

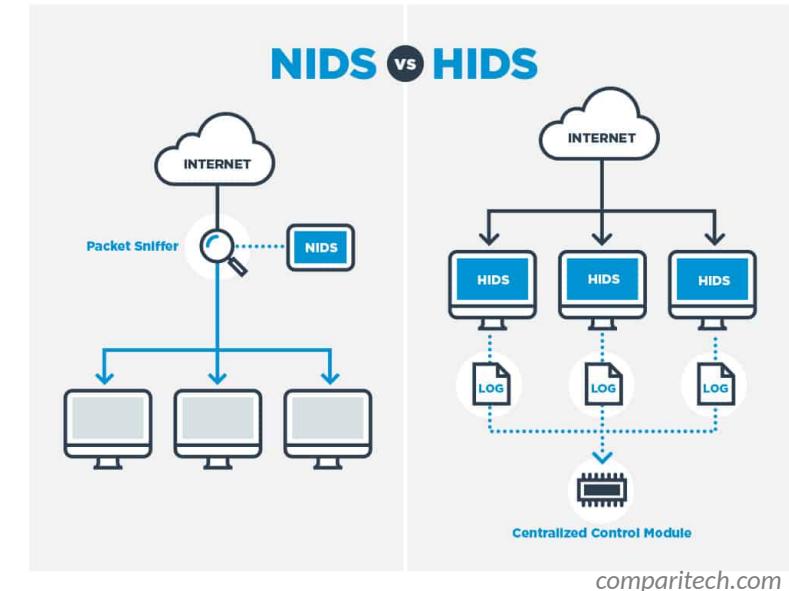
Network Traffic Analysis with **Malcolm**

A faint watermark of the Malcolm logo is visible behind the word 'Malcolm' in the title. The logo consists of a stylized yellow 'M' shape with intricate internal patterns, centered over a grid of thin grey lines.

Malcolm Development Team • Cybersecurity R&D • Idaho National Lab

Intrusion Detection Systems

- HIDS: Host Intrusion Detection Systems
 - Agents run on individual hosts or devices on a network
- NIDS: Network Intrusion Detection Systems
 - Monitor and analyze network traffic for anomalies: suspicious activity, policy violations, etc.
 - Generally passive/out-of-band; otherwise it's an Intrusion Prevention System
 - Detection methods
 - Signature-based detection (e.g., Suricata)
 - Statistical anomaly-based detection (e.g., Random Cut Forest)
 - Stateful protocol analysis detection (e.g., Zeek)



IDS: Types of Attacks

- Scanning Attack
 - Determine network topology
 - IDS highlights connections from one host to many other hosts in the network, or connection attempts to sequential IP addresses and/or ports
- Denial of Service Attack
 - Interrupt service by flooding requests or flaws in protocol implementations
 - IDS identifies large volume of traffic from or to a particular host or invalid connection states (e.g., TCP SYN/ACK with no ACK)
- Penetration Attack
 - Gain access to system resources by exploiting a software or configuration flaw
 - Trickier, but IDS may detect vulnerable software versions or simply alert on unusual operations (e.g., a “write” operation in an already-configured environment with mostly “read” operations)





- Extensible, open-source passive network analysis framework
- More than just an Intrusion Detection System:
 - Packet capture (like ~~tcpdump~~)
 - Traffic inspection (like Wireshark)
 - Intrusion detection (like SNORT)
 - Log recording (like NetFlow and syslog)
 - Scripting framework (like python™)



Strengths

- Analyzes both link-layer and application-layer behavior
- Content extraction
- Behavioral analysis
- Session correlation
- Can add support for uncommon protocols through scripts/plugins

Weaknesses

- Session metadata only (not full payload)
- Setup and configuration can be complicated
- Produces flat textual log files which can be unwieldy for in-depth analysis

Zeek Log Files

- Network Protocols
- Files
- Detection
- Network Observations

The diagram illustrates the structure of Zeek log files. It features four tables representing different types of logs:

- conn.log | IP, TCP, UDP, ICMP connection details**: This table contains fields like `ts`, `sid`, `src_ip`, `src_port`, `dst_ip`, `dst_port`, `proto`, `service`, `duration`, `seq_type`, `seq_nums`, `http_type`, `http_code`, `conn.state`, `first_orig`, `first_resp`, `max_size`, `memory`, `avg_pkts`, `avg_pkts_hex`, `avg_pkts_hex_hex`, `max_pkts`, `max_pkts_hex`, `max_pkts_hex_hex`, `ferred.parent`, `http_13_addr`, `http_13_addr_hex`, `http_13_hex`, and `inner_ifname`.
- http.log | HTTP request/reply details**: This table contains fields such as `ts`, `sid & id`, `trans_depth`, `method`, `host`, `referrer`, `user_agent`, `response_body_hex`, `response_body_hex_hex`, `status_code`, `status_msg`, `info_code`, `info_msg`, `tags`, `username`, `password`, `present`, `http_fields`, `http_themes`, `http_min_hex`, `http_hex`, `http_hex_hex`, `client_header_names`, `server_header_names`, `cookie_name`, and `url_name`.
- files.log | File analysis results**: This table contains fields like `ts`, `file`, `fs_hex`, `fs_hex_hex`, `conn_id`, `source`, `depth`, `analysis`, `minc_size`, `filename`, `duration`, `local_orig`, `is_orig`, `size_bytes`, `total_bytes`, `missing_bytes`, `overflow_bytes`, `timestamp`, `parent_file`, `modified`, `extracted`, and `entropy`.
- pe.log | Portable Executable (PE)**: This table contains fields such as `ts`, `file`, `machine`, `compile_id`, `os`, `subsystem`, `clt_end`, `clt_start`, `clt_end_hex`, `clt_start_hex`, `clt_end_hex_hex`, `clt_start_hex_hex`, `clt_end_hex_hex_hex`, `clt_start_hex_hex_hex`, `clt_end_hex_hex_hex_hex`, `clt_start_hex_hex_hex_hex`, `clt_end_hex_hex_hex_hex_hex`, `clt_start_hex_hex_hex_hex_hex`, and `section_names`.

Red lines connect the first three tables to a central point, while a red box encloses the fourth table.

corelight.com



Arkime

Strengths

- Large scale index packet capture and search tool
- Packet analysis engine with support for many common IT protocols
- Web interface for browsing, searching, analysis and PCAP carving for exporting
- PCAP payloads (not just session header/metadata) are viewable and searchable

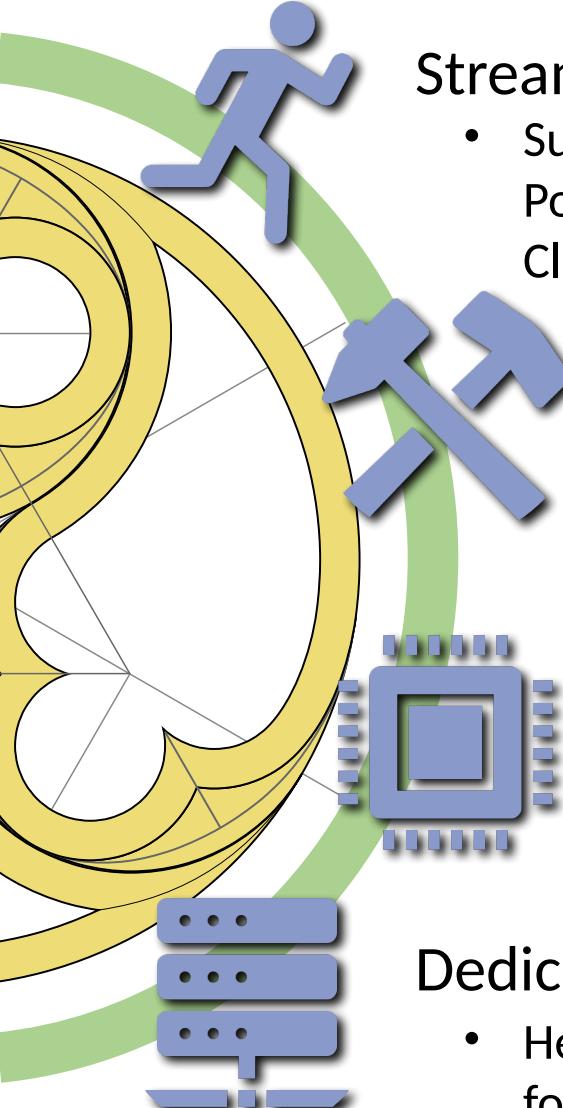
Weaknesses

- Minimal OT protocol support
- Adding new protocol parsers requires C programming



A powerful open-source network traffic analysis tool suite.

<https://idaholab.github.io/Malcolm>



Streamlined deployment

- Suitable for field use (hunt or incident response) or SOC deployment. Runs in Docker or Podman on Linux, macOS and Windows. ISO installer for bare metal installations. Cloud deployable with Kubernetes. Provides easy-to-use web-based user interfaces.

Industry-standard tools

- Uses Arkime, Zeek, and Suricata for traffic analysis; Logstash for parsing and enrichment; OpenSearch or Elasticsearch for indexing; and Dashboards and Arkime for visualization. Also leverages OpenSearch Anomaly Detection, NetBox, Strelka, CyberChef, and other proven tools for analysis of traffic and artifacts.

Expanding control systems visibility

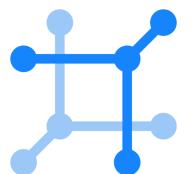
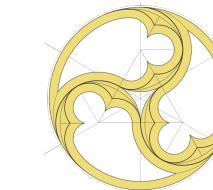
- Analyzes more protocols used in operational technology (OT) networks than other open-source or paid solutions. Ongoing development is focused on increasing the quantity and quality of industrial control systems (ICS) traffic.

Dedicated sensor appliance

- Hedgehog Linux, a hardened Linux distribution for capturing network traffic and forwarding its metadata to Malcolm.

Malcolm Origins and Milestones

- 2018.Q2 – Development begins under USBR/CISA work agreement
- 2018.Q3 to 2019.Q2 – Malcolm field-tested at USBR facilities
- 2019.Q2 – Initial public release
- 2021.Q1 – 1k stars on GitHub
- 2022.Q3 – Malcolm-based simulated engagements begin at INL's ICS Control Environment Lab Resource (CELR)
- 2022.Q3 – Malcolm discussed during session of the U.S. House of Representatives Homeland Security Committee
- 2022.Q4 – NetBox provides asset inventory and interaction analysis
- 2023.Q1 – Kali releases “Purple” distro bundling Malcolm
- 2023.Q2 – Cloud deployable with K8s
- 2024.Q2 – 2k stars on GitHub, community discussions board and new training offerings
- 2024.Q3 – First public Malcolm user conference, Mal.Con24
- 2025.Q2 – Keycloak provides SSO and role-based access control
- 2025.Q4 – Google Threat Intelligence integration
- 2026.Q1 – Enhanced file scanning with Strelka



Malcolm



What Can It Do For Me?

- Get to know your network: Malcolm **characterizes** traffic by devices and the protocols they use to communicate.
- Understand risks and threats: Malcolm **identifies** active exploits, potential attack vectors, and vulnerable devices and protocols.
- Increase visibility: Malcolm **highlights** inbound, outbound, and internal communications to inform decisions and improve security posture.



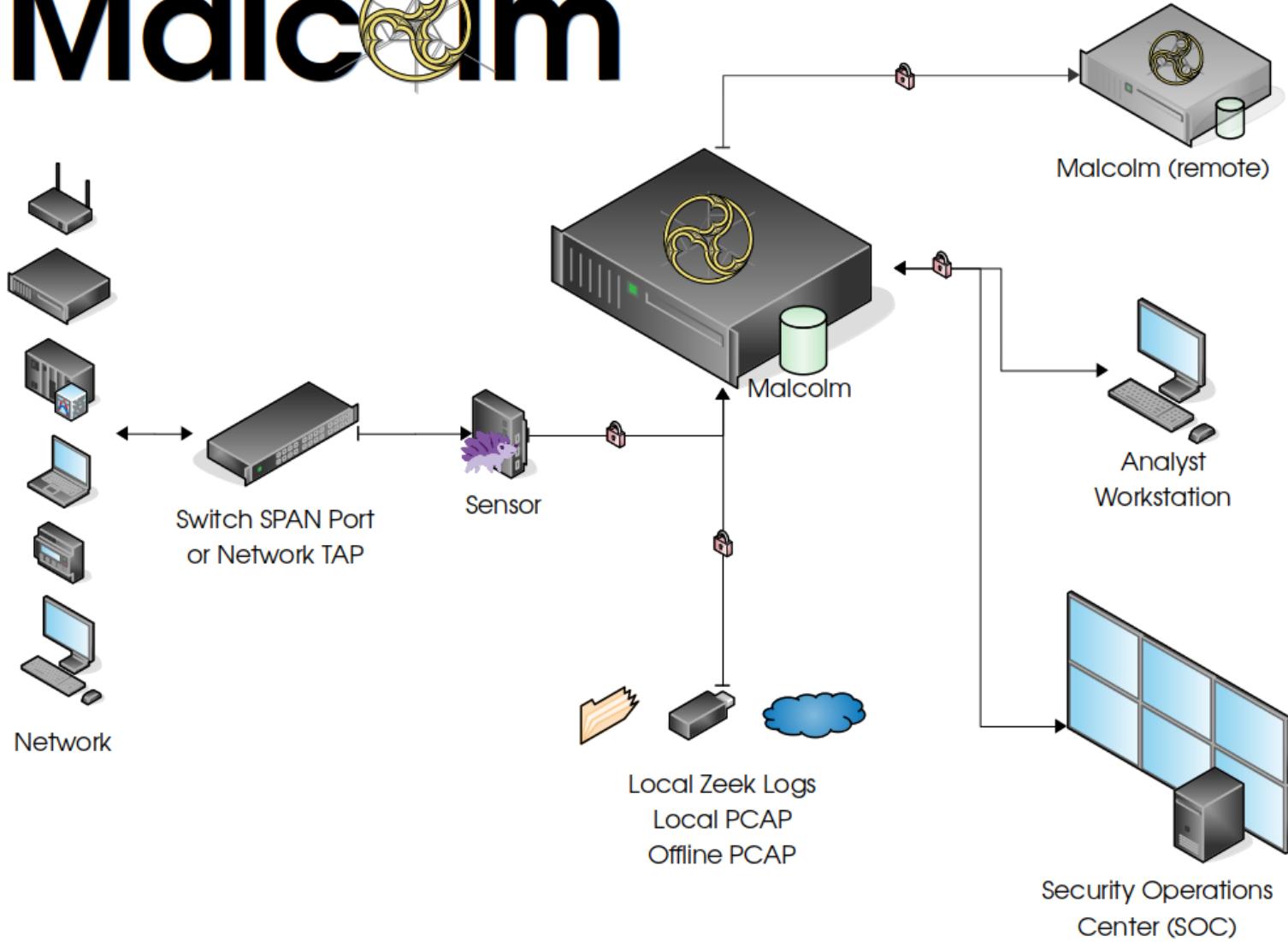
What can network traffic reveal about my cybersecurity posture?

