EdgeCon
ANNUAL CONFERENCE 2020

Thursday 3:30 – 4:15 pm

Gray Areas: Understanding Information Security Risk in your Organization

with Janine Frederick

Janine Frederick

- Systems Administrator, *Monmouth University*
- 15 years of IT-related experience
- US Cyber Challenge Camp, *Center for Internet Security and Department of Homeland Security*
- 2019 Technology award, *NJ Library Association and the NJ Chapter of the Association of College and Research Libraries*
- Working toward OSCP and Security+ certifications

https://www.linkedin.com/in/janinefrederick/

@Fackque99

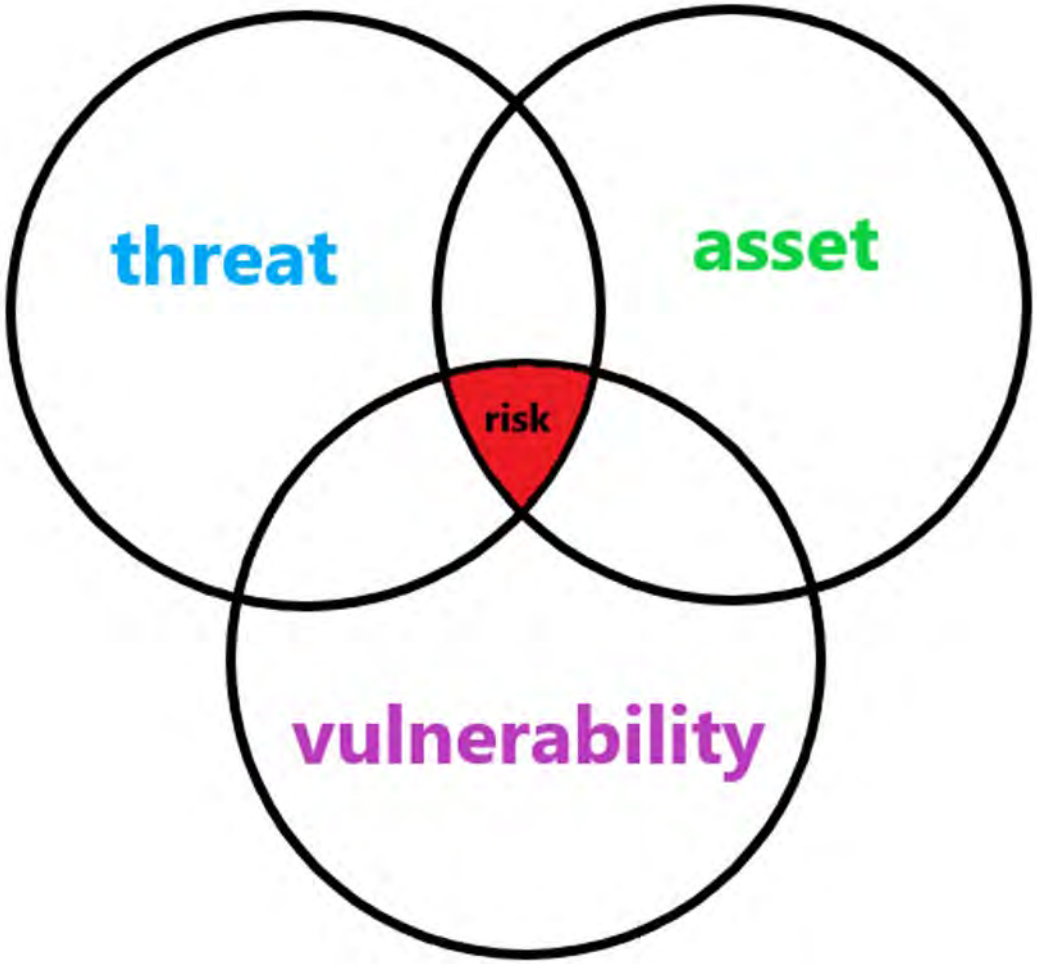
What is Information Security Risk?

Information Security Risk

The **potential for loss**, damage or destruction of an asset as a result of a vulnerability being exploited by a threat.

