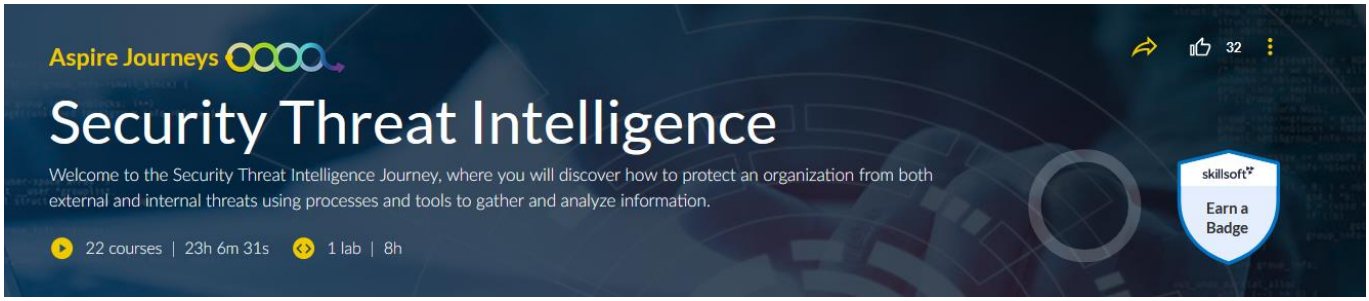
# Security Threat Intelligence

## SKILLSOFT ASPIRE JOURNEY

skillsoft




## Tracks

**Track 1: Security Threat Intelligence**

In this Skillsoft Aspire track of the Security threat Intelligence journey, the focus will be on security programming, malware removal, network survey & extractions, defensive CyberOps, network & host analysis, forensic analysis, and threat intelligence & attribution best practices.

Explore 22 courses | 23h 6m 31s | 1 lab | 8h

## PREREQUISITES

In order to fully profit from the potential of this Aspire Journey, we recommend the following prerequisite skills:

- Knowledge of network security
- Knowledge of programming



Introduction to Cyber Operations

Objectives:

- define Defensive Cyber Operations
- define Offensive Cyber Operations
- identify vulnerabilities on systems
- use offensive cybersecurity methods to test security
- compare OCO and DCO operations
- identify the purpose of the Cyber Operations Cycle
- identify the phases of the Cyber Operations Cycle
- identify the roles and responsibilities of OCO team members and how they interact within the Cyber Operations Cycle
- identify the roles and responsibilities of DCO team members and how they interact within the Cyber Operations Cycle
- identify the roles and responsibilities of supporting team members and how they interact within the Cyber Operations Cycle


Security Programming: Command Line Essentials

Objectives:

- describe the common features and properties of command line environments
- describe the command processing capabilities and environment of the Bash shell
- describe the features and capabilities of the PowerShell environment
- perform command line file editing with nano, vi, and ed
- perform basic text processing with sed, awk, and cut, and describe their differences
- repeat actions and view the command line using the bash history
- perform process control tasks including ps and kill
- schedule execution of tasks using a crontab
- use the tail and watch commands for file and command monitoring
- compare files using the diff command
- redirect the inputs and outputs of commands and files
- install, remove, and search packages using apt


Security Programming: Code Identification

Objectives:

- describe common programming paradigms and classify them based on their features
- identify bash scripts based on their features
- identify Python scripts based on their features
- identify the elements that make up a common C program
- identify the elements of a typical C++ program
- describe the similarities and differences of C# when compared to C and C++
- identify regular expressions found in typical regex engines
- identify PowerShell scripts based on their features
- identify the elements of a SQL statement
- describe common security vulnerabilities in code that can lead to exploits
- identify the structure of common executable formats based on their binary signatures
- verify the integrity of a downloaded files based on its hash value


Security Programming: Scripting Essentials

Objectives:

- describe the elements that make up a scripting language in contrast to a full-fledged computer program
- use and set variables in a Bash script
- use conditional statements in a Bash script
- use the for, while, and until loops in a Bash script
- create custom functions in a Bash script
- assign basic values to variables in a Python script
- use conditional statements in a Python script
- use the for and while loops in a Python script
- create custom functions in a Python script
- import external modules in a Python script
- read and write files in a Python script
- make web URL requests from a Python script


