

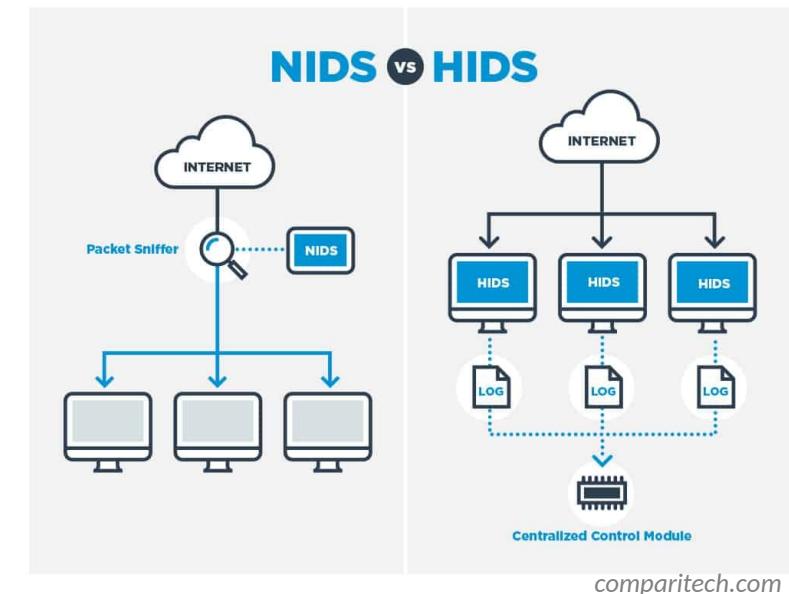
Network Traffic Analysis with **Malcolm**

A faint watermark of the Malcolm logo is visible behind the word 'Malcolm'. The logo consists of a stylized yellow 'M' shape containing a circular emblem with three interlocking rings.

Seth Grover, Malcolm developer • 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 a connection between two log files: `conn.log` and `http.log`. A red arrow points from the `conn.log` table to the `http.log` table, indicating that data from `conn.log` is being used as input for `http.log`.

conn.log IP, TCP, UDP, ICMP connection details		
FIELD	TYPE	DESCRIPTION
to	time	Timestamp of the first packet
uid	string	Unique ID of the connection
orig_ip_n	addr	Originating IP address string
orig_ip_p	port	Originating IP address PORT/UDP port for ICMP/other
resp_ip_n	addr	Responding IP address string
resp_ip_p	port	Responding IP address PORT/UDP port for ICMP/other
proto	proto	Transport layer protocol of connection
service	string	Selected application protocol, if any
duration	interval	Connection length
orig_bytes	uint64	Byte payload bytes from sequence numbers of TCP
resp_bytes	uint64	Byte payload bytes from sequence numbers of TCP
state.state	string	Connection state (see <code>conn.state</code>)
host.orig	host	IP of the client, netID
host.resp	host	IP of the destination, netID
received_pkts	uint64	Number of bytes received due to current connection (see <code>conn.state</code> , <code>host</code>)
history	string	Connection state history (see <code>conn.state</code> , <code>host</code>)
orig_pkts	uint64	Number of Orig. packets
orig_to_bytes	uint64	Number of Orig. IP bytes (see IP total, <code>orig_header.bytes</code>)
resp_pkts	uint64	Number of Resp. packets
resp_to_bytes	uint64	Number of Resp. IP bytes (see IP total, <code>orig_header.bytes</code>)
tcp_header	tcp	If tunnelled, connection-TO of encapsulating connection
orig_ip_addr	string	Low-layer address of the originator
resp_ip_addr	string	Low-layer address of the responder
site	int	The user ID# for this connection
inet_ifname	str	The inner IFNAME for this connection

http.log HTTP request/reply details		
FIELD	TYPE	DESCRIPTION
to	time	Timestamp of the HTTP request
req_id_n	string	Underlying connection info - see <code>conn.log</code>
trans_depth	uint64	Protocol depth into the connection
method	string	HTTP Request verb (GET, POST, etc.)
host	string	Name of the host header
uri	string	URI used in this request
referer	string	Value of the "Referer" header
user_agent	string	Value of the "User-Agent" header
response_body_hex	string	Uncompressed content value of the data response body hex
status_code	uint64	Status code returned by the server
status_msg	string	Status message returned by the server
info_code	uint64	Last error from HTTP reply by server
info_msg	string	Last error from HTTP reply message by server
tags	set	Indicators of various activities discovered
last_error	string	Timestamp of last error is detected
password	string	Timestamp of user auth is performed
process	set	Headers initiation of a process request
orig_host	vector	The unique Origin-Host
orig_header_name	vector	The names from Origin-Header
orig_header_type	vector	The types from Origin-Header
resp_header_name	vector	The names from Resp-Header
resp_header_type	vector	The types from Resp-Header
client_header_name	vector	The names of HTTP headers sent by client
server_header_name	vector	The names of HTTP headers sent by itself
cookie_name	vector	Variable names extracted from cookie
cf_cookie	vector	Variable names extracted from the URL
cf_params	vector	HTTP Header parameters is needed
cf_params_and_actions	vector	HTTP Header and actions are needed

files.log File analysis results		
FIELD	TYPE	DESCRIPTION
id	int	Resource identifier for each resource
file	string	Unique identifier for average file
is_header	bool	Boolean that indicated if the data
is_header	bool	Boolean that indicated if the data
content_size	int	Content size (in bytes) for which the transferred
resource	string	Unique identifier of the resource of the file data.
depth	count	Depth of the related resource
analysis_id	int	ID of the element which is performing the analysis
storage_type	string	The type of storage containing the file's signatures
filename	string	Filename, Extension, and file type
duration	interval	The duration that the file was analyzed
local_path	bool	Did the file originate locally?
is_dir	bool	Was the file a directory or a file?
used_space	float	Number of bytes consumed by the analysis engine
total_space	float	Total number of bytes that should comprise the file
missing_bytes	float	Number of bytes in the file that were missing
overflows_bytes	float	Out-of-bounds bytes in the stream due to overflow
streamed	bool	If the file analysis timed out at their source
parent_file	string	Container of the ID this was extracted from
modified	string	MD5Hash hash of the file
extracted	string	Local filename of download files, if any exist
entropy	double	Information density of the file contents

pe.log Portable Executable (PE)		
FIELD	TYPE	DESCRIPTION
is	bool	Current processing
pe	string	The file path or file name needed to be converted
machines	string	The target machine that the file was converted for
convertible_to	bool	This shows that the file was created at
os	string	The required operating system
dependencies	string[]	The dependencies that are required for run this file
is_dotnet	bool	Is the file a .NET executable or just an assembly file?
is_dll	bool	Is this file a DLL or an executable?
is_executable	bool	Does the file support .NET native? (Based on assembly extension)
is_dotnet_executable	bool	Does the file support .NET native (.NET Framework)?
is_dotnet_assembly	bool	Does the file support .NET native (.NET Core)?
is_dotnet_dll	bool	Does the file support .NET native (.NET Framework)?
has_property_table	bool	Does the file have an .NPX property table?
has_property_table2	bool	Does the file have an .NPX property table?
has_dotnet_table	bool	Does the file have an .NPX dotnet property table?
has_sharing_table	bool	Does the file have a sharing table?
section_names	string	The names of the sections, in order

corelight.com

Network Protocols

- conn - Network session tracking
 - Identified by session 4-tuple (originating IP:port, responding IP:port)
 - One session (line in a log file) for every IP connection
 - Unique identifier (UID) ties lines from other logs to a session
- http , modbus , ftp , dns, etc.
 - Protocol-specific log files created as traffic is seen
 - Contain application-layer metadata about network activities

Files

- files - File analysis results
 - Each transferred file identified with FUID
 - Associated with connection UID(s) over which file was transferred
 - File name, mime type, file size, etc. provided when available
- pe - Analysis of Portable Executable (PE) files
 - Target platform, architecture, OS, etc. for executables transferred across the network
- x509 - Analysis of X.509 public key certificates

Detection

- notice - Zeek concept of “alarms,” notices draw extra attention to an event
 - Conn::Content_Gap, DNS::External_Name, FTP::Bruteforcing, Heartbleed::SSL_Heartbeat_Attack, HTTP::SQL_Injection_Attacker, Scan::Address_Scan, Scan::Port_Scan, Software::Vulnerable_Version, SSH::Password_Guessing, SSL::Certificate_Expired, Weird::Activity, ...
 - <https://docs.zeek.org/en/stable/zeek-noticeindex.html>

Detection (cont.)

