perched

Perched Education Courses

Tailored Training Tracks and Modules

May 2, 2019

perched

Perched Tailored Education & Training Tracks

perched

Why Perched

While having a platform and capability to perform cyber operations is critical; implementation, training, and education considerations are paramount to a successful security operations center -- this is achieved by leveraging experience, knowledge, and expertise.

Perched is the only certified Elastic subcontractor for training and education and one of two certified subcontractors for Consulting.

Ideology

Beyond the pure technical expertise of the Perched staff, they all possess the firmly held belief that cyber is a human-on-human discipline. While there are platforms, tools, and technologies that can be leveraged to enable and scale defenders; it is the person at the keyboard who will ultimately prevent, detect, and evict adversaries from networks. Perched uses this foundation to build and tailor our education, training, consulting, and implementation engagements to take our clients beyond simply watching for signature-driven alerts and finding the highly-sophisticated, motivated, and resourced adversary.

Education & Training

The Perched education staff are the course creators of all educational and training tracks; which gives them a deep foundational and functional knowledge of the curriculum. This delivers instructors that are not just teaching content on a slide that was created by someone else. They are sharing years of knowledge and experiences that they have collected by performing the jobs that they are teaching about. All Perched instructors have performed security and cyber operations (Hunt and Intelligence), defending large and small networks, against highly-sophisticated adversaries.

While delivered concurrently, Perched looks at education and training as two fundamentally different concepts. Training is teaching the tool and education is teaching how to critically think beyond what the tool delivers and how to use it to quickly ask your data contextually relevant questions when pre-generated alerts aren’t enough.

We believe that training on a tool is essential to success; however, when you are squaring off against an adversary, who very much does not want to be found, you need to be able to adapt rapidly and dynamically. This requirement frequently goes outside of what the tool (whatever that tool may be) does out-of-the-box -- this is education vs. training and this is why we couple them together.

perched

Consulting & Implementation

All Perched consultants have worked in cybersecurity for the private and public sectors, at the federal and state levels, both uniformed and as civilians. This includes over 10 years of experience in vulnerability management, network security monitoring, network forensics, host forensics, node-link analysis, the application of threat models against adversary tactics (kill chain, ATT&CK, Diamond, etc.), intelligence analysis, hunt, incident response, and defensive cyber operations.

Members of the Perched consultancy and educational teams have worked on cybersecurity teams for the US intelligence community, US military (active duty and reserve), one of the largest financial institutions in the world, one of the largest genomics and biotechnology companies in the world, and an industry-leading intelligence, incident response, EDR/EPP, NSM solutions provider. Leveraging this industry knowledge, specifically defending large public and private sector clients, gives Perched unique insights into the threats facing critical infrastructure and our nation from commodity threats to highly skilled, resourced, and motivated internal and external adversaries.

Community Contributions

Members of the Perched consultancy and educational teams are the creators, and project maintainers of, the RockNSM and CAPES projects. Additionally, Perched sponsors the HELK project and contributes to the Sigma project.

RockNSM (rocknsm.io) is an open-source network security monitoring (NSM) platform that functions as the framework for the NSM solution for multiple Fortune 100 and 500 companies, incident response service providers, and multiple government agencies.

CAPES (capesstack.io) is a self-hosted incident response service hub, providing IR management, communication, documentation, VoIP, collaborative workspaces, indicator enrichment, data analysis, and data visualization.

HELK (https://github.com/Cyb3rWard0g/HELK) is an open-sourced project focused on threat hunting through endpoint data using the Elastic Stack.

Sigma (https://github.com/Neo23x0/sigma) is an open signature format that allows you to describe relevant log events in a straightforward manner. This project provides a structured form in which researchers can describe and share detection methods.

All members of the Perched team are active in the open source community by maintaining and contributing to multiple security-focused projects.

Contact Us

If you’re interested in learning more, please feel free to check out our site over at **https://www.perched.io** or send us an email at **inquiries@perched.io**.

perched

Perched Foundations

Overview

There is a common problem in technology education, in that many skills require so much prior knowledge, that it's difficult to know where to even begin teaching a skill or concept. All of these nested skills quickly pile up and can often make training overwhelming for the student. The Foundations Course solves this problem by teaching Network Security Monitoring (NSM) in a simple way that builds incrementally. The first days lay the common groundwork that will flow into the next higher concept.

Each day in Foundations is designed to be as practical and engaging as possible. Students are provided with an individual system to encourage usage of the platforms throughout the course content.

Network security is a constantly changing space and we focus on keeping our content up-to-date. While learning relevant information, the students also get practical experience with relevant tools, such as version control systems, Linux, command-line text editors, security contexts, and basic system management.

Audience

The core strength of the Foundations Course is that it is designed to accommodate a wide range of technical skills and practical experience.

Duration

5 Days | 8 hours per day

Language

English

Prerequisites

There are no prerequisites for this course.