Asking the board for a cyber security budget before a breach

Risk Assessment

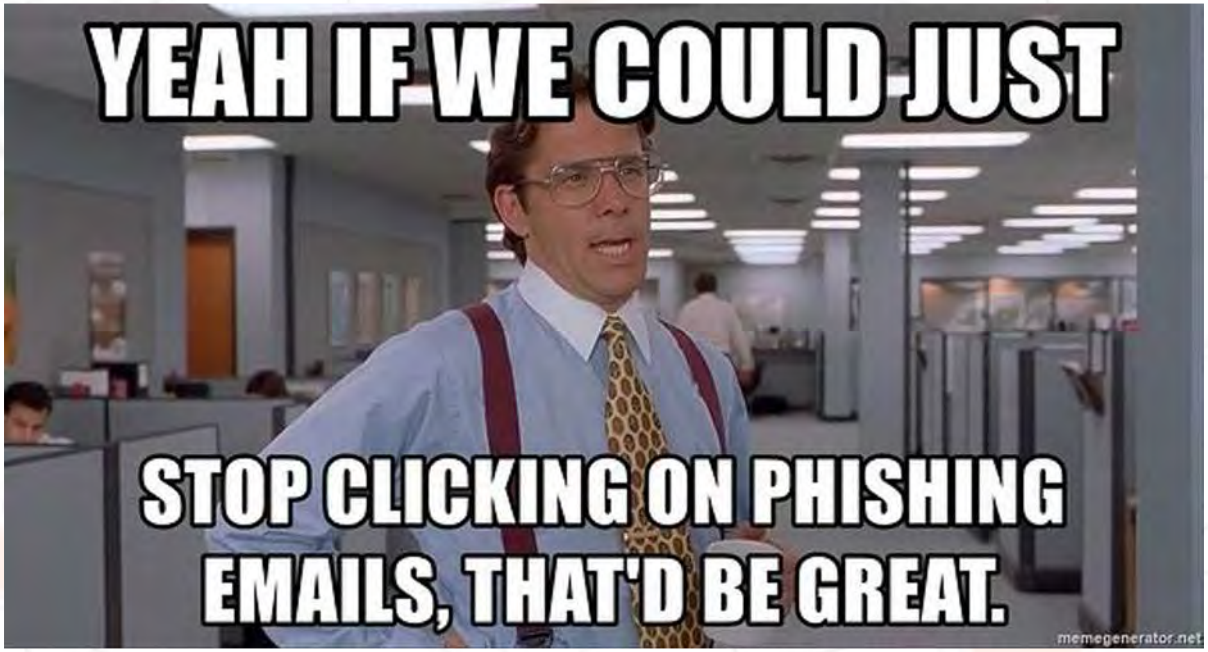


Vulnerability

Gap or weakness in security (includes physical and virtual)

Threat

Anything or anyone that can intentionally or accidentally obtain, damage, or destroy an asset.



Event vs. Incident

Event vs. Incident

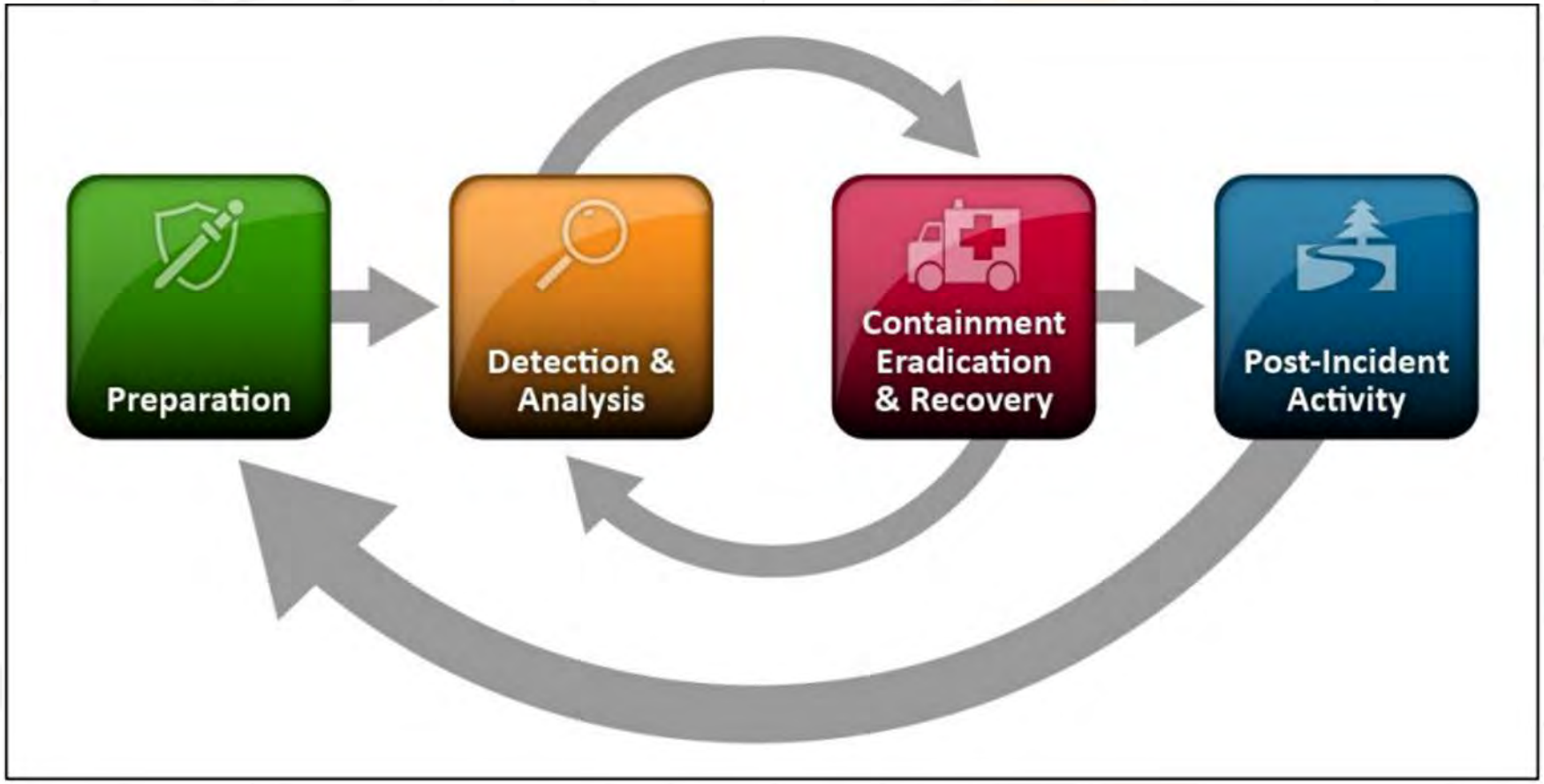
Event: any observable occurrence in a system or network.