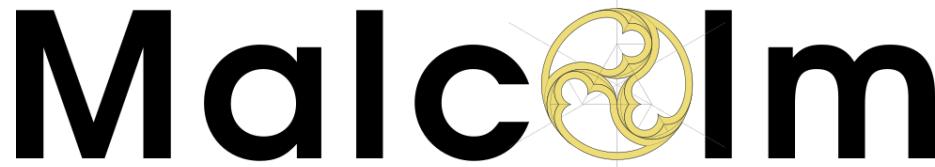
- A lot!
- Malcolm can be used to validate cyber best practices and uncover red flags in network configuration, including:
 - Proper network segmentation
 - East-West (cross-segment) and North-South traffic
 - Unsecure or outdated protocols
 - Unexpected protocols
 - Rogue devices and services
 - Suspicious file transfers
 - Sensitive unencrypted information (e.g., PII, PCII, cleartext credentials)
 - ... and much more



Image credit: kelsercorp.com

Malcolm





Supported Protocols

<https://idaholab.github.io/Malcolm/docs/protocols.html>

Internet layer (IP, TCP/IP)

ANSI C12.22

Border Gateway Protocol (BGP)

Building Automation and Control (BACnet)

Bristol Standard Asynchronous Protocol (BSAP)

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC)

Dynamic Host Configuration Protocol (DHCP)

Distributed Network Protocol 3 (DNP3)

Domain Name System (DNS)

EtherCAT

EtherNet/IP / Common Industrial Protocol (CIP)

FTP (File Transfer Protocol)

Genisys

GE Service Request Transport Protocol (SRTP)

Google Quick UDP Internet Connections (gQUIC)

Highway Addressable Remote Transducer over IP (HART-IP)

Hypertext Transfer Protocol (HTTP)

IPsec

Internet Relay Chat (IRC)

Lightweight Directory Access Protocol (LDAP)

Kerberos

Modbus

MQ Telemetry Transport (MQTT)

MySQL

NT Lan Manager (NTLM)

Network Time Protocol (NTP)

Omron Factory Interface Network Service (OMRON FINS)

Open Platform Communications Unified Architecture (OPC UA) Binary

Open Shortest Path First (OSPF)

OpenVPN

Oracle

PostgreSQL

Process Field Net (PROFINET)

Redis

Remote Authentication Dial-In User Service (RADIUS)

Remote Desktop Protocol (RDP)

Remote Framebuffer / Virtual Network Computing (RFB/VNC)

Remote Operations Controller (ROC) Plus

S7comm / Connection Oriented Transport Protocol (COTP)

Secure Shell (SSH)

Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

Session Initiation Protocol (SIP)

Server Message Block (SMB) / Common Internet File System (CIFS)

Simple Mail Transfer Protocol (SMTP)

Simple Network Management Protocol (SNMP)

SOCKS

STUN (Session Traversal Utilities for NAT)

Synchrophasor (IEEE C37.118)

Syslog

Tabular Data Stream (TDS)

Telnet / remote shell (rsh) / remote login (rlogin)

TFTP (Trivial File Transfer Protocol)

WebSocket

WireGuard

various tunnel protocols (e.g., GTP, GRE, Teredo, AYIYA, IP-in-IP, etc.)

* Industrial control systems protocols indicated with bold

Malcolm



Components

<https://idaholab.github.io/Malcolm/docs/components.html>



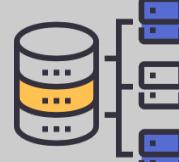
Capture &
Analysis



File Scanning



Forwarding &
Enrichment



Storage



Anomaly
Detection



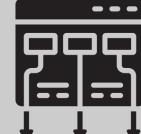
Asset
Management



Visualization



Payload
Analysis



Framework



Arkime



STRELKA



fluentbit



SURICATA



ClamAV®



logstash



OpenSearch



Anomaly
Detection Plugin



Alerting



Alerting
Plugin



netbox



OpenSearch
Dashboards



CyberChef



docker



podman



zeek



CAPA



beats



Arkime

Arkime
session PCAP
export to
WIRESHARK



kubernetes

Configuring and Running Malcolm

- Runs natively in Docker or Podman, use ISO installer for VM or bare metal install, or cloud deploy with Kubernetes or Amazon Machine Image (AMI)
- Recommended system requirements: 64+GB RAM, 16+ CPU cores, “enough” storage for PCAP and logs
- Documentation and source code on GitHub: <https://idaholab.github.io/Malcolm>
- Walkthroughs on YouTube: “Malcolm Network Traffic Analysis”



Malcolm



Dashboards

Visualize traffic or track down security concerns with dozens of [pre-built dashboards](#), or create your own



Arkime

Delve into [session details](#) including full packet payloads



NetBox

Model and document your [network infrastructure](#)



CyberChef

Slice and dice data with this web app for encryption, encoding, compression and data analysis



Documentation

Read the Malcolm user guide



Artifact Upload

[Upload](#) previously-captured PCAP files or archived Zeek logs for analysis



Keycloak Authentication

Malcolm is using [Keycloak](#) for authentication



Extracted Files

Browse the preserved [extracted files](#) carved and scanned by Malcolm

Importing Traffic Captures for Analysis

- Upload PCAP files or archived Zeek logs
- Specify tags for search and filter
- Specify NetBox site



Network Traffic Artifact Upload

Field Office Incident XYZ User-defined tags

Commit Uploaded Files

Drag & Drop your files or [Browse](#)

Advantech.pcap
40 KB

BACnet_FIU.pcap
9 MB

BACnet_Host.pcap
1.8 MB

iFix_Client86.pcap
900 KB

iFix_Server119.pcap
12 MB

MicroLogix56.pcap
9 MB

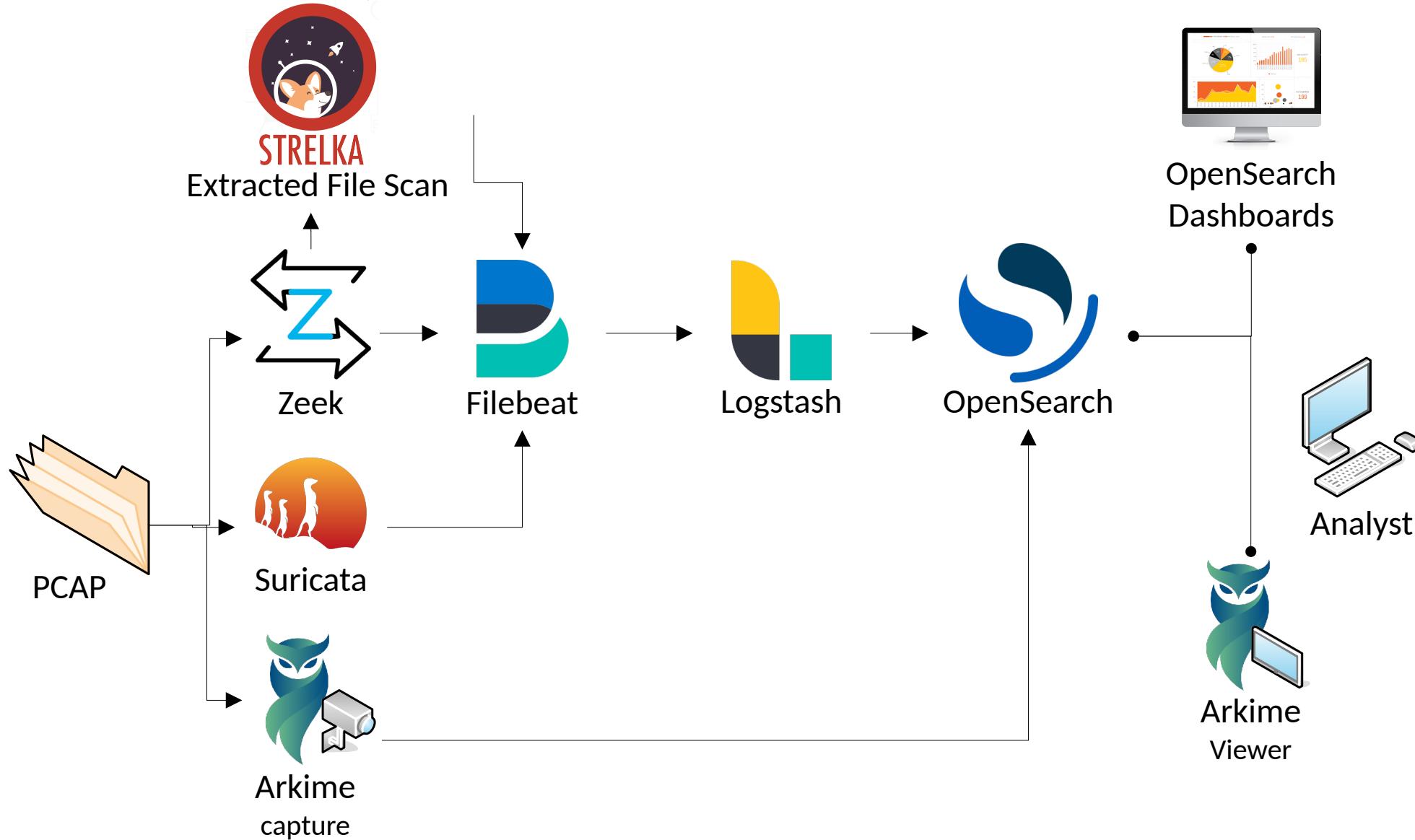
Modicon.pcap
883 KB

WinXP.pcap
3.4 MB

Malcolm

Data Pipeline

<https://idaholab.github.io/Malcolm/>

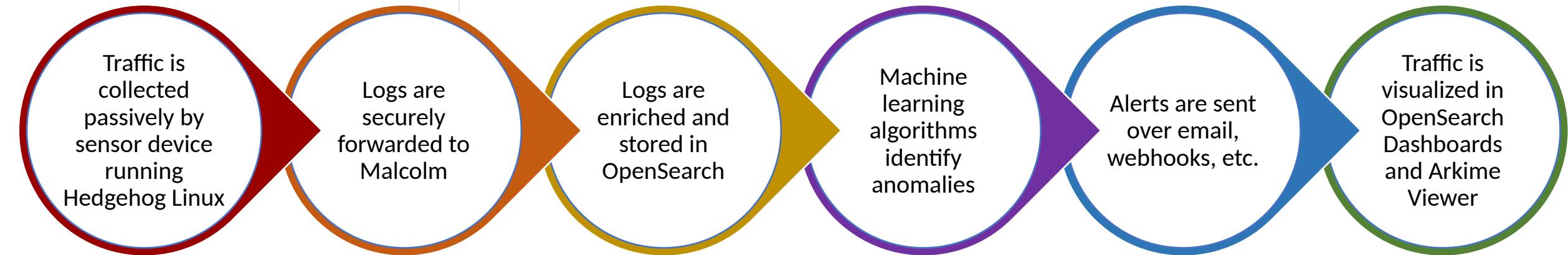


Malcolm



Data Pipeline

<https://idaholab.github.io/Malcolm/>



- Zeek, Arkime, and Suricata generate metadata about network communications
- Full PCAP is stored locally on the sensor
- Files transfers are detected, and the files scanned for threats
- PCAP may also be uploaded to or captured by Malcolm without requiring a dedicated sensor

- Communications between the sensor and aggregator are TLS-encrypted
- Sensor data including resource utilization, syslog, audit logs, temperatures, and more may also be forwarded
- Other third-party logs (e.g., Windows event logs, server host logs, etc.) may be shipped using Fluent Bit or Beats

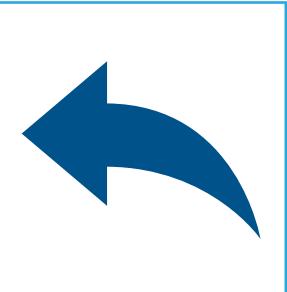
- Lookups are performed for GeoIP, ASN, MAC-to-vendor, community ID, domain name entropy, etc.
- Network events are normalized across protocols and data sources
- Best-guess techniques are applied to identify obscure OT traffic
- Enriched metadata may be forwarded to higher-tiered Malcolm instance

- Default detectors are provided for action and result, flow size, and MIME types of file transfers
- Custom detectors may be created for any aspect of any supported protocol

- Alerts may be triggered by exceeded thresholds, anomalies detected, custom queries, etc.