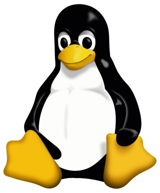
Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser

Modules

Day 1

Linux CLI



This introductory course is designed to equip a student with basic survival skills for the Linux command line. It is not intended to make them an expert, but rather familiarize them enough that Linux isn't a barrier to their success.

Syllabus

- Design Principles
- File System Layout (w/ lab)
- Using Vim (w/ lab)
- Viewing Logs (w/ lab)
- Package Management (w/ lab)
- Working With Services (w/ lab)
- SELinux Basics (w/ lab)
- Linux Administrative Skills (w/ lab)

Day 2

Introduction to Zeek

An understanding of Zeek is a foundational skill for anyone that wishes to use RockNSM. This course is designed to take an operator or analyst who has never used Zeek and bring them up to speed with its capabilities.

Syllabus

- System Setup
- What is Zeek?
- Zeek Project History
- Zeek vs. Wireshark (w/ lab)
- Analyzing a packet capture (w/ lab)
- Running Zeek from the Command Line (w/ lab)
- ASCII Logs Overview (w/ lab)
- Filtering and Sorting Data (w/ lab)
- Capture the Flag (w/ lab)

Day 3

Introduction to Kafka

This course will cover what message queuing is all about, how it is used, and why Kafka was chosen for ROCK. This is not a lab-intensive course; it is designed to provide an overview of what is happening in the background with RockNSM.

Syllabus

- What is a Messaging Queue?
- Kafka Overview
- Publishers and Subscribers
- Topics and Partitions
- Kafka and RockNSM History

Introduction to the File Scanning Framework

File Scanning Framework (FSF) is an open source project by Emerson Electric that enables recursive file scanning with a combination of YARA rules and programming logic. This course will familiarize students with the tool's capabilities and provide an overview of YARA rules.

Syllabus

- Project Overview
- What is Recursive File Scanning?
- YARA Rules (w/ lab)
- Scanning a File (w/ lab)
- Interpreting Scan Results (w/ lab)
- Using jq

Day 4

Introduction to the Elastic Stack

Elastic is an open source data company whose products are integral to RockNSM and CAPES. This course will provide an overview of the products offered and an introduction to using the three primary products, commonly known as the Elastic stack.

Syllabus

- Elastic Company Overview
- Elasticsearch (w/ lab)

- Logstash (w/ lab)
- Kibana (w/ lab)
- Beats (w/ lab)

Day 5

Introduction to CAPES

CAPES is a scalable, open source and free Security Incident Response Platform, designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. This course is designed to take an operator or analyst who has never used the CAPES technology stack and bring them up to speed with its capabilities.

Syllabus

- System Setup (w/ lab)
- What is CAPES?
- CAPES Services Introduction (w/ lab)

Introduction to Git

Whether you're organizing config files or deploying an application, modern operations happen using version control systems. Git has quickly become the new standard and learning to get work done in Git is a critical skill for students. This skill will immediately pay off in creating a documentation repository for the entire course.

Syllabus

- System Setup
- What is versioning?
- Git Overview & History
- Basic CLI usage (w/ lab)
- External Repositories (w/ lab)
- GUI Tools (w/ lab)
- Advanced Usage (w/ lab)
- Student Docs Repo Lab

perched

Perched Operator

Overview

This instructor-led course is designed for operators that serve or are interested in serving as the “human-in-the-loop” to a suite of cybersecurity tools. This course focuses primarily on the best of breed open source security tools, but the knowledge gained aims to be tool agnostic.

You will start with a discussion of operations process models, to provide a big picture roadmap of putting it all together. The remainder of the course will dig into the individual topics, each building upon the last.

This is a lab-intensive course. After a discussion of each topic, you will apply the new knowledge to a provided data sample, followed by a class discussion of what worked and what didn’t.

The course ends with a 1-day guided hunt capstone containing multiple scenarios that will engage the newly learned skills to find the adversary in the traffic. Each scenario will increase in difficulty to keep the challenge coming.

Audience

Cybersecurity operators who need to work as part of a team to analyze data to find evil lurking in their network as part of a machine-assisted, human-driven operation.

Duration

5 Days | 8 hours per day

Language

English

Prerequisites

While there are no prerequisites for this course, completion of the Perched Foundation course is highly recommended.

Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser
- An OpenSSH-compatible secure-shell client

Modules

Day 1

Introduction to Packet Analysis

This course will introduce operators to doing fine-grained packet analysis and filtering and then address strategies to analyze packets at scale using Google Stenographer.

Syllabus

- Packet analysis overview
- Berkeley Packet Filters (w/ lab)
- Stenographer (w/ lab)
- Docket (w/ lab)

Day 2

Advanced Zeek

This course builds on the Introduction to Zeek course from the Foundations track and teaches operators how to leverage Zeek for Hunting.

Syllabus

- Zeek Scripting Overview
- Zeek Event Engine
- Frameworks Overview
- Intel Framework (w/ lab)
- Files Framework (w/ lab)

Day 3

Intrusion Detection Systems

This course will cover passive network operations. Students will focus on extending the foundational knowledge gained previously in the course through theory, concepts, and practical exercises with these platforms.

