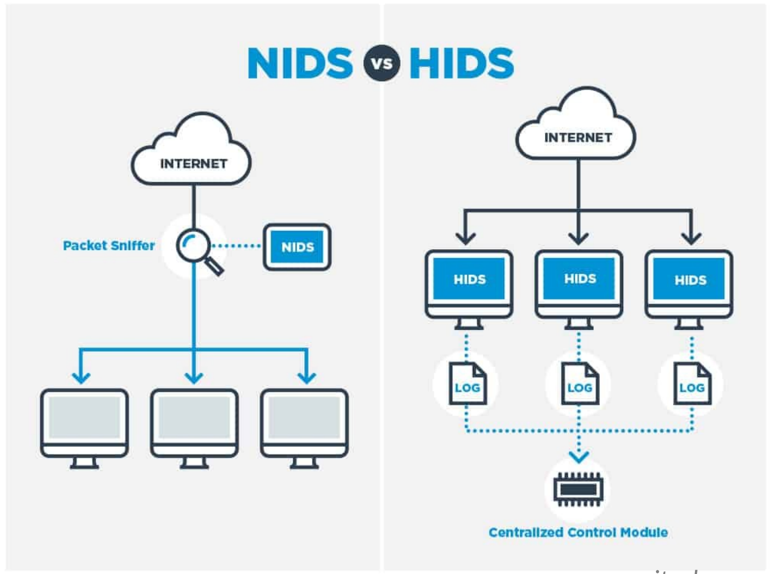
Network Traffic Analysis with Malcolm

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
  - Not what we're talking about today
- 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)



comparitech.com

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)

zeek

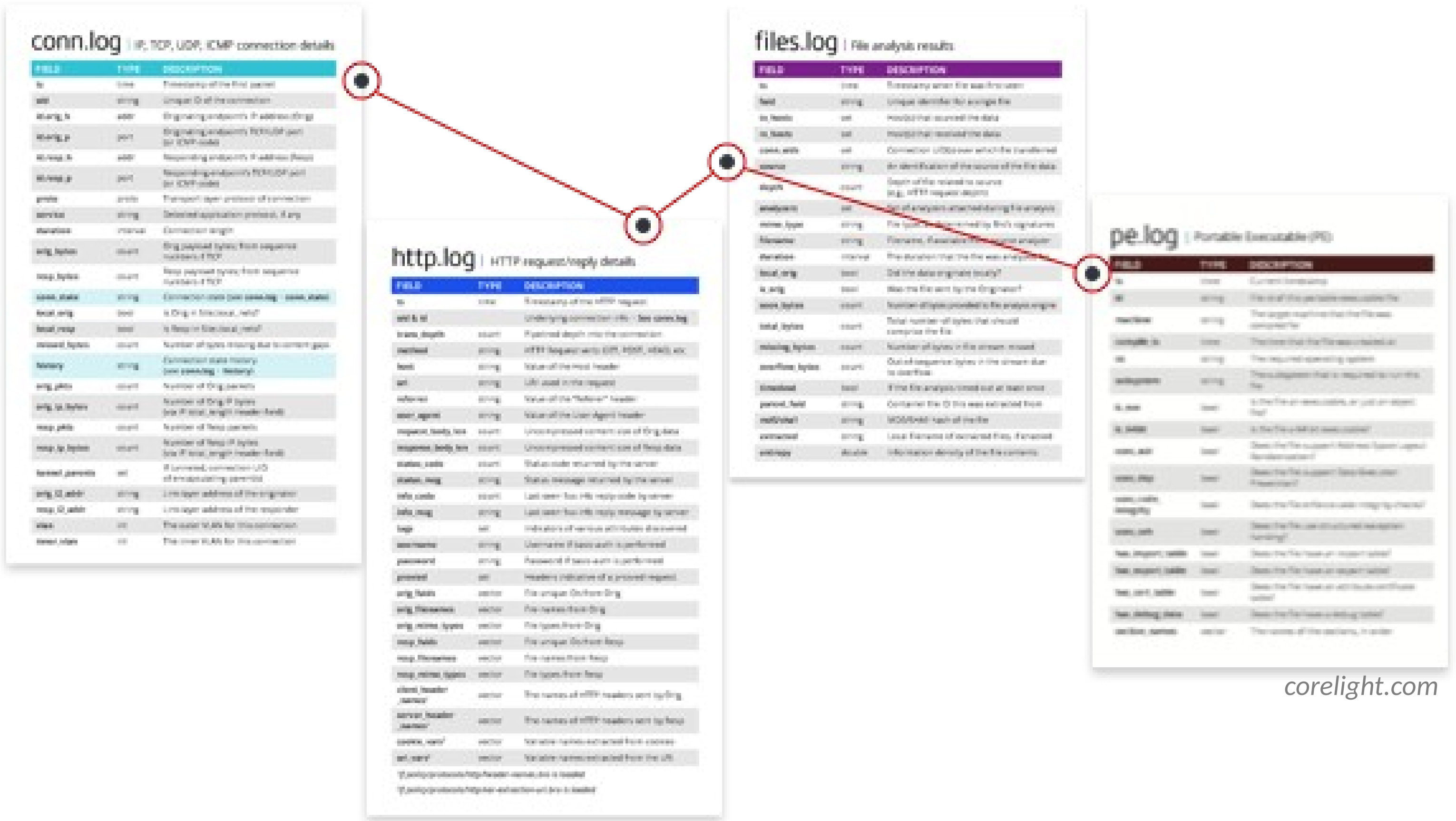
- Extensible, open-source passive network analysis framework
- More than just an Intrusion Detection System:
  - Packet capture (like TCPDUMP)
  - Traffic inspection (like Wireshark)
  - Intrusion detection (like SNORT)
  - Log recording (like NetFlow and syslog)
  - Scripting framework (like python™)

