THE CHALLENGE

While endpoint detection and response (EDR) data underpins multiple functions in the SOC, the large data volumes often put a strain on organizations' SIEM platforms.

THE SOLUTION

Cribl Stream enables teams to route full-fidelity EDR data to low-cost object storage for long-term retention and investigation needs, optimizing the data for SIEM consumption and streamlining workflows across the SOC.

THE BENEFITS

- Increase alignment with popular CSFs such as MITRE ATT&CK
- Route to multiple destinations, including object storage for long-term retention
- Format, filter, reduce, and enrich EDR data as needed for any tooling schema
- Optimize EDR data to reduce infrastructure budget and improving the analytic tool performance
- Provide deeper visibility and response capabilities at the endpoint

SOLUTION BRIEF

Better Together: Cribl Stream and Endpoint Detection and Response (EDR)

Leveraging Cribl Stream with EDR data forms the foundation for a defense-in-depth strategy while aligning to popular cybersecurity frameworks (CSFs) like MITRE ATT&CK.

The Challenge

EDR solutions provide deep visibility and response capabilities at the endpoint and are now more relevant than ever considering the move from corporate networks to a remote workforce. This increased visibility results in a large increase in data volumes and processing requirements for enterprise SIEM platforms. EDR vendors will typically provide access to the data via a cloud storage bucket which is then ingested by the SIEM platform for processing and analysis.

This EDR data generally consists of the following types of events:

- Behavioral Alerts
- Information about processes (create, listen, termination, modification)
- Commands and scripts run
- Registry modifications
- Domain Name Service (DNS) activity
- Netflow
- File activity (create, modify, delete)
- Scheduled task or start-up modifications
- HTTP activity

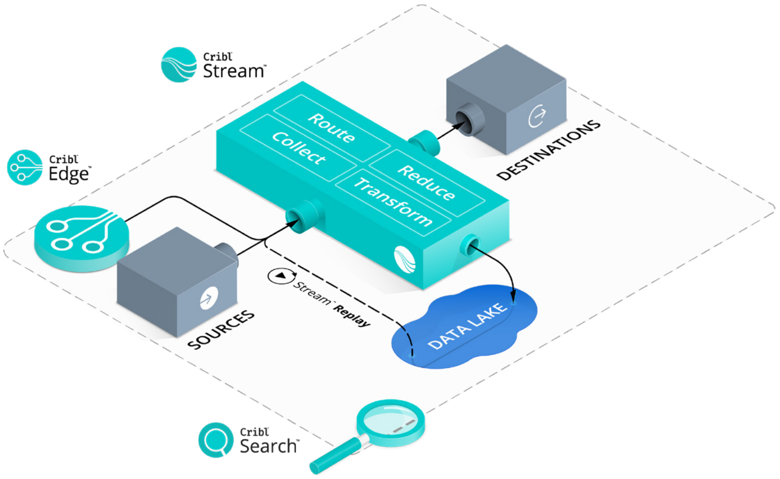
Achieve Best-in-Class SIEM Optimization and Data Reduction

While these security-relevant event types are among the most important sources to the security and compliance organizations, the verbosity of the events is usually too taxing for most analytics platforms such as a SIEM. A solution for satisfying long-term investigative and compliance requirements while also optimizing the data sent to the analytics platforms is needed.

Solution

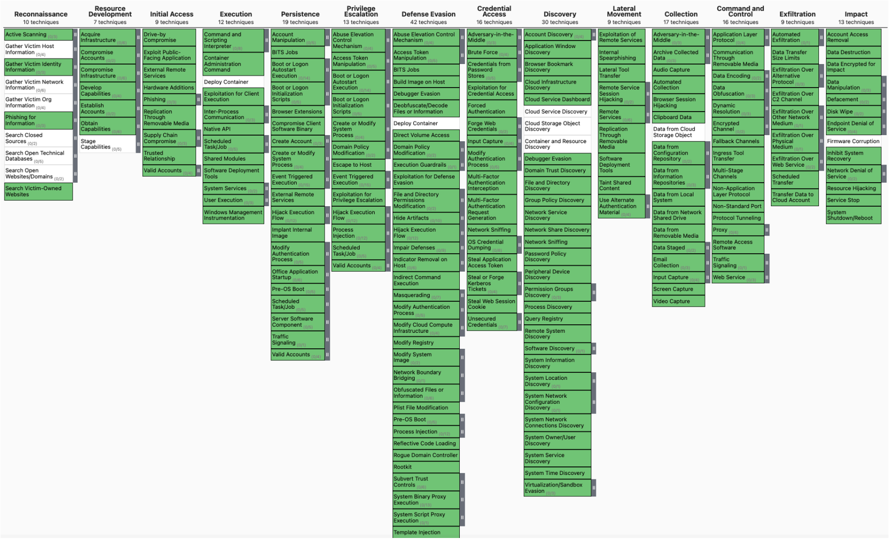
Cribl Stream complements EDR data by providing the ability to make strategic choices instead of compromises while architecting next-gen workflows.   EDR data can now be optimized and routed to multiple destinations such as a SIEM, UEBA, or low-cost object storage. By providing the ability to optimize, filter, and enrich on a per-destination basis, you can now better manage costs and improve system performance while preserving insights and remaining compliant.