- weird - Unexpected network-level activity
 - > 150 weirdness indicators across many protocols
 - <https://docs.zeek.org/en/stable/scripts/base/frameworks/notice/weird.zeek.html#id1>
- signatures - Signature matches, including hits from enabled carved file scanners like ClamAV, YARA and capa

Network Observations

- Periodic dump of entities seen over the last day
 - known_certs - SSL certificates
 - known_devices - MAC addresses
 - known_hosts - Hosts with TCP handshakes
 - known_modbus - Modbus masters and slaves
 - known_services - Services (TCP “servers”)
 - software - Software being used on the network (e.g., Apache, OpenSSH, etc.)
 - Could be used for identifying vulnerable versions of software or firmware



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

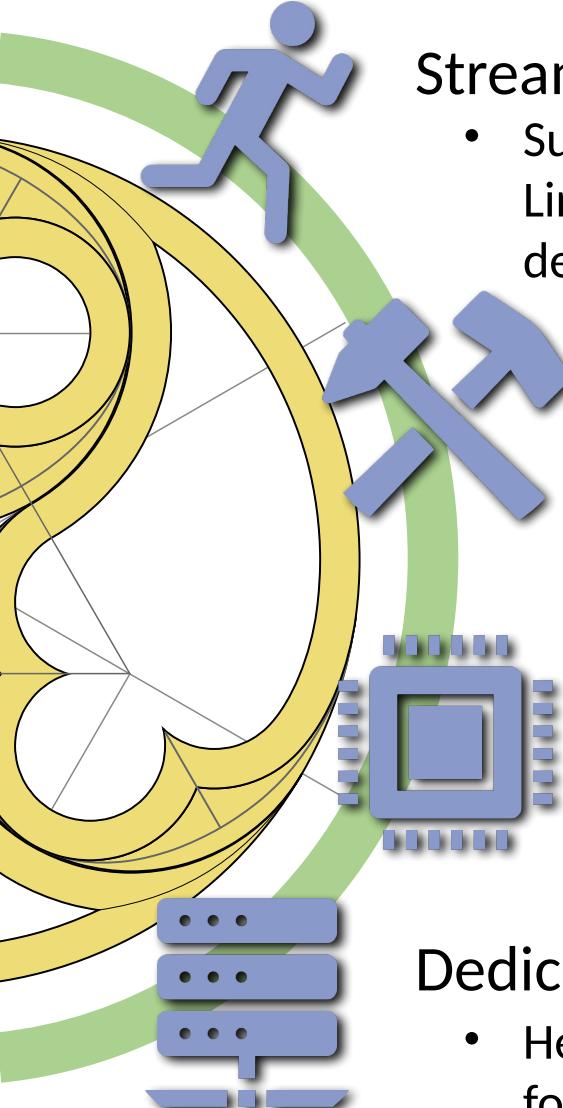
Weaknesses

- No 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 on Linux, macOS and Windows platforms. ISO installer for bare metal installations. Cloud-deployable with Kubernetes. Provides easy-to-use web-based user interfaces.

Industry-standard tools

- Uses Arkime and Zeek for network traffic capture, Logstash for parsing and enrichment, OpenSearch for indexing and Dashboards, and Arkime Viewer for visualization. Also leverages OpenSearch Anomaly Detection, Suricata IDS, YARA, capa, ClamAV, CyberChef, and other proven tools for analysis of traffic and artifacts.

Expanding control systems visibility

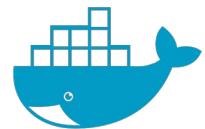
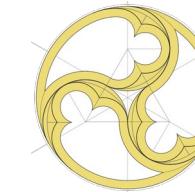
- Analyzes more protocols used in operational technology (OT) networks than other open-source or paid solutions. Ongoing development is focused on increasing the quantity and quality of industrial control systems (ICS) traffic.

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 on project (later dubbed “Malcolm”) as part of USBR/CISA work agreement
- 2018.Q3 to 2019.Q2 – Malcolm field tested in deployments at USBR facilities
- 2019.Q2 – Initial public release
- 2019.Q4 – Hedgehog Linux released
- 2021.Q1 – 1k st★rs on GitHub
- 2021.Q4 – Migration from Elastic to OpenSearch
- 2022.Q3 – First Malcolm-based simulated engagements 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 added for network modeling and asset interaction analysis
- 2023.Q1 – Kali announces “Purple” distro bundling Malcolm
- 2023.Q2 – Cloud deployable with K8s



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.



Malcolm



Components

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



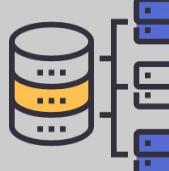
Capture &
Analysis



File Scanning



Forwarding &
Enrichment



Storage



Anomaly
Detection



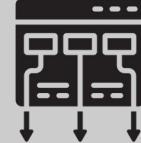
Asset
Management



Visualization



Payload
Analysis



Framework



TCPDUMP



fluentbit



logstash



beats



OpenSearch



Anomaly
Detection
Plugin



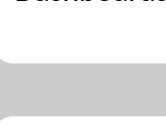
Alerting



Alerting
Plugin



netbox



OpenSearch
Dashboards



Arkime



CyberChef



docker



NGINX



kubernetes



Supported Protocols

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

Internet layer

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)

Genysis

Google Quick UDP Internet Connections
(gQUIC)

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)

Oracle

Open Platform Communications Unified Architecture (OPC UA) Binary

Open Shortest Path First (OSPF)

OpenVPN

PostgreSQL

Process Field Net (PROFINET)

Remote Authentication Dial-In User Service (RADIUS)

Remote Desktop Protocol (RDP)

Remote Framebuffer / Virtual Network Computing (RFB/VNC)

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)

WireGuard

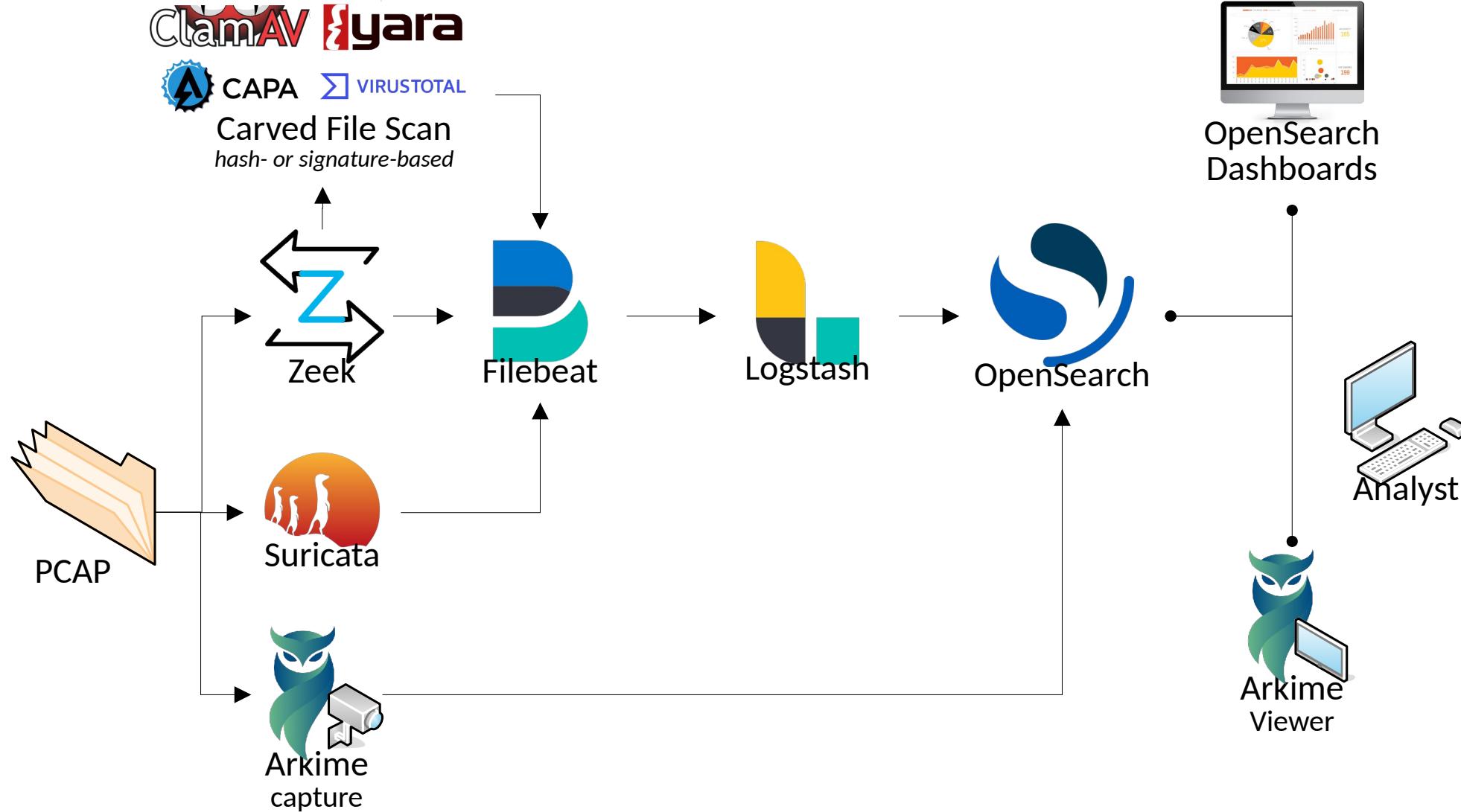
various tunnel protocols (e.g., GTP, GRE, Teredo, AYIYA, IP-in-IP, etc.)