Incident: a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

National Institute of Standards and Technology (NIST) SP.800-61 R2

Managing Information Security Risk

Incident Response Life Cycle



National Institute of Standards and Technology (NIST) SP.800-61 R2

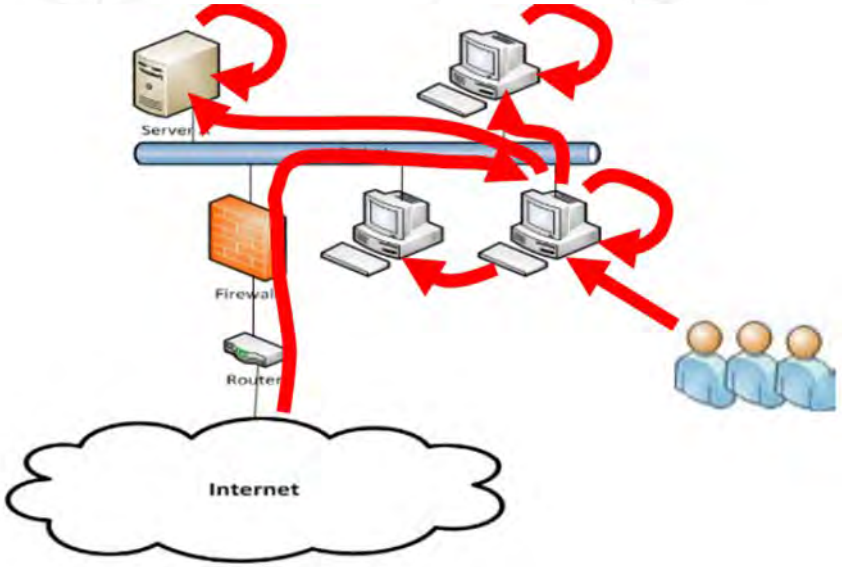
Prepare!