- Dozens of custom dashboards are provided for all supported protocols
- PCAP payloads are retrieved from sensor on demand
- Create custom visualizations via drag-and-drop interface
- Malcolm authenticates users from its own list, with SSO via Keycloak, or using Active Directory / LDAP

Log Enrichment



Reverse DNS

Domain Name
Entropy
Calculation

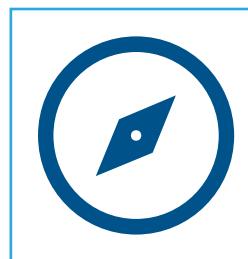
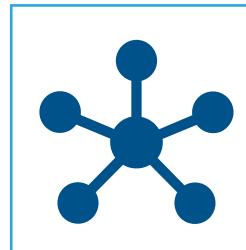


Severity Scoring



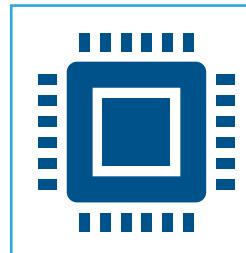
Tagging

GeolP and ASN
Lookups



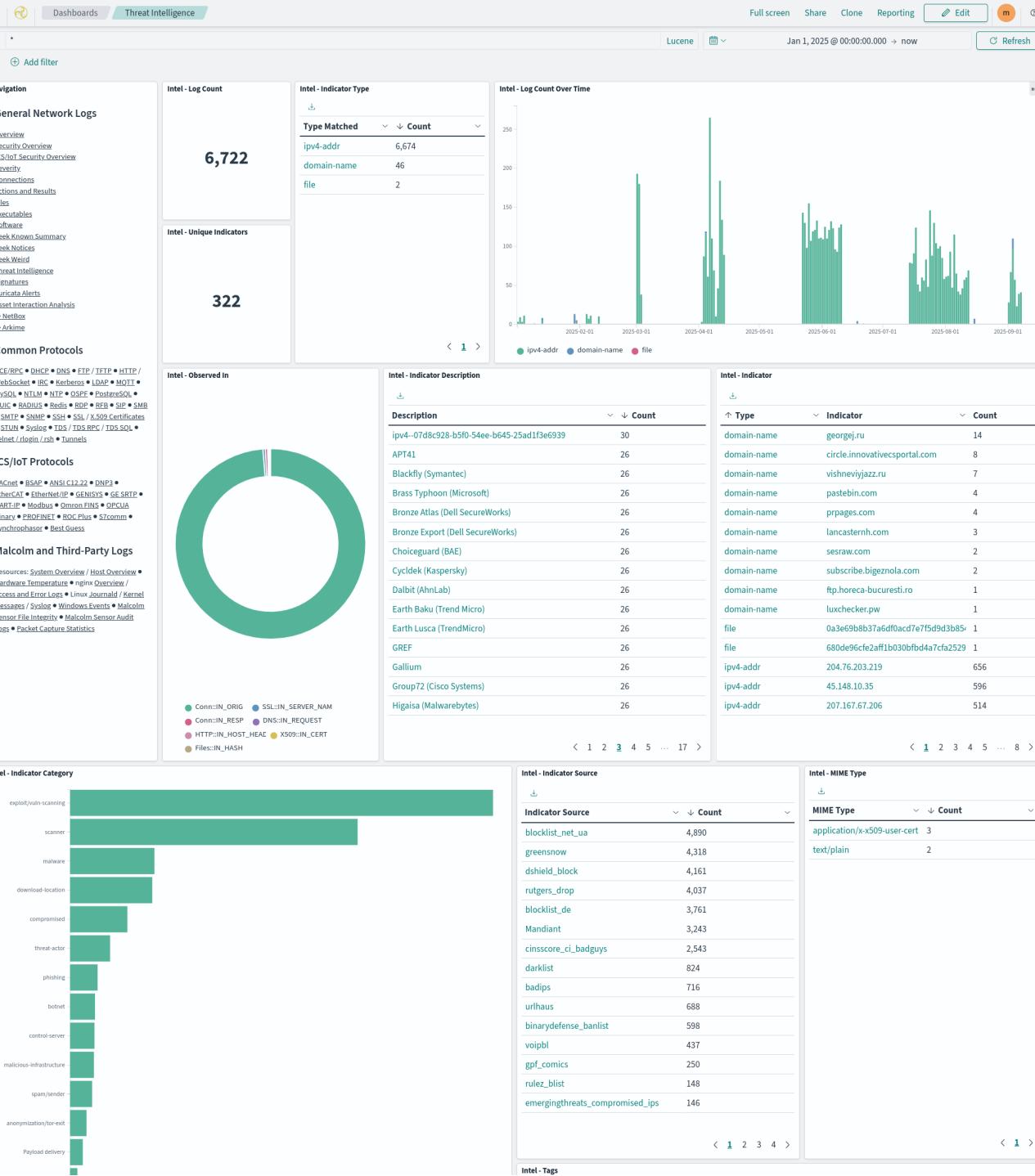
Network
Direction

Hardware Vendor
OUI Lookups



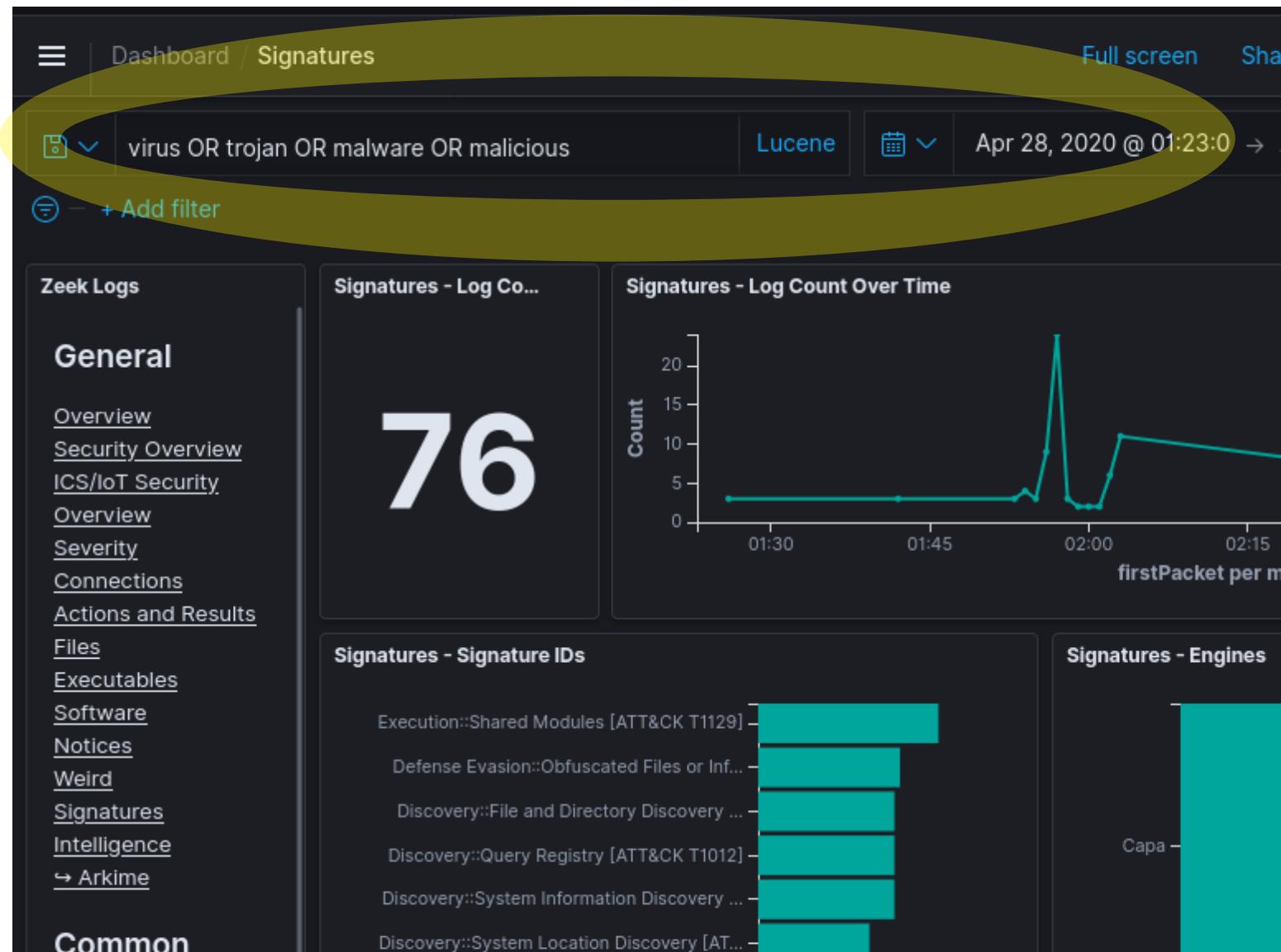
OpenSearch Dashboards

- Front end for Zeek logs and Suricata alerts
- Prebuilt visualizations for all supported protocols
- WYSIWYG editors to create custom visualizations and dashboards
- Drill down from high-level trends to specific items of interest



Dashboards Filters and Search

- Time filter: define search time frame
- Query bar: write queries in Lucene syntax or DQL (Dashboards Query Language)
- Filter bar: define filters using a UI
 - Pin filters as you move across dashboards
- Save queries and filters for reuse



Overview Dashboards

- High-level view of trends, sessions and events
- Populated from logs across all protocols
- Good jumping-off place for investigation

Navigation

General Network Logs

[Overview](#)

[Security Overview](#)

[ICS/IoT Security Overview](#)

[Severity](#)

[Connections](#)

[Connections Tree](#)

[Actions and Results](#)

[Threat Intelligence](#)

[Files](#)

[File Scanning](#)

[Executables](#)

[Software](#)

[Zeek Known Summary](#)

[Zeek Notices](#)

[Zeek Weird](#)

[Zeek Signatures](#)

[Suricata Alerts](#)

[Asset Interaction Analysis](#)

[Validated Architecture Design Review](#)

[↪ NetBox](#)

[↪ Arkime](#)

Common Protocols

Zeek Notices

- Zeek notices are things that are odd or potentially bad
- In addition to Zeek's defaults, Malcolm raises notices for recent critical vulnerabilities and attack techniques

Malcolm

Dashboard / Zeek Notices

+ Add filter

Network Logs

General

- [Overview](#)
- [Security Overview](#)
- [ICS/IoT Security Overview](#)
- [Severity](#)
- [Connections](#)
- [Actions and Results](#)
- [Files](#)
- [Executables](#)
- [Software](#)
- [Zeek Intelligence](#)
- [Zeek Notices](#)
- [Zeek Weird](#)
- [Signatures](#)
- [Suricata Alerts](#)
- [Arkime](#)

Common Protocols

- DCE/RPC
- DHCP
- DNS
- FTP / TFTP
- HTTP
- IRC
- Kerberos
- LDAP
- MQTT
- MySQL
- NTLM
- NTP
- OSPF
- QUIC
- RADIUS
- RDP
- RFB
- SIP
- SMB
- SMTP
- SNMP
- SSH
- SSL / X.509
- Certificates
- STUN
- Syslog
- TDS / TDS RPC
- TDS SQL
- Telnet / rlogin / rsh
- Tunnels

ICS/IoT Protocols

Notices - Log Count

749

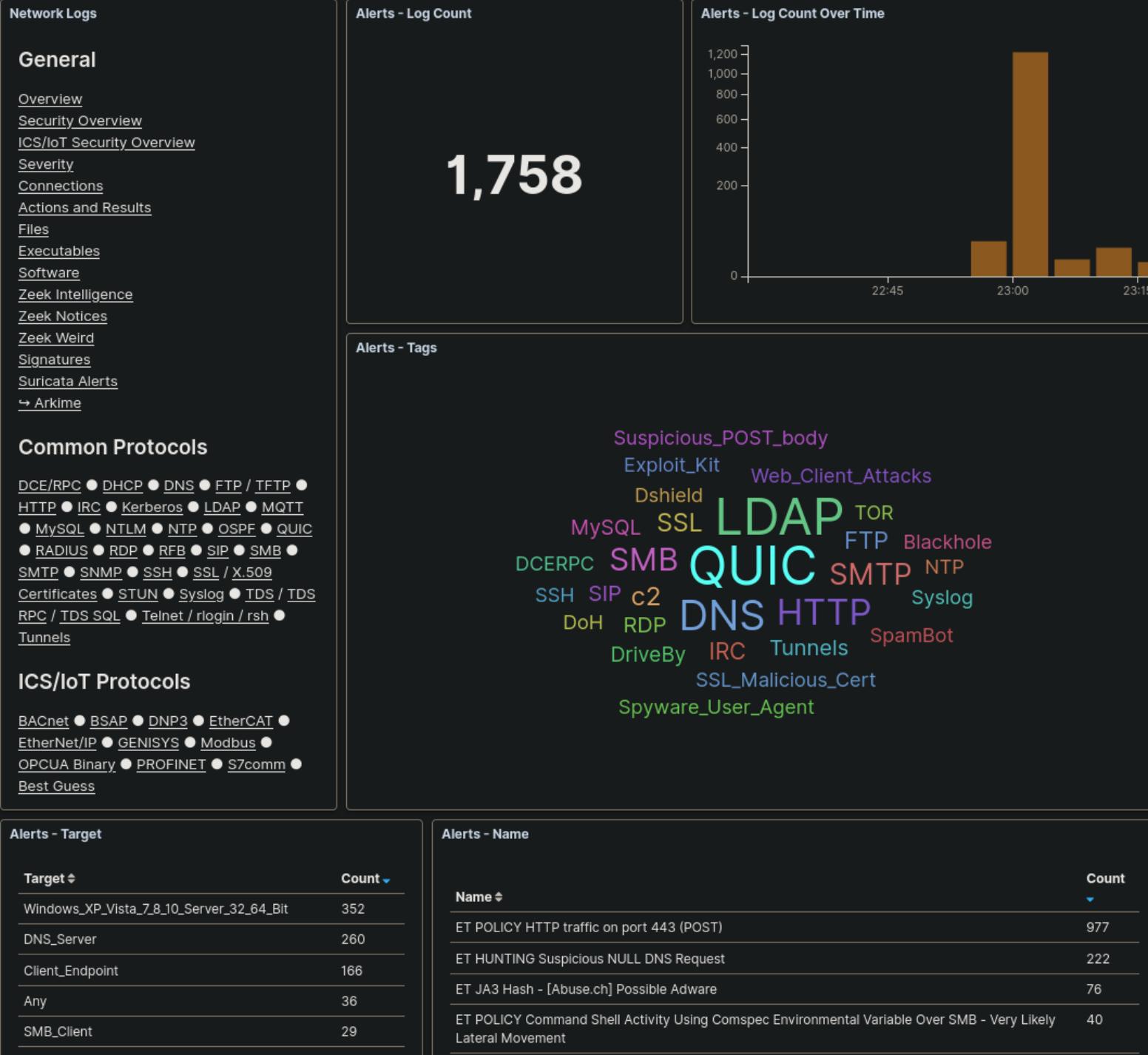
Notices - Log Count Over Time

Notices - Notice Type

Notice Category	Notice Subcategory	Count
SSL	Invalid_Server_Cert	512
ATTACK	Execution	60
ATTACK	Lateral_Movement	39
EternalSafety	ViolationTx2Cmd	28
Signatures	Sensitive_Signature	26
EternalSafety	ViolationNtRename	22
ATTACK	Discovery	15
EternalSafety	EternalBlue	13
EternalSafety	DoublePulsar	10
ATTACK	Lateral_Movement_Multiple_Attempts	6

