LA-UR-22-31176

Approved for public release; distribution is unlimited.

Title:	Network Security Operation Center
Author(s):	Egan, Ashleigh Ann
Intended for:	University Presentation
Issued:	2022-10-21

Network Security Operations Center

Ashleigh Egan

Network Infrastructure and Engineering – Engineering and Security Services

October 27th, 2022

A Little about me

- Started with Degree in Psychology
- Switched to an IT degree in Networking
- Worked at Symantec for one year
- Worked at Los Alamos National Lab 4 years as member of the Network Security Operations Center

What does an NSOC do?

- Depends on the NSOC!
- Often a mix of networking, device management, and incident response
- Most often responsible for first line of defense
- Sometimes just called a Security Operations Center (SOC)

Los Alamos National Lab Network Security Operations Center

- Responsible for setting up and maintaining security devices
- Act as first responders for our Computer Security Incident Response Team (CSIRT)

Devices Common to an NSOC

- Firewall
- IPS
- IDS
- WAF
- Email firewall

Next-Gen Firewall

- A step up from the traditional “Layer 4” Firewall
- Used for Perimeter or specific areas like a Datacenter
- Current trend is trying to be the “Security Solution”- or having a firewall do everything all the devices can do.

Web Application Firewall (WAF)

- Used specifically to protect Webservers
- Works as an intermediary
  - Web traffic goes through a “virtual server” on the waf, through the firewall, before being able to view content on the actual server (Traffic never touches the server itself)

- Can make specific policies, screen out specific scanning, bot attacks, etc.

IDS/IPS

- Nowadays, often grouped on the same device- sometimes even added as features to firewalls
- IPS – Signature based
  - Blocks
- IDS – Behavior based
  - Documents and alerts

Recommended- Snort and Zeek

Email Firewall

- An email server that filters emails
- Often what you see as the mx record or headers
- Capabilities usually include:
  - Spam Detection
  - Phish Detection
  - Link/Malware sandboxing
  - Ability to create custom rules

Other Tools we use daily-

- SEIM
  - Free option -Elk Stack
- Packet Analyzer
  - Free option - Wireshark
- Tool for Decoding
  - Cyber chef, or even notepad++
- Regex Coach
  - regexr
- Virtual Machines
  - VM ware or Virtual Box

Incident Response

- Responding to Potential Security threats
- NSOC does initial triage to determine false or true positives
- Threats reported by:
  - Users
  - Device Alerts
  - Logging alerts