Security Programming: System Essentials

Objectives:

- connect to a remote server securely using ssh
- create, modify, and delete user accounts in a Linux system
- identify and describe the elements of an Internet Protocol routing table
- describe the elements of a network interface using the ifconfig command
- perform Domain Name System lookups
- describe the important log files on a Linux system that are used to monitor for critical events
- use the ps command to get process information
- query disk space use, partition information, and directory contents of a Linux system
- monitor user activity on a Linux system
- use system monitoring tools to monitor Linux activity
- configure time servers and set the correct date, time, and time zone on a system
- describe important system configurations found in the /etc folder of a UNIX-based system


Malware Removal: Identifying Malware Types & Classification Approaches

Objectives:

- identify different types of malware attacks
- describe worm viruses and Trojan viruses and how to prevent them
- describe ransomware and how to prevent it
- describe symptoms of an infected system
- recognize what tools are best to use to fight against malware
- classify the severity of malware


Malware Removal: Analyzing an Infected System

Objectives:

- recognize why malware analysis is important
- describe the purpose of static malware analysis
- identify the purpose of dynamic malware analysis
- recognize common malware characteristics at the Windows API level (registry manipulation, keylogging, HTTP communications, droppers)
- inspect the static properties of malware
- perform dynamic malware analysis
- recognize the impacts of the malware you discover
- locate open ports and running processes used by malware and terminate the malware process
- use tools to monitor malware processes
- use Wireshark to monitor malware network activity
- inspect malicious code and follow program control flow to recognize decision points during execution


Malware Removal: Remediating an Infected System

Objectives:

- describe symptoms of an infected system
- recognize best practices for removing malware
- identify different remediation approaches for various types of malware
- remove a virus from an infected system
- use System Restore to remove a virus
- use the System Restore recovery tool and restore points
- restore a system backup
- recognize when to remove vs. complete re-install
- identify the steps to use when malware makes a system unbootable
- use system repair to fix boot issues


Malware Removal: Reporting Findings & Preventing Future Infections

Objectives:

- identify key steps when responding to malware incidents
- recognize who needs to be informed of malware attacks
- recognize next steps to ensure you are better protected from future malware attacks
- identify preparation steps to plan for recovery
- create a system image to use in recovery after a malware attack


Network Survey & Extraction: Network Analysis

Objectives:

- recognize different tools used for network scanning
- identify common network vulnerabilities found during scanning
- recognize best practices for documenting physical and alternative network vulnerabilities
- prioritize network scanning activities to maximize efficiency
- perform reverse DNS lookups on IP addresses
- identify and enumerate services using a basic scan
- identify operating systems and versions using network scanning
- perform a network discovery using UDP scanning techniques
- perform a scan using stealth methods to evade detection
- perform TCP connect scans using Nmap
- perform an idle scan through a zombie host
- perform ARP scans to find hidden hosts on a network


Network Survey & Extraction: Network Monitoring

Objectives:

- recognize tips and tricks for monitoring services
- develop data management practices for network data collected from scans
- identify network vulnerability metrics
- develop strategies for network reporting and record keeping
- perform DNS host discovery
- perform requests with netcat and other tools to pull banner information from services
- filter connection information from network data using tcpdump
- filter protocol details from network data using tcpdump
- collect server and network technology and infrastructure data
- detect firewall type and version information
- scan for SSL/TLS version and cipher capabilities
- test for SMTP version information and open relay vulnerabilities


Network & Host Analysis: Protocol Analysis

Objectives:

- describe common analysis patterns for network data
- outline the Open Systems Interconnection (OSI) model for network communications
- characterize the passive and active approaches to scanning
- capture network traffic using Wireshark
- apply traffic filters using Wireshark
- customize packet capturing in Wireshark
- save and export packet captures in the PCAP format in Wireshark
- use coloring rules to examine traffic using Wireshark
- extract files transferred in the clear using Wireshark
- use configuration profiles to save preferences in Wireshark
- apply display filters to control which packets are shown in Wireshark
- combine capture and display filters to packets in Wireshark


Network & Host Analysis: Network Protocols

Objectives:

- apply DNS filters and examine DNS queries in Wireshark
- apply generic TCP filters by port and address in Wireshark
- apply generic UDP filters by port and address in Wireshark
- capture ICMP traffic using Wireshark
- capture and examine HTTP traffic using Wireshark
- inspect SSH traffic using Wireshark
- extract data from FTP traffic using Wireshark
- apply email protocol filters for POP, IMAP, and SMTP using Wireshark
- capture ARP traffic using Wireshark
- capture DHCP traffic using Wireshark
- monitor a Telnet session using Wireshark
- capture only IPv6-based traffic in Wireshark


Network & Host Analysis: Network Observations

Objectives:

- display the tree of protocol traffic captured by Wireshark
- identify network endpoints from captured network traffic using Wireshark
- describe considerations when visualizing network nodes
- create a simple network diagram using Visio
- outline effective approaches to assessing network security
- recognize the use of various baselines for network management
- work with baseline activity monitoring in Wireshark
- describe the different capture engines used in Wireshark
- create firewall rules based on Wireshark
- detect Nmap scans using Wireshark
- monitor traffic remotely using Wireshark and SSH tunneling


Network & Host Analysis: Network Analysis Formats

Objectives:

- describe the function and characteristics of the NetFlow and IPFIX network flow protocols
- describe how NetFlow is used to baseline a network
- recognize the importance of audit logs for security
- identify the goals, capabilities, and types of application-based blocking for network access
- outline techniques used to tap network traffic
- outline techniques for collecting and forwarding logs
- outline techniques for event queuing and handling
- describe how SNMP is used for network management and monitoring
- describe how PCAP is implemented for packet capture and filtering programs
- outline the process for whitelisting and blacklisting applications
- use Wireshark to detect an anomalous or potentially dangerous event
- import and export captured traffic in the PCAP format using Wireshark


Network & Host Analysis: Network Operations

Objectives:

- compare and contrast various network defense tools
- recognize the characteristics of NSM and outline how to implement it as part of a network defense strategy
- describe how SIEMs are used to detect threat activity
- install and configure Suricata to be used for network defensive operations, including NSM, IDS, and IPS
- apply a Suricata rule and illustrate the action, header, and rule options
- create an alert using a Suricata rule
- configure Suricata output in JSON using the EVE output facility
- install prerequisites for ELK Stack and Suricata from the command line
- install ELK stack in preparation for it to serve as a SIEM for Suricata
- integrate Suricata logs with ELK Stack using Filebeat and Logstash
- navigate ELK Stack's Kibana dashboards for SIEM use when connected to Suricata
- output a PCAP log from Suricata to be read by Wireshark


Forensic Analysis: Cybercrime Investigations

Objectives:

- define packet capturing and outline how it relates to CyberOps forensics
- define network forensics and describe some types of vulnerabilities
- demonstrate the use of packet capturing to gain intelligence from an attack
- illustrate how to reconstruct artifacts and files from a PCAP file using Wireshark
- define volatile data and identify the possible data contained within
- compare available tools used to analyze a computer's memory
- demonstrate how to use the volatility framework to process extraction of computer memory
- describe the Windows Registry and recognize the valuable information stored within
- navigate the Windows Registry and use it to locate changes made a to system
- differentiate between Windows Registry tools and the techniques used for analyzing changes to the registry
- differentiate between categories of digital evidence, including computer, mobile, network, and database
- outline how to gather digital evidence, including identification, collection, acquisition, and preservation
- identify tools available for computer forensic analysis and their features
- describe the features of the SIFT computer forensics tool
- illustrate how to mount evidence using SIFT


CyberOps Windows Hardening: Windows Server Hardening Best Practices

Objectives:

- outline key concepts related to Windows Server hardening
- remove unneeded software from a Windows server
- disable an unneeded service on a Windows server and illustrate how to modify the security context of that service
- outline security best practices to harden Windows Server user accounts
- implement a password policy to prevent dictionary attacks on a Windows server
- implement an account lockout policy on a Windows server to stop brute force attacks
- control or limit group membership on a Windows server
- describe common techniques to secure Windows Server file systems
- add additional security by customizing the user rights of a Windows server
- outline advanced steps used to harden a Windows server
- use techniques to harden Windows DNS servers
- use techniques to harden Windows IIS web servers
- define what is meant by auditing and interrelate it to Windows Server hardening
- monitor activity using Windows Server auditing