Suricata Alerts

- Protocol-aware Suricata signatures generate alerts for suspect traffic
- Use the default Emerging Threats Open ruleset or custom signatures from other sources



Security & ICS/IoT Security Overviews

Network Logs

General

- Overview
- Security Overview
- ICS/IoT Security Overview
- Severity
- Connections
- Actions and Results
- Files
- Executables
- Software
- Zeek Intelligence
- Zeek Notices
- Zeek Weird
- Signatures
- Suricata Alerts
- Arkime

Common Protocols

- DCE/RPC • DHCP • DNS • FTP / TFTP • HTTP • IRC • Kerberos • LDAP • MQTT • MySQL • NTLM • NTP • OSPF • QUIC • RADIUS • RDP • REB • SIP • SMB • SMTP • SNMP • SSH • SSL / X.509 Certificates • STUN • Syslog • TDS / TDS-RPC • TDS-SQL • Telnet / login / rsh • Tunnels

ICS/IoT Protocols

- BACnet • BSAP • DNP3 • EtherCAT • EtherNet/IP • GENIUS • Modbus • OPCUA Binary • PROFINET • S7comm • Best Guess

Outdated/Insecure Application Protocols

Application Protocol	Protocol Version	Count
smb	1	124,835
ftp	-	3,099
tls	TLSV10	422
tls	TLSV11	253
tls	-	239
ntp	3	90
ftp	-	84

Vulnerabilities

Data Source	Log Type	Vulnerability ID	Last Seen
zeek	notice	CVE_2021_44228	Mar 4, 2021 @ 14:01:48.003
zeek	notice	CVE_2020_0601	Mar 2, 2021 @ 00:00:00.145
suricata	alert	CVE_2021_44228	Mar 1, 2021 @ 23:59:59.509
suricata	alert	CVE_2020_1472	Mar 1, 2021 @ 23:03:47.273
zeek	notice	CVE_2020_16898	Mar 1, 2021 @ 23:00:13.033
zeek	notice	CVE_2020_13777	Mar 1, 2021 @ 23:00:09.423
zeek	notice	CVE_2021_41773	Mar 1, 2021 @ 23:00:03.326

Network Layer

Normalized Event Category

Notice, Alert, Signature and Weird - Summary

Provider	Dataset	Category	Name
suricata	alert	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
zeek	notice	SSL	Invalid_Server_Cert
suricata	alert	Attempted Administrator Privilege Gain	ET EXPLOIT Possible Zerologon NetServerAuthenticate (CVE-2020-1472)
zeek	weird	-	line_terminated_with_single_CR
zeek	weird	-	end-of-data reached before &until expression found (/op /spicy-lisp/analyzer/lisp.spicy:165:18)
suricata	alert	Misc activity	ET HUNTING Suspicious NULL DNS Request
suricata	alert	Attempted Administrator Privilege Gain	ET EXPLOIT Possible Zerologon Phase 1/3 - NetServerChallenge (CVE-2020-1472)
zeek	weird	-	possible_split_routing
zeek	weird	-	data_before_established
zeek	weird	-	premature_connection_reuse
zeek	notice	ATTACK	Execution
suricata	alert	Unknown Traffic	ET JA3 Hash - [Abuse.ch] Possible Adware
zeek	weird	-	
zeek	notice	ATT	
suricata	alert	Atten Gain	
zeek	notice	Sign	
zeek	weird	-	
suricata	alert	Poter	

Malcolm

Dashboard | ICS/IoT Security Overview

Full screen Share Clone Reporting

ICS/IoT Log Counts

General

- Overview
- Security Overview
- ICS/IoT Security Overview
- Severity
- Connections
- Actions and Results
- Files
- Executables
- Software
- Notices
- Weird
- Signatures
- Intel Feeds
- Arkime

Zeek Logs

ICS/IoT Log Counts

ICS/IoT Traffic Over Time

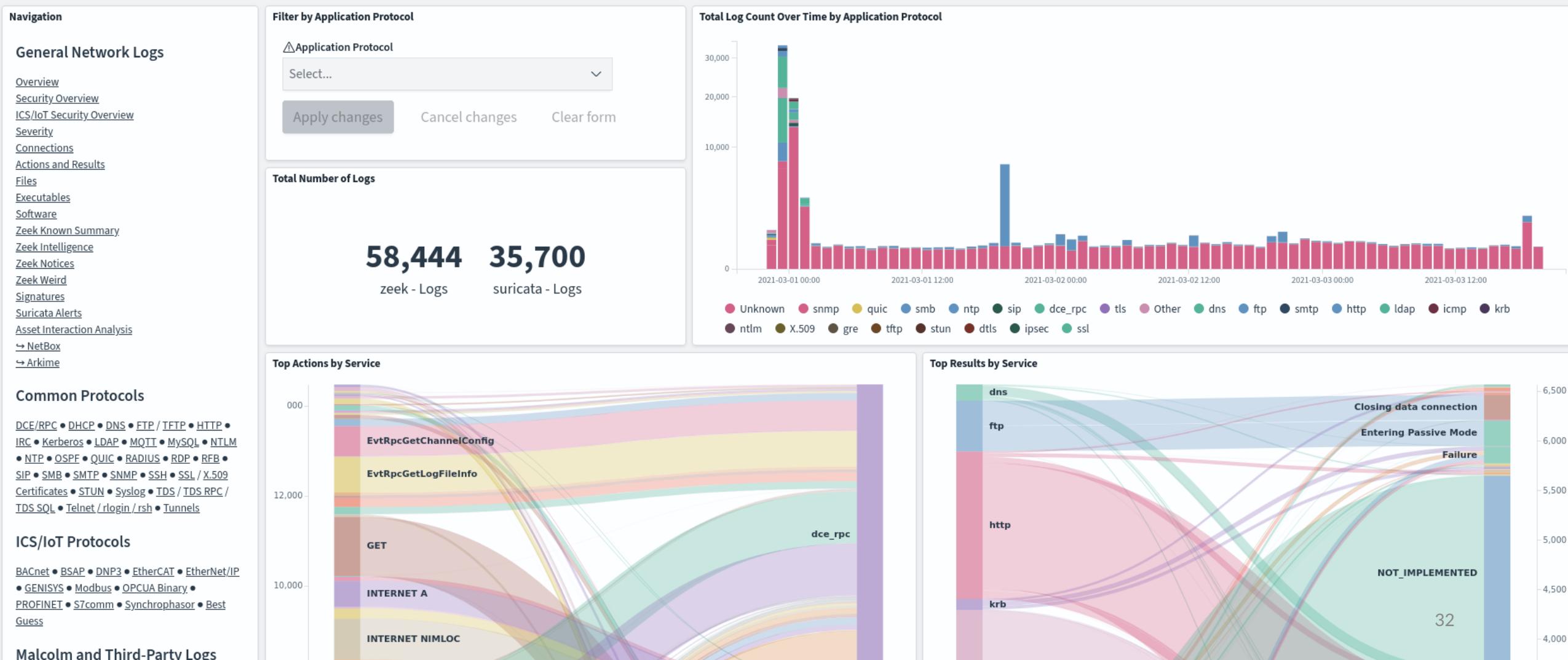
ICS/IoT External Traffic

Protocol

Protocol	Source IP	Source Country	Destination IP	Destination Country	Count
cotp	134.249.62.202	Ukraine	134.249.61.182	Ukraine	679
s7comm	134.249.62.202	Ukraine	134.249.61.182	Ukraine	411
modbus	118.189.96.132	Singapore	118.189.96.132	Singapore	32
modbus	192.168.66.235	-	166.161.16.230	United States	15
s7comm	134.249.62.206	Ukraine	134.249.61.163	Ukraine	5
s7comm	134.249.62.199	Ukraine	134.249.61.163	Ukraine	5

Actions and Results

- Malcolm normalizes “action” (e.g., write, read, create file, logon, logoff, etc.) and “result” (e.g., success, failure, access denied, not found) across protocols



Protocol Dashboards

- Highlight application-specific fields of interest
- Grouped by common IT protocols and ICS/IoT protocols
- Dashboards also included for host logs (Windows event logs, syslog, Journald messages, etc.) and other data sources (system resource utilization, packet capture statistics, sensor temperature, etc.)

Common Protocols

[DCE/RPC](#) • [DHCP](#) • [DNS](#) • [FTP / TFTP](#) • [HTTP / WebSocket](#) • [IRC](#) • [Kerberos](#) • [LDAP](#) • [MQTT](#) • [MySQL](#) • [NTLM](#) • [NTP](#) • [OSPF](#) • [PostgreSQL](#) • [QUIC](#) • [RADIUS](#) • [Redis](#) • [RDP](#) • [RFB](#) • [SIP](#) • [SMB](#) • [SMTP](#) • [SNMP](#) • [SSH](#) • [SSL / X.509 Certificates](#) • [STUN](#) • [Syslog](#) • [TDS / TDS RPC / TDS SQL](#) • [Telnet / rlogin / rsh](#) • [Tunnels](#)

ICS/IoT Protocols

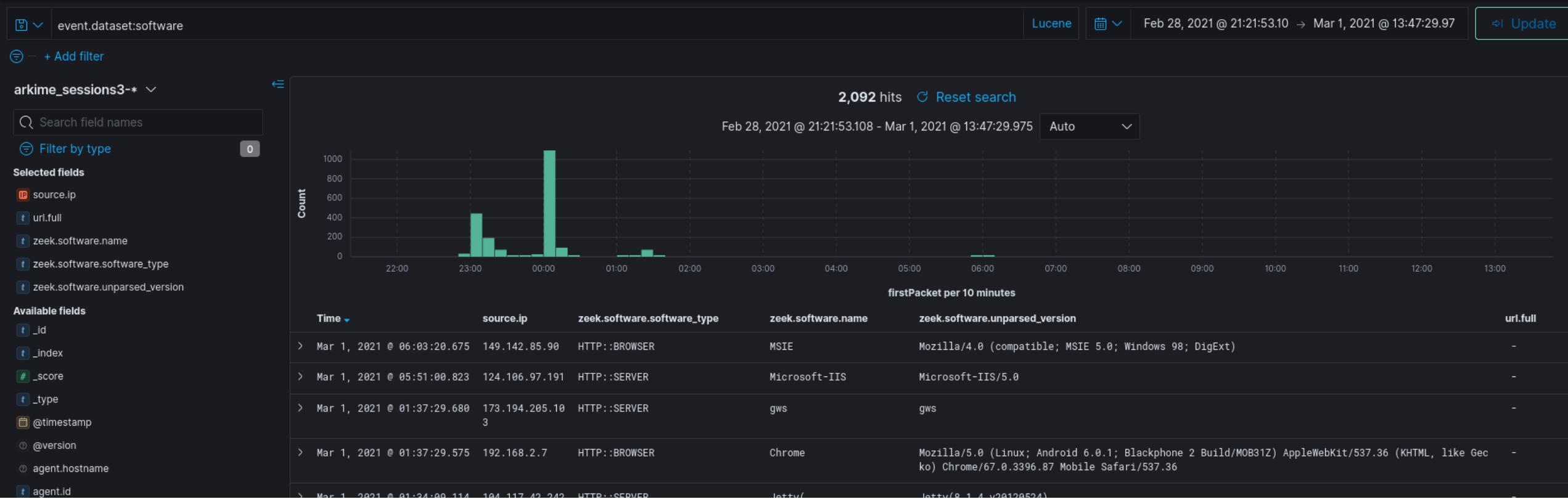
[BACnet](#) • [BSAP](#) • [ANSI C12.22](#) • [DNP3](#) • [EtherCAT](#) • [EtherNet/IP](#) • [GENISYS](#) • [GE SRTP](#) • [HART-IP](#) • [Modbus](#) • [Omron FINS](#) • [OPCUA Binary](#) • [PROFINET](#) • [ROC Plus](#) • [S7comm](#) • [Synchrophasor](#) • [Best Guess](#)

Malcolm and Third-Party Logs

Resources: [System Overview](#) / [Host Overview](#) • [Hardware Temperature](#) • [nginx Overview](#) / [Access and Error Logs](#) • [Linux Journald](#) / [Kernel Messages](#) / [Syslog](#) • [Windows Events](#) • [Malcolm System File Integrity](#) • [Malcolm System Audit Logs](#) • [Packet Capture Statistics](#)

Discover

- Field-level details of logs matching filter criteria
- Create and view saved searches and column configurations
- View other events just before and after an event

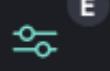


New Visualization

Filter



Area



Controls



Coordinate
Map



Data Table



Gantt Chart



Gauge



Goal



Heat Map



Horizontal Bar



Line



Markdown



Metric



Pie



Region Map



Sankey
Diagram



TSVB



Tag Cloud



Timeline



Vega



Vertical Bar

Custom Visualizations

- Create new visualizations from scratch or based on existing charts or dashboards

Search Syntax Comparison

	Arkime	Dashboards (Lucene)	Dashboards (DQL)
Field exists	<code>event.dataset == EXISTS!</code>	<code>_exists_:event.dataset</code>	<code>event.dataset:*</code>
Field does not exist	<code>event.dataset != EXISTS!</code>	<code>NOT _exists_:event.dataset</code>	<code>NOT event.dataset:*</code>
Field matches a value	<code>port.dst == 22</code>	<code>destination.port:22</code>	<code>destination.port:22</code>
Field does not match a value	<code>port.dst != 22</code>	<code>NOT destination.port:22</code>	<code>NOT destination.port:22</code>
Field matches at least one of a list of values	<code>tags == [external_source, external_destination]</code>	<code>tags:(external_source OR external_destination)</code>	<code>tags:(external_source or external_destination)</code>
Field range (inclusive)	<code>http.statuscode >= 200 && http.statuscode <= 300</code>	<code>http.statuscode:[200 TO 300]</code>	<code>http.statuscode >= 200 and http.statuscode <= 300</code>

Search Syntax Comparison (cont.)