SURICATA

Syllabus

- Intrusion Detection Systems Overview
- Humans over Hardware
- Anatomy of a Signature
- Signature Writing (w/ lab)
- Introduction to Suricata (w/ lab)

Day 4

Kibana for Operators

This course builds on the Kibana training from the Foundations track and teaches operators how to use Kibana to support them in their hunting.

Syllabus

- Building Dashboards to Visualize Anomalies (w/ lab)
- Security Beats and their dashboards: osquery and NetFlow (w/ lab)
- Using Graph to Find The Enemy Footprint (w/ lab)
- Using Machine Learning for Hunting (w/ lab)
- Leverage Alerting for Automation Actions (w/ lab)

Day 5

Guided Hunt

This capstone course is designed to walk an operator through a series of hunt missions designed to expand their understanding of the hunt tools and techniques.

Hunt Preparation

- Selecting the Right Tool
- When to Dig Deeper
- Incident Response operations

Individual Hunt

- **Challenge:** Find the Beacons (beginner)
- **Challenge:** Find the Beacons (advanced)
- Group Review

Team Hunt

- **Challenge:** Enemy Objectives
- **Challenge:** Applying the Kill Chain
- **Challenge:** Full-Spectrum Adversary Detection
- Group Review

Perched Engineering

Overview

This instructor-led course is focused around the deployment of the Elastic Stack in a security context; specifically how to build the different parts of the Elastic Stack and how to ensure that they are performant.

You will start with an overview of the Elastic Stack and the different components of it. From there the students will build network security monitor (NSM) sensors in a variety of configurations; each course will build on the previous content.

After completing each module, you will apply what you have learned in a series of hands-on labs. By the end of the training, you will be able to build the Elastic Stack from the ground up to analyze the data sources from your network and various systems in order to paint a more complete security picture.

Audience

Security Engineers who are responsible for installing, operating, and maintaining the Elastic Stack and network security monitoring platforms.

Duration

10 Days | 8 hours per day

Language

English

Prerequisites

There are no prerequisites for this course.

Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser

Day 1

Ansible

Building and configuring the sensors to use for NSM operations is done by completing a checklist of many tasks. The vast majority of these tasks are repeatable and can be completed with "Configuration Management". There are many CM tool sets available, but we believe that Ansible does things right. This course teaches the basics of Ansible and students will complete labs that incrementally grow in complexity.

Syllabus

- How things used to be done
- Ansible Overview
- Environment Setup
- Ad-Hoc Commands (w/ lab)
- Playbooks (w/ lab)
- Modules (w/ lab)
- Variables & Templates (w/ lab)
- Real-World Walkthrough

Day 2

Zeek Install, Operate, and Maintain

This course is designed to familiarize sensor engineers with the various ways to install and configure Zeek. It will also briefly cover ongoing maintenance that should be performed against an installation.

Syllabus

- Installation options
- Source (w/ lab)
- RPM (w/ lab)
- Deployment Options
- Standalone (w/ lab)
- Cluster (w/ lab)
- Capture Methods
- AF_PACKET (w/ lab)
- PF_RING
- Maintenance
- Zeekctl
- Zeek-cron

Day 3

Zeek Performance Tuning

This course will walk sensor engineers through how to tune Zeek for optimal performance.

Syllabus

- Monitoring Incoming Bandwidth (w/ lab)
- Identifying Performance Bottlenecks (w/ lab)
- Selecting the Right Capture Cards
- Tuning the Network Layer (w/ lab)
- Tuning the Storage Layer (w/ lab)
- CPU Pinning and NUMA Alignment (w/ lab)
- Filtering What Zeek Captures (w/ lab)

Kafka Install, Operate, and Maintain

It is important that a sensor engineer deploying RockNSM understand how to optimize relaying messages from the NIC through a data pipeline effectively in order to provide near real-time analysis and prevent data loss.

Syllabus

- Installation Overview
- Setup Prerequisites (w/ lab)
- Install Zookeeper Cluster (w/ lab)
- Install Kafka Cluster (w/ lab)
- Using kafkacat
- Creating Topics (w/ lab)

Day 4

Passive Operations and Tapping

It is important that a sensor engineer deploying RockNSM understand that it is a passive system and what that actually means. This course should clearly define the difference and explain how to utilize different tapping technologies so that students can weigh their options and make the best choice for their environment.

Syllabus

- What are Passive Operations?
- What are Active Operations?
- Spanning Port Tap (w/ lab)
- Inline Tapping (w/ lab)
- Tap placement Whiteboard Exercises

CAPES Install, Operate, and Maintain

CAPES is a self-hosted incident response service hub, providing IR management, communication, documentation, VoIP, collaborative workspaces, indicator enrichment, data analysis, and data visualization. This course is designed to take an operator or analyst who has never used the CAPES technology stack and bring them up to speed with its capabilities.