* *Operational Technology (OT) protocols indicated with **bold***

Malcolm

Data Pipeline

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

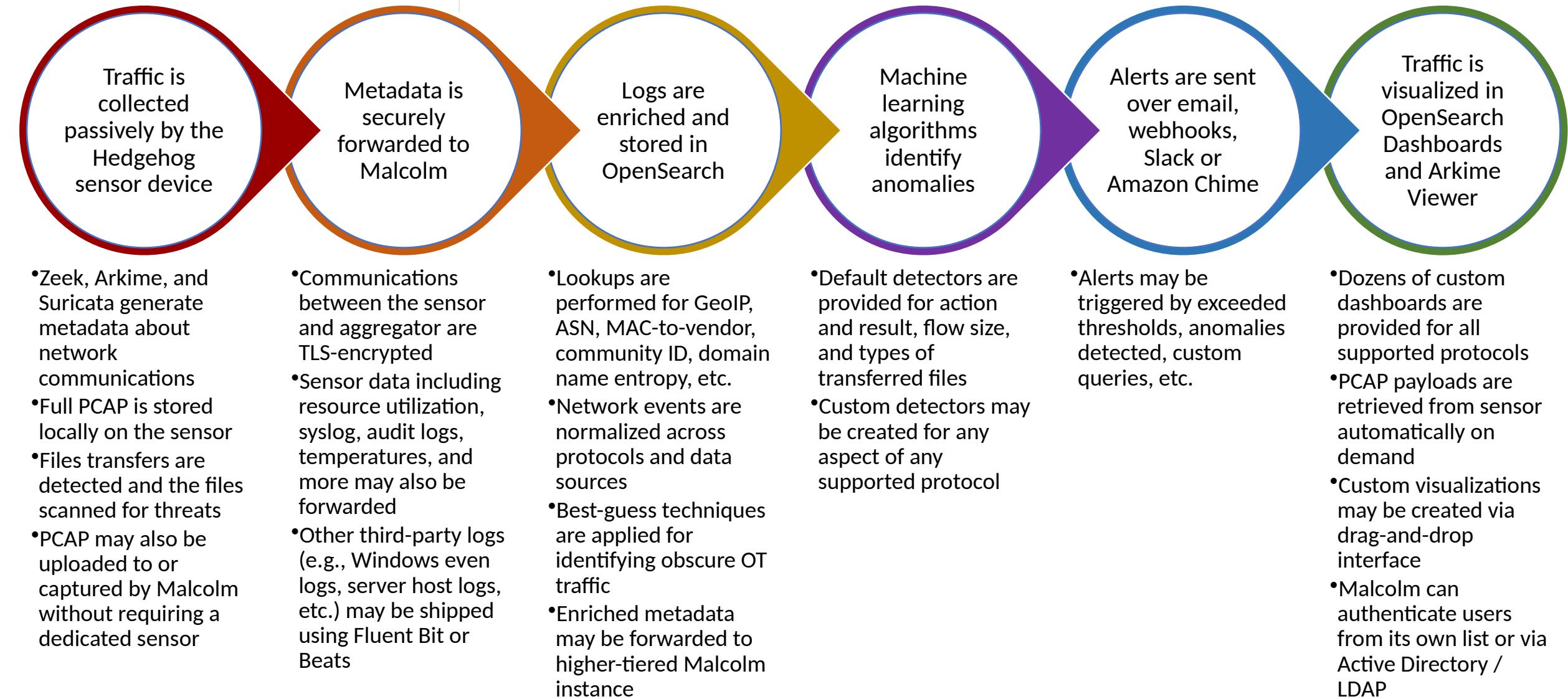


Malcolm



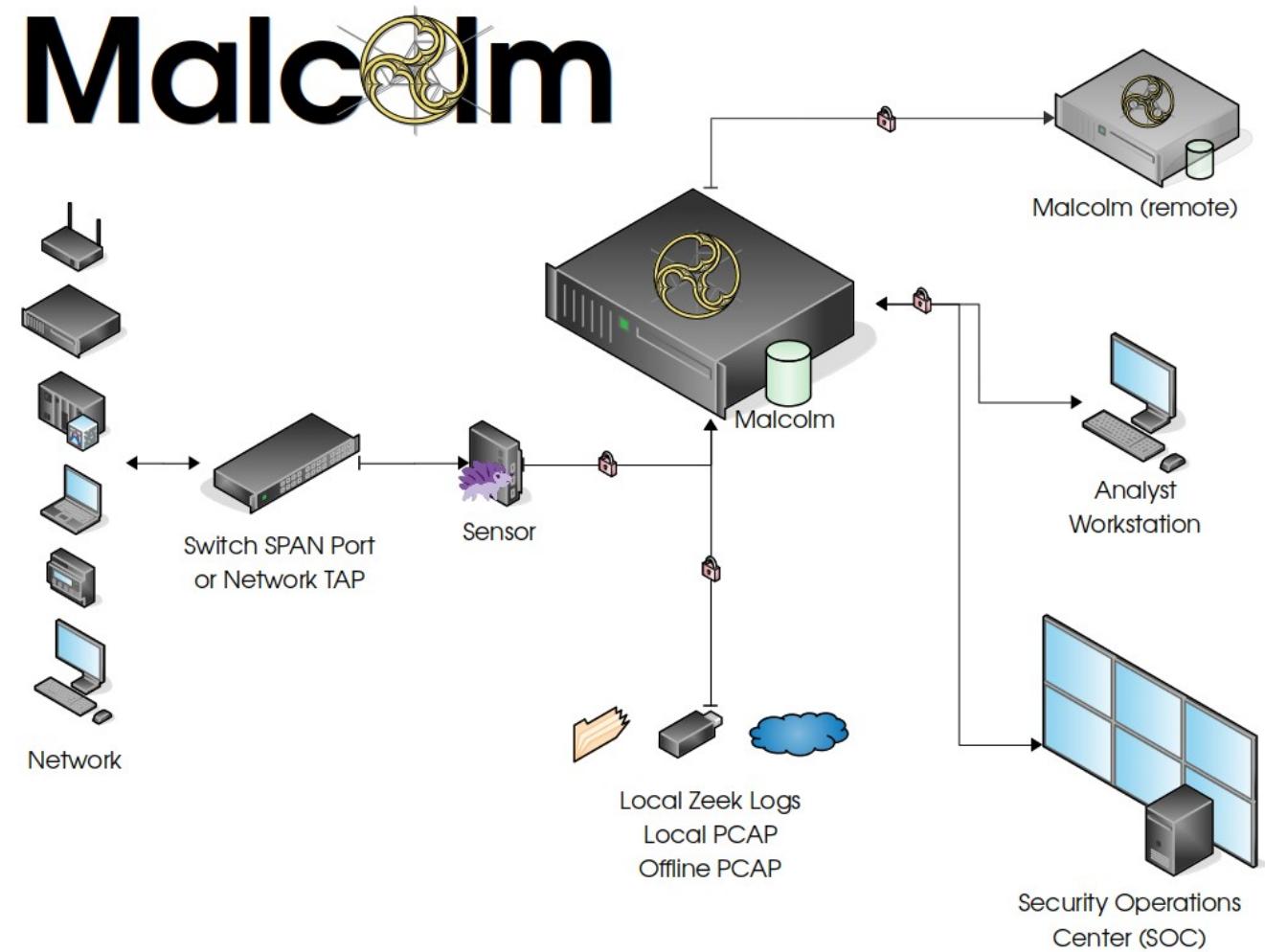
Data Pipeline

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



Configuring and Running Malcolm

- Runs natively in Docker, use ISO installer for VM or bare metal install, or cloud deploy with Kubernetes
- 16+GB RAM, 4+ 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”



Identifying Network Hosts and Subnets

- Assign custom names to network devices and subnets prior to PCAP import
- Allows identification of cross-segment traffic and network log enrichment
- Define in NetBox: <https://<host or IP>/netbox>

The screenshot displays the NetBox web interface, which is a powerful tool for managing network infrastructure. On the left, a sidebar navigation menu includes links for Organization, Devices, Connections, Wireless, IPAM, IP Addresses, IP Ranges, and ASNs. The IPAM section is currently active, showing a table for Prefixes with 6 results. The table columns include Prefix, Status, Children, VRF, Utilization, Tenant, and Site. A row for '10.10.10.0/24' is selected, showing details for the 'Battery Network'.

The main content area has two tabs: 'Prefixes' and 'Devices'. The 'Devices' tab is currently selected, showing a table with 32 results. The table includes columns for Name, Status, Tenant, Site, Location, Rack, Role, Manufacturer, Type, and IP Address. Several network hosts are listed, such as 'SolarHMI09', 'WINDHMI09', and various historian and modem units. Each device entry includes a 'Edit' icon.

Asset Interaction Analysis

Network Logs

Source Device Type			
Manufacturer	Type	Role	Count
Dell	PowerEdge	Historian	11,081
Digi	WR-21	Modem	650
Schneider Electric	-	HMI	288
Dell	Precision 3460	Workstation	245
Schneider Electric	-	SCADA	128
-	Virtual Machine	Server	86
Dell	Precision 3460	HMI	40
Dell	PowerEdge R640	Server	26
Dell	Precision 3460	SCADA	25
-	Virtual Machine	Historian	20

Export: Raw ▲ Formatted ▲

1 2 *

Traffic by Network Segment

Site	Direction	Source Segment	Destination Segment	Log Count	Total Packets	Total Bytes
Cyberville	Internal	Battery Network	Battery Network	1,187	160,478	155,259,285
Cyberville	Internal	Combined Cycle BOP	Combined Cycle BOP	11,059	66,463	12,094,546
Cyberville	Internal	Solar Panel Network	Solar Panel Network	174	23,092	11,531,840
Cyberville	Internal	Site Office Network	Site Office Network	40	9,908	5,474,349
Cyberville	Internal	Wind Turbine Network	Wind Turbine Network	57	5,308	2,495,593
Cyberville	Internal	Battery Network	-	180	889	221,930
Cyberville	Internal	Substation Network	Substation Network	5	1,789	114,302
Cyberville	Internal	Solar Panel Network	-	117	412	85,385
Cyberville	Internal	Wind Turbine Network	-	87	407	56,602
Cyberville	Internal	Combined Cycle BOP	-	25	79	23,296

Export: Raw ▲ Formatted ▲

1 2 3 *

Common Protocols

Destination Device Type			
Manufacturer	Type	Role	Count
Dell	PowerEdge R640	Server	11,008
Schneider Electric	-	SCADA	608
Digi	WR-21	Modem	371
Dell	Precision 3460	Workstation	226
Schneider Electric	-	SCADA	96
Dell	PowerEdge	Historian	85
RuggedCom	-	Server	51
Dell	Precision 3460	SCADA	34
-	Virtual Machine	Server	26
Dell	PowerEdge R310	SCADA	23