	Arkime	Dashboards (Lucene)	Dashboards (DQL)
Field range (exclusive)	<code>http.statuscode > 200 && http.statuscode < 300</code>	<code>http.statuscode:{200 TO 300}</code>	<code>http.statuscode > 200 and http.statuscode < 300</code>
Field range (mixed exclusivity)	<code>http.statuscode >= 200 && http.statuscode < 300</code>	<code>http.statuscode:[200 TO 300}</code>	<code>http.statuscode >= 200 and http.statuscode < 300</code>
Match all search terms (AND)	<code>(tags == [external_source, external_destination]) && (http.statuscode == 401)</code>	<code>tags:(external_source OR external_destination) AND http.statuscode:401</code>	<code>tags:(external_source or external_destination) and http.statuscode:401</code>
Match any search terms (OR)	<code>(zeek_ftp.password == EXISTS!) (zeek_http.password == EXISTS!) (zeek.user == "anonymous")</code>	<code>_exists_:zeek_ftp.password OR _exists_:zeek_http.password OR zeek.user:"anonymous"</code>	<code>zeek_ftp.password:* or zeek_http.password:* or zeek.user:"anonymous"</code>

Search Syntax Comparison (cont.)

	Arkime	Dashboards (Lucene)	Dashboards (DQL)
Global string search (anywhere in the document)	all Arkime search expressions are field-based	microsoft	microsoft
Wildcards	host.dns == "*micro?oft*" (? for single character, * for any characters)	dns.host:*micro?oft* (? for single character, * for any characters)	dns.host:*micro*ft* (* for any characters)
Regex	host.http == /.*www\.f.*k\.com.*/	zeek http.host: /.*www_.f.*k\.com.*/	Dashboards Query Language does not currently support regex
IPv4 values	ip == 0.0.0.0/0	source.ip:"0.0.0.0/0" OR destination.ip:"0.0.0.0/0"	source.ip:"0.0.0.0/0" OR destination.ip:"0.0.0.0/0"
IPv6 values	(ip.src == EXISTS! ip.dst == EXISTS!) && (ip != 0.0.0.0/0)	(_exists_:source.ip AND NOT source.ip:"0.0.0.0/0") OR (_exists_:destination.ip AND NOT destination.ip:"0.0.0.0/0")	(source.ip:* and not source.ip:"0.0.0.0/0") or (destination.ip:* and not destination.ip:"0.0.0.0/0")

Search Syntax Comparison (cont.)

	Arkime	Dashboards (Lucene)	Dashboards (DQL)
GeoIP information available	country == EXISTS!	_exists_:destination.geo OR _exists_:source.geo	destination.geo:* or source.geo:*
Log type	event.dataset == notice	event.dataset:notice	event.dataset:notice
IP CIDR Subnets	ip.src == 172.16.0.0/12	source.ip:"172.16.0.0/12"	source.ip:"172.16.0.0/12"
Search time frame	Use Arkime time bounding controls under the search bar	Use Dashboards time range controls in the upper right-hand corner	Use Dashboards time range controls in the upper right-hand corner
GeoIP information available	country == EXISTS!	_exists_:destination.geo OR _exists_:source.geo	destination.geo:* or source.geo:*

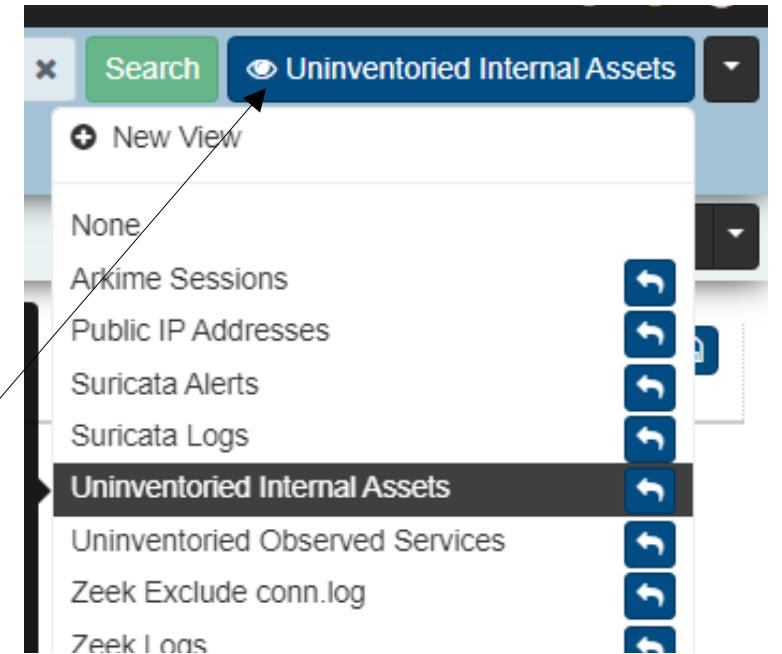


Arkime

- Front end for enriched Zeek logs, Suricata alerts **and Arkime sessions**
 - Malcolm's custom Arkime data source adds full support for Zeek and Suricata logs to Arkime, including ICS protocols
- Filter by data source (Zeek, Suricata or Arkime); or, view together
- “Wireshark at scale”: full PCAP availability for
 - viewing packet payload
 - exporting filtered and joined PCAP sessions
 - running deep-packet searches

Arkime Filters and Search

- Time filter: define search time frame
- Map filter: restrict results to geolocation
- Query bar: write queries in Arkime syntax
- Views: overlay previously-specified filters on current search



Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings Users

v3.1.1 ? ⓘ 🔍

tags == Cyberville

Custom Start 2020/04/27 23:58:59 End 2020/04/28 03:30:23 Bounding Last Packet Interval Auto 03:31:24

50 per page « < 1 2 3 4 5 > » Showing 101 - 150 of 3,504 entries

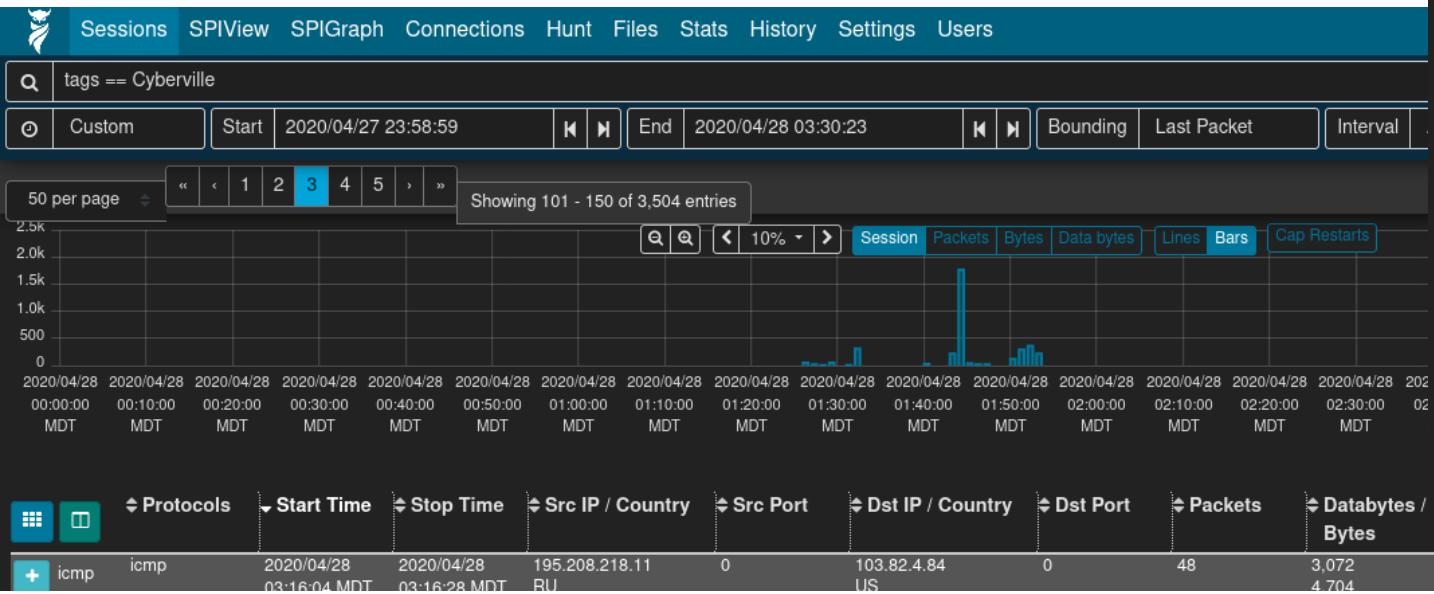
Session Packets Bytes Data bytes Lines Bars Cap Restarts

Protocol: icmp
Start Time: 2020/04/28 03:16:04 MDT
Stop Time: 2020/04/28 03:16:28 MDT
Src IP / Country: 195.208.218.11 RU
Dst IP / Country: 103.82.4.84 US
Packets: 48
Bytes: 3,072
Tags: Cyberville

Protocol: icmp
Start Time: 2020/04/28 03:16:04 MDT
Stop Time: 2020/04/28 03:16:28 MDT
Src IP / Country: 195.208.218.11 RU
Dst IP / Country: 103.82.4.84 US
Packets: 48
Bytes: 2,688
Tags: Cyberville external_source external_destination

Sessions

- Field-level details of sessions/logs matching filters
- Similar to Dashboards' Discover



The screenshot shows the Zeek SPIView interface. At the top, there's a navigation bar with links: Sessions, SPIView, SPIGraph, Connections, Hunt, Files, Stats, History, Settings, and Users. Below the navigation bar is a search bar with the query "protocols == http && tags == external_destination". Underneath the search bar are controls for "Custom" search, "Start" and "End" times (set to 2020/11/11 06:23:48 and 2021/05/30 06:00:53), and buttons for "Bounding", "Last Packet", and "Interval". A "50 per page" dropdown is also present. The main area displays a table of session details, showing 12,150 entries. The table includes columns for Log Type (http), Malcolm Data Source (zeek), Malcolm Node (filebeat), Originating Host (217.226.31.170), Originating GeoIP Country (Germany), Originating GeoIP City (Bremen), Responding Host (124.106.97.191), Responding GeoIP Country (Philippines), Responding GeoIP City (Santa Elena), Originating Port (4230), Responding Port (80), Related IP (217.226.31.170 124.106.97.191), Protocol (tcp), Service (http), Service Version (1.1), Action (GET), Result (Bad Gateway), Severity (20), Risk Score (20), Severity Tags (External traffic), and File Magic (text/html).

Zeek http.log

This screenshot shows a detailed view of a session from the Zeek http.log. It includes a table with columns: Pipeline Depth (1), Request Method (GET), URI (/vti_bin/.../winnt/system32/cmd.exe?/c+dir+x:\c+dir+x:\c+dir+x:\), and Version (1.1). The table also includes columns for Protocols, Start Time, Stop Time, Src IP / Country, Src Port, Dst IP / Country, Dst Port, Packets, Databytes / Bytes, Tags, and Info. The session details show a single entry for ICMP traffic from 195.208.218.11 to 103.82.4.84.