Syllabus

- What is CAPES?
- System Setup (w/ lab)
- Installation (w/ lab)
- Configuration (w/ lab)
- Administration (w/ lab)
- Maintenance (w/ lab)

Day 5, 6, 7

Elastic Stack Install, Operate, and Maintain

This course is designed to familiarize sensor engineers with the various ways to install, configure, and tune the various Elastic products.

Syllabus

- Environment Preparation (w/ lab)
- Node Types
- Components
- Elasticsearch
- Logstash
- Beats
- Kibana
- Install and Configure Elastic Stack (w/ lab)
- Configure SAML (w/ lab)
- Configure Logstash and Beats to Read Files Into Elasticsearch (w/ lab)

- Maintenance
- Viewing Log Files (w/ lab)
- Elasticsearch API (w/ lab)
- Kibana Console (w/ lab)
- Identifying Performance Bottlenecks (w/ lab)
- Monitoring Performance (w/ lab)
- System Sizing Considerations
- General Performance Tuning (w/ lab)
- Tuning the Java Virtual Machine (w/ lab)
- Tuning for Indexing Speed (w/ lab)
- Tuning or Search Speed (w/ lab)

Day 8

Suricata Rule Management and Tuning

This course is designed to provide an engineer with the foundational knowledge required to: maintain up-to-date rulesets, create custom rules, and manage the performance of a Suricata sensor.

Syllabus

- Suricata Rules Overview
- Managing Rulesets
- Anatomy of a rule
- Writing Custom Rules

Day 9

Sensor Troubleshooting

This course is designed to provide an engineer with the foundational knowledge required to: troubleshoot and correct sensor or configuration errors

Syllabus

- Troubleshooting Concepts and Flow
- Sensor Services
- Troubleshooting Logs
- Journalctl
- SELinux Troubleshooting

Day 10

Engineer Capstone Event

This capstone will have an engineer build a sensor from the ground up and will then have to troubleshoot and fix errors introduced to their working sensors.

Syllabus

- Build a Complete Sensor
- Troubleshoot & Identify Issues
- Repair and Return to Service a Sensor

Perched Analyst

Overview

This instructor-led course is designed for Intelligence Analysts and focuses on intelligence theory, threat modeling, analysis using enrichment tools, research and analysis methodologies, and leveraging Kibana to analyze data.

This course builds on itself daily, starting with intelligence theory around how intelligence analysis is applied to the cyberspace domain. From there, the course introduces the student to multiple threat models and discusses how to apply them and using open source tools to enrich data. After those frameworks are established, the student will apply those concepts to advanced research and analysis methodologies. Finally, the student will use Kibana to function as a cyber analyst.

After completing each module, the student will apply that knowledge in a series of hands-on labs. By the end of the training, the student will be able to use the Kibana to analyze the data sources from various systems in order to paint a more complete security picture.

Audience

Intelligence Analysts who are providing cyber research and analysis support for Defensive Cyber Operations (DCO), Incident Response, and Security Monitoring.

Duration

5 Days | 8 hours per day

Language

English

Prerequisites

While there are no prerequisites for this course, however, completion of the Perched Foundation course is recommended.

Requirements

- Mac, Linux, or Windows
- Virtualization platform (VMWare, VirtualBox, etc.)
- A modern web Zeekwser

Modules

Day 1

Intelligence in a Cyber World

As an intelligence professional transitions from domain to domain, the topics, terminology, and entities change. What does not change, however, are the core analytical thought processes that make an analyst an indispensable member of a kinetic warfare team are just as relevant and necessary in Cyber as in any other domain.

Syllabus

- Introduction to Cyber Intelligence – Yes, You Are Relevant
- Building an Intelligence Program
- Lexicon
- Strategic/Operational/Tactical Intelligence

Day 2

Intelligence Pipelines, Modeling, and Application

While a great deal of intelligence work is subjective in nature, our ability as professionals to represent subjective analysis in an objective way is crucial to providing relevant, repeatable, and controlled information to decision makers.

Syllabus

- The Intelligence Pipeline (incl. lab)
- Threat Modeling (incl. lab)
- Applying Threat Modeling (incl. lab)
- Working with Hunt, Incident Responders, and Security Monitoring Professionals

Intelligence Tools Sets

A great analyst makes the tool, not the other way around; but it's important to remember that of all the things that human beings can do, scaling isn't one of them. Let's take a look at the tools we can use to automate, enrich, and integrate our capabilities.

Syllabus

- Threat Intelligence Platforms (incl. lab)
- Node-Link Analysis (incl. lab)
- Indicator Enrichment (incl. lab)
- Leveraging Tools for Enrichment (incl. lab)

Day 3

Intelligence Research and Analysis

When it comes to tracking an adversary campaign, there is a lot of information that can be gathered from public sources about the enemy, their tools, and their resources. This course will familiarize analysts with how to use these public sources to enrich the data being provided by their operators.

