
DEV/SECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR / LESSON THREE

Agenda

- Tying it all together
 - Why do we go through the trouble?
 - Where to get started?
 - Incident Response

Why

- Knowing what's going on is half the battle
 - Indispensable in large environments
 - Legal ramifications of not doing due diligence
- Prevention is ideal, **detection** is essential
 - Bad guys will get in
 - Minimizing our reaction time is critical

Where to get started?

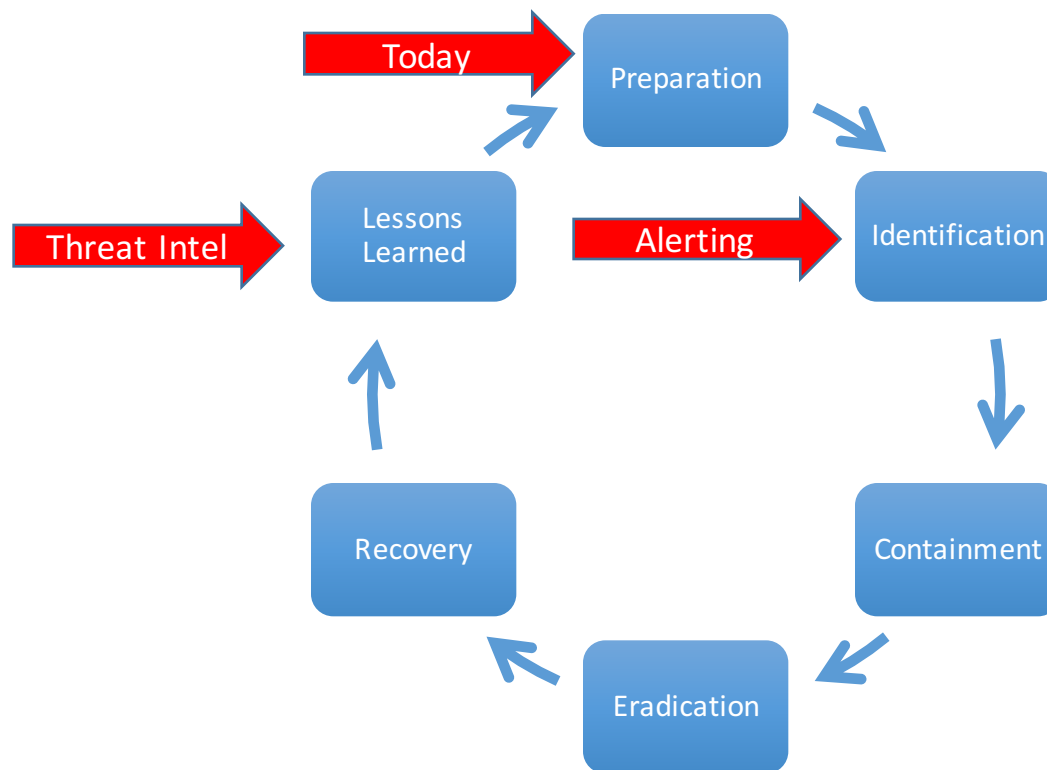
- Hunt
 - Familiarize yourself with logs/data
 - Look for evidence of misuse
 - Investigate
 - Remediate
 - Create alerts

Where to get started?

- Types of threat intel
 - Open source
 - Vendor provided
 - Home grown

Open source + Vendor provided + Home grown => High fidelity alerts

Incident Response



NIST/SANS Incident Response Methodology

Questions?

Lab 3

- If you weren't here last week team up with someone who was or quickly do week 3 lab 2 (get AWS credentials from Instructor)
- If you were here last week:
 - Run through the exercises in week 3 lab 3 if Splunk searches return no data