Incident Response Process

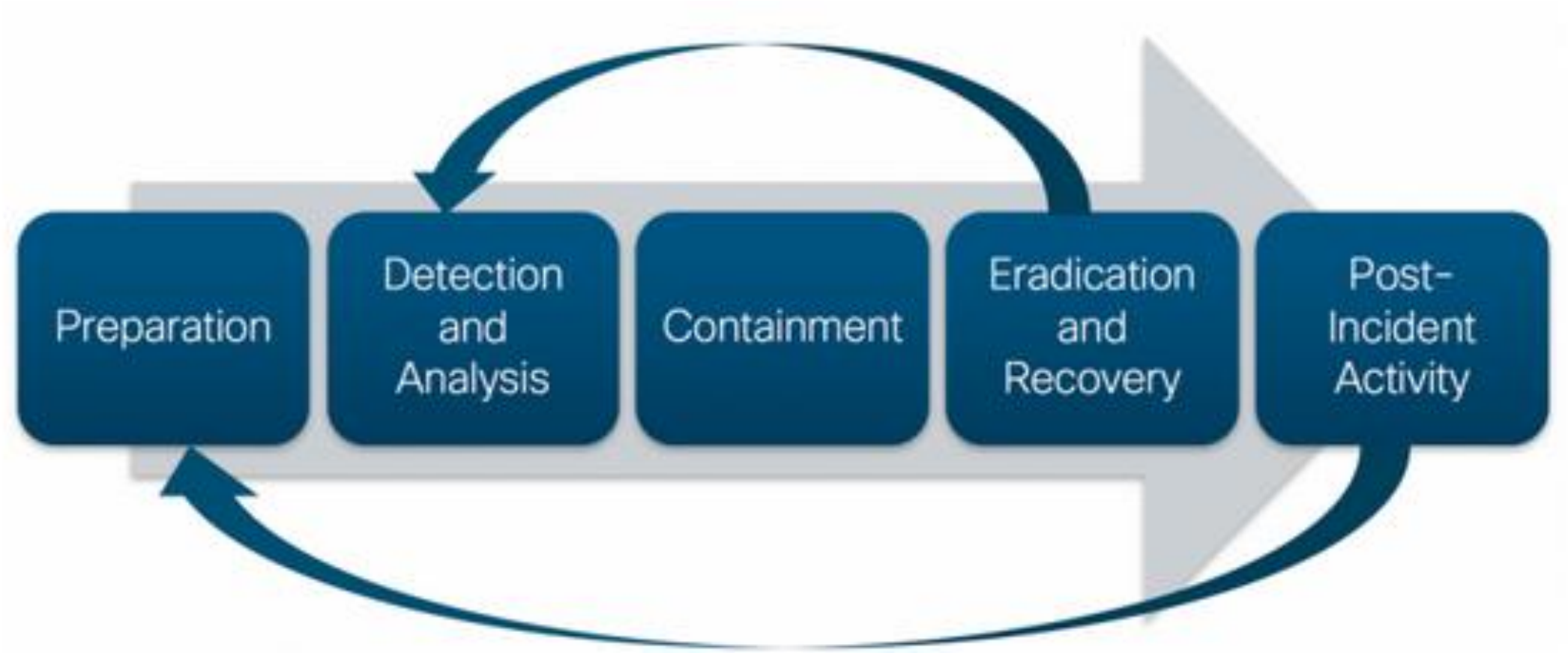
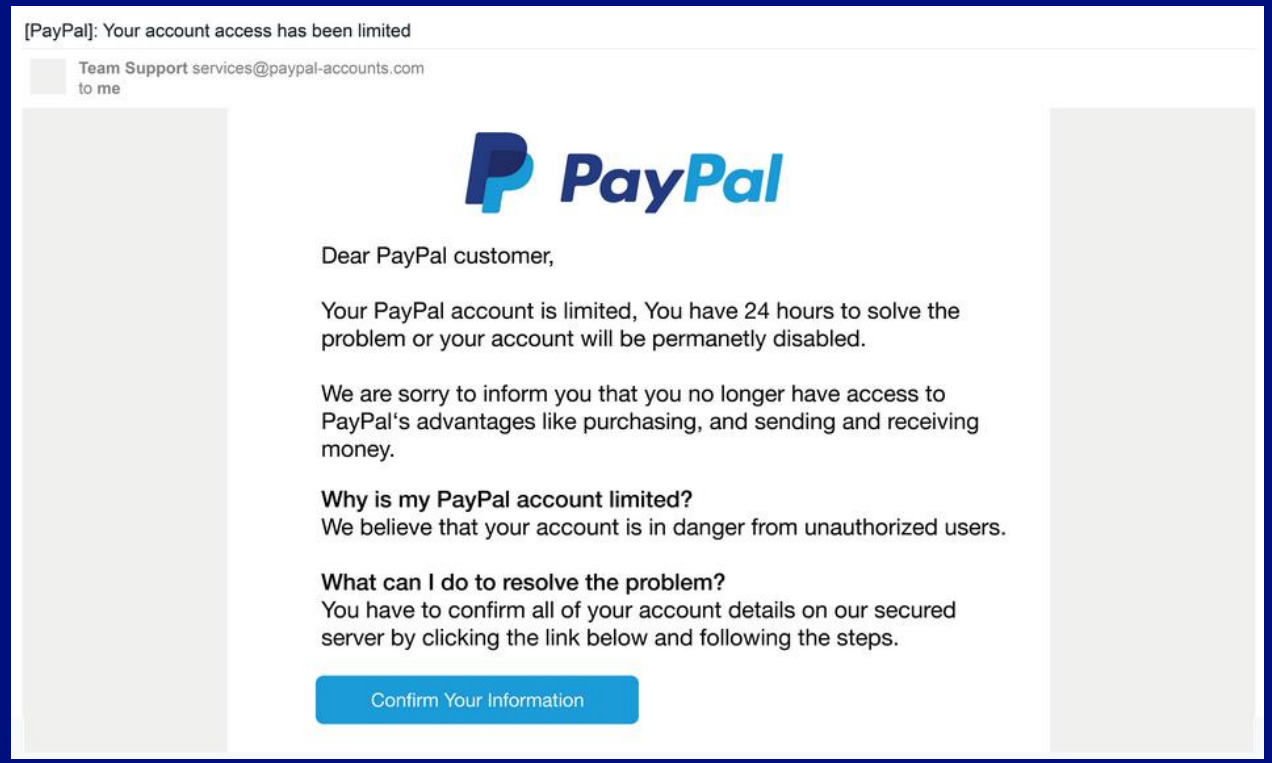


