Incident Response for Cyberinfrastructure

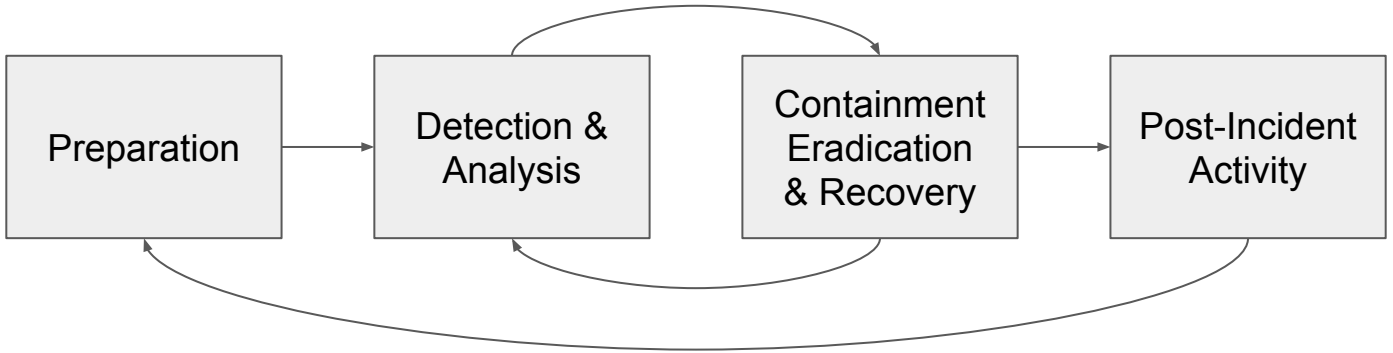
Jim Basney and John Zage

This material is based upon work supported by the National Science Foundation under grant number 1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

What is a computer security incident?

- Phishing
- Worms
- Vulnerabilities
- Insider Threat
- Hacked Accounts
- Pivoting
- Policy Violation
- Intellectual Property Loss/Theft
- Data Loss
- Brute Force Attack
- Denial of Service (DoS)

Computer Security Incident Handling (NIST 800-61)



SANS Critical Security Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability

https://www.sans.org/critical-security-controls

SANS Critical Security Controls

11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://www.sans.org/critical-security-controls

How do the security controls help when responding to real incidents?

HPC Bitcoin – Insider attack

HPC Pivot Attack – Shared credential incident

Heartbleed – Zero day

Crimea – PR attack

HPC Bitcoin

- *Alert* – An HPC admin identified an issue with the job scheduler and questioned whether the jobs were MPMD (multiple program multiple data) jobs.
- The admin used a script to review user jobs and confirm whether these were MPMD jobs, which they were not.

- Upon reviewing the job, he saw the word "bitcoin":

```
aprun -n 1024 -N 1 -d 16 -j 1
        ./alpha-test.x
 -url=http://213.133.127.145:8332
 -user=bitcoin_user@yahoo.com cpu
    -password=foo -threads=16
      -workrefreshms=2000
```

- The PoC for the grant allocation was contacted and suggested to escalate the investigation.
- The Admin further researched jobs showing apparent bitcoin activity and found 75,000 node-hours had been used.

HPC Pivot Attack/ Shared Credential Incident

- IRT saw an announcement that a partner site had an incident
  - Not long after the campus cluster was having problems
  - Security noticed that the incident was similar to the partner site's incident.
  - Sysadmins received calls from users reporting problems accessing head nodes
  - Investigation showed the head nodes were up but there were "oddities" in syslog

Heartbleed
Zero-Day Response

- Vulnerability reported in OpenSSL library in April 2014
  - Potential exposure of confidential data (session cookies, passwords, keys)
  - IR team had to determine if there were any affected systems
  - Determining the impact of the vulnerability
    - How many systems were affected?
    - Did all users need to change passwords?
    - Did all administrators need to change private keys?