Syllabus

- Incident Response Process - Overview
- Passive vs. Interactive Open Source Analysis (incl. lab)
- When to Analyze
- Public Information Sources (incl. lab)
- Exploit Databases (incl. lab)

Day 4 & 5

Kibana for Analysts

This course builds on the Kibana training from the Foundations track and teaches analysts how to use Kibana to support them in their analysis.

Syllabus

- Why Visualize Data?
- Setting Up Kibana (incl. lab)
- Kibana Orientation (incl. lab)
- Adding Data to Elastic from Kibana (incl. lab)
- Basic Search Parameters (incl. lab)
- Advanced Search Parameters (incl. lab)
- Basic Visualizations (incl. lab)
- Advanced Visualizations (incl. lab)
- Filters vs. Visualizations (incl. lab)
- Building Dashboards (incl. lab)
- A quick look at Canvas & Vega
- Using Elastic's Graph for Analysis (incl. lab)
- Using Elastic's Machine Learning for Analysis (incl. lab)

perched

Perched Network Operations Center

Overview

While network sensors are frequently used in a security context, their visibility of the network give insights beyond security and can be used by network operators as well.

This instructor-led course is focused around the usage of network sensors to perform network operations such as flow monitoring, service availability, performance bottlenecks, and overall network health.

Audience

Network operators responsible for the health and maintenance of network sensor platforms and the Elastic Stack.

Duration

5 Days | 8 hours per day

Language

English

Prerequisites

There are no prerequisites for this course.

Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser

Day 1, 2, 3

Elastic Stack Operate and Maintain

This course is designed to familiarize sensor maintainers with the various ways to install, configure, and tune the various Elastic products.

Syllabus

- Environment Preparation (w/ lab)
- Node Types
- Components
- Elasticsearch
- Logstash
- Beats
- Kibana
- Maintenance
- Viewing Log Files (w/ lab)
- Elasticsearch API (w/ lab)
- Kibana Console (w/ lab)
- Identifying Performance Bottlenecks (w/ lab)
- Monitoring Performance (w/ lab)

Day 4

Platform Health Monitoring

This course is designed to familiarize infrastructure maintainers with the Elastic Beats family and how to use them to monitor infrastructure.

Syllabus

- Deploy Metricbeat to collect information from systems and services
- Deploy Auditbeat to monitor user activity and processes on Linux systems using the Linux audit framework
- Deploy Winlogbeat to collect Windows Event logs
- Deploy Heartbeat to monitor network-facing applications for downtime

perched

Day 5

Kibana for Network Operations

This course familiarizes network operators on analyzing data collected from the Elastic Beats family to monitor infrastructure and detect potential issues before they become problems.

Syllabus

- Building Dashboards to Visualize Performance Anomalies (w/ lab)
- Beats and Dashboards (w/ lab)
- Using Machine Learning for Performance and Anomaly Detection (w/ lab)
- Leverage Alerting for Automation Actions (w/ lab)

Perched Hunt

Overview

This instructor-led course is designed for Operators and Analysts that serve or are interested in serving as part of a Hunt team. This course focuses primarily on the best of breed open source security tools, but the knowledge gained aims to be tool agnostic.

The student will start with a discussion of operations process models, to provide a big picture roadmap of “putting it all together”. The remainder of the course will multiple threat scenarios.

This is a lab-intensive course. After a discussion of each topic, you will apply the new knowledge to a provided data sample, followed by a class discussion of what worked and what didn’t.

Audience

Cybersecurity Operators and Analysts who need to work as part of a Hunt team.

Duration

2 Days | 8 hours per day

Language

English

Prerequisites

While there are no prerequisites for this course, completion of the Perched Foundations and Operators courses are highly recommended.

Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser
- An OpenSSH-compatible secure-shell client
- Virtualization platform (VMWare, VirtualBox, etc.) [optional]

Day 1

Hunt Preparation

- Selecting the Right Tool
- When to Dig Deeper
- Incident Response operations

Individual Hunt

- **Challenge:** Find the Beacons (beginner)
- **Challenge:** Find the Beacons (advanced)
- Group Review

Day 2

Team Hunt

- **Challenge:** Enemy Objectives
- **Challenge:** Applying the Kill Chain
- **Challenge:** Full-Spectrum Adversary Detection
- Group Review

perched

Perched CVA/H Operator Course

Overview

There is a common problem in technology education, in that many skills require so much prior knowledge, that it's difficult to know where to even begin teaching a skill or concept. All of these nested skills quickly pile up and can often make training overwhelming for the student. The CVA/H Operator Course solves this problem by teaching Network Security Monitoring (NSM) in a simple way that builds incrementally. The first days lay the common groundwork that will flow into the next higher concept.

Each day in the course is designed to be as practical and engaging as possible. Students are provided with an individual system to encourage usage of the platforms throughout the course content.

You will start with a discussion of foundational skills and process models, to provide a big picture roadmap, and the skills, to put it all together. The remainder of the course will dig into the individual topics, each building upon the last.

