The Pedagogical Value Behind Setting Up a Virtualized SOC

Dr. George Dimitoglou
dimitoglou@hood.edu

Dept. of Computer Science & Information Technology
Center of Computer Security and Information Assurance
Hood College
Frederick, Maryland

Security Operations Center (SOC)

- Centralized cybersecurity hub
- Monitors, detects, and responds to threats
- Combines people, processes, and technology

Typical SOC Functions

Monitoring and Detection

24/7/365, Threat Detection, Log Analysis

Incident Response and Reporting

Triage, Containment, Remediation, Forensic Investigation

Threat Intelligence

Threat Hunting, Intelligence Sharing, Analysis of Threat Trends

Vulnerability Management

Scanning and Assessment, Patch Management, Mitigation

Security Policy Enforcement

Access Control Management, Policy Compliance

SOC Operation Modes

- **24x7 monitoring** (round-the-clock teams)
- **Follow-the-sun model** (regional time zones)
- **On-demand monitoring** (ad-hoc or scheduled)
- **Hybrid models** (combining approaches)

Minimum Staffing Requirements for SOC Modes

Mode	Number of Analysts Needed	Notes
24x7	4-5 per shift	Covers 3 shifts per day
Follow-the-sun	2-3 per region	Regional time zones
On-demand	1-2	Task-specific

Challenges of Buiding a Physical SOC

(in an educational environment)

- High costs of physical setup
- Limited scalability
- Restricted real-world scenarios
- Resource and time intensive

LSU's Cyber Command Center

Building a Virtualized SOC (vSOC)

Def. vSOC → Simulated SOC environment

- ***Cloud-based*** or ***virtual machines***
  - ***"Safe"*** and ***controlled*** learning space
  - ***Scalable*** and ***flexible***

Pedagogical Benefits of a vSOC

- Hands-on, ***practical experience***
- Immediate ***feedback*** and analysis
- Collaborative team scenarios
- ***Adaptable*** to various skill levels

Two learning “threads”:

1. **Setting up the vSOC**: *Systems, Networking …and more*
2. **Using the vSOC***: Threat Intelligence, Incident response* …and more