Heartbleed

Example of Vulnerability

```
0210: 6B 69 65 3A 20 50 48 50 53 45 53 53 49 44 3D 38  kie: PHPSESSID=8
0220: 32 62 33 32 61 33 66 64 61 33 61 30 34 33 37 62  2b32a3fda3a0437b
0230: 31 64 39 37 37 34 32 31 37 32 30 66 31 36 35 3B  1d977421720f165;
0240: 20 63 6F 6F 6B 69 65 5F 74 65 73 74 3D 31 33 39   cookie_test=139
0250: 37 31 34 35 30 35 37 0D 0A 0D 0A 5F 5F 63 73 72  7145057...__csr
0260: 66 5F 6D 61 67 69 63 3D 73 69 64 25 33 41 33 32  f_magic=sid%3A32
0270: 37 34 33 66 33 38 39 65 66 62 35 38 63 33 65 36  743f389efb58c3e6
0280: 34 63 36 62 65 62 62 38 63 65 62 39 36 35 33 32  4c6bebb8ceb96532
0290: 33 39 37 66 36 36 25 32 43 31 33 39 37 31 34 31  397f66%2C1397141
02a0: 34 35 37 26 75 73 65 72 6E 61 6D 65 66 6C 64 3D  457&usernamefld=
02b0: 61 64 6D 69 6E 26 70 61 73 73 77 6F 72 64 66 6C  admin&passwordfl
02c0: 64 3D 78 36 38 61 70 68 75 66 61 70 68 61 26 6C  d=x68aphufapha&l
02d0: 6F 67 69 6E 3D 4C 6F 67 69 6E 30 75 83 31 CE 8E  ogin=Login0u.1..
```

Crimea
Overview

A pro-Russian Crimean Referendum site was hit with a denial of service attack (DDoS) in March, 2014
NCSA's PR team was contacted by American media outlets to comment on the DDoS attack, *because...*

Voice of Russia media outlet reported the University of Illinois campus network as the origin of the attack
The cybersecurity team was able to confirm the University did not contribute to the attack

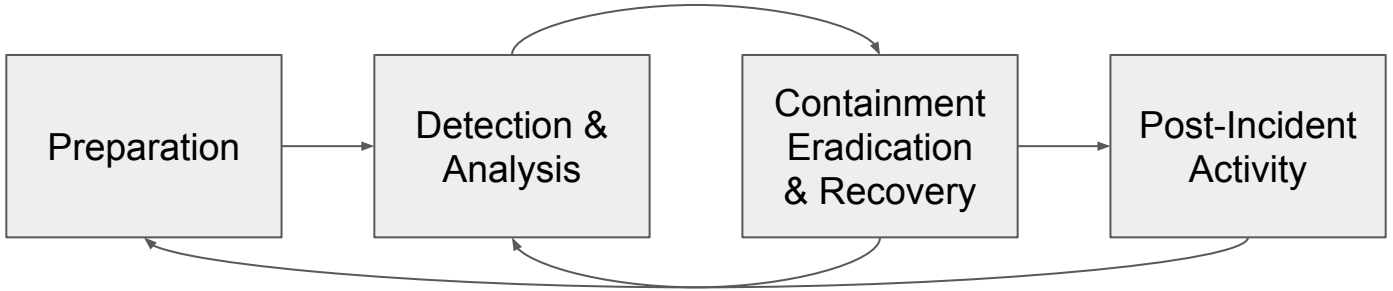
Crimea
The Voice of Russia

Quoted from **Voice of Russia,** "US hackers target Crimean referendum website," March 16, 2014:

> *"Our IT safety experts managed to find out where those attacks came from. It is University of Illinois at Urbana Champaign. The most powerful scanning of servers before the attack was carried out exactly from there.*
>
> *It is significant that Urbana – Champaign, with a population of 37,000, has the highest number of subnets with IP addresses. Let's take for example subnet 192.17.0.0 – 192.17. 255.255 whose range makes it possible to offer approximately 500 IP to each citizen, and there are at least five such subnets in the city.*
>
> *In other words, the technological and technical potentialities of this city exceed by thousands of times the needs of its residents.*
>
> *Besides, there are three airports in Urbana. There is no official information about the location of military bases on its territory, but there signs that one of the headquarters of the National Security Agency is situated there."*

IR Exercises

- Pick a security control that could help with each example incident
  - How would it help? Which phase(s) would it help with?
- Scenarios:
  - HPC Bitcoin – Insider attack
  - HPC Pivot Attack – Shared credential incident
  - Heartbleed – Zero day
  - Crimea – PR attack



Additional resources

- NIST SP 800-61 - https://doi.org/10.6028/NIST.SP.800-61r2
- Handbook for Computer Security Incident Response Teams (CSIRTs) http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305
- CTSC training materials - https://trustedci.org/trainingmaterials/
    - http://hdl.handle.net/2022/21528 - Computer Incident Response