Cribl Stream simplifies the process of replaying data from long-term object storage to SIEM platforms should investigative or threat hunting timelines extend beyond the SIEM retention period. With Stream, organizations can also utilize a single console to encrypt or mask sensitive data in real-time before it is forwarded to and stored at a destination, keeping PII safe.



The Benefits of Leveraging Cribl Stream to Operationalize EDR Data

As organizations adopt and align to cyber security frameworks like MITRE ATT&CK, endpoint-sourced data such as that from EDR solutions quickly becomes the most impactful data source for increasing coverage. As of August 2022, over half of the documented MITRE ATT&CK techniques can be covered by analyzing EDR event types specific to processes, commands, files, and registry modifications. These event types in addition to DNS, Netflow, and Web are too voluminous for most SIEMs from a cost and performance perspective. Cribl Stream can provide volume reductions for many of the event types by more than 90% by eliminating irrelevant content, deduplicating, or aggregating. These volume reductions make aligning to MITRE ATT&CK a reality.



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Escape to Host	Deploy Container
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Direct Volume Access
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)
			User Execution (0/3)	Hijack Execution Flow (0/12)	Process Injection (0/12)	Exploitation for Defense Evasion
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)
				Modify Authentication Process (0/5)	Valid Accounts (0/4)	Hide Artifacts (0/10)
				Office Application Startup (0/6)		Hijack Execution Flow (0/12)
				Pre-OS Boot (0/5)		Impair Defenses (0/9)
				Scheduled Task/Job (0/5)		Indicator Removal on Host (0/6)
				Server Software Component (0/5)		Indirect Command Execution
				Traffic Signaling (0/1)		Masquerading (0/7)
				Valid Accounts (0/4)		Modify Authentication Process (0/5)
						Modify Cloud Compute Infrastructure (0/4)
						Modify Registry
						Modify System Image (0/2)
						Network Boundary Bridging (0/1)
						Obfuscated Files or Information (0/6)
						Plist File Modification
						Pre-OS Boot (0/5)
						Process Injection (0/12)
						Reflective Code Loading
						Rogue Domain Controller
						Rootkit
						Subvert Trust Controls (0/6)
						System Binary Proxy Execution (0/13)
						System Script Proxy Execution (0/1)
						Template Injection

Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Modify Authentication Process (0/5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Application Access Token	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
Steal or Forge Kerberos Tickets (0/4)	Network Share Discovery		Email Collection (0/3)	Remote Access Software		
Steal Web Session Cookie	Network Sniffing		Input Capture (0/4)	Traffic Signaling (0/1)		
Unsecured Credentials (0/7)	Password Policy Discovery		Screen Capture	Web Service (0/3)		
	Peripheral Device Discovery		Video Capture			
	Permission Groups Discovery (0/3)					
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery (0/1)					
	System Information Discovery					
	System Location Discovery (0/1)					
	System Network Configuration Discovery (0/1)					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (0/3)					

The increased visibility provided by the EDR vendors results in alerts containing much more security-relevant context which reduces the time Security Analysts spent triaging or investigating alerts. From a Threat Intelligence perspective, the SOC also has a much richer collection of possible Indicators of Compromise (IOC) due to the presence of file hashes, domain names, Netflow IP Addresses, commands, registry locations, etc. These IOCs form the foundation not just for matching against known indicators but also for expanding existing threat-hunting functions.

Suspicious activities aligned to MITRE ATT&CK techniques are often analyzed by threat hunters or detection engineers to examine behavioural aggregations, emerging threats, or entity relationships. For example, while the EDR data can be very noisy even when aligned to MITRE ATT&CK, the process of identifying systems or users with activity spanning multiple techniques or tactics becomes very effective.

While quantitatively improving coverage of the MITRE ATT&CK matrix with EDR-based detections, the process of validating your controls becomes increasingly important as the Tactics, Techniques, and Procedures (TTP) leveraged by threat actors are constantly evolving. There are many vendors and tools providing Adversary Simulation services that are aligned to MITRE ATT&CK which effectively closes the loop on a continual validation process.