Packet Payloads

- Displayed for Arkime sessions with full PCAP (i.e., not Zeek logs)
- File carving on the fly
- Download session PCAP
- Examine payload with CyberChef

Source

```
GET /PostExploitation/PCAnyPass.exe HTTP/1.1
Accept: text/html, application/xhtml+xml, /*
Referer: http://10.10.10.11/PostExploitation/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 10.10.10.11
Connection: Keep-Alive
```

Destination

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.17
Date: Fri, 17 Apr 2020 19:21:32 GMT
Content-type: application/x-msdos-program
Content-Length: 49152
Last-Modified: Fri, 16 Apr 2010 19:09:50 GMT
```

[PCAnyPass.exe](#)

Export PCAP

- Creates a new PCAP file from filtered sessions
- Include open, visible or all matching sessions
- Apply “Arkime Sessions” view to sessions first
- Narrow as much as possible prior to exporting (huge PCAP files are a pain)

The screenshot shows the Arkime interface with the following details:

- Header:** Sessions, SPIView, SPIGraph, Connections, Hunt, Files, Stats, History, Settings, Users.
- Search Bar:** country != US && protocols == http
- Filter Bar:** Custom, Start: 2021/02/28 23:59:11, End: 2021/03/01 00:28:26, Interval: Auto, Duration: 00:29:15.
- Session View Buttons:** Open Items, Visible Items, Matching Items, Include: same time period, linked segments (slow), Filename: US_HTTP.pcap.
- Export Button:** Export PCAP.
- Map View:** A world map showing traffic distribution.
- Bottom Filter Bar:** Protocols: tcp, http, Start Time: 2021/03/01, Stop Time: 2021/03/01, Src IP / Country: 10.0.52.164, Src Port: 2550, Dst IP / Country: 61.8.0.17, Dst Port: 80, Packets: 7,195, Databytes / Bytes: 5,160,414, Tags: HTTP, out-of-order-dst, Info: URI - mirror.pacific.net.au/openoffice/stable/2.0.0/OOo_2.0.0_Win32Intel_install.exe.

SPIView

- Explore “top n ” and field cardinality for all fields of both Arkime sessions and Zeek logs
- Apply filters or pivot to Sessions or SPIGraph view for field values of interest
- Limit search to ≤ 1 week before using (it runs many queries)



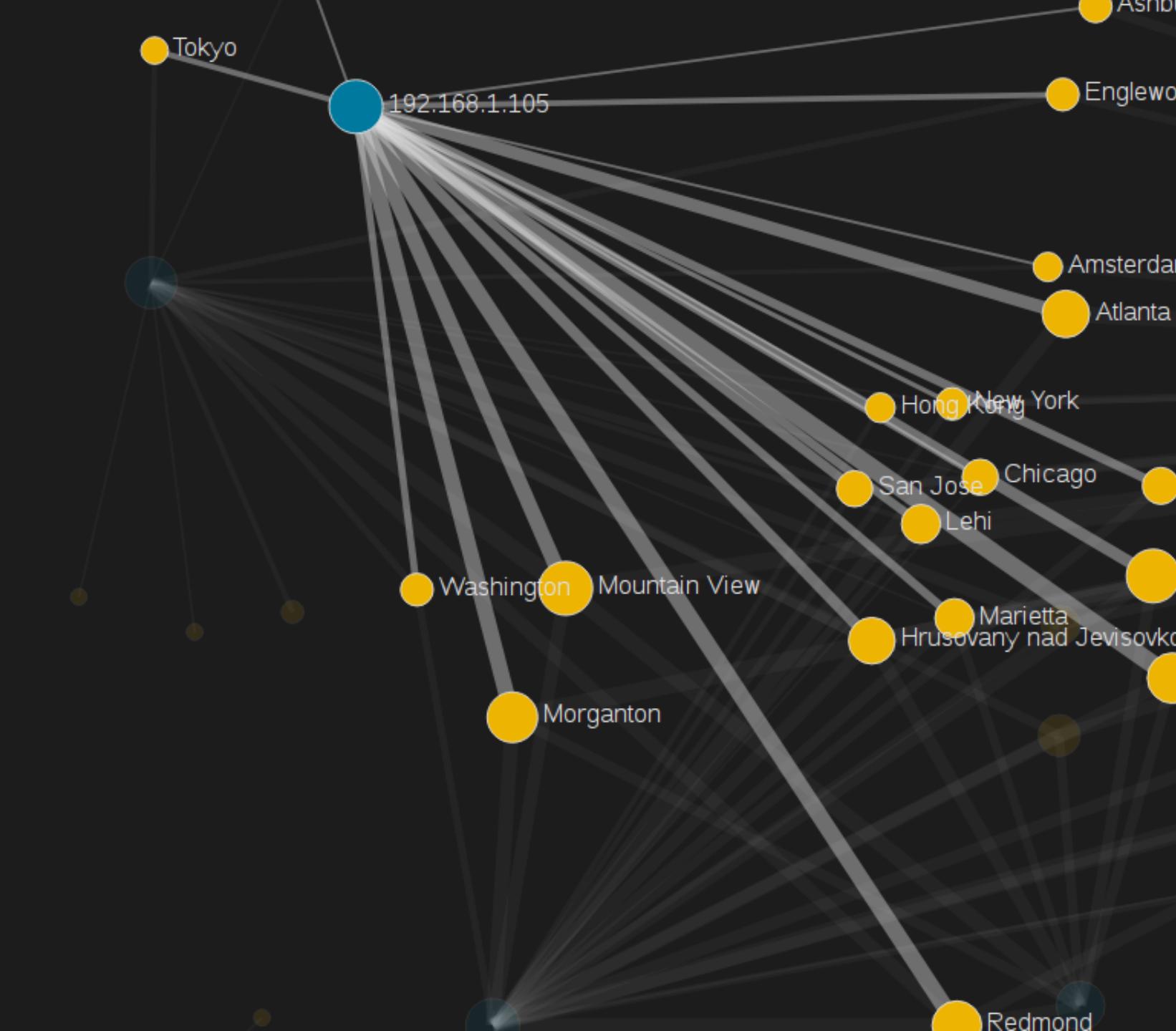
SPIGraph

- View “top n ” field values chronologically and geographically
- Identify trends and patterns in network traffic



Connections

- Visualize logical relationship between hosts
- Use any combination of fields for source and destination nodes
- Compare current vs. previous (baseline) traffic



Packet Search (“Hunt”)

- Deep-packet search (“PCAP grep”) of session payloads
- Search for ASCII, hex codes or regular expression matches
- Apply “Arkime Sessions” view to sessions first

The screenshot shows the Arkime interface with the "Hunt" tab selected in the top navigation bar. The main search bar contains the query "protocols == http". Below the search bar, there are filters for "All (careful)", "Start" (1969/12/31 17:00:00), "End" (2021/12/06 12:10:02), "Bounding", and "Last Packet". A status message indicates "Creating a new packet search job will search the packets of 2,906 sessions." On the right, a button says "Create a packet search job".

Hunt Job History

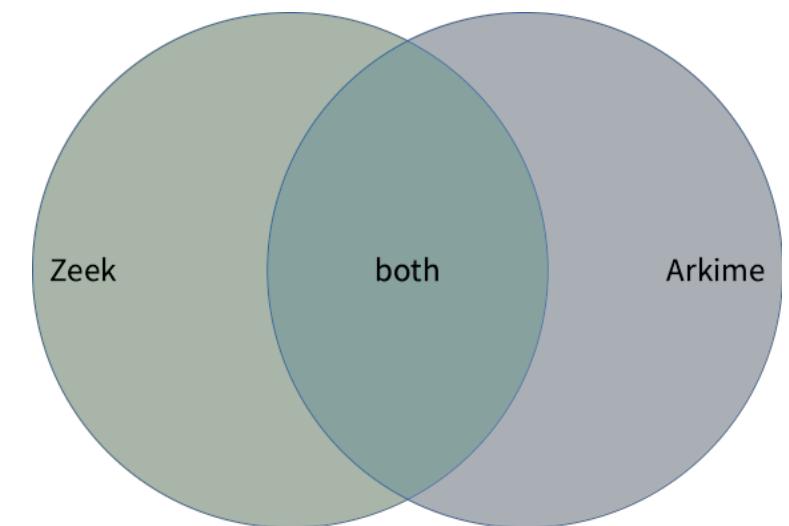
Search your packet search job history

Status	Matches	Name	User	Search text	Notify	Created	ID
<input checked="" type="checkbox"/> 100%	141	HTTP with password		password (ascii)		2021/12/06 12:12:27 MST	s5YpkX0BTA40FhD4X7dA

This hunt is **finished**.
Found 141 sessions matching **password** (ascii) of 2,908 sessions searched.
Created: 2021/12/06 12:12:27 MST
Last Updated: 2021/12/06 12:12:32 MST
Examining 500 raw source and destination packets per session
The sessions query expression was: **protocols == http**
The sessions query view was: **Arkime Sessions**
The sessions query time range was from 1969/12/31 17:00:00 MST to 2021/12/06 12:10:02 MST

Data Source Correlation

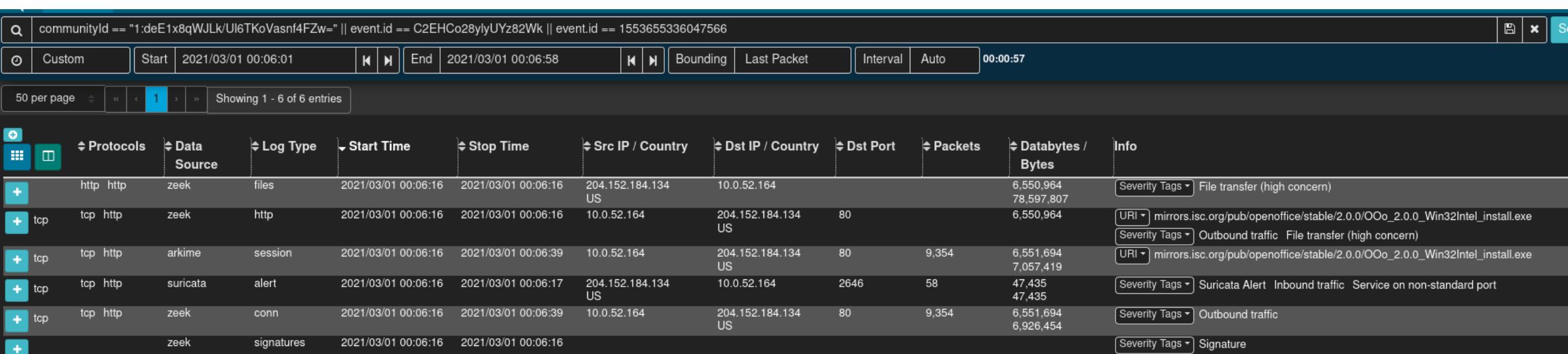
- Search syntax is different between Arkime and Dashboards (and in some cases, so are field names)
 - See search syntax comparison table, Malcolm and Arkime docs
- Despite considerable overlap, there are differences in protocol parser support among Zeek, Suricata and Arkime
 - Learning the strengths of each will help you more effectively find the good stuff



Correlate Zeek or Suricata Logs and Packet Payloads

- Correlate Zeek or Suricata logs and Arkime sessions using common fields
- communityId fingerprints flows to bridge data sources
- rootId/event.id filters logs for the same session
- Filter community ID OR'ed with event.id to see all Arkime sessions and Zeek or Suricata logs for the same traffic