Figure 1. Incident Response Process, “Dissecting a Breach: The Process of Incident Response,” 29 November 2017 , blogs.cisco.com/security/dissecting-a-breach-the-process-of-incident-response. Accessed 27 Sep 2022

So what do I do with this all day?! Example:

- A user reports a suspicious email that they received.



- Figure 2. Paypay Phishing Example, “Phishing Email Example,” 2021 , hooksecurity.co/phishing-examples/paypal-phishing-example. Accessed 19 Oct, 2022

Investigate

- Headers
  - Mailfrom
  - From
  - Reply-to
- Links
  - Check Reputation
  - Check proxy/dns logs for activity
- Attachments
  - Check hashes
  - Sandbox if possible
- **Pivot on indicators**

Figure 3. Example of blank headers

Received: from (these contain IPs and ciphers used from each hop, as well as time stamps, etc. The top is the final recipient, and goes backwards)
Received: from
Received: from
Received: from
Received: from
Received: from
Received: from
Received: from
Authentication-Results: (DOMAIN); spf=pass smtp.mailfrom=; dkim= header.s= header.d=; dmarc= header.from=
Received: from
Received: by
X-Received: by
Received: by
Reply-To:
From:
Date:
Message-ID:
To: ;
Content-Type:
MIME-Version:
Subject:
Return-Path:

How can I keep this from happening again?

- Email Firewall
- Watch for trends
- Block Senders, domains, IPs

Uh oh- another user got it and clicked the link

- Where does the site take them- sandbox the site
- How is the site trying to get them?
  - Cred harvester
  - Malware download
  - Other

The User Downloaded something from the malicious site

- There is now likely malware on the machine- what do we want to look for?
  - Unusual proxy activity
  - Changes to the Registry
  - Privilege Escalation
  - And more…

- Escalate and report- this is above my paygrade!
  - CSIRT team will run forensics, determine scope of issue, and perform any needed remediation

What if the email had not been reported?

- Alerts looking for broad malware activity
  - Even without the reported email, alerts would be triggered in the case of malware

- Learning from new cases to create more alerts

How can I be prepared next time?