Export: Raw ▲ Formatted ▲

1 2 *

ICS/LoT Protocols

Source Device Role			
Role	Historian	Server	Modem
Historian	11,008	0	0
Server	0	180	0
Modem	0	0	371
HMI	0	0	85
Role	0	0	0
Workstation	0	0	226
SCADA	0	0	96
SCADA	0	0	0
Server	0	0	0

Destination Device Role

Role	Historian	Server	Modem
Historian	0	0	0
Server	0	180	0
Modem	0	0	371
HMI	0	0	85
Role	0	0	0
Workstation	0	0	226
SCADA	0	0	96
SCADA	0	0	0
Historian	0	0	0

Cross Segment Traffic

Protocol by Network Segment

Network Segment	Family	Transport	Protocol	Count
Battery Network	ip4v	tcp	http	536
Battery Network	ip4v	tcp	smbs	515
-	ip6v	udp	dns	264
Battery Network	ip4v	tcp	nttms	249
Battery Network	ip4v	tcp	grisapt	247
zeen	notice	Cyberville	Combined Cycle BOP	42

Notice, Alert and Signature by Network Segment

Provider	Dataset	Site	Network Segment	Category	Count
suricata	alert	Cyberville	Battery Network	Generic Protocol Command Decode	148
suricata	alert	Cyberville	Battery Network	Misc activity	144
suricata	alert	Cyberville	Solar Panel Network	Generic Protocol Command Decode	48
suricata	alert	Cyberville	Combined Cycle BOP	Generic Protocol Command Decode	47
zeen	notice	Cyberville	Combined Cycle BOP	ATTACK	42

Event Severity by Network Segment

Site	Network Segment	Severity Tag	Count	High Raw Severity
Cyberville	Site Office Network	Service on non-standard port	1	181
Cyberville	Site Office Network	Suricata Alert	2	181
Cyberville	Site Office Network	Insecure or outdated protocol	2	181
Cyberville	Wind Turbine Network	File transfer (high concern)	1	135
Cyberville	Wind Turbine Network	Notice (other)	7	135

	netbox	
	Organization	
	Devices	
	Connections	
	Wireless	
	IPAM	
IP ADDRESSES		
IP Addresses	 	
IP Ranges	 	
DEVICES		
Devices	 	
Modules	 	
Device Roles	 	
Platforms	 	
Virtual Chassis	 	
Virtual Device Contexts	 	
DEVICE TYPES		
Device Types	 	
Module Types	 	
Manufacturers	 	
DEVICE COMPONENTS		
Interfaces	 	
Front Ports	 	

Prefixes

Results 6 Filters

Quick search

Configure Table

Prefix	Status	Children	VRF	Utilization	Tenant	Site	VLAN	Role	Description
10.10.10.0/24	Active	0	Battery Network	7.1%	—	Cyberville	—	—	edit
192.168.0.0/24	Active	0	Solar Panel Network	1.6%	—	Cyberville	—	—	edit
10.10.20.0/24	Active	0	Combined Cycle BOP	2.0%	—	Cyberville	—	—	edit
10.10.100.0/24	Active	0	Substation Network	0.8%	—	Cyberville	—	—	edit

Search

guest

Devices

Results 32 Filters

Quick search

Configure Table

Name	Status	Tenant	Site	Location	Rack	Role	Manufacturer	Type	IP Address	
SolarHMI09	Active	—	Cyberville	—	—	HMI	Dell	Precision 3460	192.168.0.128/32	edit
WINDHMI09	Active	—	Cyberville	—	—	HMI	Dell	Precision 3460	10.10.30.130/32	edit
Battery HMI	Active	—	Cyberville	—	—	HMI	Schneider Electric	Unspecified	10.10.10.3/32	edit
Combined Cycle BOP Historian	Active	—	Cyberville	—	—	Historian	Dell	PowerEdge	10.10.20.5/32	edit
Substation Historian	Active	—	Cyberville	—	—	Historian	Unspecified	Unspecified	10.10.100.5/32	edit
Battery Historian	Active	—	Cyberville	—	—	Historian	Dell	PowerEdge	10.10.10.5/32	edit
Solar Panel Historian	Active	—	Cyberville	—	—	Historian	Dell	PowerEdge	192.168.0.5/32	edit
Cellular Modem	Active	—	Cyberville	—	—	Modem	Digi	WR-21	10.10.10.11/32	edit

Importing Traffic Captures for Analysis

- Specify tags for search and filter
- Enable Suricata and/or Zeek analysis and file extraction
 - Or configure as global defaults
- Upload PCAP files or archived Zeek logs
 - pcapng not supported yet
- <https://<host or IP>/upload>

The screenshot shows the Malc0lm web interface for capturing and analyzing network traffic. At the top right, the logo "Malc0lm" is displayed with a yellow circular emblem, followed by the text "Capture File and Log Archive Upload". Below the logo is a dark header bar with three buttons: "Add files..." (blue), "Start upload" (green), and "Cancel upload" (red). To the right of these buttons is a checkbox labeled "Select all". Underneath the header, there is a section for "Tags" with two green buttons: "Field Office" and "Incident XYZ", each with a delete icon. Below the tags are two checked checkboxes: "Analyze with Suricata" and "Analyze with Zeek". A dropdown menu for "Zeek File Extraction" is set to "Files with mime types of common attack vectors". The main area displays a list of six uploaded files, each with a progress bar and a "Start" button:

- acme_pcap-01.pcap (89.08 MB)
- acme_pcap-02.pcap (67.19 MB)
- acme_pcap-03.pcap (91.41 MB)
- acme_pcap-04.pcap (100.00 MB)
- acme_pcap-05.pcap (100.00 MB)
- acme_pcap-06.pcap (100.00 MB)

Each file entry has a green "Start" button on the right.

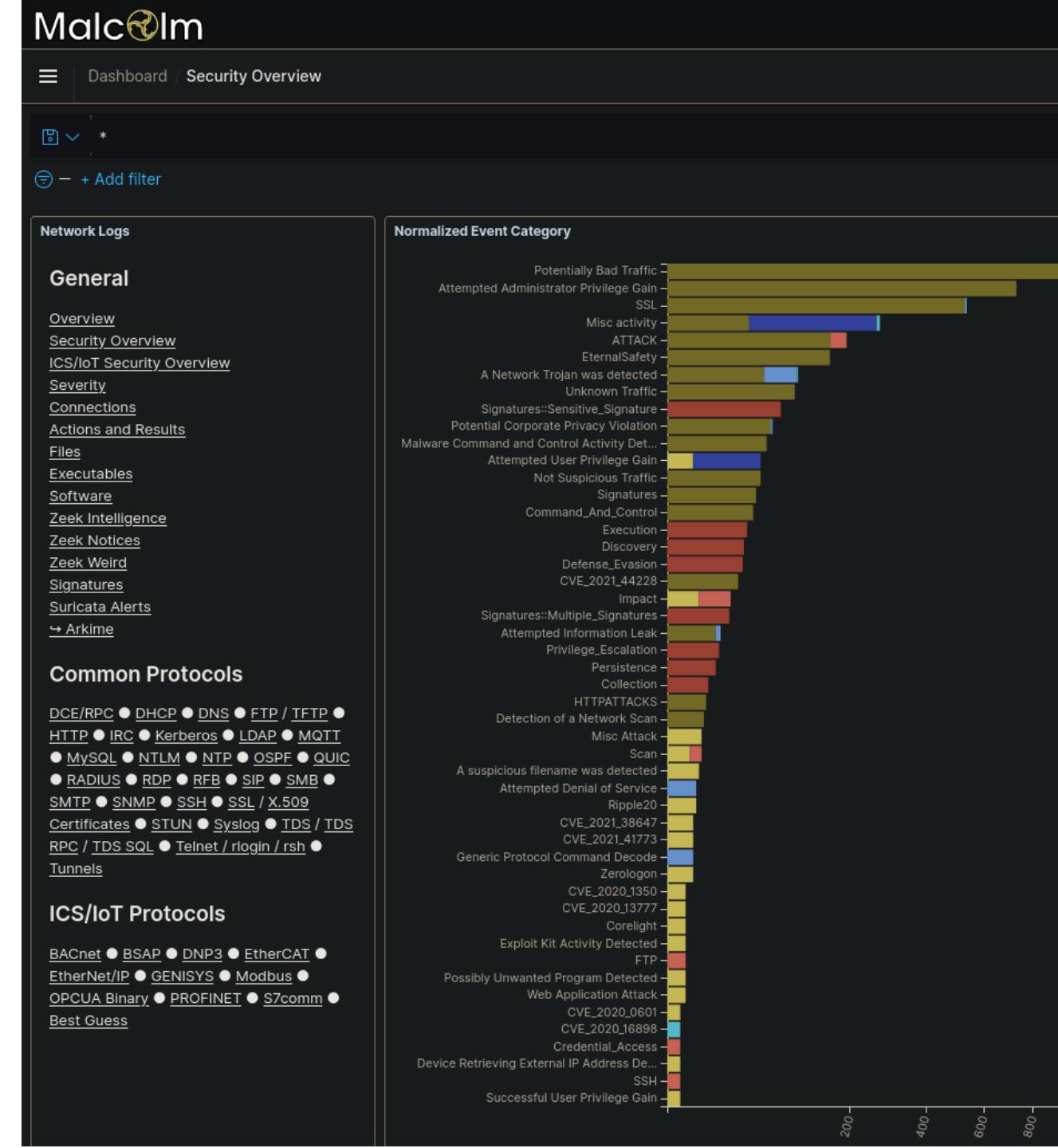
Data Tagging and Enrichment



- Logstash enriches Zeek and Suricata log metadata
 - MAC addresses to hardware vendor
 - GeoIP and ASN lookups
 - Internal/external traffic based on IP ranges
 - Reverse DNS lookups
 - DNS query and hostname entropy analysis
 - Connection fingerprinting (JA3 for TLS, HASSH for SSH, Community ID for flows)
- **tags field**
 - Populated for Arkime sessions, Zeek logs and Arkime alerts with tags provided on upload and words extracted from PCAP filenames
 - `ics`,
`ics_best_guess`,
`cross_segment`,
etc.

