MITRE ATT&CK® Coverage

Corelight puts a spotlight on ATT&CK

ATT&CK is a repository of tactics, techniques, and procedures (TTPs) curated by the MITRE Corporation that helps organizations classify and interpret the full range of techniques that adversaries use, even as they constantly evolve. It's a common language that defenders can rally around, and an increasingly important starting point for planning defensive strategies.

Corelight Sensors uncover network evidence that can help you identify and root out a wide variety of TTPs. Although no single tool can address all of the ATT&CK framework, Corelight counters tactics that other security measures can't, excelling when all the tools built to keep out adversaries have failed.

Coverage where it counts

Command & Control (C2)

Adversaries only need one successful attempt out of thousands to access your network, which makes fending them off seem almost impossible. But once they're inside, they must traverse your network over and over again to communicate with the systems they've compromised. Corelight gives you a master record of network activity so you can flip the script: catch a single stray transmission, and unravel an entire attack.

Exfiltration

Exfiltration turns a compromised network into a breached network. There are massive consequences for failing to catch it, but with the right tools, you can stop it. Corelight identifies exfiltration in highly entropic networks by capturing the movement of all files even if they're hidden in other protocols. With Corelight logs, you can see changes in traffic patterns and evidence of unusual activity that suggest staging is taking place or that exfiltration has occurred.

Lateral Movement

When you only search for intruders at the gates, you will completely miss the ones who've already snuck in, not to mention the insiders trying to do harm. Likewise, north-south security is important but it leaves organizations in the dark about the movements of bad actors inside their networks where the majority of their traffic flows. Corelight delivers deep insight into east-west traffic, illuminating the pathways where bad actors move so you can spot them more readily.

MITRE ATT&CK® Coverage

Techniques Corelight reveals:

Initial Access	Execution	Persistence	Defensive Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control (C2)	Exfiltration
Spearphishing Attachment	Compiled HTML file	External Remote Services	Port Knocking	Account Manipulation	Account Discovery	Distributed Component Object Model	Automated Collection	Commonly Used Port	Automated Exfiltration
Spearphishing Link	Execution Through API	Port Knocking		Brute Force	Network Service Scanning	Exploitation of Remote Services	Data from Network Shared Drive	Connection Proxy	Data Compressed
Valid Accounts	PowerShell	Redundant Access		Credentials in Files	Network Share Discovery	Pass the Hash	Data Staged	Custom Command & Control Protocol	Data Encrypted
	Windows Management Instrumentation			Forced Authentication	Remote System Discovery	Pass the Ticket		Custom Cryptographic Protocol	Data Transfer Size Limits
	Windows Remote Management			Kerberoasting		Remote Desktop Protocol		Data Encoding	Exfiltration Over Alternative Protocol
				LLMNR/NBT-NS Poisoning and Relay		Remote File Copy		Data Obfuscation	Exfiltration Over Command and Control Channel
				Private Keys		Shared Webroot		Fallback Channels	Exfiltration Over Other Network Medium
						Third-party Software		Multi-hop Proxy	Scheduled Transfer
						Windows Admin Shares		Multi-Stage Channels	
								Multiband Communication	
								Multilayer Encryption	
								Port Knocking	
								Remote Access Tools	
								Remote File Copy	
								Standard Application Layer Protocol	
								Standard Cryptographic Protocol	
								Standard Non-Application Layer Protocol	
								Uncommonly Used Port	
								Web Service	

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497