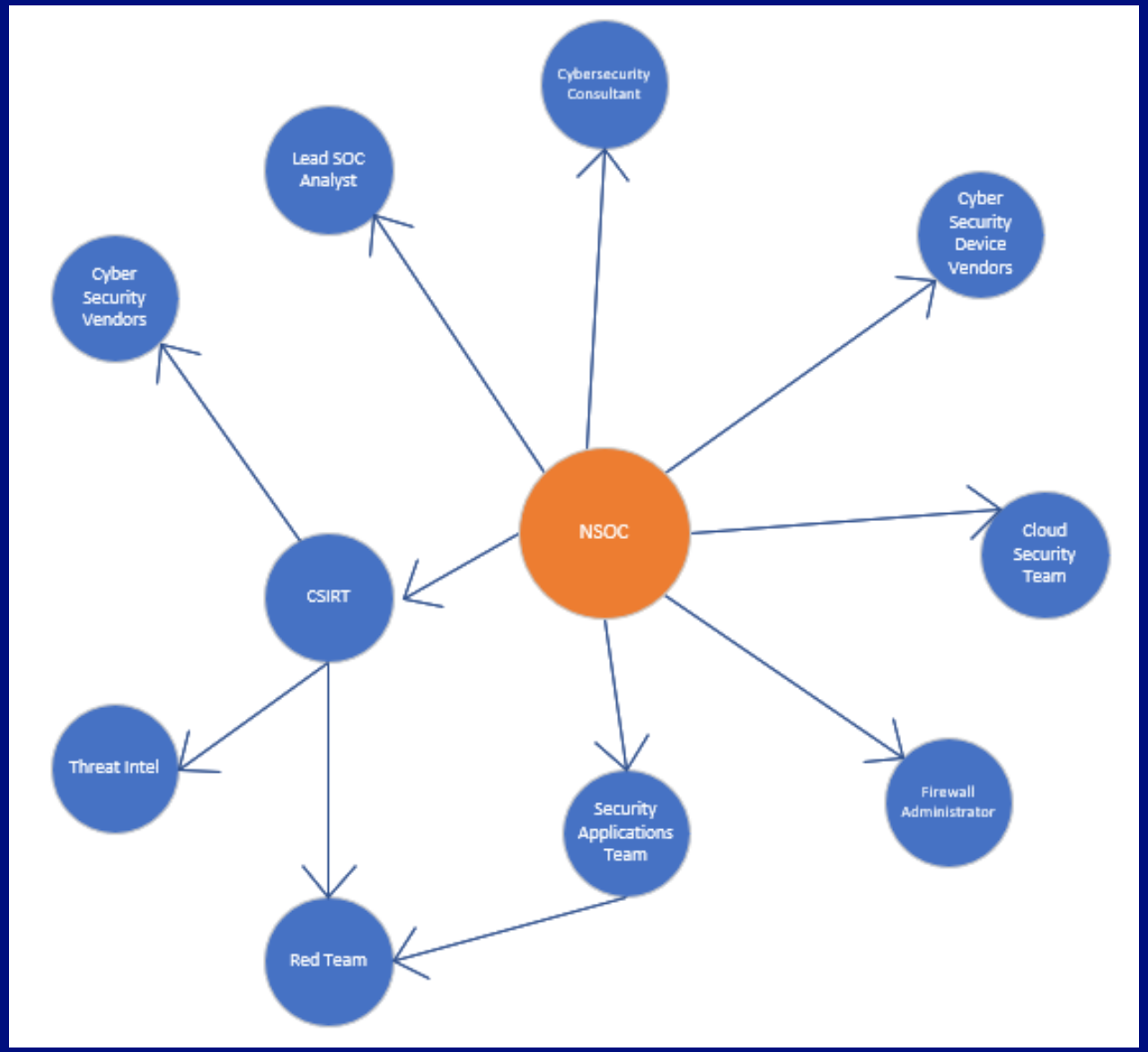
- Review Lessons learned
- Keep up with current vulnerabilities
- Stay updated/patched
- Know your devices
  - Can I stop any stage of this on a firewall? With an IPS? Could we see any activity in the IDS?

Why an NSOC

- Great introduction to Cybersecurity
- Exposure to many facets of cyber
- Great start for various careers

Where does it take you-

- Working in an NSOC can give a variety of experiences
- Helps find what really interests you
- Many opportunities in IT, Cyber, Incident Response



- Figure 4. Diagram of some careers that have stemmed from the NSOC

Any Questions?