```
communityId == "1:r7tGG//fXP1P0+BXH3zXETCtEFI=" || event.id == "CQcoro2z6adgtGlk42"
```



The screenshot shows the Arkime interface with a search bar at the top containing the query: "communityId == "1:r7tGG//fXP1P0+BXH3zXETCtEFI=" || event.id == "CQcoro2z6adgtGlk42"".

Below the search bar are various filtering and search controls: "Custom", "Start" (set to 2021/03/01 00:06:01), "End" (set to 2021/03/01 00:06:58), "Bounding", "Last Packet", "Interval" (set to Auto), and a timestamp of "00:00:57".

The main area displays a table of log entries. The columns are: Protocols, Data Source, Log Type, Start Time, Stop Time, Src IP / Country, Dst IP / Country, Dst Port, Packets, Databytes / Bytes, and Info.

Protocols	Data Source	Log Type	Start Time	Stop Time	Src IP / Country	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Info
http http	zeek	files	2021/03/01 00:06:16	2021/03/01 00:06:16	204.152.184.134 US	10.0.52.164			6,550,964 78,597,807	Severity Tags ▾ File transfer (high concern)
tcp http	zeek	http	2021/03/01 00:06:16	2021/03/01 00:06:16	10.0.52.164	204.152.184.134 US	80		6,550,964	URI ▾ mirrors.isc.org/pub/openoffice/stable/2.0.0/OOo_2.0.0_Win32Intel_install.exe Severity Tags ▾ Outbound traffic File transfer (high concern)
tcp http	arkime	session	2021/03/01 00:06:16	2021/03/01 00:06:39	10.0.52.164	204.152.184.134 US	80	9,354	6,551,694 7,057,419	URI ▾ mirrors.isc.org/pub/openoffice/stable/2.0.0/OOo_2.0.0_Win32Intel_install.exe
tcp http	suricata	alert	2021/03/01 00:06:16	2021/03/01 00:06:17	204.152.184.134 US	10.0.52.164	2646	58	47,435 47,435	Severity Tags ▾ Suricata Alert Inbound traffic Service on non-standard port
tcp http	zeek	conn	2021/03/01 00:06:16	2021/03/01 00:06:39	10.0.52.164	204.152.184.134 US	80	9,354	6,551,694 6,926,454	Severity Tags ▾ Outbound traffic
	zeek	signatures	2021/03/01 00:06:16	2021/03/01 00:06:16						Severity Tags ▾ Signature

Verify Network Segmentation with NetBox and Asset Interaction Analysis

- Flat networks are problematic (and unfortunately common)
- Security-minded network design incorporates segregating (isolating) and segmenting (dividing) assets into zones with differing levels of trust and well-defined boundaries
 - Enterprise
 - DMZ
 - Operation and Control
 - Supervisory Control
 - Process
 - etc.

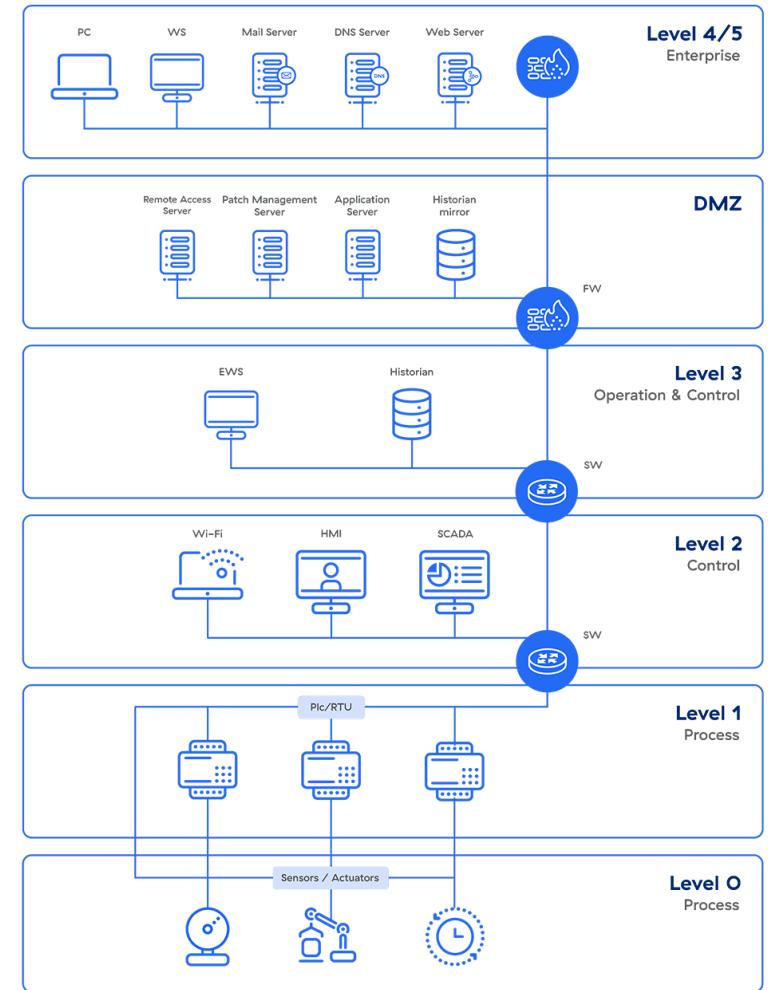
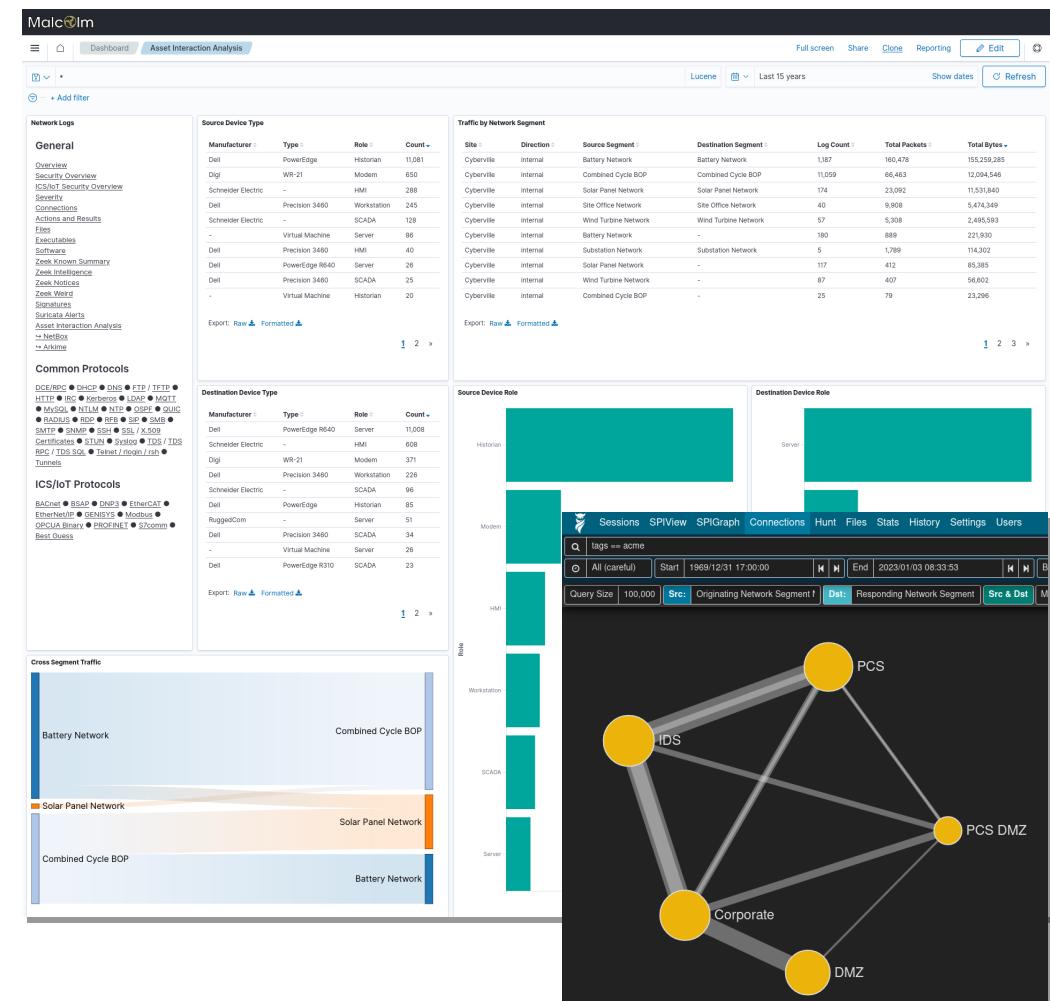


Image credit: Zscaler.com

Verify Network Segmentation with NetBox and Asset Interaction Analysis

- Network prefixes are identified by name and CIDR subnet in NetBox
- Observed network traffic is cross-referenced against inventory
- Malcolm dashboards such as **Asset Interaction Analysis** highlight relationships among network segments



Pinpoint Rogue Devices and Services

- Networked devices can be inventoried in NetBox
 - Name
 - IP address
 - Manufacturer
 - SKU or model number
 - Role
- Expected services (application protocols) can be specified for the devices that provide them

Devices

Results 52 Filters 1

× Site: Cyberville Save

Quick search

<input type="checkbox"/>	NAME	STATUS	SITE	ROLE	MANUFACTURER	TYPE	IP ADDRESS	TAGS
<input type="checkbox"/>	4yH2O0Z20tmgmH8v	Active	Cyberville	Unspecified	Microsoft Corporation	Unspecified	192.168.0.129/32	Autopopulated
<input type="checkbox"/>	Battery HMI	Active	Cyberville	HMI	Schneider Electric	Unspecified	10.10.10.3/32	—
<input type="checkbox"/>	Battery Historian	Active	Cyberville	Historian	Dell	PowerEdge	10.10.10.5/32	—
<input type="checkbox"/>	Cellular Modem	Active	Cyberville	Modem	Digi	WR-21	10.10.10.11/32	—
<input type="checkbox"/>	Combined Cycle BOP Historian	Active	Cyberville	Historian	Dell	PowerEdge	10.10.20.5/32	—
<input type="checkbox"/>	DROP200	Active	Cyberville	Server	Dell	PowerEdge R640	10.10.20.10/32	—
<input type="checkbox"/>	ENG_WORKSTATION	Active	Cyberville	Workstation	Dell	Precision 3460	10.10.20.8/32	—
<input type="checkbox"/>	Microsoft Corporation @ 10.0.0.130	Active	Cyberville	Unspecified	Microsoft Corporation	Unspecified	10.0.0.130/32	Autopopulated
<input type="checkbox"/>	Modbus Client 12	Active	Cyberville	SCADA	Schneider Electric	Unspecified	10.10.10.12/32	—
<input type="checkbox"/>	Modbus Client 55	Active	Cyberville	SCADA	Dell	Precision 3460	10.10.10.55/32	—
<input type="checkbox"/>	Modbus Client 64	Active	Cyberville	SCADA	Schneider Electric	Unspecified	10.10.10.64/32	—

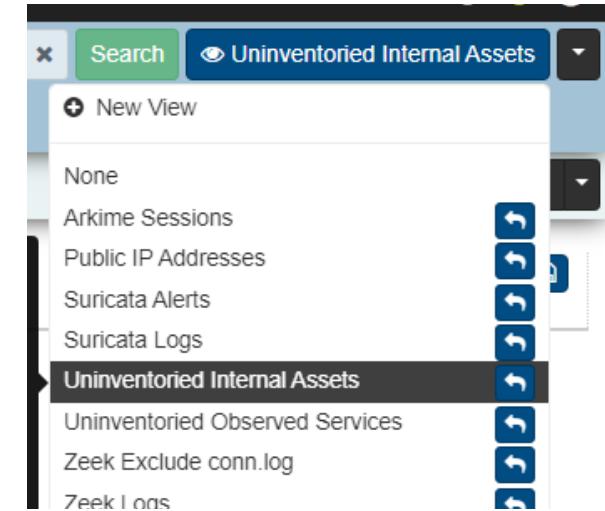
Pinpoint Rogue Devices and Services

- Dashboards highlight “uninventoried” devices and services (observed but not accounted for in NetBox)
 - Zeek Known Summary
 - Asset Interaction Analysis
- Premade Arkime views
 - Uninventoried Internal Assets
 - Uninventoried Observed Services

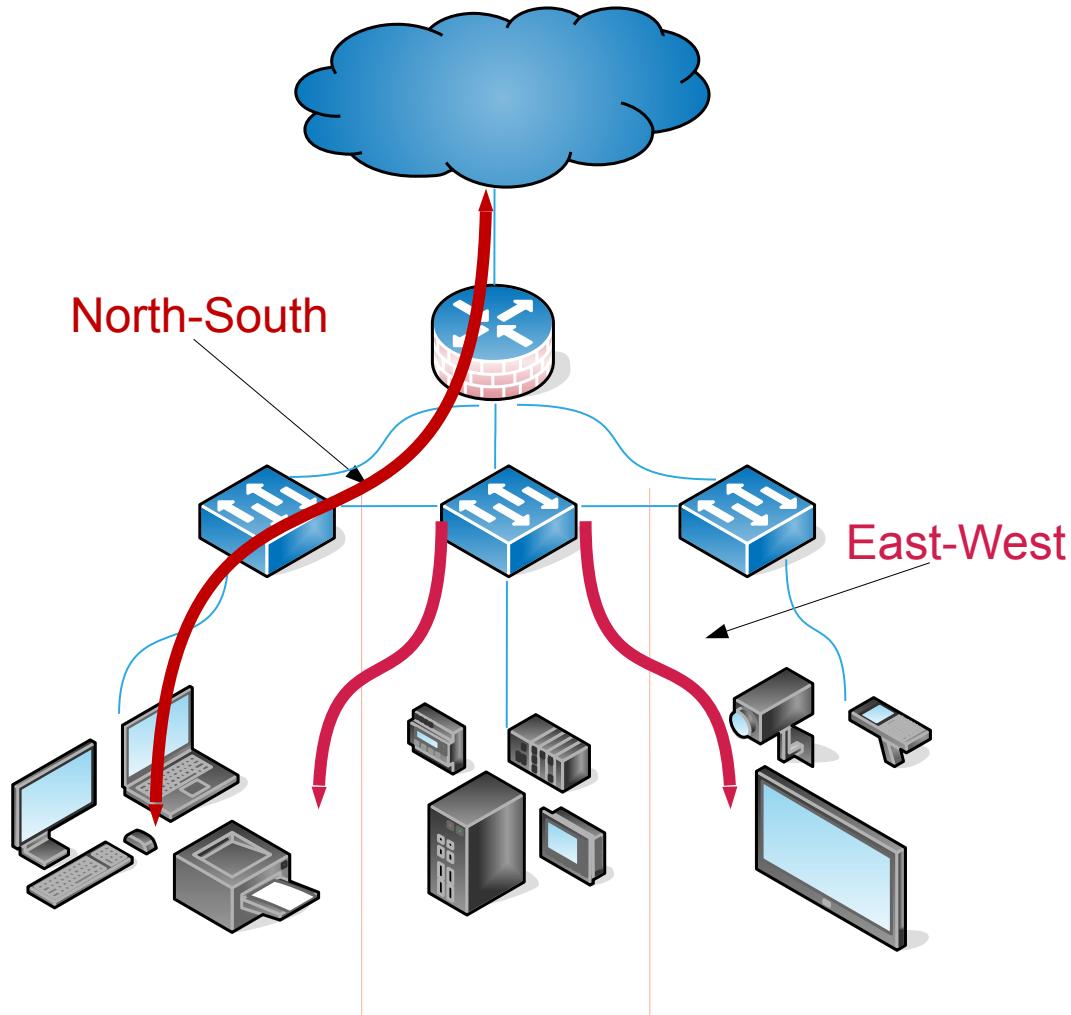
Uninventoried Internal Source IPs			
IP Address	Site	Segment	Count
10.10.10.5	Cyberville	Battery Network	295
192.168.95.128	-	-	30
10.10.30.129	Cyberville	Wind Turbine Network	11
192.168.0.129	Cyberville	Solar Panel Network	10
10.10.100.50	Cyberville	Substation Network	10
192.168.95.1	-	-	9
10.0.0.133	Cyberville	Site Office Network	9
10.0.0.120	Cyberville	Site Office Network	8
10.0.0.40	Cyberville	Site Office Network	8
192.168.95.134	-	-	6

Uninventoried Internal Destination IPs			
IP Address	Site	Segment	Count
192.168.95.1	-	-	31
192.168.95.254	-	-	26
192.168.0.255	Cyberville	Solar Panel Network	24
10.10.10.255	Cyberville	Battery Network	18
192.168.0.129	Cyberville	Solar Panel Network	11
10.10.30.131	Cyberville	Wind Turbine Network	11
10.0.0.128	Cyberville	Site Office Network	9
10.0.0.40	Cyberville	Site Office Network	8
10.0.0.120	Cyberville	Site Office Network	6
10.10.255.255	-	-	5

Uninventoried Internal Assets - Logs												
Time	network.transport	network.protocol	event.provider	event.dataset	source.segment.name	source.oui	source.ip	destination.segment.name	destination.oui	destination.ip	event.id	
> Apr 28, 2020 @ 03:20:09.973	tcp	smb	suricata	alert	Battery Network	-	10.10.10.5	Battery Network	-	10.10.10.10	83713027856898	
> Apr 28, 2020 @ 03:20:09.973	tcp	smb	suricata	alert	Battery Network	-	10.10.10.5	Battery Network	-	10.10.10.10	83713027856898	
> Apr 28, 2020 @ 03:20:09.973	tcp	-	zeek	conn	Battery Network	VMware, Inc.	10.10.10.5	Battery Network	RuadedCom Inc.	10.10.10.10	CcfCMn2Jff01JL	



Survey East-West and North-South Traffic



network.direction field

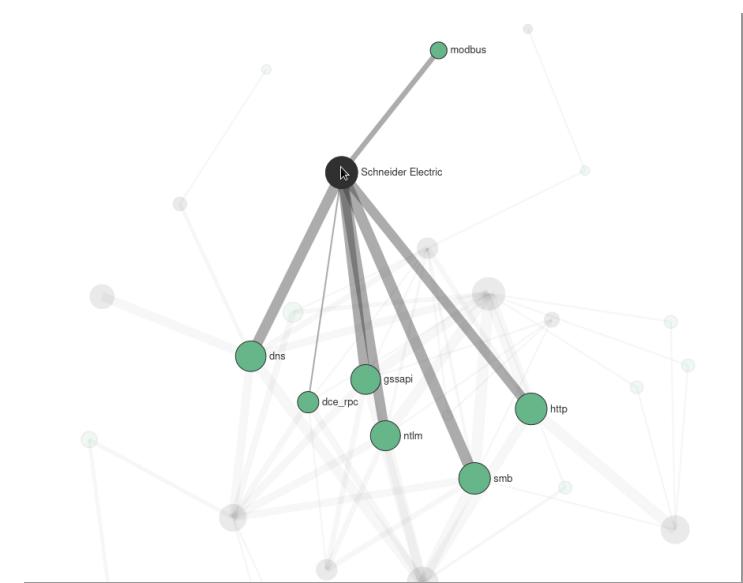
- **internal**: East-West
- **inbound**: “Southbound”
- **outbound**: “Northbound”

Review Observed Network Protocols

- Unsecure or outdated protocols
 - SSH < v2
 - TLS < v1.2
 - NTP < v4
 - VNC < v3.8
 - RDP < v6
 - LDAP < v3
 - FTP/TFTP
 - SMB < v3
 - telnet/rlogin/rsh
 - etc.
- Unexpected protocols (traffic that should not be present in a network segment)
 - IPv6
 - DNS
 - DHCP
 - Remote desktop
 - Automatic software updates

Outdated/Insecure Application Protocols		
Application Protocol	Protocol Version	Count
smb	1	124,835
ftp	-	3,099
tls	TLSv10	422
tls	TLSv11	253
tls	-	239
ntp	3	90
tftp	-	84
snmp	1	59
snmp	2c	31
telnet	-	10

Vulnerabilities	
Data Source	Log Type
zeek	notice
zeek	notice
suricata	alert
suricata	alert
zeek	notice
suricata	alert



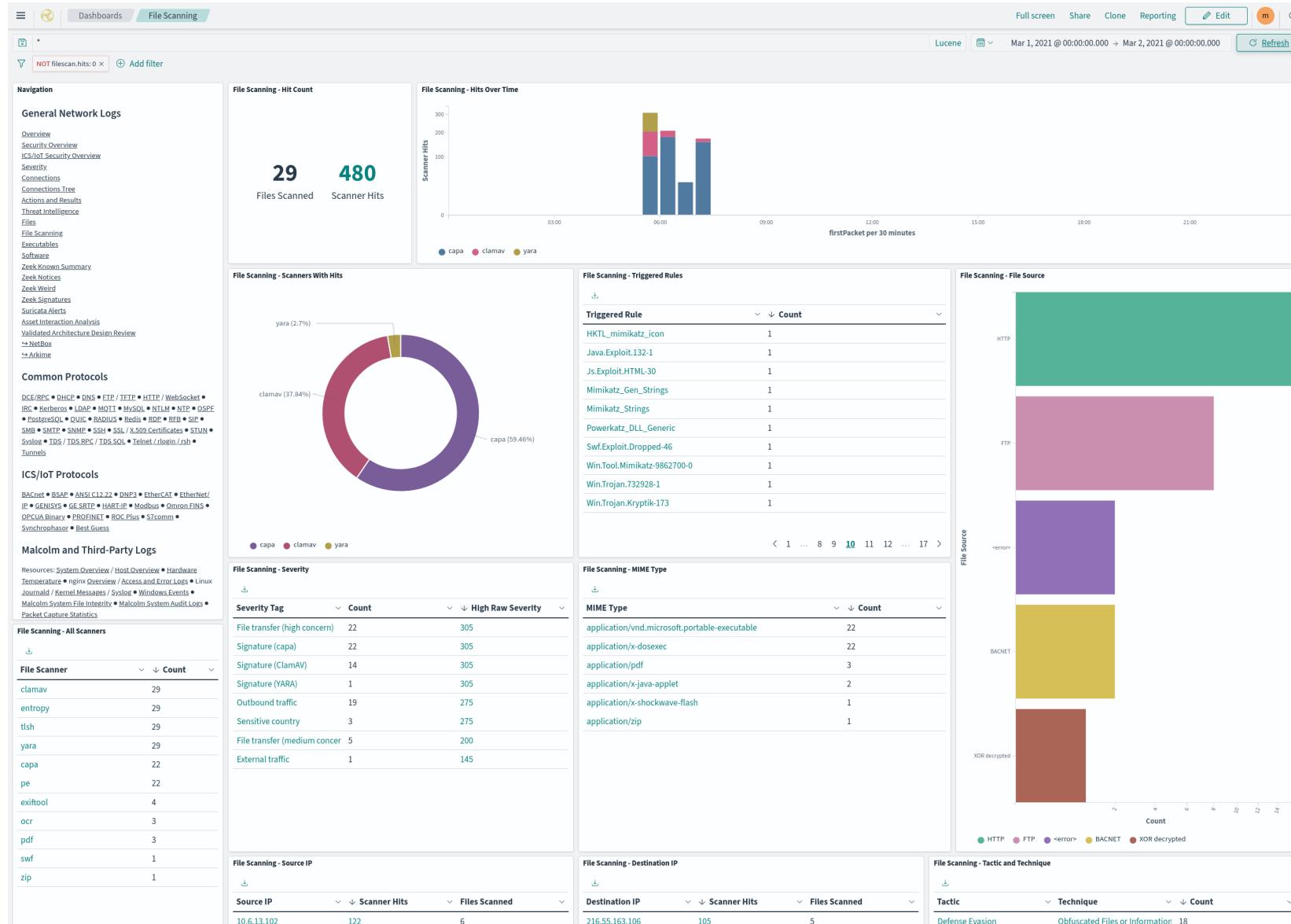
Investigate Suspicious File Transfers

- File transfers are detected in network traffic
 - SMB/CIFS (Windows file shares)
 - SMTP (Email)
 - HTTP (Web downloads)
 - etc.
- Files automatically extracted by Zeek and scanned with Strelka
 - YARA - general-purpose scanner to identify and classify malware
 - ClamAV - antimalware toolkit able to detect many types of malware, including viruses
 - capa - executable capabilities analyzer
 - Dozens of other customizable scanners



File Scanning Dashboard

Summarizes hits from file scanning engines and provides full Strelka scan reports for files extracted from network traffic.



File Transfers: Preserved Files

Files identified as potentially malicious are flagged and optionally preserved for further investigation

HTTP-F0joG01ZpxOl9fc...	text/plain	9.1KiB	HTTP	Cbr24h1HZxRCaZTFkc F0joG01ZpxOl9fcSN8	2024-08-01 17:11:09
HTTP-F0xURA1fatUCF6x...	application/octet-stream	200.0B	HTTP	CP83GU157AS9a3MMG5 F0xURA1fatUCF6xke6	2024-08-01 17:06:49
HTTP-F1AUDG3YVEB45Pl...	application/x-executable	2.5MiB	HTTP	CKI3cA387MUBTT3hG9 F1AUDG3YVEB45Plu3	2024-08-01 17:19:48
HTTP-F1CbYm1PWuPjHV3...	text/html	6.9KiB	HTTP	CSxEQV3MW30sI3U5sh F1CbYm1PWuPjHV3hEc	2024-08-01 17:09:40
HTTP-F1GA1N2fe1qQo4p...	application/octet-stream	160.0B	HTTP	C8gQXv40SN245pNi4d F1GA1N2fe1qQo4pd93	2024-08-01 17:38:03

200 packets ▾ natural ▾ Packet Options ▾ Src Dst UnXOR Brute GZip Header UnXOR Unbase64

Source (10.10.10.5:3453)