Learning Objectives

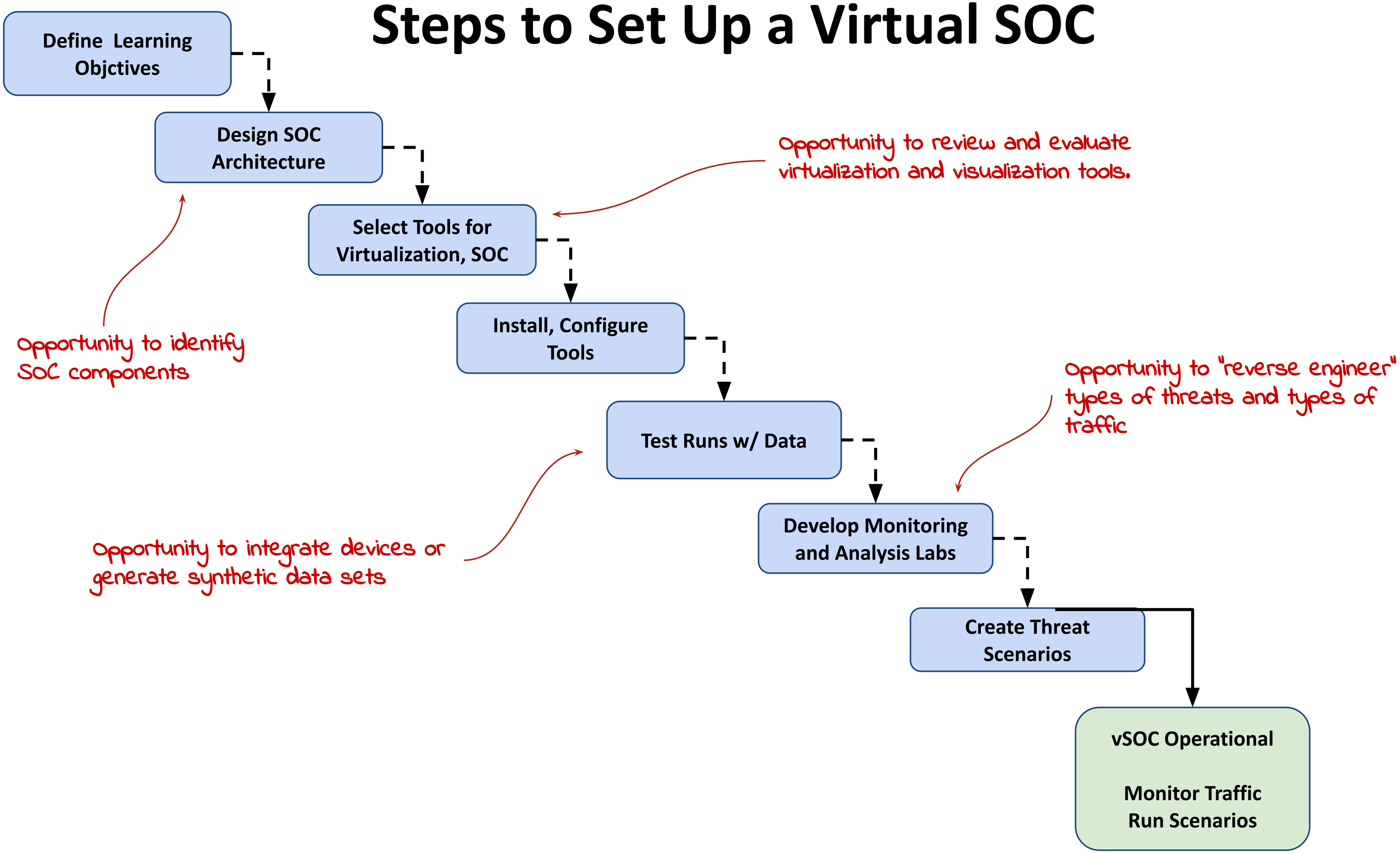
Setting Up a vSOC

- Configure ***virtualized environments*** and related tools
- Configure ***data sources*** and ***log pipelines***
- ***Integrate*** tools (e.g., firewalls, SIEM, log aggregators) and monitoring platforms

Using a vSOC

- ***Monitor*** and ***analyze*** incoming logs
- ***Identify*** and ***respond*** to threats
- ***Collaborate*** in incident response
- **Generate** and ***present*** reports
- Design and implement threat scenarios

Steps to Set Up a Virtual SOC



Define Learning Objctives

Design SOC Architecture

Select Tools for Virtualization, SOC

Install, Configure Tools

Test Runs w/ Data

Develop Monitoring and Analysis Labs

Create Threat Scenarios

vSOC Operational

Monitor Traffic
Run Scenarios

Opportunity to identify SOC components

Opportunity to review and evaluate virtualization and visualization tools.

Opportunity to integrate devices or generate synthetic data sets

Opportunity to "reverse engineer" types of threats and types of traffic

Tools and Platforms - Commercial, Industry Use

(aka 'tools we could not afford to use')

- **SIEM**
  - Splunk, IBM QRadar, Microsoft Sentinel
- **Threat Emulators**
  - Cobalt Strike, Core Impact, SafeBreach
- **Endpoint Detection and Response (EDR)**
  - CrowdStrike Falcon, Microsoft Defender for Endpoint, Carbon Black
- **Virtualization Platforms**
  - VMware ESXi, Citrix Hypervisor, Microsoft Hyper-V
- **Visualization Tools**
  - Tableau, Power BI, Splunk Dashboards
- **Network Monitoring/Analysis**
  - SolarWinds, Cisco Stealthwatch, Palo Alto Cortex XDR
- **Threat Intelligence**
  - Recorded Future, ThreatConnect, Anomali