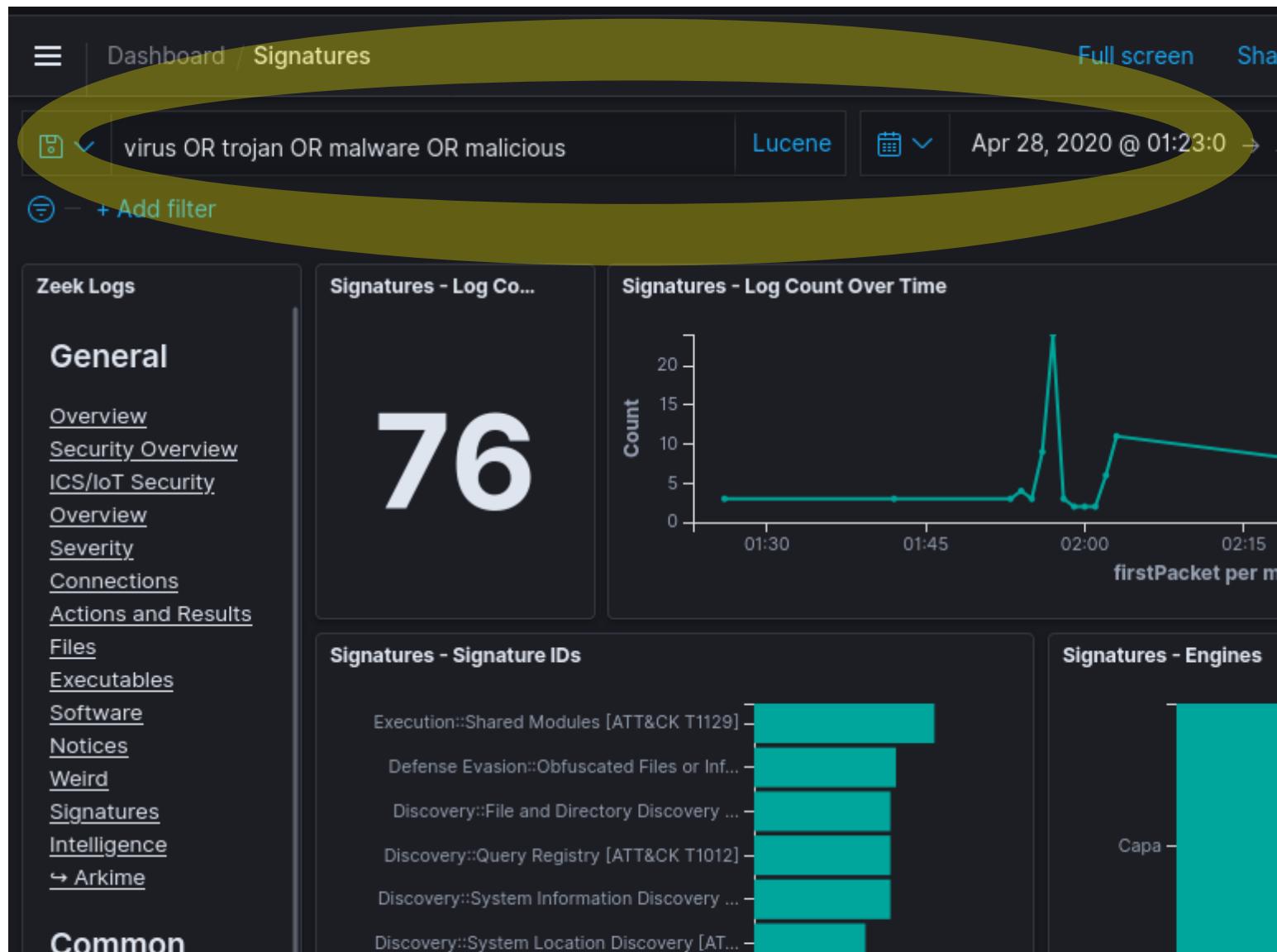
OpenSearch Dashboards

- Front end for Zeek logs and Suricata alerts
- Prebuilt visualizations for all protocols Malcolm parses
- WYSIWYG editors to create custom visualizations and dashboards
- Drill down from high-level trends to specific items of interest
- <https://<host or IP>/dashboards>



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

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 / TDSX](#)

Normalized Event Categories

Protocol

Attempted Administra

A Network T

Signatures::

Potential Corpora

Malware Command and C

Attempted

No

Com

Signatures::

Attempted

Detec

A suspicious file

Attempted

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

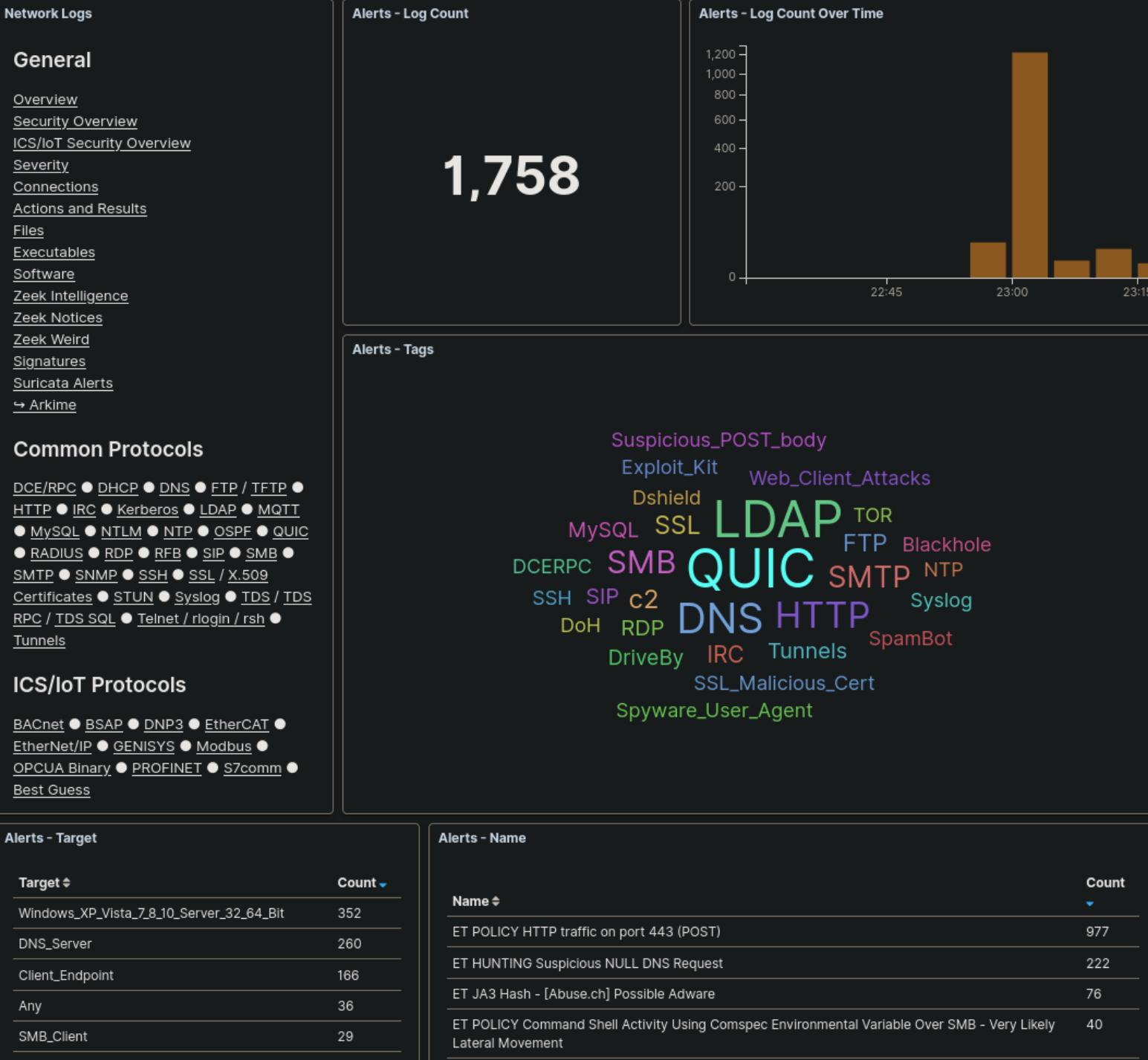
Notices - Log Count Over Time

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

Malcolm

Dashboard | ICS/IoT Security Overview

Full screen Share Clone Reporting

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	-	NUL_in_line
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
suricata	alert	Unknown Traffic	ET JA3 Hash - [Abuse.ch] Possible Adware
zeek	weird	-	
zeek	notice	ATT	Execution
suricata	alert	Atten Gain	
zeek	notice	Sign	
zeek	weird	-	
suricata	alert	Poter	