```
GET /__utm.gif HTTP/1.0
Accept: /*
Cookie: tJDITvSBUfmkbw6PCGOUWJ8BLelApsLN4/NnJAtbb1cCAso8DUXqXgxUEjENFDZkSYkWM/Udc9Hk9Z1+3heBnnGwJtTDeuEgdLkts52v
/XIKfTHiEXKvakotKJYevVY4tWeQjh5waD8mFQYSIYeZ2v7Ws7DdHyOCzKooJaEwg8=
Host: [F14G-c2-host-header]
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Connection: Keep-Alive
Pragma: no-cache
```

Destination (10.10.10.11:80)

```
HTTP/1.1 200 OK
Date: Mon, 20 Apr 2020 20:22:44 GMT
Content-Type: application/octet-stream
Content-Length: 160

__utm.gif
```

Extracted File Downloads	Click the zeek.files.extracted_uri value to download the file, if available.	192.168.1.31 33	3
Complete Scan Results	Some scan result fields aren't indexed. Expand a document and click JSON to view the full data in the strelka field.	192.168.146.1 32	2
File Scanning - Logs		192.168.106.131 27	7
Time	source.ip	destination.ip	file.mime_type zeek.files.filename
> Mar 1, 2021 @ 07:06:16.928	10.0.52.164	204.152.184.134	application/x-dosexec, 00_2.0.0_Win32Intel_in
			application/vnd.micros oft.portable-executabl e
> Mar 1, 2021 @ 07:03:45.422	10.0.52.164	61.8.0.17	application/x-dosexec, 00_2.0.0_Win32Intel_in
			application/vnd.micros oft.portable-executabl e
> Mar 1, 2021 @ 07:00:56.237	10.0.2.15	212.98.162.62	application/x-dosexec, KB971033.exe
			application/vnd.micros oft.portable-executabl e
> Mar 1, 2021 @ 07:00:53.373	10.0.2.15	83.69.233.156	application/x-dosexec, calc.exe
			application/vnd.micros oft.portable-executabl e

Examine Sensitive Unencrypted Data

- Observed cleartext credentials are normalized (e.g., **related.user** and **related.password**) for ease of locating them across protocols
- Arkime Hunt feature can deep-packet search session payloads for strings, hex codes, or regular expression matches

The screenshot shows the Arkime application interface. At the top, there's a navigation bar with links like Sessions, SPIView, SPIGraph, Connections, Hunt, Files, Stats, History, and Settings. Below the navigation bar is a search bar with the query "protocols == http". Underneath the search bar are buttons for "All (careful)", "Start" (set to 1969/12/31 17:00:00), "End" (set to 2023/01/12 10:24:28), "Bounding", and "Last Packet". A message says "Creating a new packet search job will search the packets of 6,511 sessions." There's a green button labeled "Create a packet search job". On the right side of the interface, there are page navigation buttons (1, 2, 3, etc.).

In the main area, there's a progress bar indicating "Running Hunt Job: HTTP with password by tlacuache" at 88.7%. Below the progress bar is a "Hunt Job Queue" table with columns: Status, Matches, Name, User, Search text, Notify, Created, and ID. One entry in the queue is "HTTP with password" by user "tlacuache" with 137 matches, created on 2023/01/12 10:24:55, and ID "ezADp4UBDnyT0P6PZAK4". To the right of the table are several small icons for managing the hunt job.

At the bottom of the interface, there are three informational messages:

- This hunt is running
- No description
- Found 137 sessions matching password (ascii) of 5,773 sessions searched
- Still need to search 738 of 6511 total sessions

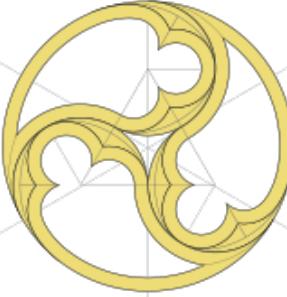
Clear-text Transmission of Passwords		
Application Protocol	Username	Count
ftp	anonymous	1,414
http	Login	102
http	maint	88
ftp	ind@psg420.com	20
ftp	DWSDataXfer	8
ftp	salesxfer	5
ldap	nginx_bind_dn@localdomain.lan	4
http	Unknown	4
ftp	sean@infosecs.cf	3
telnet	fake	2

Towards the Future

- Hunt- and IR-focused analytics and correlation capabilities
- Support generic (Sigma) rules and analytics
- Cross-reference against Common Security Advisory Framework (CSAF) and KEV (Known Exploited Vulnerabilities) catalog
- Improve cloud deployment
- Improve upgrade workflow
- Revamp installation/configuration tool with GUI
- Distributed rule/policy management for network sensors
- Explore the possibility of ML/AI/LLM integrations
- Improve integration and correlation of third-party and host logs
- Increase OT/ICS protocol support



Malcolm



Thank you!

Visit [Malcolm on GitHub](#) to read
the docs, make suggestions,
report issues and st★r to show
your support!