corelight

MITRE | ATT&CK®

Corelight puts a spotlight on MITRE ATT&CK®

CORELIGHT'S MITRE ATT&CK APPROACH

Corelight drives broad coverage across the MITRE ATT&CK TTPs using an approach focused on visibility and explainable, evidence-based analytics. The foundation of this approach is Zeek® network telemetry, data that captures activity across a broad set of network protocols and fuels advanced analytics. With these analytics, Corelight provides machine learning models, behavioral alerts, and Suricata-based IDS and SIEM rules to detect the relevant ATT&CK tactics, techniques, and procedures. Corelight's Open NDR Platform allows you to build your own detection content or use community contributions such as MITRE's BZAR package.

COMPREHENSIVE APPROACH

- Broad coverage of network-based techniques
- Detection of over 75 TTPs
- Highly effective against Discovery and C2

CORELIGHT'S STRENGTH OF COVERAGE INCLUDES:

INITIAL ACCESS

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Phishing
- Valid Accounts

DEFENSE EVASION

- Exploitation for Defense Evasion
- Hijack Execution Flow
- Indicator Removal on Host
- Masquerading
- Modify Authentication Process
- Modify Registry
- Process Injection
- Rogue Domain Controller
- Subvert Trust Controls
- Valid Accounts

CREDENTIAL ACCESS

- Brute Force
- Credentials from Password Stores
- Forced Authentication
- Man-in-the-Middle
- Modify Authentication Processes
- OS Credential Dumping
- Steal or Forge Kerberos Tickets

DISCOVERY

- Account Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Permission Groups Discovery
- Remote System Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Time Discovery

LATERAL MOVEMENT

- Exploitation of Remote Services
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services

C2

- Application Layer Protocol
- Data Encoding
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Web Service

ADDITIONAL AREAS OF COVERAGE:

RECONNAISSANCE	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	COLLECTION	EXFILTRATION	IMPACT
Active Scanning	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Archive Collected Data	Automated Exfiltration	Endpoint Denial of Service
Gather Victim Network Information	Inter-Process Communication	Create or Modify System Process	Create or Modify System Process	Data from Local System	Data Transfer Size Limits	Resource Hijacking
Search Open Technical Databases	Scheduled Task/Job	Event Triggered Execution	Event Triggered Execution	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
Search Open Websites/ Domains	System Services	External Remote Services	External Remote Services	Data Staged	Exfiltration Over C2 Channel	
	User Execution	Hijack Execution Flow	Hijack Execution Flow	Man-in-the-Middle	Exfiltration Over Web Service	
	Windows Management Instrumentation	Modify Authentication Process	Process Injection		Transfer Data to Cloud Account	
		Office Application Startup	Scheduled Task/Job			
		Scheduled Task/Job	Valid Accounts			
		Valid Accounts				

To learn more about how Corelight fits into the MITRE ATT&CK framework, request a demo at **corelight.com/contact** and visit **mitre-attack.corelight.com**

corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497