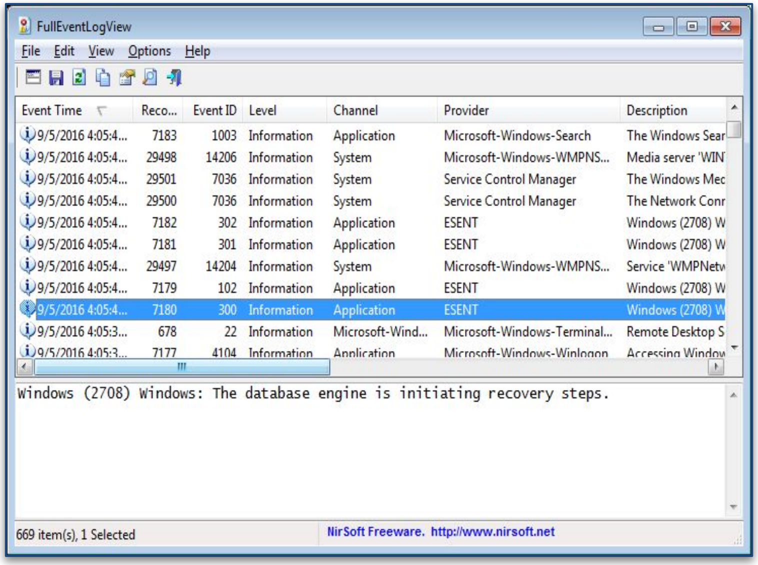
Tools and Platforms - Open Source

(aka 'tools we can afford to use')

- **SIEM**
  - OSSIM, Wazuh, ELK
- **Data collector**
  - Fluentd
- **Log Management**
  - Greylog
- **Network Monitoring**
  - Zabbix
- **Threat/Attack emulator**
  - Metasploit
- **Virtualization software**
  - VMware, VirtualBox
- **Visualization tools**
  - Grafana

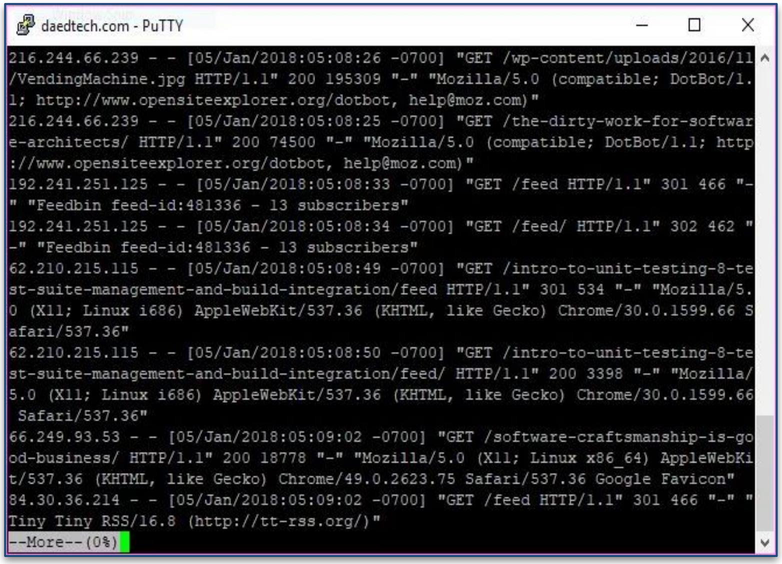
Data Sources and Logs for vSOC

- **System logs** (e.g., Windows Event Logs)
- **Application logs** (e.g., Apache, NGINX)
- **Network traffic logs** (e.g., firewall, IDS/IPS)
- **Endpoint detection logs** (e.g., antivirus, EDR)
- **Cloud platform logs** (e.g., AWS CloudTrail)