CyberOps Windows Hardening: Windows Workstation Hardening Best Practices

Objectives:

- list common BIOS/UEFI settings used to help secure a Windows system
- demonstrate how to harden user accounts on a Windows workstation
- demonstrate how to restrict the software that can run on a Windows workstation using an AppLocker policy
- demonstrate how to uninstall unneeded Windows components and harden Windows services on a Windows workstation
- illustrate the importance of patching a Windows system
- demonstrate how to create a password policy on a Windows workstation to prevent dictionary attacks
- demonstrate how to create an account lockout policy on a Windows workstation to prevent brute force attacks
- demonstrate how to manipulate Windows user rights
- demonstrate how to implement full disk encryption with BitLocker
- demonstrate how to use BitLocker To Go to encrypt removable media
- demonstrate the configuration of Windows Defender as antimalware
- demonstrate how to configure auditing on a Windows workstation
- demonstrate the use of security templates on a Windows system


Threat Intelligence & Attribution Best Practices: Threat Intelligence Concepts

Objectives:

- recognize the purpose and benefits of threat intelligence and outline its various definitions
- list the core characteristics of threat intelligence
- name the parties who can benefit from threat intelligence
- describe when and how to use threat intelligence including before, during, and after an attack
- categorize and identify the different cyber threat actors
- list common indicators of compromise
- differentiate among intelligence, data, and information
- outline the 6 phases of the threat intelligence lifecycle
- describe what is meant by strategic threat intelligence and list some common sources of information for it
- define what is meant by tactical threat intelligence and recognize key components and benefits of it
- define what is meant by operational threat intelligence and outline some associated challenges and solutions
- define what is meant by technical threat intelligence and describe its purpose
- describe how machine learning can improve threat intelligence
- define what is involved in risk analysis and risk modeling as they relate to threat intelligence and outline the FAIR risk model and framework
- list the various use cases for threat intelligence
- describe how threat intelligence can help map the threat landscape
- recognize why intrusion detection is the heart of threat intelligence and outline the kill chain and diamond models of analysis
- differentiate between different threat intelligent sources, such as credentials, mobile apps, social media


Threat Intelligence & Attribution Best Practices: Attribution Analysis

Objectives:

- summarize what is meant by attribution analysis and describe how it can relate to threat intelligence
- differentiation between attribution types such as machine, human, and adversary
- describe the different levels of attribution, including cyberweapon, country or city, and person or organization
- list techniques and tools used by cybercrime investigators for performing cyber attribution
- list common challenges related to cyber attribution
- list key indicators that enable attribution
- outline best practices for determining attribution
- outline best practices for presenting attribution analysis
- describe how attribution judgments are made
- recognize the importance of identifying and preserving forensic artifacts and list common errors when dealing with digital evidence
- outline how to manage digital evidence properly
- describe how attribution analysis can affect geopolitical dynamics
- identify national-level partners in the Intelligence Community that can assist with attribution
- summarize what is meant by malware cyber threats and interpret how reverse engineering malware can lead to attribution
- recognize different code sharing analysis techniques that lead to attribution
- describe network behavior analysis techniques that lead to attribution
- recognize legal implications related to cyber threats and attribution
- define indirect attribution and interrelate it to machine learning, social networks, and political ideologies

Final Exam: Security Threat Intelligence

Objectives:

