LA-UR-18-30641
Approved for public release; distribution is unlimited.

Title: Incident Response and Malware Analysis

Author(s): Pearce, Lauren

Intended for: Presentation at recruiting visit to a university

Issued: 2018-11-06

Incident Response and Malware Analysis

National Nuclear Security Administration
Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

- Introduction
- Incident Response Life Cycle
- Working in Incident Response
- Malware Analysis in Incident Response
- About Los Alamos National Laboratory

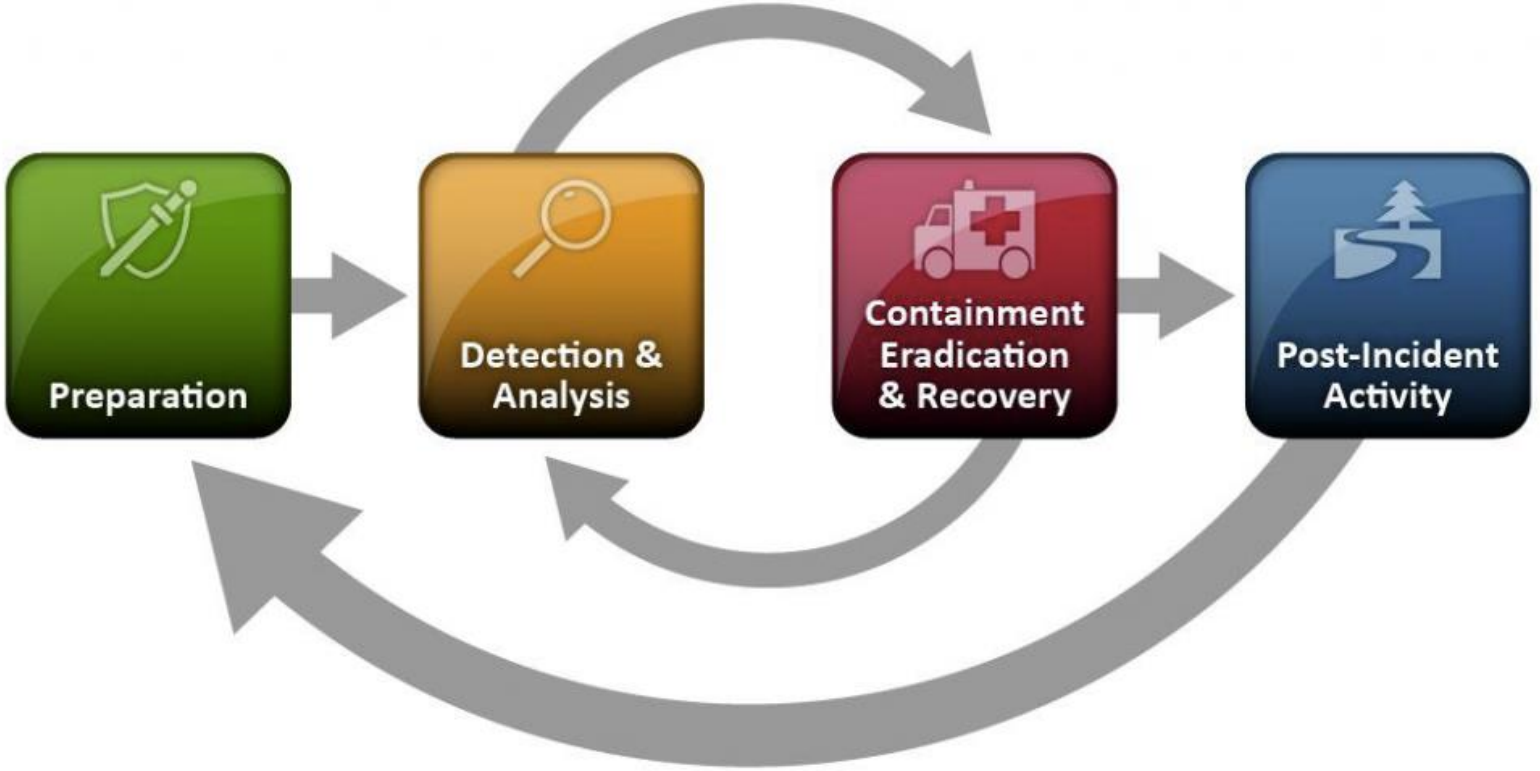
whoami

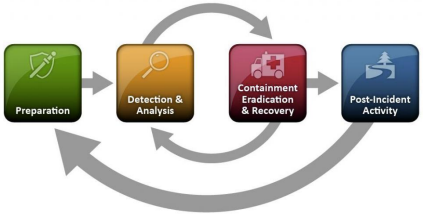
- Graduated FSU with MS in Computer Criminology in spring 2015
- Started working for Los Alamos National Laboratory's Computer Security Incident Response Team (CSIRT) at the end of summer 2015
- Still work for CSIRT, specializing in malware analysis