Zeek Logs

ICS/IoT Log Counts

ICS/IoT Traffic Over Time

ICS/IoT External Traffic

General

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

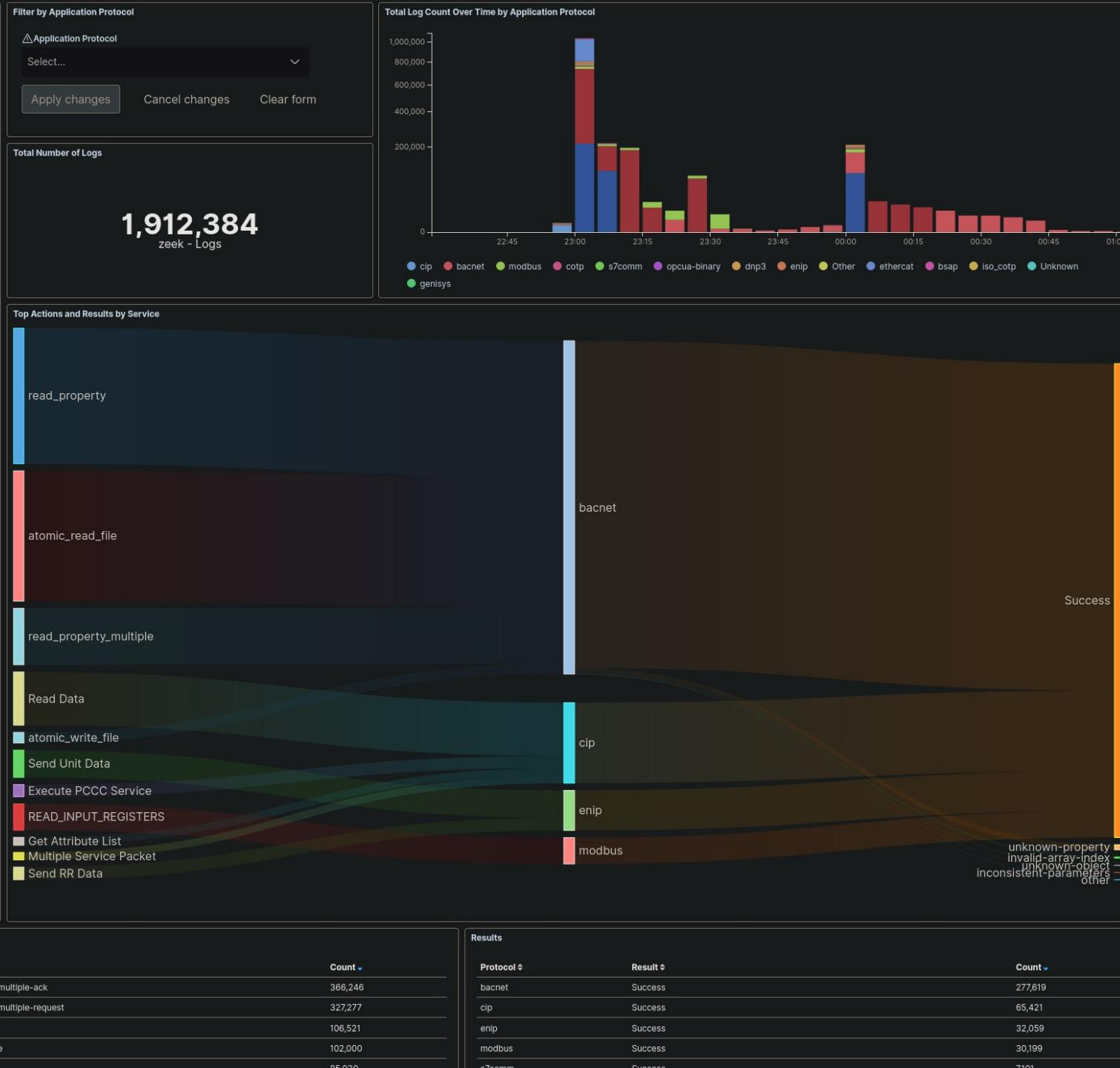
Common Protocols

- 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 • Modbus • PROFINET • S7comm • Best Guess

Network Layer



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
- ICS protocols
 - BACnet
 - BSAP
 - DNP3
 - EtherCAT
 - EtherNet/IP
 - GENISYS
 - Modbus
 - OPCUA Binary
 - PROFINET
 - S7comm
 - Synchrophasor (IEEE-C37.118)

[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

[BACnet](#) ● [BSAP](#) ● [DNP3](#) ● [EtherCAT](#) ●
[EtherNet/IP](#) ● [GENISYS](#) ● [Modbus](#) ●
[OPCUA Binary](#) ● [PROFINET](#) ● [S7comm](#) ●
[Best Guess](#)

Notices - Notice Type

Notice Category ▾

SSL

ATTACK

ATTACK

EternalSafety

Signatures

EternalSafety

ATTACK

EternalSafety

EternalSafety

ATTACK

Export: Raw  For

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

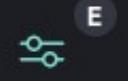


New Visualization

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.)

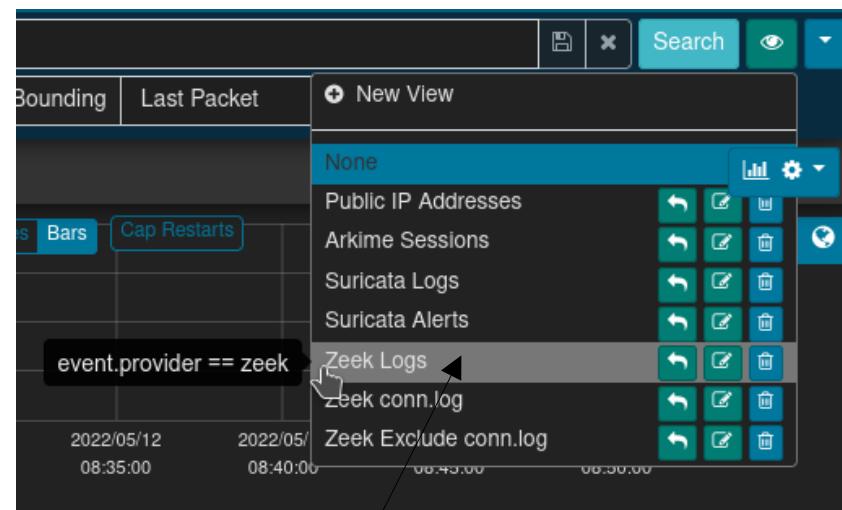
	Arkime	Dashboards (Lucene)	Dashboards (DQL)
GeolP information available	country == EXISTS!	_exists_:destination.geo OR _exists_:source.geo	destination.geo:* or source.geo:*
Log type	event.dataset == notice	event.dataset:notice	event.dataset:notice
IP CIDR Subnets	ip.src == 172.16.0.0/12	source.ip:"172.16.0.0/12"	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
GeolP information available	country == EXISTS!	_exists_:destination.geo OR _exists_:source.geo	destination.geo:* or source.geo:*



- Front end for **both** enriched Zeek logs, Suricata alerts and Arkime sessions
 - Malcolm's custom Arkime Zeek data source adds full support for Zeek 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
- <https://<host or IP>>

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



A screenshot of the Arkime interface. At the top, there is a navigation bar with links: Sessions, SPIView, SPIGraph, Connections, Hunt, Files, Stats, History, Settings, and Users. Below the navigation bar is a search bar containing the query "tags == Cyberville". Underneath the search bar are two time selection fields: "Custom" and "Start" (2020/04/27 23:58:59) and "End" (2020/04/28 03:30:23). To the right of these are buttons for "Bounding", "Last Packet", "Interval", and "Auto". The status bar shows "03:31:24".

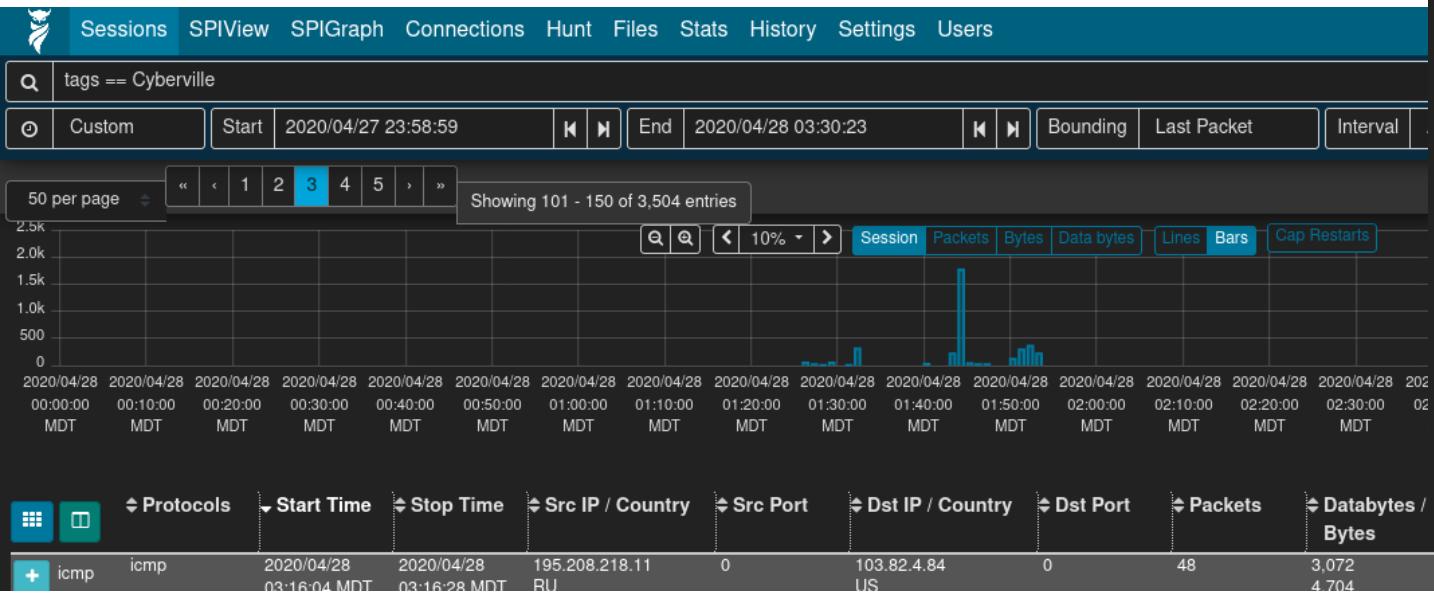
The main area features a timeline chart showing network traffic over time. A legend below the chart includes "Session", "Packets", "Bytes", "Data bytes", "Lines", "Bars", and "Cap Restarts". The chart displays several spikes in activity, notably around 2020/04/28 01:40:00 MDT. To the right of the chart is a world map with various regions highlighted in different shades of gray, indicating geographical context for the search results.