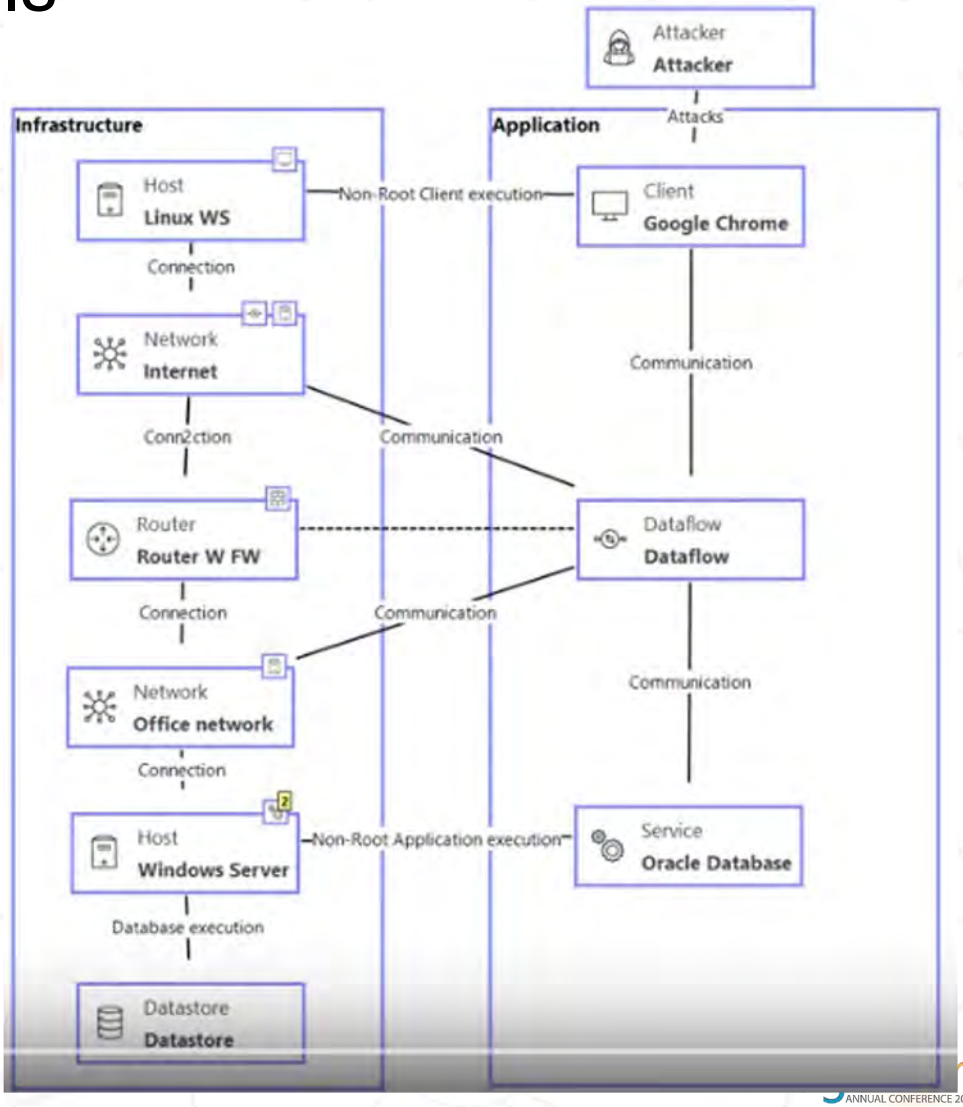
- Create a Threat Model
- Establish Information Security policies
- Add an Incident Response (IR) Plan to your Disaster Recovery Plan
- Deploy a Security Information and Event Management (SIEM) system
- Deploy an Intrusion Detection System (IDS)
- Pick your IR Team (includes your blue team)
- Offer training

Threat Modeling

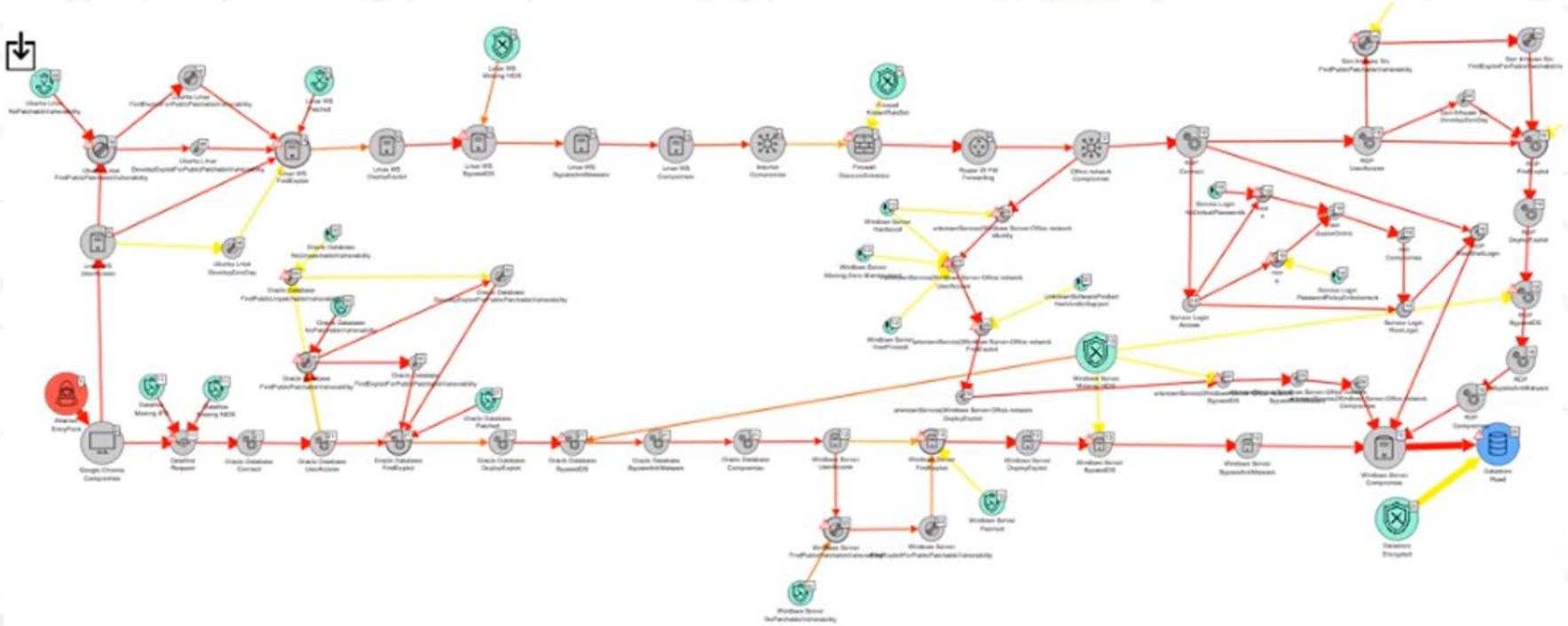
- What/where are your assets and resources?
- What are your vulnerabilities and/or threat probability?
- What are your safeguards?
- Risk=Impact x Probability / Cost
- What/where are the “crown jewels” of your network?
- Your threat model can be very helpful during incident response!