This is a lab-intensive course. After a discussion of each topic, you will apply the new knowledge to a provided data sample, followed by a class discussion of what worked and what didn't.

The course ends with a 2-day guided hunt capstone containing multiple scenarios that will engage the newly learned skills to find the adversary in the traffic. Each scenario will increase in difficulty to keep the challenge coming.

Throughout the entire course, the Operator will learn and hone individual tasks, but this also focuses on team-based operations to teach the Operators how to function as a CVA/H team.

Audience

CVA/H Operators who need to work as part of a team to analyze data to find evil lurking in their network as part of a machine-assisted and human-driven operation.

Duration

10 Days | 8 hours per day

Air Force Specialty Code (AFSC) Recommendations

For Air Force Operators, the recommended AFSCs are 17S, 1B471, 3D172, or 3D072.

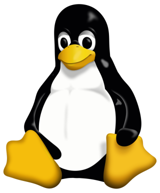
Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser
- An OpenSSH-compatible secure-shell client

Modules

Day 1

CVA/H Linux Foundations



This introductory course is designed to give a foundational level of knowledge with hands-on skills required to operate the CVA/H platform. This lab-intensive module covers a strong baseline in the Linux Operating System allowing an operator to perform necessary administrative and engineering tasks on the CVA/H.

Syllabus

- Design Principles
- File System Layout (w/ lab)
- Using Vim (w/ lab)
- Viewing Logs (w/ lab)
- Package Management (w/ lab)
- Working With Services (w/ lab)
- SELinux Basics (w/ lab)
- Linux Administrative Skills (w/ lab)

Day 2

CVA/H Networking Foundations

This course expands upon the OSI model to give a full analysis of protocols and encapsulation. This is complemented by advanced analysis and hunting techniques with CVA/H.

Syllabus

- Protocol Analysis (w/ lab)
- Encapsulation (w/ lab)
- Routing protocols and network flow (w/ lab)
- Advanced analysis with tcpdump and Wireshark (w/ lab)

Day 3

Intrusion Detection Systems and CVA/H

This course will introduce operators to the leading IDS, Suricata, and cover when and how to employ the IDS technology to support hunt operations using the CVA/H platform

Syllabus

- Intrusion Detection Systems Overview
- Humans over Hardware
- Anatomy of a Signature
- Signature Writing (w/ lab)
- Suricata vs. Snort
- IDS and Kibana dashboards (w/ lab)

Day 4

The Zeek (Bro) Protocol Analyzer

An understanding of Zeek is a foundational skill for anyone that wishes to use the CVA/H platform. This course is designed to take an operator or analyst who has never used Zeek and bring them up to speed with its capabilities.

Syllabus

- System Setup
- What is Zeek?
- Zeek Project History
- Zeek vs. Wireshark (w/ lab)
- Analyzing a packet capture (w/ lab)
- Running Zeek from the Command Line (w/ lab)
- ASCII Logs Overview (w/ lab)
- Filtering and Sorting Data (w/ lab)
- Capture the Flag (w/ lab)

Day 5

Elastic for CVA/H

Elastic is a data company whose products are integral to CVA/H. This course will provide an overview of the products offered and an introduction to using the three primary products, commonly known as the Elastic Stack.

Syllabus

- Elastic Company Overview
- Elasticsearch (w/ lab)
- Logstash (w/ lab)
- Kibana (w/ lab)
- Beats (w/ lab)

Day 6

Kibana for Operators

This course builds on the Kibana training and teaches operators how to use Kibana to support them in their hunting with the CVA/H platform.

Syllabus

- Building Dashboards to Visualize Anomalies (w/ lab)
- Security Beats and their dashboards: osquery and NetFlow (w/ lab)
- Using Graph to Find The Enemy Footprint (w/ lab)
- Using Machine Learning for Hunting (w/ lab)
- Leverage Alerting for Automation Actions (w/ lab)

Day 7

CVA/H Architecture

This course covers the engineering overview for the CVA/H along with the necessary administrative skills required for managing the build.

Syllabus

- Architecture Review
- Confluence Documentation (w/ lab)
- Docker and Kubernetes (w/ lab)

Day 7 (cont.)

Collection and Analysis with Moloch

This course teaches operators how to perform network collection at scale with the Moloch capture service and session analysis with Moloch viewer.

Syllabus

- Network collection with Moloch Capture (w/ lab)
- Session Analysis with Moloch Viewer (w/ lab)

Day 8

Endpoint Detection and Response

This course will introduce operators to Endpoint Detection and Response (EDR) with CVA/H. The course material covers baselining, capturing volatile artifacts, and basic endpoint hunt operations with a test environment for hands-on experience.

Syllabus

- Endpoint Detection and Response Overview
- “Agentless” Monitoring with PowerShell (w/ lab)
- Winlogbeat and Filebeat (w/ lab)
- GRR Rapid Response (w/ lab)

Day 9 & Day 10

Assisted Hunt

This capstone course is designed to walk a CVA/H Operator through a series of hunt missions designed to expand their understanding of the hunt tools and techniques.