Event Time	Reco...	Event ID	Level	Channel	Provider	Description
9/5/2016 4:05:4...	7183	1003	Information	Application	Microsoft-Windows-Search	The Windows Sear
9/5/2016 4:05:4...	29498	14206	Information	System	Microsoft-Windows-WMPNS...	Media server 'WIN
9/5/2016 4:05:4...	29501	7036	Information	System	Service Control Manager	The Windows Mec
9/5/2016 4:05:4...	29500	7036	Information	System	Service Control Manager	The Network Conr
9/5/2016 4:05:4...	7182	302	Information	Application	ESENT	Windows (2708) W
9/5/2016 4:05:4...	7181	301	Information	Application	ESENT	Windows (2708) W
9/5/2016 4:05:4...	29497	14204	Information	System	Microsoft-Windows-WMPNS...	Service 'WMPNetw
9/5/2016 4:05:4...	7179	102	Information	Application	ESENT	Windows (2708) W
9/5/2016 4:05:4...	7180	300	Information	Application	ESENT	Windows (2708) W
9/5/2016 4:05:3...	678	22	Information	Microsoft-Wind...	Microsoft-Windows-Terminal...	Remote Desktop S
9/5/2016 4:05:3...	7177	4104	Information	Application	Microsoft-Windows-Winlogon	Accessing Window

```
Windows (2708) Windows: The database engine is initiating recovery steps.
```



```
216.244.66.239 - - [05/Jan/2018:05:08:26 -0700] "GET /wp-content/uploads/2016/11
/VendingMachine.jpg HTTP/1.1" 200 195309 "-" "Mozilla/5.0 (compatible; DotBot/1.
1; http://www.opensiteexplorer.org/dotbot, help@moz.com)"
216.244.66.239 - - [05/Jan/2018:05:08:25 -0700] "GET /the-dirty-work-for-softwar
e-architects/ HTTP/1.1" 200 74500 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http
://www.opensiteexplorer.org/dotbot, help@moz.com)"
192.241.251.125 - - [05/Jan/2018:05:08:33 -0700] "GET /feed HTTP/1.1" 301 466 "-
" "Feedbin feed-id:481336 - 13 subscribers"
192.241.251.125 - - [05/Jan/2018:05:08:34 -0700] "GET /feed/ HTTP/1.1" 302 462 "
-" "Feedbin feed-id:481336 - 13 subscribers"
62.210.215.115 - - [05/Jan/2018:05:08:49 -0700] "GET /intro-to-unit-testing-8-te
st-suite-management-and-build-integration/feed HTTP/1.1" 301 534 "-" "Mozilla/5.
0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.66 S
afari/537.36"
62.210.215.115 - - [05/Jan/2018:05:08:50 -0700] "GET /intro-to-unit-testing-8-te
st-suite-management-and-build-integration/feed/ HTTP/1.1" 200 3398 "-" "Mozilla/
5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.66
 Safari/537.36"
66.249.93.53 - - [05/Jan/2018:05:09:02 -0700] "GET /software-craftsmanship-is-go
od-business/ HTTP/1.1" 200 18778 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKi
t/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 Google Favicon"
84.30.36.214 - - [05/Jan/2018:05:09:02 -0700] "GET /feed HTTP/1.1" 301 466 "-" "
Tiny Tiny RSS/16.8 (http://tt-rss.org/)"
--More--(0%)
```

CHALLENGING

Connecting endpoint feeds to vSOC

- All about data ingestion!

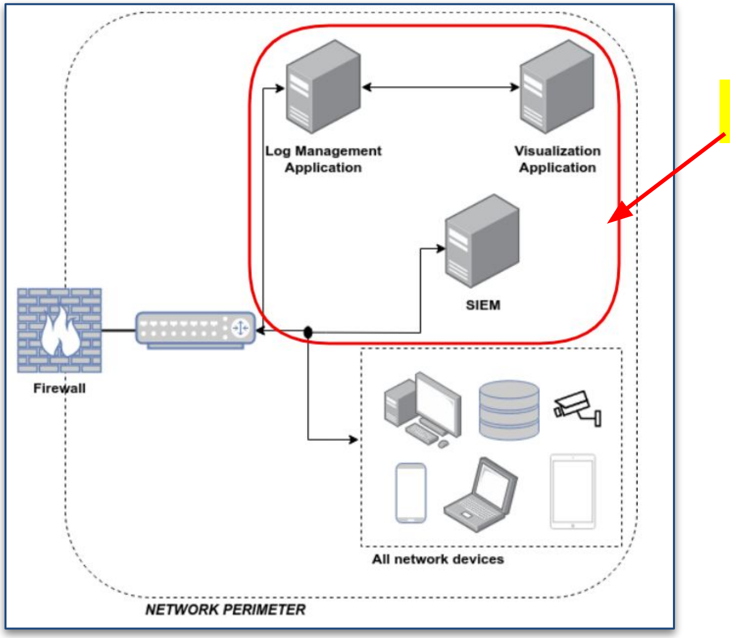
- Getting the necessary data from various devices
  - Install and configure ***log agents*** (e.g., Fluentd)
  - Set up ***secure channels*** (e.g., HTTPS, VPN)
  - Define ***log formats*** (e.g., JSON, syslog)