Topological Threat Models





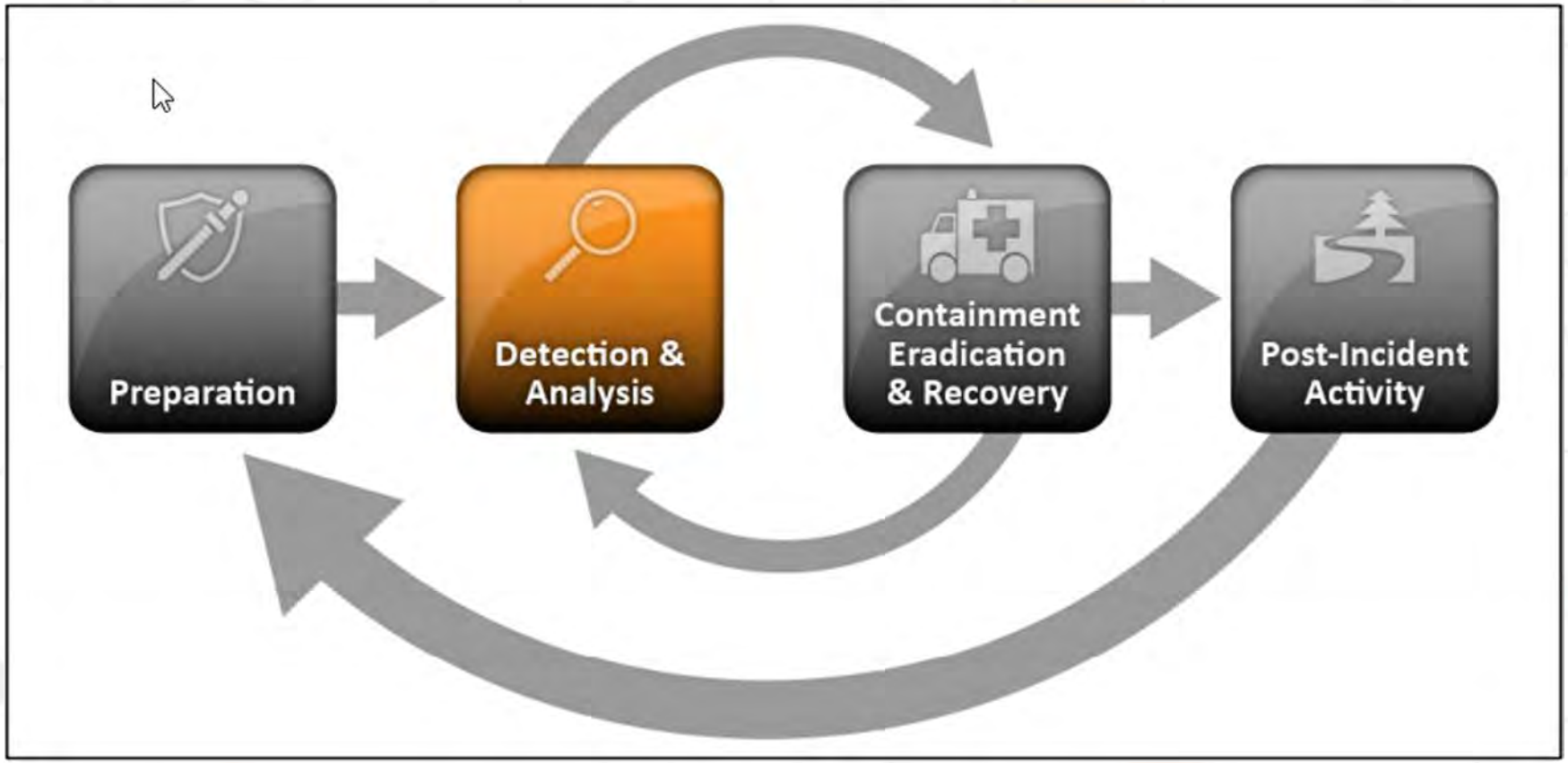
Attack Path Analysis Example



Picking your IR team

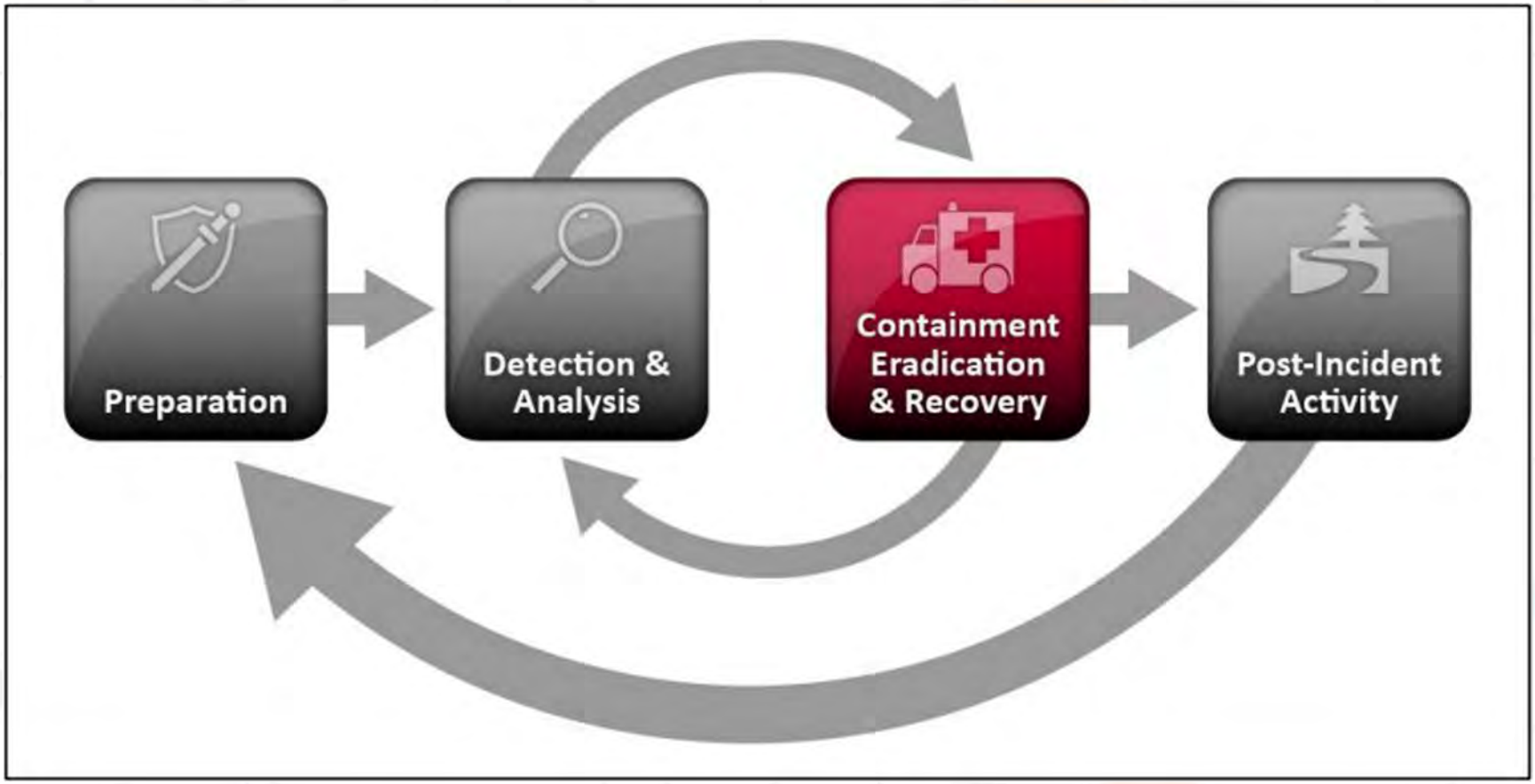
- Choose the right people, not the highest.
- Communication is important
- Communication is important
- Communication is important
- ICS-100: Designate an Incident Commander, Liaison, and Operations staff
- War Room