At the bottom, there is a detailed table of network events:

Protocol	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Tags	Info
icmp	2020/04/28 03:16:04 MDT	2020/04/28 03:16:28 MDT	195.208.218.11 RU	0	103.82.4.84 US	0	48	3,072 4,704	Cyberville	
icmp	2020/04/28 03:16:04 MDT	2020/04/28 03:16:28 MDT	195.208.218.11 RU	8	103.82.4.84 US	0	48	2,688 4,032	Cyberville external_source external_destination	

Sessions

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



The screenshot shows the Sessions interface with the following search parameters and results:

- Search Query:** protocols == http && tags == external_destination
- Log Type:** http
- Malcolm Data Source:** zeek
- Malcolm Node:** filebeat
- Showing 1 - 50 of 12,150 entries**
- Results (Selected):**
 - 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
 - File Magic: text/html

Zeek http.log

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. Version v3.1.1.
- Search Bar:** country != US && protocols == http. Includes a "Search" button and a "Arkime Sessions" dropdown.
- Filter Bar:** Custom, Start: 2021/02/28 23:59:11, End: 2021/03/01 00:28:26, Bounding, Last Packet, Interval: Auto, Duration: 00:29:15.
- Session View Buttons:** Open Items, Visible Items, Matching Items. Includes "Include same time period" and "linked segments (slow)" checkboxes, and a "Filename" field set to US_HTTP.pcap.
- Export Options:** An "Export PCAP" button is located on the right.
- Table Navigation:** Shows 50 per page, page 1 of 120 entries.
- Timeline:** A timeline chart showing packet counts over time from 2021/03/01 00:00:00 to 2021/03/01 00:28:00. It includes a zoom control (10%), search, and various data series selection buttons (Session, Packets, Bytes, Data bytes, Lines, Bars, Cap Restarts).
- Map:** A world map showing network traffic distribution.
- Session List:** Headers include Protocols, Start Time, Stop Time, Src IP / Country, Src Port, Dst IP / Country, Dst Port, Packets, Databytes / Bytes, Tags, and Info. One entry is shown: tcp, http, 2021/03/01, 2021/03/01, 10.0.52.164, 2550, 61.8.0.17, 80, 7,195, 5,160,414, HTTP, out-of-order-dst, 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)



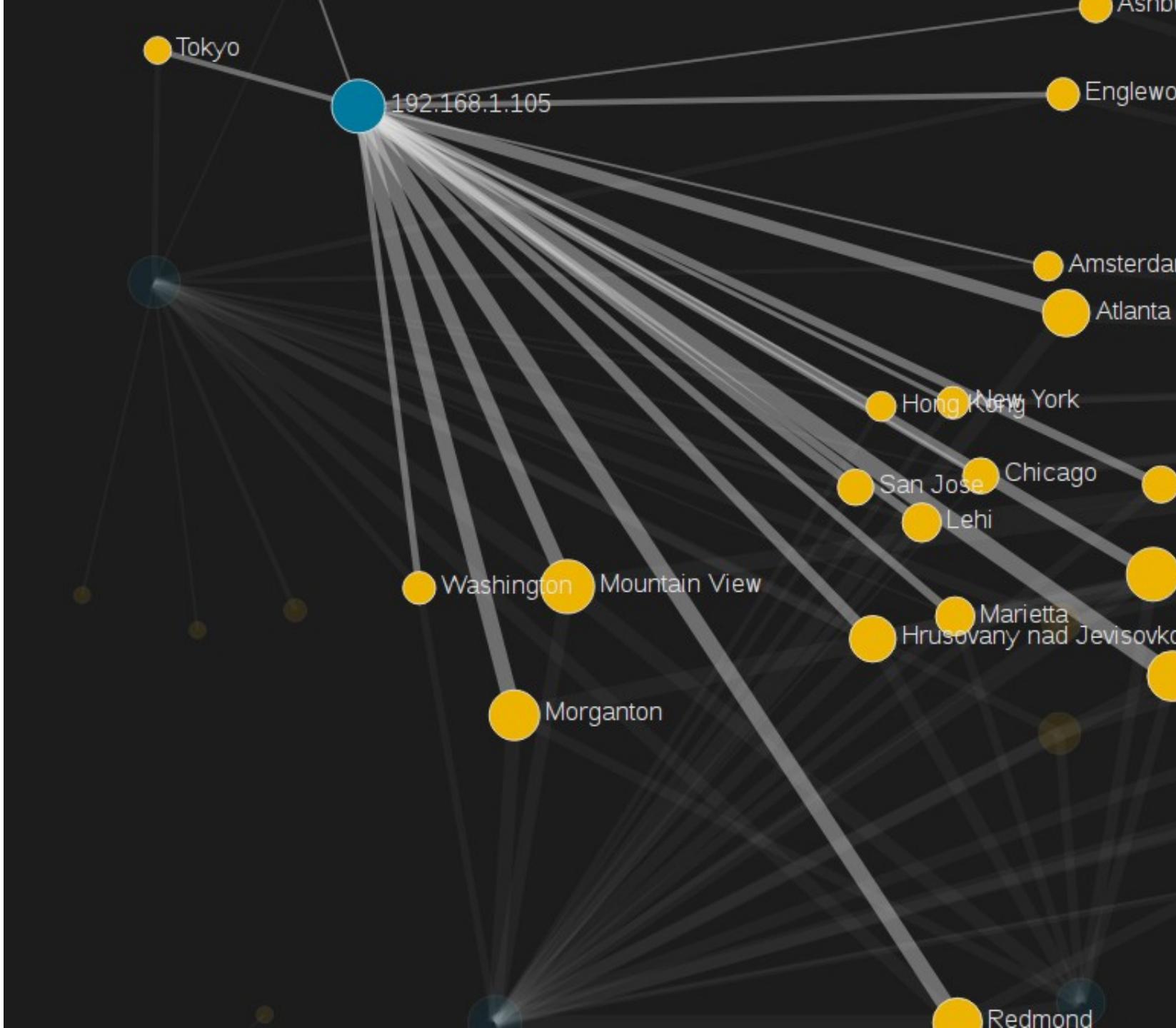
SPIGraph

- 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

Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings Users v3.1.1 ? ! 🔍

protocols == http Search Arkime Sessions

All (careful) Start 1969/12/31 17:00:00 End 2021/12/06 12:10:02 Bounding Last Packet

Creating a new packet search job will search the packets of 2,906 sessions. Create a packet search job

Hunt Job History

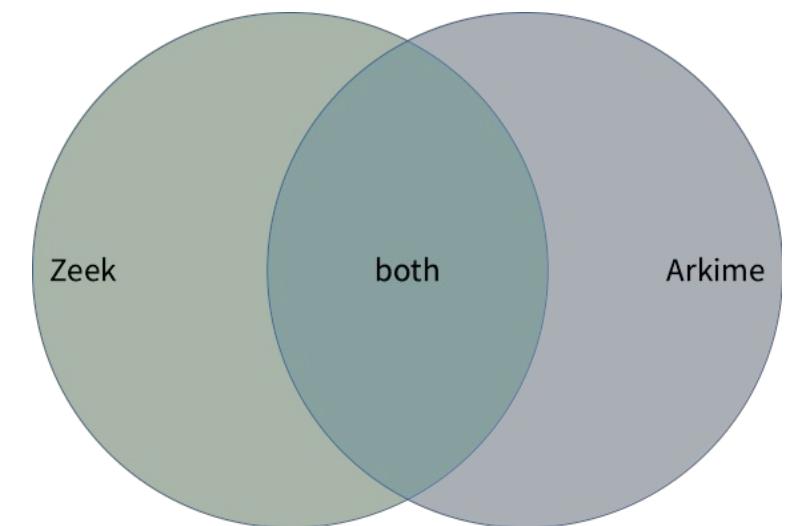
Search your packet search job history 50 per page 1 Showing 1 - 1 of 1 entries

Status	Matches	Name	User	Search text	Notify	Created	ID	Actions
✓ 100%	141	HTTP with password		password (ascii)		2021/12/06 12:12:27 MST	s5YpkX0BTA40FhD4X7dA	C U D X E

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

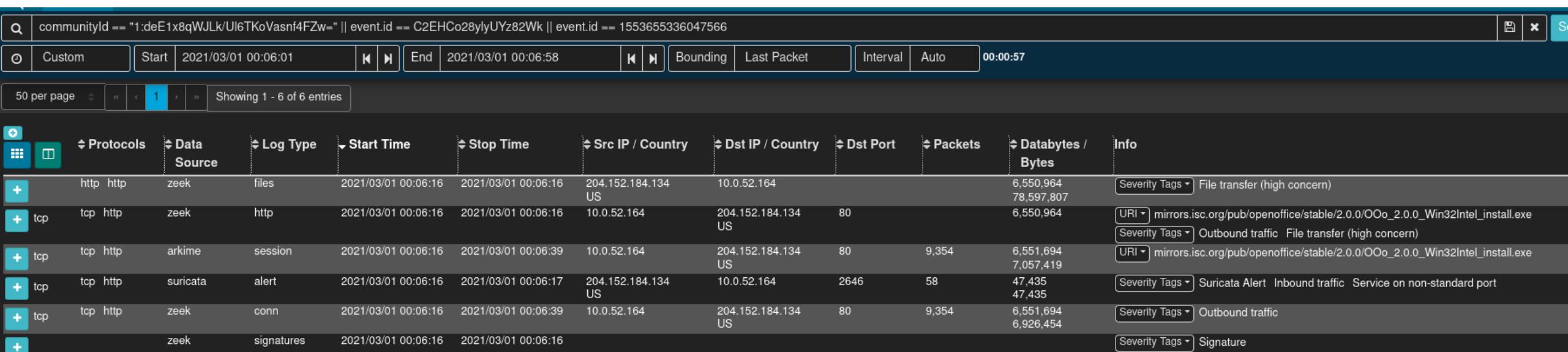
- Search syntax is different between Arkime and Dashboards (and in some cases, so are field names)
 - See search syntax comparison table, Malcolm and Arkime docs
- Despite considerable overlap, there are differences in protocol parser support among Zeek, Suricata and Arkime
 - Learning the strengths 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 timeline controls. The timeline shows a single session from "2021/03/01 00:06:01" to "2021/03/01 00:06:58".

