Drinking from the Fire Hose

ONE YEAR INTO INCIDENT RESPONSE

PRESENTED BY GOLGOTHUS (ZACH, HE/HIM)

Whoami: Golgothus / Zach (he/him)

Work Experience

- Cyber Security Associate Engineer (Incident Response, 1 year)
- Previously Endpoint Protection (3 years)
- Help Desk UTA (1 year)

Accreditations

- CySA+
- Pentest+

Social Media

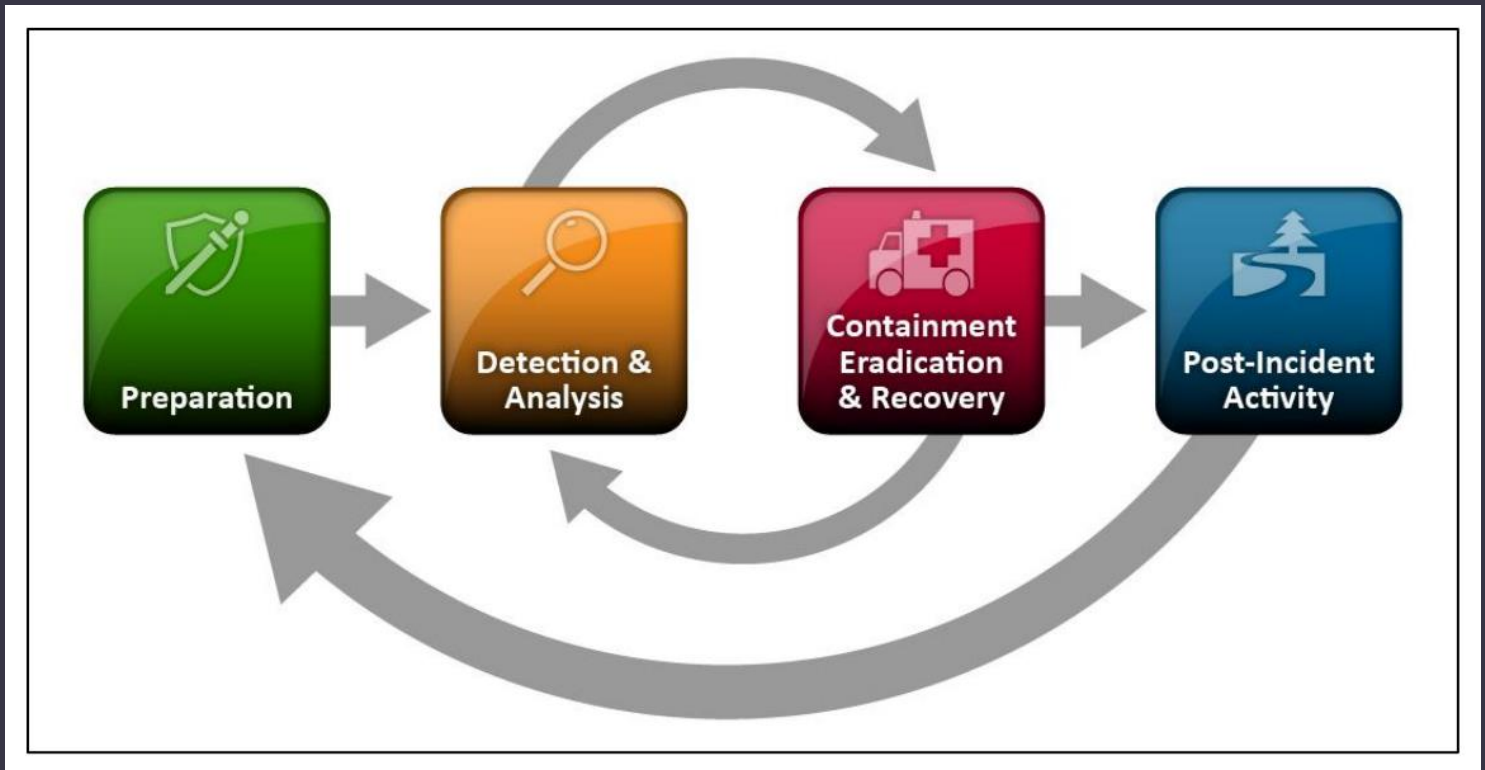
- ghost$ (golgothus.tech)
- Golgothus (Zach He/Him) (@Golgothus) / Twitter

In the Beginning

- Incident Response is a tough, but fun job
- Knowing your environment is beneficial
- Logs are your life source
- Every organization is different
- Know your process
  - “Who, What, When, Where, Why”
- Take notes!
- “Teamwork to makes the dream work”

In the Beginning (Cont.)

Incident Response Process:



Know Your Scope

- Advice I've received:
  - Know the difference between a security incident vs. security compliance
- Verify your alert activity
  - Sometimes the "NMAP Scan" won't be "true positive" activity
  - No point in burning cycles to investigate known normal / benign activity
- Keep communication channels open, and get to know your team

Tools of the trade

URL

- Remnux + Burpsuite to review re-direct links for payloads
- URL Redirect Checker | WhereGoes
- URL and website scanner - urlscan.io
- Shodan Search Engine

Hash

- VirusTotal - Home
- AlienVault - Open Threat Exchange
- ANY.RUN - Interactive Online Malware Sandbox

Work Smarter, Not Harder

- If documentation doesn’t exist, make it
- Prevent alert burnout by reducing the noise
- Incorporate searches / sub-searches to enrich your data
- Throwback to notation. Playbooks, ‘case templates’, or case management systems can be priceless to your team
- https://twitter.com/Cyb3rSn0rlax/status/1549179670406512641

The Future is Now

- Don’t spread yourself to thin
- It’s OK to specialize, just share the knowledge
- Current outlook
  - Azure Pipelines and Azure DevOps
  - Azure Kubernetes Service
  - Azure LAWS / Sentinel
  - Kubernetes / Docker

The Future is Now (cont.)

Detections as Code (DaC)

- Splunk has a few solid blog posts on this (referenced in notes)
- Usage of streamlined processes to create refined detections

CI/CD Pipeline

- Azure Boards help correlate tasks to specific Pull Requests, this can be useful for Change Advisory Boards and metrics
- Automate updates and deployments via the DevOps Pipeline
- Review modifications to branches, code, environment from a single pane

DevSecOops

- Usage of DevOps pipeline / tooling
  - Git (local repo)
  - Github
  - Bitbucket
  - GitLab
- Azure DevOps Services | Microsoft Azure
- Terraform
- Azure DevOps Hands-On Labs | Azure DevOps Hands-on-Labs (azuredevopslabs.com)

Resources

- Azure Repos documentation - Azure DevOps | Microsoft Docs
- Microsoft Certified: Azure Administrator Associate - Learn | Microsoft Docs
- Exam AZ-400: Designing and Implementing Microsoft DevOps Solutions - Learn | Microsoft Docs
- Exam SC-200: Microsoft Security Operations Analyst - Learn | Microsoft Docs

Honorable Mentions:

- SiegeCast: Azure Ad Basics with Alex Norman and Justin Palk – YouTube
- Penetration Testing Azure for Ethical Hackers | Packt (packtpub.com)
- Welcome to Kubernetes Goat | Kubernetes Goat (madhuakula.com)
- 12 Days of Defense - Day 1: PDF and Office Doc Malware IOC Extraction - YouTube