Detection & Analysis



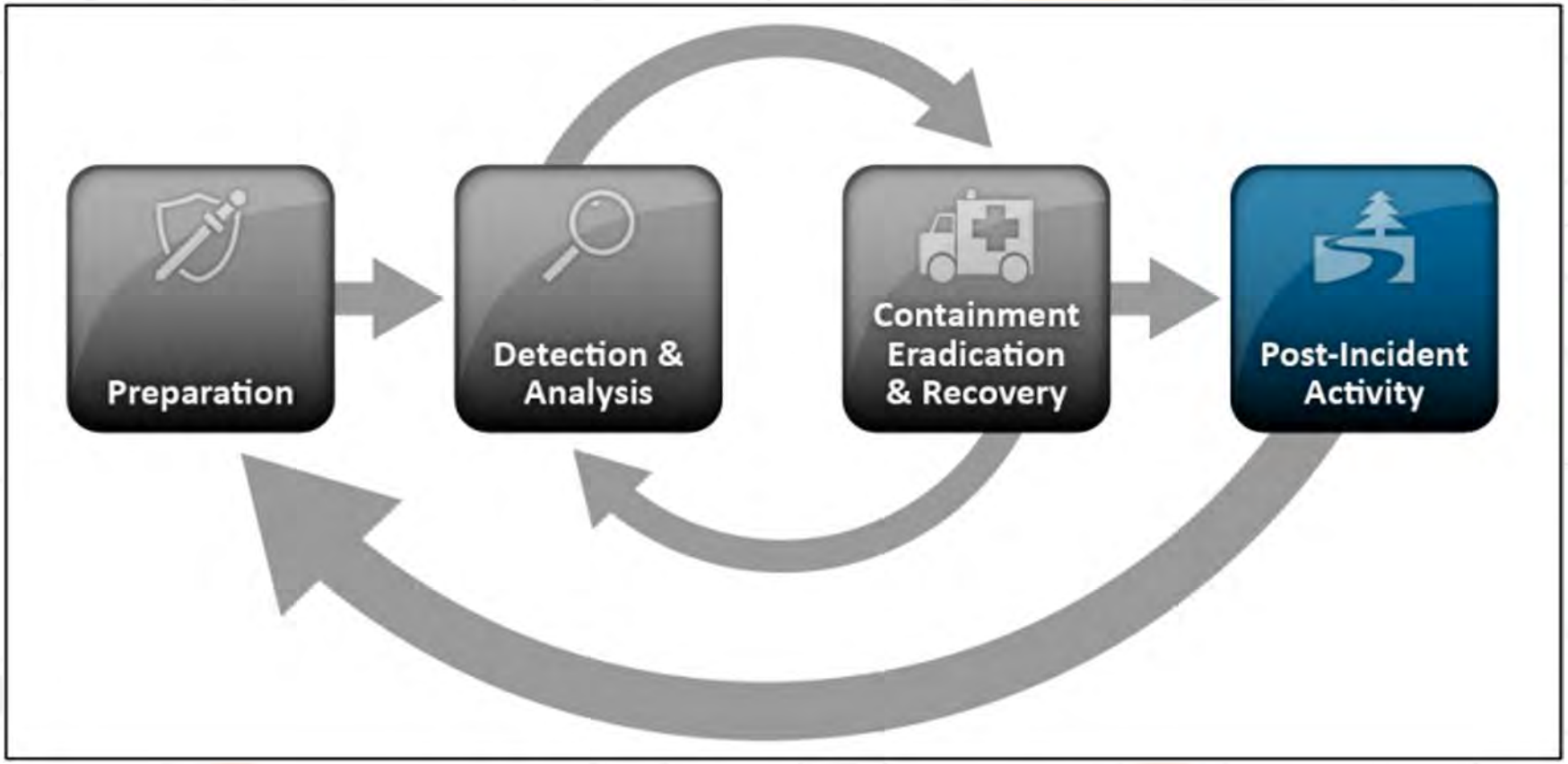
National Institute of Standards and Technology (NIST) SP.800-61 R2

Containment, Eradication, & Recovery



National Institute of Standards and Technology (NIST) SP.800-61 R2

Post-Incident Activity



National Institute of Standards and Technology (NIST) SP.800-61 R2

Let’s have some fun!

Scenario 1:

You have a separate wireless network for students to use on campus. The rise in IOT device adoption in the dorms has increased your wireless traffic exponentially over the past few years. Troubleshooting has determined that wireless access points in the dorms are being overwhelmed leading to connection issues. Your budget is limited and your most recent site study determined that adding any more wireless access points may cause channel overlap in many areas.

What is your immediate reaction and why?

What are some possible approaches?

Let’s have some more fun!