Hunt Preparation

- Selecting the Right Tool
- When to Dig Deeper
- Incident Response operations

Day 9 & Day 10 (cont.)

Individual Hunt

- **Challenge:** Find the Beacons (beginner)
- **Challenge:** Find the Beacons (advanced)
- Group Review

Team Hunt

- **Challenge:** Enemy Objectives
- **Challenge:** Applying the Kill Chain
- **Challenge:** Full-Spectrum Adversary Detection
- Group Review

perched

Security Monitoring with SOC Prime

Overview

This instructor-led course is designed for Analysts and Operators that currently use, or are interested in using, the Elastic Stack with SOC Prime for security event collection, analytics, and case management.

You will start with an overview of SOC Prime and the Elastic Stack, exploring the various components and some of the use cases they can serve. The remainder of this course will take an in-depth look at Kibana, including basic discovery, visualizations and dashboards, and advanced components like Canvas, Vega, and Machine Learning.

After completing each module, you will apply what you have learned in a series of hands-on labs. By the end of the training, you will be able to use SOC Prime and the Elastic Stack to analyze the data sources from your network and various systems in order to paint a more complete security picture.

Audience

Security analysts who are researching, building, or leveraging SOC Prime as a part of their security monitoring program

Duration

3 Days | 8 hours per day

Language

English

Prerequisites

While no prior knowledge is required, completion of the Perched Foundations and the Perched Operator or Analyst courses are recommended.

Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser

Modules

Day 1

Introduction to Elastic

- Learn about the products that make up the Elastic Stack and how they integrate.
- **Hands-On Lab:** Starting an Elastic Cluster

Kibana Basics

- Kibana is the visualization component of the Elastic Stack. This chapter will provide a high-level overview of the UI and prepare students for a deep-dive on each component that is relevant to a successful hunt.
- **Hands-On Lab:** Getting started with Kibana

Introduction to SOC Prime

- Learn about the components of SOC Prime and discuss how it can be used as a Security Incident and Event Management (SIEM) and case management system.
- **Hands-On Lab:** Navigating through SOC Prime

Day 2

Building Visualizations

- Visualizations are a powerful way to summarize a large set of data and spot anomalies. Learn all about how to leverage visualizations to tell a story about your data
- **Hands-On Lab:** Summarizing data with visualizations

Dashboards and Use Cases

- Learn how to build basic dashboards and then more advanced content focused on protocols or specific use-cases.
- **Hands-On Lab:** Build basic and advanced dashboards and use-cases

Canvas and Vega

- Learn all about the advanced tools available in Kibana for building visualizations.
- **Hands-On Lab:** Building visualizations with Canvas and Vega

Machine Learning and Alerting

- Humans are great at spotting visual anomalies, but computers are king when it comes to keeping track of trends and deviations. Learn how to build ML jobs and alerts to find things the human eye might miss.
- **Hands-On Lab:** Building ML jobs and creating alerts

Case Management

- Anomalies without proper case management can lead to poor communication and overlap. Learn how to leverage SOC Prime for case management.
- **Hands-On Lab:** Case management with SOC Prime

Day 3

Guided Hunt

- Spend a full day applying the concepts that you have learned in class. This is designed to be very hands-on and flexible to the needs and desires of the students.
- The typical flow is to spend 30 minutes looking for anomalies in the data, working within the SIEM, and case management modules. Throughout the day, the class will regroup and review what everyone has found and logged in their case manager.
- Instructors will work with the pace of the students and guide them through an entire campaign; this ensures the proper amount of challenge, but no one is left behind.

Perched Threat Hunting With Corelight

Overview

This instructor-led course is designed for Analysts and Operators that currently use, or are interested in using, Corelight with the Elastic Stack for Network Security Monitoring.

After completing each module, you will apply what you have learned in a series of hands-on labs. The coursework is culminated by a 2-day capstone event in which the students will perform a series of increasingly difficult hunting operations using the Corelight data. This capstone is instructor assisted to ensure that no students are left behind.

By the end of the training, you will be able to use Corelight Zeek data and the Elastic Stack to analyze your network traffic and catch bad guys.

Audience

Security analysts who are researching, building or leveraging Corelight as a part of their security monitoring program

Duration

5 Days | 8 hours per day

Language

English

Prerequisites

While no prior knowledge is required, completion of the Perched Foundations and the Perched Operator or Analyst courses are recommended.

Requirements

- Mac, Linux, or Windows
- A modern web Zeekwser

Modules

Day 1

Passive Operations and Tapping

This course will clearly define the difference between active and passive operations and explain how to utilize different tapping technologies so that students can weigh their options and make the best choice for their environment.

Syllabus

- What are Passive Operations?
- What are Active Operations?
- Spanning Port Tap (w/ lab)
- Network Tapping Methodologies (w/ lab)
- Tap placement Whiteboard Exercises

Introduction to Zeek

This course is designed to take an operator or analyst who has never used Zeek and bring them up to speed with its capabilities.