zeek

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



conn.log | IP, TCP, UDP, ICMP connection details
http.log | HTTP request/reply details
files.log | File analysis results
pe.log | Portable Executable (PE)
FIELD
TYPE
DESCRIPTION

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	Weaknesses
• 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	• No OT protocol support • Adding new protocol parsers requires C programming

Malcolm

A powerful open-source network traffic analysis tool suite.
https://github.com/idaholab/Malcolm

Streamlined deployment

- Suitable for field use (hunt or incident response) or SOC deployment. Runs in Docker on Linux, macOS and Windows platforms. 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

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

Malcolm Components

https://github.com/idaholab/Malcolm/#Components

Capture & Analysis
- zeek
- Arkime
- SURICATA
- netsniff-ng
- TCPDUMP

File Scanning
- yara
- ClamAV
- CAPA
- VIRUSTOTAL

Forwarding & Enrichment
- fluentbit
- logstash
- beats

Storage
- OpenSearch

Anomaly Detection
- Anomaly Detection Plugin
- Alerting
- Alerting Plugin

Asset Management
- netbox

Visualization
- OpenSearch Dashboards
- Arkime

Payload Analysis
- CyberChef
- Arkime session PCAP export to WIRESHARK

Framework
- docker
- NGINX

Malcolm

Supported Protocols

https://github.com/idaholab/Malcolm/#Protocols

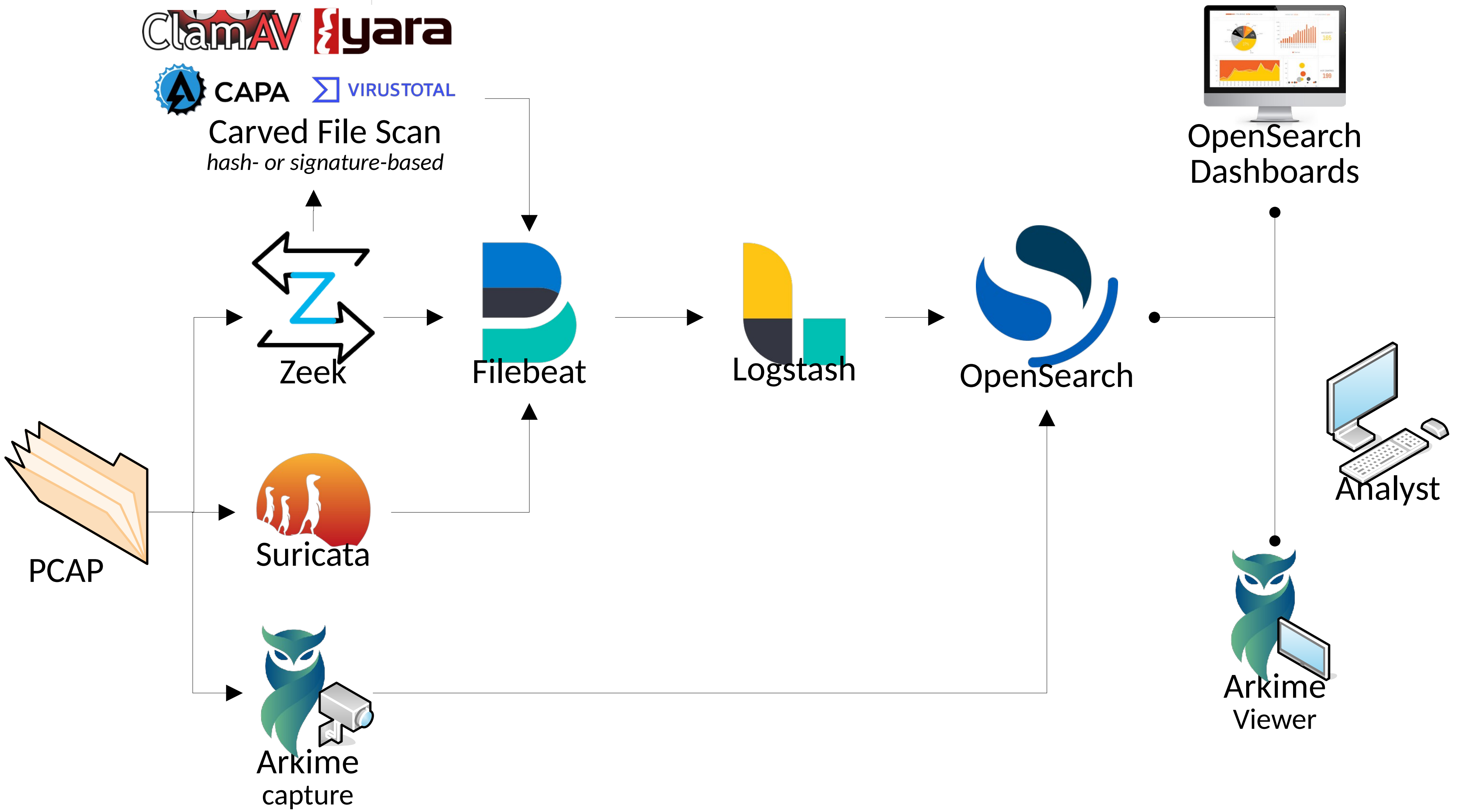
Internet layer
Border Gateway Protocol (BGP)
Building Automation and Control (BACnet)
Bristol Standard Asynchronous Protocol (BSAP)
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC)
Dynamic Host Configuration Protocol (DHCP)
Distributed Network Protocol 3 (DNP3)
Domain Name System (DNS)
EtherCAT
EtherNet/IP / Common Industrial Protocol (CIP)
FTP (File Transfer Protocol)
GENISYS
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)
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.)

** Industrial control systems protocols indicated with **bold***

Malcolm

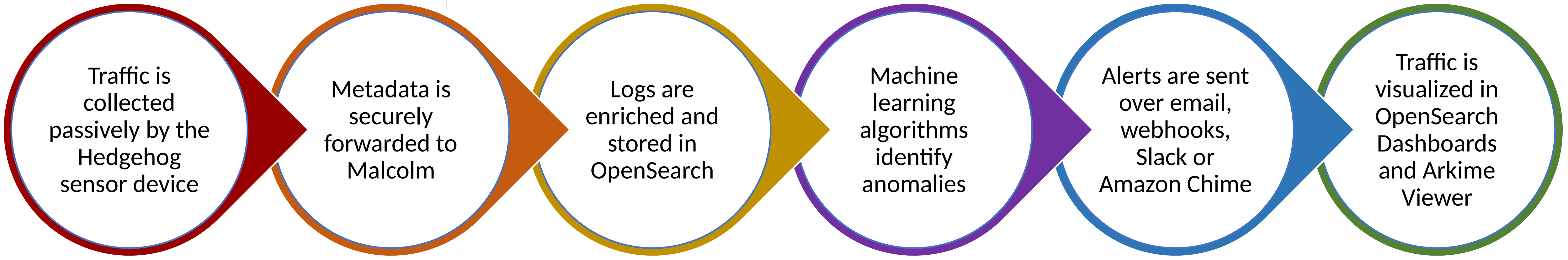
Data Pipeline

https://github.com/idaholab/Malcolm



Malcolm Data Pipeline

https://github.com/idaholab/Malcolm



Traffic is collected passively by the Hedgehog sensor device

Metadata is securely forwarded to Malcolm

Logs are enriched and stored in OpenSearch

Machine learning algorithms identify anomalies

Alerts are sent over email, webhooks, Slack or Amazon Chime

Traffic is visualized in OpenSearch Dashboards and Arkime Viewer

- Zeek, Arkime Capture and Suricata generate metadata about network communications
- Full PCAP may be 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