  - Send logs to SIEM or log collectors for ***ingestion***

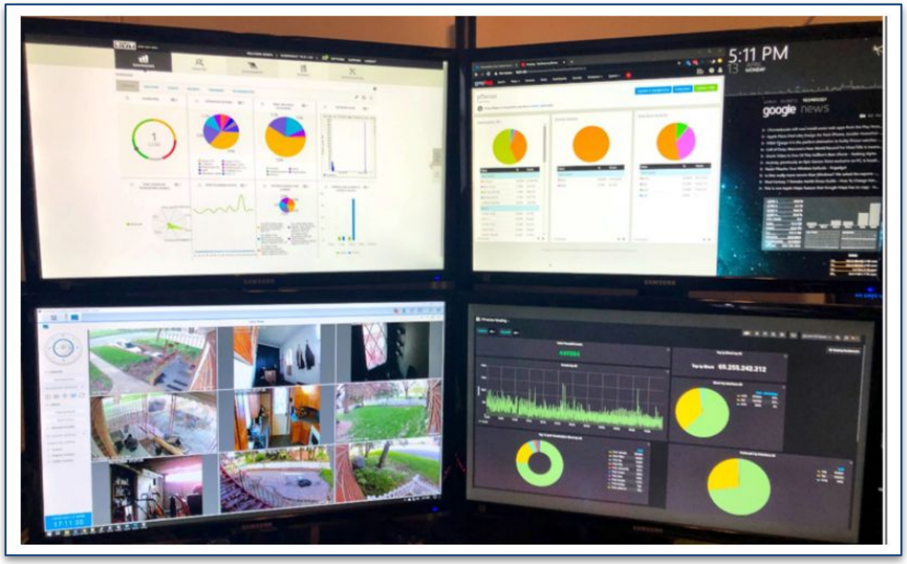
- Cadence of data feed (if not real-time)

Having data feed(s) = use of vSOC can start!

Our vSOC Prototype



Multiple VMs on a single hypervisor



SOC Component	Description (qty.)
Hardware	
Hardware Firewall Device	Qotom Q330G4 MiniPC, 4 NICs (1)
Host (hypervisor)	Dell R720 (1)
Monitors	Samsung 24”(4)
Storage server	Synology DiskStation DS218 (1)
CCTV Cameras	FosCam HD Indoor/Outdoor (9)
Software	
Operating System (hypervisor)	MS Windows Server 2016 Datacenter Edition; Hyper-V
Firewall	pfSense
Intrusion detection system	snort
Log Management Application	Graylog
Visualization Application	Grafana
SIEM Application	OSSIM 1
Packet analyzer	Wireshark
Physical Security Monitoring Application	ZoneMinder

Our vSOC Prototype - Results

The Good

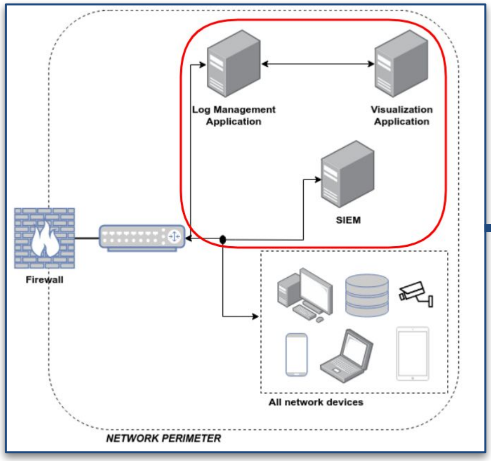
- Great learning experience
- Easy to add our endpoints
- Once set-up, it runs!

The …not so Good

- Minimized configuration learning past setup (“consumer effect”)
- Hard to add diverse endpoints
- Not homework-friendly

Our Current vSOC Attempt

from…



to…

Hypervisor with Multiple VMs

Single, Minimal, Isolated VM

Our Current vSOC Attempt - Challenges

Single, Minimal, Isolated VM

Table 1: Resource Budget per VM

TOOL	CPU (cores)	RAM (GB)	STORAGE (GB)
ELK Stack Elasticsearch/Logstash/-Kibana	2	4.0	50.0
Wazuh	2	4.0	50.0
Metasploit	1	2.0	1.0
Fluentd	1	0.5-1.0	1.0
Grafana	1	1.0-2.0	1.0
VirtualBox	1	2.0-4.0	20.0
Total	8	13.5-17.0	123.0

Student Learning Opportunities

Student Skill-Building

Incident Response Training

- Practice or develop incident response playbooks for containment and mitigation

Threat Intelligence Analysis

- Use tools to analyze Indicators of Compromise (IOCs)

Vulnerability Assessments

- Review and prioritize vulnerabilities (severity, impact)

Compliance Auditing

- Review logs to ensure adherence to security policies and standards (e.g., PCI DSS, GDPR)

Case Study Template - Example

Organization	DataCareless, Inc.
Scenario	The vSOC gets notice of a phishing email with a malicious link, simulating a real-world cyberattack. Clicking the link triggers simulated malware that encrypts critical files in a test environment and displays a ransom note demanding payment. Detect the attack, execute incident response actions, and recover by isolating affected systems and restoring data from backups.
Outcome	Partially able to restore data from backups.
Lessons Learned	Confusion during escalation showed a need for clearer communication protocols. It also emphasized the importance of regularly testing and updating backups.