Syllabus

- System Setup
- What is Zeek?
- Zeek Project History
- Zeek vs. Wireshark (w/ lab)
- Analyzing a packet capture (w/ lab)
- ASCII Logs Overview (w/ lab)
- Filtering and Sorting Data (w/ lab)
- **Hands-On Lab:** Capture the Flag

Day 2

Zeek Performance Tuning

This course will walk sensor engineers through how to tune Zeek for optimal performance.

Syllabus

- Monitoring Incoming Bandwidth (w/ lab)
- Identifying Performance Bottlenecks (w/ lab)
- Filtering What Zeek Captures (w/ lab)

Advanced Zeek

This course builds on the Introduction to Zeek course from the Foundations track and teaches operators how to leverage Zeek for Hunting.

Syllabus

- Zeek Scripting Overview (w/ lab)
- Zeek Event Engine (w/ lab)
- Frameworks Overview
- Intel Framework (w/ lab)
- File Extraction (w/ lab)

Day 3

Introduction to Elastic

- Learn about the products that make up the Elastic Stack and how they interoperate.
- **Hands-On Lab:** Starting an Elastic Cluster

Data Ingestion

- Learn how to move data from Zeek to Elastic in an efficient and scalable manner.
    - Logstash (w/ lab)
    - Beats
    - Data Enrichment (w/ lab)

Kibana Basics

- Kibana is the visualization component of the Elastic Stack. This chapter will provide a high-level overview of the UI and prepare students for a deep-dive on each component that is relevant to a successful hunt.
- **Hands-On Lab:** Getting started with Kibana

Building Visualizations

- Visualizations are a powerful way to summarize a large set of data and spot anomalies. Learn all about how to leverage visualizations to tell a story about your data
- **Hands-On Lab:** Summarizing data with visualizations

Dashboards and Use Cases

- Learn how to build basic dashboards and then more advanced content focused on protocols or specific use-cases.

- **Hands-On Lab:** Build basic and advanced dashboards and use-cases

Day 4 & 5

Assisted Hunt

This capstone course is designed to walk an operator through a series of hunt missions designed to expand their understanding of the hunt tools and techniques.

Hunt Preparation

- Selecting the Right Tool
- When to Dig Deeper
- Incident Response operations

Individual Hunt

- **Challenge:** Find the Beacons (beginner)
- **Challenge:** Find the Beacons (advanced)
- Group Review

Team Hunt

- **Challenge:** Enemy Objectives
- **Challenge:** Applying the Kill Chain
- **Challenge:** Full-Spectrum Adversary Detection
- Group Review

Static Malware Analysis with OMEGA316

Overview

This customized, interactive two-day course is designed to help attendees learn and apply the fundamental principles of malware analysis.

Through the effective use of the Socratic method of teaching, the instructor provides students with an applied understanding of how to analyze malicious files. This applied technique is crucial for detecting and defending the network against today's evolving and sophisticated malware.

Additionally, the course will equip attendees with Techniques, Tactics, and Procedures (TTPs) necessary to identify and extract indicators from suspicious files.

Students will be inspired with practical hands-on labs with simulated and real-world malware. Additionally, they will be introduced to the unique concept of power sessions, a key learning accelerator to gain applied knowledge.

Audience

Those interested in introductory malware analysis techniques.

Duration

2 Days | 8 hours per day

Language

English

Prerequisites

While there are no prerequisites for this course.

Requirements

- Mac, Linux, or Windows
- Virtualization platform (VMWare, VirtualBox, etc.)

Modules

Day 1

Applied Kill Chain Analysis

This section of the course deals with providing practical hands-on skills for understanding the techniques used by threat actors to create malicious payloads. Students are first presented with some fundamental concepts that illustrate the attacker's mindset through the Kill Chain framework. They are then introduced to Kali Linux, one of the most popular penetration testing toolkits with practical exploit tools.

Syllabus

- Baseline skills assessment
- Introduction to Kali Linux
- Overview of lab topology
- **Hands-on Lab:** Compromising systems using malicious payloads
- **Hands-on Lab:** Payload injections
- **Hands-on Lab:** Power session

Day 2

Static Malware Analysis

The central focus of this section is analyzing different types of malicious payloads. Students will learn the process of analyzing malicious Portable Executable (PE) files. They will also employ the use of static analysis techniques against document files such as Microsoft Office documents and Adobe PDFs.

Syllabus

- Principles of malware analysis
- Types of malware
- Evasion techniques
- Document analysis
- Static analysis of PE files
- **Hands-on Lab:** Static malware analysis

perched

Dynamic Malware Analysis

Attendees will examine the debugging of malware and the process of interactive dynamic analysis including techniques for unpacking packed malware.

Syllabus

- Debugging malware for analysis
- Analyzing packed malware
- **Hands-on Lab:** Dynamic analysis
- **Hands-on Lab:** Power session