Event Brief

Corelight's Capture the Flag Exercise

Building Skills for Success

Overview

Bring your team for an immersive lab-based, instructor-led defensive Capture the Flag exercise with Corelight. Participants will dive into one or more real-world scenarios to detect and respond to threats using logs from Corelight's Open NDR.

Agenda

- Introduction to Zeek: Brief overview of Zeek and its role in network security. Understanding how to leverage Zeek data for threat detection.
- Hands-on Hunting: Participants will actively engage in a variety of hunting exercises across different protocols. Use your wits to identify and respond to potential threats discovered in Zeek data. Questions are encouraged, but participants have full control at the keyboard.
- Competition and Scoreboard: Participants compete against each other in a friendly competition. Scores will be tracked on a real-time scoreboard.
- Debriefing: Discussion on the attacks witnessed during the exercise. Brief overview of how Corelight can enhance threat detection and response capabilities.
- Corelight Integration: Learn how Corelight can be integrated into your network defense strategy. Understand the added value Corelight brings to Zeek-powered threat detection.

Requirements

Each participant will need their own laptop, a standard web browser, and a connection to the Internet.

Continuing Professional Education (CPE)

Participants may request a certificate documenting their participation in the Capture the Flag exercise for CPE credits, to help maintain Information Security certifications.

Conclusion

Whether this exercise is administered by your Sales Engineer or as part of a formal Corelight training, participants will build their understanding of the power of Corelight. At the end of the event, participants will not only have honed their threat detection skills but will also have gained insights into leveraging Corelight for effective network defense.

Exercises Available

Corelight has the following exercises available to choose from, to customize your Capture the Flag experience.

Name	Duration	Difficulty	Platforms Available
PCAP 1	⏱ 50-60 Minutes	●○○	Elastic, Falcon LogScale, Splunk
✎ Investigating an Emotet banking trojan infection back to the source of infection.			
PCAP 2	⏱ 25-30 Minutes	●○○	Elastic, Falcon LogScale, Splunk
✎ Investigating a TrickBot trojan infection.			
PCAP 4	⏱ 50-60 Minutes	●●●	Splunk
✎ An exploration of SSH inferences from the Corelight Encrypted Traffic Collection and how they can be used to investigate adversary behaviors in SSH tunnels.			
PCAP 5	⏱ 25-30 Minutes	●●○	Falcon LogScale, Splunk
✎ An investigation of a Suricata IDS alert to determine root cause and the malware family associated with the behavior.			
PCAP 8	⏱ 25-30 Minutes	●●○	Falcon LogScale, Splunk
✎ An investigation of a ransomware infection on a workstation.			
PCAP 9	⏱ 25-30 Minutes	●●○	Splunk
✎ A client is sending an abnormally large amount of DNS traffic. Is it a misconfiguration, or a malicious behavior?			
PCAP 10	⏱ 50-60 Minutes	●●●	Splunk
✎ An adversary gained access to an IP address that was allowed access to an SSH server hosted in AWS, and subsequently compromised the AWS infrastructure.			
PCAP 11*	⏱ 50-60 Minutes	●●●	Splunk
✎ (*Continues from PCAP 10) An adversary was able to exploit a finance workstation, impersonate a domain controller and successfully execute a DC sync attack to obtain user credentials from Active Directory.			
PCAP 12*	⏱ 30-45 Minutes	●●●	Splunk
✎ (*Continues from PCAP 11) Additional investigation of the SSH tunnels used by the adversary to move laterally within the environment.			

Exercises Available (cont.)

Name	Duration	Difficulty	Platforms Available
CoreStrike 1	⏱ 25-30 Minutes	●○○	Falcon LogScale
CoreStrike 2*	⏱ 25-30 Minutes	●○○	Falcon LogScale
CoreStrike 3*	⏱ 25-30 Minutes	●○○	Falcon LogScale
CoreStrike 4*	⏱ 50-60 Minutes	●●●	Falcon LogScale
CoreStrike 5*	⏱ 50-60 Minutes	●●●	Falcon LogScale
CoreStrike 6*	⏱ 50-60 Minutes	●●●	Falcon LogScale

✎ Each of CoreStrike 1 through 6 is a deep-dive using Corelight and CrowdStrike Falcon evidence together to investigate an adversary campaign. The adversary uses commonly available tools, such as Bore, Empire, Impacket, NMAP, and the PowerSploit framework, and their behaviors run the length of the ATT&CK chain, from initial access through exfiltration and everything in between. (*Continues from previous CoreStrike exercise)

Shadows ⏱ 100-120 Minutes ●●● Corelight Investigator

✎ Corelight sensors have flagged potential data exfiltration to AWS S3 from the Public VPC, possibly linked to a known malicious IP.

Echoes ⏱ 50-65 Minutes ●●○ Splunk

✎ You have detected a potential attack coming from an external IP which exploited a vulnerability in a Fortinet FortiNAC. The attacker appears to have gained a foothold and is moving through the network, possibly preparing for a ransomware deployment.

NKorea ⏱ 50-65 Minutes ●●○ Splunk

✎ An urgent alert shows that a critical network has been breached. Initial evidence suggests the involvement of a notorious and sophisticated North Korean APT group known for their cyber tactics.

CustomCrypto ⏱ 30-40 Minutes ●●● Splunk

✎ Suspicious network traffic shows signs of being a command-and-control channel using custom cryptography to evade detection.

PCR ⏱ 15-20 Minutes ●●● Splunk

✎ Hunting through Producer/Consumer Ratio (PCR) data, you notice suspicious patterns of behavior that could be command-and-control or exfiltration of data.

Exercises Available (cont.)

DoubleDip ⏱ 10-15 Minutes ●○○ Splunk

✎ A file with a suspicious double extension has been downloaded on an employee's workstation. As a cybersecurity investigator, your mission is to delve into this anomaly, analyze the file, and determine if it's a potential threat.

Cannon ⏱ 15-20 Minutes ●●○ Splunk

✎ A critical server that stores your organization's most sensitive and valuable data—the crown jewels—is showing signs of compromise.

WhisperNet ⏱ 40-50 Minutes ●●○ Splunk

✎ Unusual activity has been detected within your organization's Industrial Control Systems (ICS) that manage critical infrastructure operations.