Case Study Scenarios - Examples

	TYPE	SCENARIOS
Incident Response	Ransomware	A healthcare organization faces a ransomware attack that locks patient data. Review logs to trace the point of entry, develop an incident response strategy to minimize damage, recover the data, and strengthen defenses to prevent future incidents.
	Data Breach	An online retailer detects unauthorized access to its customer database. Analyze access logs to uncover the attacker's techniques, secure the database, and notify stakeholders about the breach while ensuring compliance with regulatory standards.
Threat Inteligence	Zero-Day Exploit	Analyze threat intelligence feeds and match them against internal vulnerabilities to evaluate the organization's risk to a zero-day exploit. The exercise involves compiling a detailed report for management to guide informed decision-making.
	Hacktivsm	Investigate threat actor activities related to a political conflict, mapping indicators of compromise (IOCs) to internal systems and developing strategic recommendations for strengthening proactive defenses.
Vulnerability Assessment	Misconfiguration	A legacy firewall permits unencrypted traffic, posing a security risk. Perform a vulnerability scan to detect misconfigurations and recommend updated rules and policies to address the issues.
Compliance Audit	Audit	Simulate a compliance audit to verify adherence to industry regulations and internal security policies. Examine system logs, configurations, and access controls to identify gaps or deviations from a selected standard such as GDPR, HIPAA, or PCI DSS. Generate an audit report, including remediation steps.

Challenges and Lessons Learned

- **Technical expertise***
  - One “thread” per semester
- **Hardware Resource constraints**
  - Hypervisor CPU, RAM, storage
  - Many of the vSOC tools resource-intensive

(make compromises) without misalignment with real-world practices

* Student academic and skills preparation (next slide)

Student Preparation and Background

Students Setting Up a vSOC

Networking

TCP/IP, DNS, firewalls

System Administration

Course in *Operating Systems*, familiarity with Linux and Windows environments

Virtualization

Familiarity with VMware or VirtualBox

Scripting and Automation

Course in *Intro to Python* (or Bash), familiarity with basic scripting

Cyber Fundamentals

Course in *InfoSec*, SOC components (e.g., SIEM, firewalls)

Students Using the vSOC

Log Analysis Basics

regex, familiarity with syslogs, Windows Event Logs, and network traffic

Threat Intelligence

Course in *InfoSec*, understanding common attack vectors and Indicators of Compromise (IOCs)

SIEM

Exposure to relevant tools

Incident Response

Course in *Incident Response and Forensics*, familiarity with basic steps for incident handling

Data Analysis

Interpreting patterns and anomalies

Future Directions

Goal #1: Scale up prototype to a full vSOC and offer monitoring service

- Campus community
- External local partners

Goal #2: Scale down prototype to *vSOC-in-a-box*

Goal #3: Build vSOC case studies, exercises, labs into existing curriculum

Goal #4: Attract Multidisciplinary Projects

- AI/ML, Visualization, UI

Goal #5: Collect metric, assess learning

Conclusion

- Bridges **theoretical - practical** knowledge
- vSOC = **cost-effective** and scalable training
- Prepares individuals and teams for **real-world** conditions
- Enhances cybersecurity workforce

Questions

Thank you for your attention!

Useful resources for anyone interested in SOC-building and Operations:

Don Murdoch, *Blue Team Handbook: SOC, Siem, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter*, Blue Team Handbook, 2019.

Kathryn Knerler, Ingrid Parker, Carson Zimmerman, *11 Strategies of a World-Class Cybersecurity Operations Center*, MITRE, 2022.

Carson Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE Corporation, 2014.

Dr. George Dimitoglou
dimitoglou@hood.edu

Dept. of Computer Science & Information Technology
Center of Computer Security and Information Assurance
Hood College
Frederick, Maryland