**Incident Management Response**

Benjamin M. Brandhorst

University of Maryland Global Campus

SDEV 360 6380 Secure Software Engineering

Professor Kevin Woodson

March 8th, 2020

For the ATM system incident, we will be following the United States (U.S.) Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) incident management best practice model.

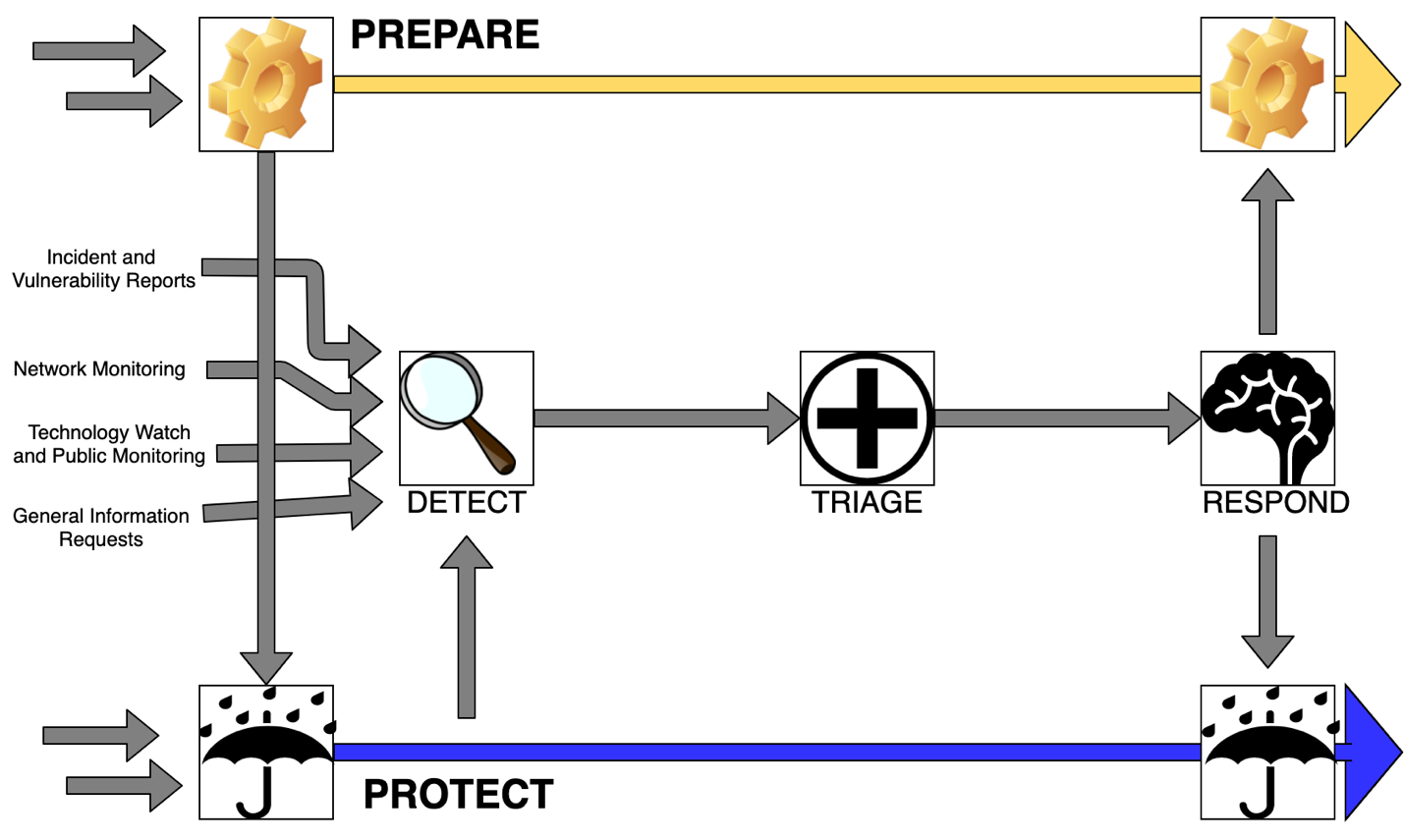


Figure 1 – Incident management best practice model (Diagram format source: (Killcrece, 2005))

Our Incident Response Plan (IRP) will focus on the following:

* Identifying security incidents
* Resolving an incident quickly
* Protecting assets and reducing losses
* Recovering from a security event
* Mitigating future organizational risks or exposures
* Reducing the chaos of crises
* Proper and consistent documentation

**Detection and Reporting**

Our incident response is modeled after the example provided by Digital Guardian “The Five Steps of Incident Response” (Bandos, 2019). In this scenario, large sums of money were withdrawn from several networked ATM systems by the same User ID. All bank employees should be trained and familiar with our incident response plan and should have available to them the hotline with which they can report the incident. A backup organizational mailbox should also be available for any employee to send reports of potential incidents. Once the alert has been given, an incident ticket should be created by an analyst which documents the initial findings and provides an initial incident classification.

**Tr****iage and Analysis**

In this step we spend most of our effort trying to understand the scale of and effects of the security incident. Here we will use our resources to collect data from tools and systems to analyze for indications of compromise. Our focus will primarily be in three areas:

* Endpoint Analysis
  + Determine if tracks were left by threat actor
  + Gather artifacts to build timeline of activities
  + Bit-for-bit analysis of copy of systems from a forensic perspective
* Binary Analysis
  + Investigate malicious binaries or tools used by attacker and document program functionalities. This can be done by:
    - Behavioral Analysis: Execute program in a Virtual Machine
    - Static Analysis: Reverse Engineer the program
* Enterprise Hunting
  + Analyze existing systems and event logs to determine scope of compromise
  + Document all compromised accounts and machines so that effective containment and neutralization can be performed.

**Containment and Neutralization**

Using the evidence and information gathered in the previous steps, we are now prepared to contain and neutralize the threat. This happens by conducting a coordinated shutdown of all compromised systems within the environment. All Incident Response (IR) members should be notified so that the shutdown timing is coordinated. All of the infected devices should be rebuilt from the ground up. Additionally, any compromised account passwords should also be reset. If any domains or IP addresses were identified as being leveraged by bad actors for command and control, be communication from all channels connected to those domains should be blocked.

**Post-Incident Activity**

An incident report that documents all of the details of the incident should be completed. This will help the incident response plan and compliment additional security measures to help mitigate against similar security incidents in the future. Post incident monitoring should continue to look for bad actors attempting the same exploitation again. Based on information gathered in the Triage and Analysis step, mitigations against further exploitations of this vulnerability should be developed and implemented.

References

Bandos, T. (2019, June 26). The five steps of incident response. Retrieved from https://digitalguardian.com/blog/five-steps-incident-response

Killcrece, G. (2005, December 19). Incident management. Retrieved from https://www.us-cert.gov/bsi/articles/best-practices/incident-management/incident-management