Incident Response Lifecycle

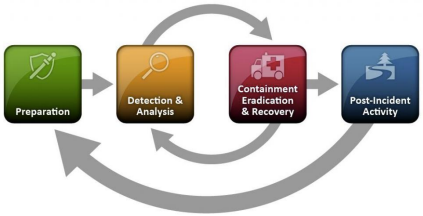
Incident Response Lifecycle

Defined in NIST SP 800-61

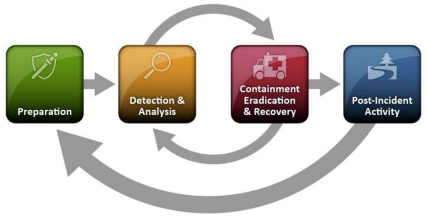




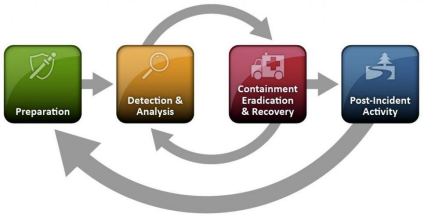
- **Analyze and act on threat intelligence**
  - External Threat Intelligence – Extract indicators from incident reports made available to us and research such as malware analysis.
  - Internal Threat Intelligence – Extract indicators from the attacks we see hitting our edges. We also learn from past incidents.
  - We write alerts to notify us when indicators extracted from threat intelligence are seen on our networks.
- **Less IR Specific:**
  - Insure regular patching across the network
  - Put tools in place to increase visibility
  - Educate users



- **Methods of Detection:**
  - Previously written internal alert fires
  - Manual search by team member reviewing threat intelligence turns up result
  - User notifies team of suspicious activity
  - External notification
- **When an event is detected, first tier responders either rule it as a false positive or minor threat and close the alert, or they escalate it.**
  - If escalated, next tier examines the ticket, takes appropriate action. May declare an incident.

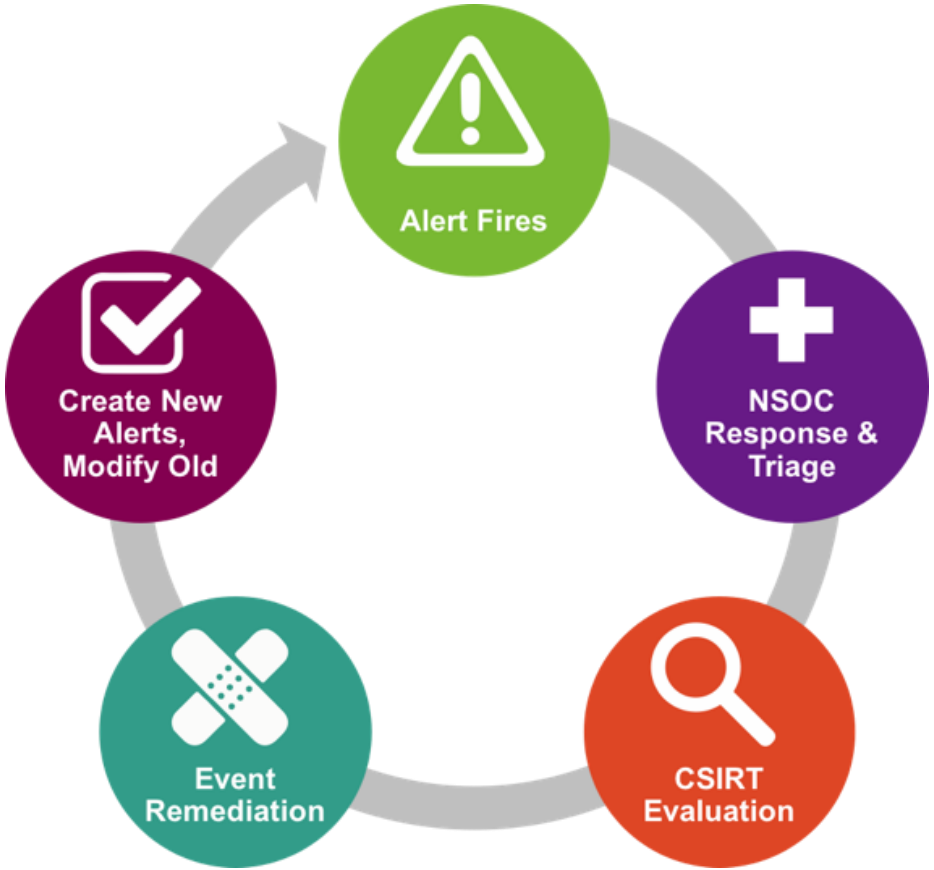


- **Removing an advanced adversary from a network is not easy. Often they've spread out, dug in, and only reveal themselves from a single "beachhead" machine.**
- **Is common for teams to think they've contained and eradicated a threat, only to see it reemerge with different tactics, techniques, and/or procedures (TTPs). That is why this step loops back to the previous step, "Detection and Analysis".**
  - It is best to try to avoid this game of "Whack a Mole" by making sure you have a complete picture of the intrusion before beginning remediation actions.
  - In an ideal world, but the time an adversary realizes that you know about their intrusion, they're completely removed from the network.