The main table displays the correlation results:

Protocol	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

File Analysis

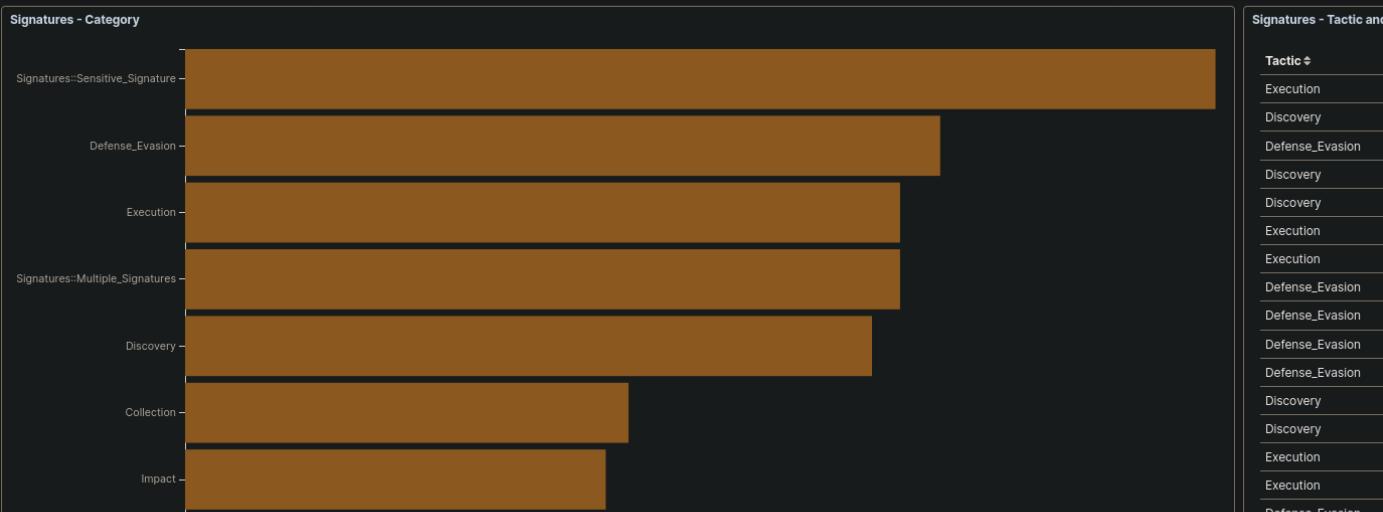
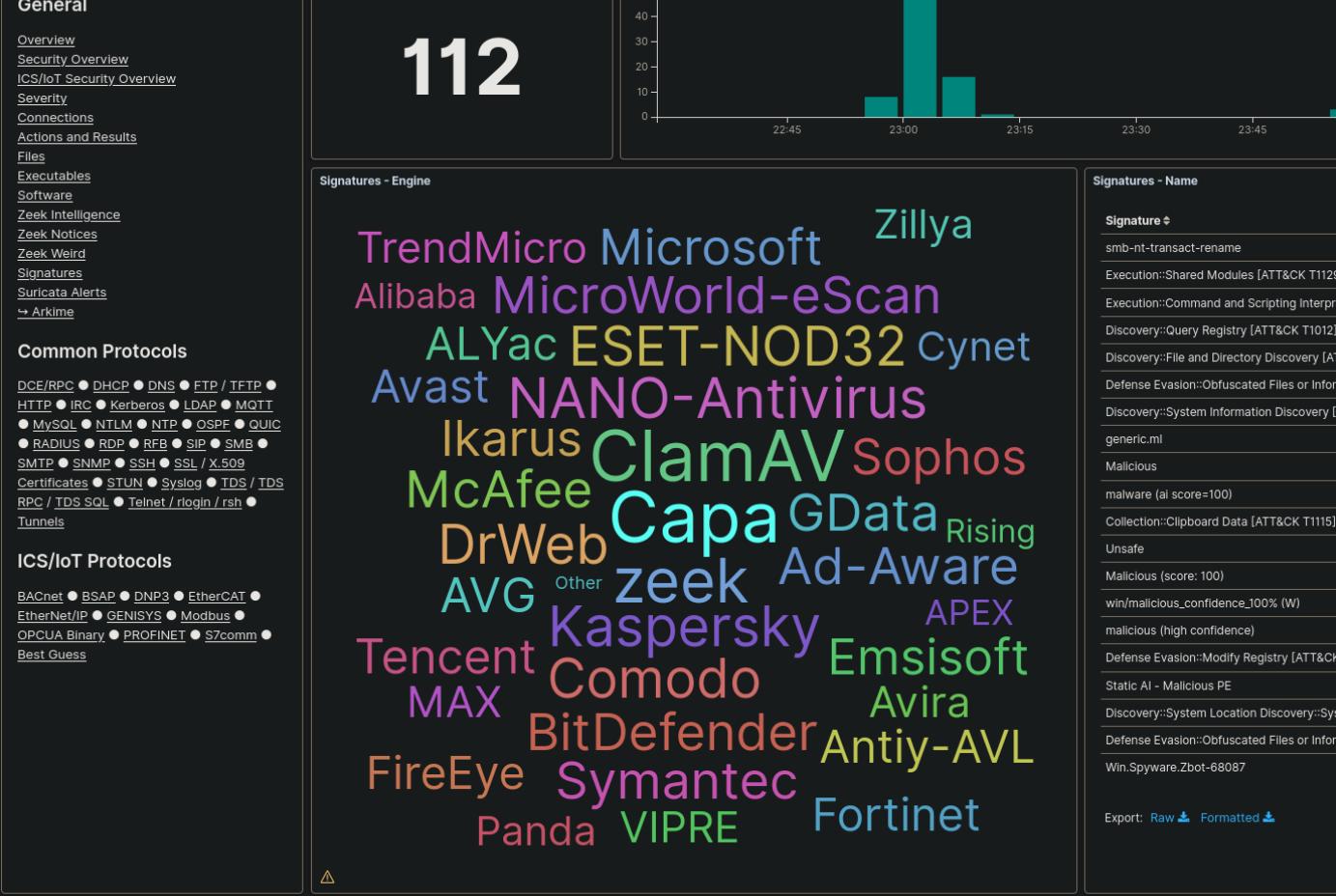


- Zeek can “carve” file transfers from common protocols
- Malcolm can examine carved files and flag hits
 - ClamAV - open source antivirus engine
 - YARA - pattern matching swiss army knife
 - Capa - portable executable capabilities analyzer
 - VirusTotal - online database of file hashes
 - requires API token and internet connection
- Triggering files can be saved to
zeek-logs/extract_files under Malcolm
directory for further analysis
 - Be careful! Carved files may contain live malware!



Signatures

- Signatures dashboard in Dashboards shows scanned file hits
- event.id field contains zeek.fuid and zeek.uid: use it to pivot from the *Signatures - Logs* table to other dashboards with pertinent session details



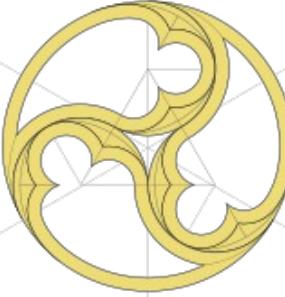
Search Tips

- Always check your search time frame
- “Zoom in” (apply filters) for a particular field value, pivot to another field then “zoom out” (remove filters)
- Most UI controls can work with any data field (3000+)
- Filter on `event.dataset` (e.g., `conn` to see `conn.log`)
- Filter on `protocol` regardless of data source (e.g., `protocol: http` in Dashboards and `protocols == http` in Arkime)
- Use tags

Towards the Future

- 
- Community Building
 - Official CISA-hosted Slack channel
 - Additional tutorial videos on YouTube
 - Prepackaged training modules
 - Vulnerability/IOC Sharing, Identification (CSAF), and Exploitation Visibility (KEV)
 - Support Generic (Sigma) Rules
 - Improve Asset Inventory Capabilities for OT and IT
 - Passive auto-population
 - Active scanning
 - Improve Cloud Deployment
 - Improve Integration of Third-Party and Host Logs
 - Increase OT/ICS Protocol Support
 - HART-IP
 - ANSI C12.22
 - PROFINET-IO CM
 - ...

Malcolm



Thank you!

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

Malcolm is Copyright © 2023 Battelle Energy Alliance, LLC, and is developed and released as open-source software through the cooperation of the Cybersecurity and Infrastructure Security Agency of the US Department of Homeland Security.