- apply DNS filters and examine DNS queries in Wireshark
- capture and examine HTTP traffic using Wireshark
- change file and folder permissions from a Bash script
- compare and use conditionals in C and C++
- connect to a remote server securely using ssh
- create custom functions in a Python script
- create loops in PowerShell
- create, modify, and delete user accounts in a Linux system
- define what is involved in risk analysis and risk modeling as they relate to threat intelligence and outline the FAIR risk model and framework
- demonstrate how to create a password policy on a Windows workstation to prevent dictionary attacks
- demonstrate how to implement an account lockout policy to stop brute force attacks
- demonstrate how to implement full disk encryption with BitLocker
- demonstrate techniques to harden Windows DNS Servers
- demonstrate the use of packet capturing to gain intelligence from an attack
- describe and compare the different types of DCO missions
- describe common security vulnerabilities in code that can lead to exploits
- describe how machine learning can improve threat intelligence
- describe how SIEMs are used to detect threat activity
- describe how to gather digital evidence, including identification, collection, acquisition, and preservation
- describe malware cyber threats and how reverse engineering malware can lead to attribution
- describe symptoms of an infected system
- describe the command processing capabilities and environment of the Bash shell
- describe the common features and properties of command line environments
- describe the function and characteristics of the NetFlow and IPFIX network flow protocols
- describe the Open Systems Interconnection (OSI) model for network communications
- describe the operations of DCO in terms of missions, actions, and forces
- describe when and how to use threat intelligence, including before, during, and after an attack
- differentiation between attribution types such as machine, human, adversary
- discuss common BIOS/UEFI settings that are used to help secure the system
- discuss common techniques to secure the file system
- identify bash scripts based on their features
- identify different types of malware attacks
- identify different types of PowerShell cmdlets and objects
- identify key steps when responding to malware incidents
- identify network endpoints from captured network traffic using Wireshark
- identify the phases of the Cyber Operations Cycle
- identify the roles and responsibilities of OCO team members and how they interact within the cyber operations cycle

- implement the for and while loops in a Python script
- inspect the static properties of malware
- install ELK stack in preparation for it to serve as a SIEM for Suricata
- navigate ELK Stack's Kibana dashboards for SIEM use when connected to Suricata
- outline how to gather digital evidence, including identification, collection, acquisition, and preservation
- outline the Open Systems Interconnection (OSI) model for network communications
- perform ARP scans to find hidden hosts on a network
- perform DNS host discovery
- perform requests with netcat and other tools to pull banner information from services
- provide an overview of malware cyber threats and how reverse engineering malware can lead to attribution
- recognize best practices for removing malware
- recognize common malware characteristics at the Windows API level (registry manipulation, keylogging, HTTP communications, droppers)
- recognize different tools used for network scanning
- recognize the importance of audit logs for security
- recognize the importance of identifying and preserving forensic artifacts and list common errors when dealing with digital evidence
- recognize the use of various baselines for network management
- recognize why intrusion detection is the heart of threat intelligence and outline the kill chain and diamond models of analysis
- set variables in a Bash script
- use and set variables in a Bash script
- use loops in C and C++
- use the for and while loops in a Python script
- use the for, while, and until loops in a Bash script
- use the for, while, and until loops in a Bash script


Security Threat Intelligence

Objectives:

- In this lab, you will perform security threat intelligence tasks such as scanning networks, connecting to remote hosts, scanning websites for vulnerabilities and using Wireshark to save packet captures. Then perform packet filtering, program verification, scripting and test a service for weaknesses or vulnerabilities.

## Bookshelf

Optional


BOOK

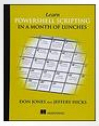
**Building an Effective Cybersecurity Program, 2n...**

3


BOOK

**Bash in Easy Steps**

3



BOOK

**Learn PowerShell Scripting in a Month of Lunches**

38


BOOK

**Rootkits and Bootkits: Reversing Modern Malware...**

5


BOOK

**Windows Virus and Malware Troubleshooting**

5


BOOK

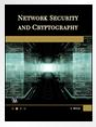
**Advanced Malware Analysis**

1


BOOK

**Malware Diffusion Models for Modern Complex...**

1




BOOK

**Network Security and Cryptography: A Self-...**

9


BOOK

**Network Security Attacks and Countermeasures**

2


BOOK

**Introduction to Network Security: Theory and Practice**

4


BOOK

**Network Hardening: An Automated Approach to...**

9


BOOK

**Network Security and its Impact on Business Strategy**

1


BOOK

**Python for Graph and Network Analysis**


BOOK

**Advanced Methods for Complex Network Analysis**


BOOK

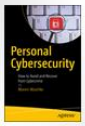
**Hiding Behind the Keyboard: Uncovering Covert...**

1


BOOK

**How to Define and Build an Effective Cyber Threat...**

8




BOOK

**Personal Cybersecurity: How to Avoid and Recover from...**

1

## FOLLOW US ON:

**www.skilltech.pl**

**email: biuro@skilltech.pl**

**tel. +48 22 44 88 827**

SkillTech

Technology hired for excellence