- Continue to review collected evidence for any previously missed indicators or tools.
- Continue to reverse engineer the adversary's tools with the goal of extracting indicators.
- Write alerts based off of indicators so that, at a minimum, you'll notice if they attempt to use any of their old toolsets on your network again.
- Write reports and share intelligence

Incident Response Process – Operational View



Working in Incident Response

Broad Skill Set

- **When on call, must be able to triage and respond to anything alone – a tall order in a very broad field**
- **Most (but not all) of us specialize in something, but are capable generalists**
- **When we work together as a team, we each play to our strengths**
- **Going through my team we have, in addition to several amazing generalists:**
  - The host forensics guy
  - The malware guy
  - The red team guy
  - The sys admin

Pace

- **Bad guys don’t work 9-5 and take federal holidays off**
- **Someone is always on call**
  - Stressful initially, fun once you’re good at it
  - Exposes you to a variety of threat vectors
  - Fastest place to learn, easiest place to screw up

Entering the Field - Advice

- **Look for a company that cares about security. Good IR requires good network visibility. Good network visibility costs money.**
- **When interviewing, know what tier you're interviewing for. Most entry level positions are for tier 1 or mid tier. This is an excellent position from which to learn about enterprise network defense.**
  - Entering at top tier is occasionally possible, but can be overwhelming.
- **Read about major intrusions and incidents. Watch conference talks from professional incident response companies such as Mandiant.**
- **Soft skills are important:**
  - Communication, both written and spoken
  - Humility to admit when you're wrong
  - Flexibility to roll with the punches

Malware Analysis in Incident Response

What is Malware?

- **“Software that is intended to damage or disable computers and computer systems”**
- **It’s ultimately just code, just like any other program.**
- **It does need a few things to survive and be successful, some of which are unique from most goodware**
  - Covert persistence
  - Covert network communication

Role of Malware Analysis in Incident Response

- **Malware is the method by which bad guys gain a foothold in a system**
  - To detect a bad guys trying to get into a system, know their toolset.
- **Malware is the method by which bad guys maintain their presence in a network**
  - To know how bad guys are exfiltrating data, and consequently what was exfiltrated, know their toolset.
- **Malware is the method by which bad guys exfiltrate data**
  - To know how bad guys are maintaining their persistence, and consequently, how to get them out of your networks, know their toolset.

Why Did I Choose Malware?

- It is an unsolved problem.
- Not many people know how to do it.
- It’s a puzzle, a very hard puzzle, but one to which you know there’s an answer.
- It’s necessary to effective incident response

Knowledge Required for Malware Analysis

- **Background Knowledge:**
  - Familiarity with x86 assembly and calling conventions
  - Strong knowledge of a low level programming language (C works)
  - Strong understanding of computer organization and operating systems
  - Ability to Google

- **Specific Knowledge:**
  - IdaPro, Binary Ninja, Radare2, or similar decompiler
  - OllyDbg, WinDbg, x64, or similar debugger
  - Understanding of bitwise operations and their use in encoding

Soft Skills for Malware Analysis

- A desire to solve puzzles
- Patience
- A touch of OCD
- A willingness to dream about assembly code
- More patience

Los Alamos National Laboratory

Los Alamos National Laboratory

- **Mission: To solve national security challenges through scientific excellence**
- **FY16 Budget: Approximately $2.55 billion**
- **Approximately 11,500 employees**
- **Approximately 40 square miles encompassing 1,000 buildings, 13 nuclear facilities, and 198 miles of road.**

An Academic Environment

- With secrets.
- Conflict between the open sharing of information associated with and valued by academia, and the need for secrecy associated with working on national security issues
- Working in incident response, this conflict is apparent daily
- Our goal is to enable the science, but keep the science secure

A Casual Environment

- **Jeans every day**
- **Flexible working schedule**
  - Most work 9 hour days, then take every other Friday off
- **Values service to community**
  - “STEM Education Time” – Coach a Youth Cyber Defense Competition team, partially on the clock.

A Small Town

- **Population 12,019**
- **Fantastic Schools**
- **Low crime rates**
- **Sometimes, seems stuck in a different era**
  - Good luck finding food after 9
  - One bar, open to 11 most nights
  - No Walmart or Target
  - You'll bump into people you know all over the place
  - People help each other
  - Kids play in the park, bike on the streets

Surrounded by Outdoor Activity

- **Rock Climbing**
- **Skiing (XC and Downhill)**
- **Hiking and Backpacking**
  - 13,000’ peaks
- **Mountain Biking**
- **Fly Fishing**

Questions?