Scenario 2:

Your network’s server topology has expanded over the last 15 years. There is a hodgepodge of new mixed with old and reorganization tends to happen piece-meal, as new servers are added and old ones are replaced or repurposed.

While creating your threat model over summer break, you discover that one of your two load balanced domain controllers is configured with a host IP (not the load balancer service IP) on the same VLAN as your webserver. Your organization has VLAN segmentation, but not VACL isolation. This server’s hardware is 8 years old and has been on this VLAN since its initial configuration. A rule is set on your enterprise firewall that blocks external traffic from accessing this host directly, but the domain controller’s firewall is configured, but turned off.

What are the risks?

The NIST Framework

NIST Cyber Security Framework (CSF)

Core: (shown right)

Implementation Tiers:

- to find your baseline

Profile:

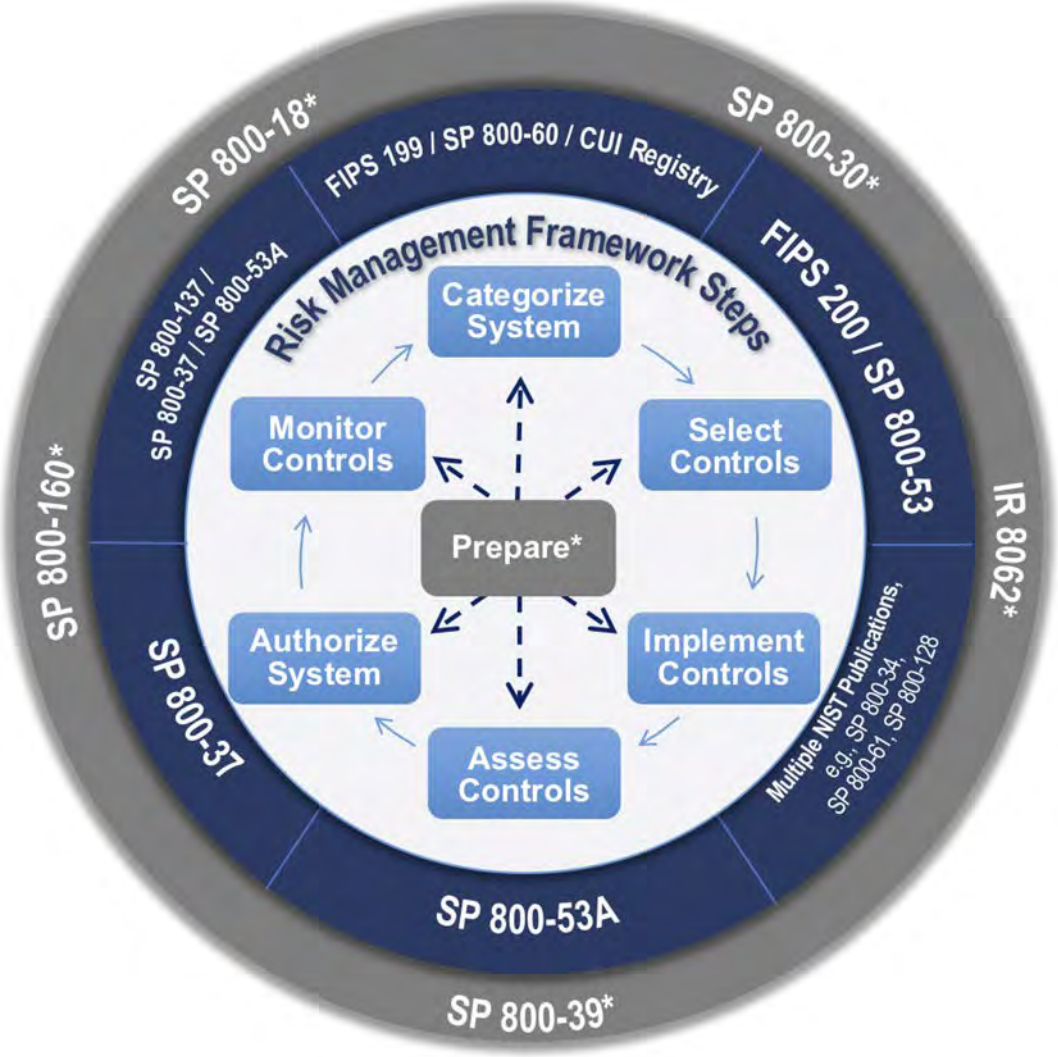
- Baseline
- Goals
- Gaps
- Roadmap

nist.gov/cyberframework

NIST CSF Implementation Tiers

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk[1.1]** • benefits my sharing or receiving information from outside parties			

NIST Risk Management Framework (RMF)




WE'RE FINALLY SECURE
I CHECKED ALL THE BOXES