Community of Practice: https://ask.cyberinfrastructure.org/c/rsoc

Follow ResearchSOC on Twitter @IUResearchSOC

Upcoming ResearchSOC Events

Webinars:

How to secure SCADA/ICS systems:

10 strategies that work

February 20, 2020 3pm EST

How to select and use operational cybersecurity metrics to make cybersecurity operations more effective

March 19, 2020 3pm EST

https://researchsoc.iu.edu/webinars

Conferences:

Internet2

March 29-April 1

Educause SPC

April 21-23

PEARC

July 26-30

Thank you!

Josh Drake
drakejc@iu.edu

researchsoc.iu.edu

We thank the National Science Foundation (grant 1840034) for supporting our work.

Additional Resources:

Presentation adapted from “Security Exercises” article by Susan Sons from linuxjournal.com (Nov 2016)
http://go.iu.edu/2c10

ResearchSOC