Domain 1: Blue Team Operations Architecture

- Building a successful SOC
- Functions of SOC
- SOC Models & Types
- SOC Teams & Roles
- Heart of SOC- SIEM
- Gartner’s magic quadrant – TOP SIEM
- SIEM guidelines and architecture

Domain 2: SOC Tools

1. Splunk:
    - Industrial requirements of Splunk in various fields
    - Splunk terminologies, search processing language, and various industry use cases
    - Splunk universal forwarder, data inputs, Correlating Events, Search fields
2. Security Onion:
    - Introduction to Security Onion : NSM
    - Security Onion Architecture
    - Walkthrough to Analyst Tools
    - Alert Triage and Detection
    - Hunt with Onion

Domain 3: DFIR

Fundamentals of Digital Forensics

- Forensics Fundamentals
- Introduction to Digital Forensics
- Hard Drive Basics
    - Platters, sectors, clusters, slack space
- SSD Drive Basics
    - Garbage, collection, TRIM, wear leveling
- File Systems
    - FAT16, FAT32, NTFS, EXT3/EXT4, HFS+/APFS
- Metadata & File Carving
- Memory, Page File, and Hibernation File
- Order of Volatility
- Evidence Forms
- Volatile Evidence
    - Memory RAM, Cache, Registers content, Routing tables, ARP cache, process table, kernel statistics, temporary file system/swap space
- Disk Evidence
    - Data on Hard Disk or SSD
- Network Evidence
    - Remotely Logged Data, Network Connections/Netflow, PCAPs, Proxy logs
- Web & Cloud Evidence
    - Cloud storage/backups, chat rooms, forums, social media posts, blog posts
- Evidence Forms

  - Laptops, desktops, phones, hard drives, tablets, digital cameras, smartwatches, GPS
- Chain of Custody
- What is the Chain of Custody?
- Why is it Important?
  - In regard to evidence integrity and examiner authenticity
- Guide for Following the Chain of Custody
  - Evidence collection, reporting/documentation, evidence hashing, write-blockers, working on a copy of original evidence
- Windows Investigations
- Artifacts
  - Registry, Event Logs, Prefetch, .LNK files, DLLs, services, drivers, common malicious locations, schedules tasks, start-up files

*nix Investigations

- Artifacts
- Equipment
  - Non-static bags, faraday cage, labels, clean hard drives, forensic workstations, Disk imagers, hardware write blockers, cabling, blank media, photographs, Laptops, desktops, phones, hard drives, tablets, websites, forum posts, blog posts, social media posts, chat rooms, Types of Hard Drive Copies visible data, bit for bit, slackspace
- Live Forensics
- Live Acquisition
  - What is a live acquisition/live forensics? Why is it beneficial?
- Products
  - SysInternals, Encase, memory analysis with agents, Custom Scripts
- Potential Consequences
  - Damaging or modifying evidence making it invalid
- Post-Investigation
- Report Writing
- Evidence Retention
  - Legal retention periods, internal retention periods
- Evidence Destruction
  - Overwriting, degaussing, shredding, wiping
- Further Reading

Tools exposure provided in the above section:

- Command-LINE for Windows / Linux
- Network Analysis: Wireshark, Network Miner
- Disk Based Forensics: FTK IMAGER, AUTOPSY, Encase
- Memory Forensics: MAGNATE & BELKASOFT RAM CAPTURE, DumpIt, Volatility, Volatility WorkBench
- Email Forensics: Manual & Automated Analysis

Incident Response Basics

- Introduction to Incident Response

- What is an Incident Response?
- Why is IR Needed?
- Security Events vs. Security Incidents
- Incident Response Lifecycle – NIST SP 800 61r2
- Incident Response Plan : Preparation, Detection & Analysis, Containment, Eradication, Recovery, Lessons Learned
- Case Study : Cyber Kill Chain in Incident Response
- Lockheed Martin Cyber Kill Chain
  - What is it, why is it used
- MITRE ATT&CK Framework
  - What is it, why is it used
- Preparation
- Incident Response Plans, Policies, and Procedures
- The Need for an IR Team
- Asset Inventory and Risk Assessment to Identify High-Value Assets
- DMZ and Honeypots
- Host Defences
  - HIDS, NIDS
  - Antivirus, EDR
  - Local Firewall
  - User Accounts
  - GPO
- Network Defences
  - NIDS
  - NIPS
  - Proxy
  - Firewalls
  - NAC
- Email Defences
  - Spam Filter
  - Attachment Filter
  - Attachment Sandboxing
  - Email Tagging
- Physical Defences
  - Deterrents
  - Access Controls
  - Monitoring Controls
- Human Defences
  - Security Awareness Training
  - Security Policies
  - Incentives

Detection and Analysis

- Common Events and Incidents
- Establishing Baselines and Behavior Profiles
- Central Logging (SIEM Aggregation)
- Analysis (SIEM Correlation)

Containment, Eradication, Recovery

- CSIRT and CERT Explained
    - What are they, and why are they useful?
- Containment Measures
    - Network Isolation, Single VLAN, Powering System(s) Down, Honeypot Lure
- Taking Forensic Images of Affected Hosts
    - Linking Back to Digital Forensics Domain
- Identifying and Removing Malicious Artefacts
    - Memory and disk analysis to identify artefacts and securely remove them
- Identifying Root Cause and Recovery Measures

Lessons Learned

- What Went Well?
    - Highlights from the Incident Response
- What Could be Improved?
    - Issues from the Incident Response, and How These Can be Addressed
- Important of Documentation
    - Creating Runbooks for Future Similar Incidents, Audit Trail
- Metrics and Reporting
    - Presenting Data in Metric Form
- Further Reading

Tools exposure provided in the above section:

- SYSINTERNAL SUITE
- Hash Calculator
- Online Sources
- CyberChef

Domain 4: TI

- Introduction To Threat Intelligence
- Threat Actors
- Types of Threat Intelligence :
    - Operational Intelligence
    - Strategical Intelligence
    - Tactical Intelligence
- CTI Skills: NIST NICE – CTI Analyst
- OODA Loop, Diamond Model of Intrusion Analysis
- Unleashing Threat Intel with Maltego, AlienVault OTX
- LOTL Based Techniques
- Malware Campaigns & APTs