- All communications between the sensor and aggregator are TLS-encrypted
- Sensor data including resource utilization, syslog, audit logs, temperatures and more may also be forwarded

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

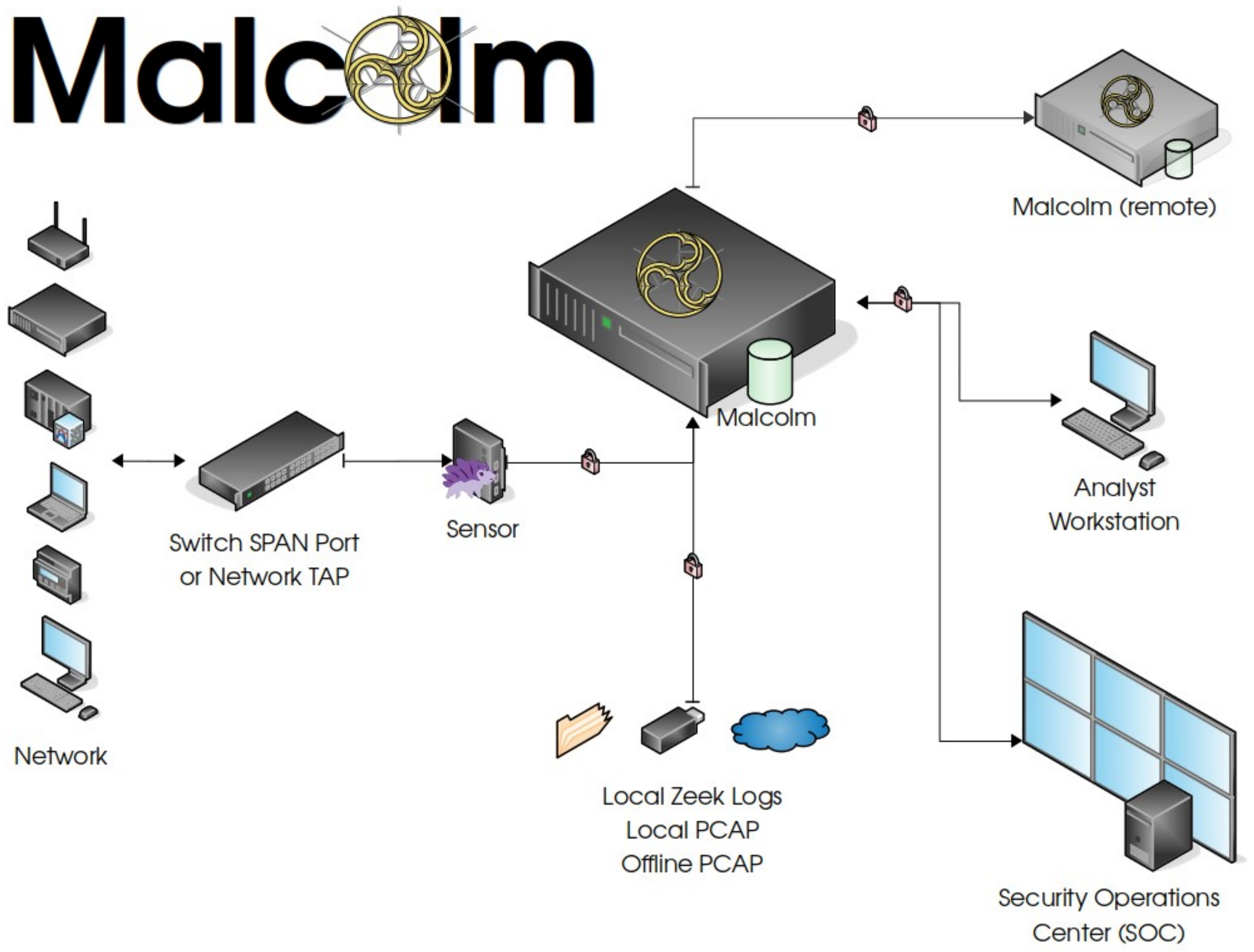
- Default detectors are provided for action and result, flow size and types of transferred files
- Custom detectors may be created for any aspect of any supported protocol

- 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 automatically on demand
- Custom visualizations may be created via drag-and-drop interface
- Malcolm can authenticate users from its own list or via Active Directory / LDAP

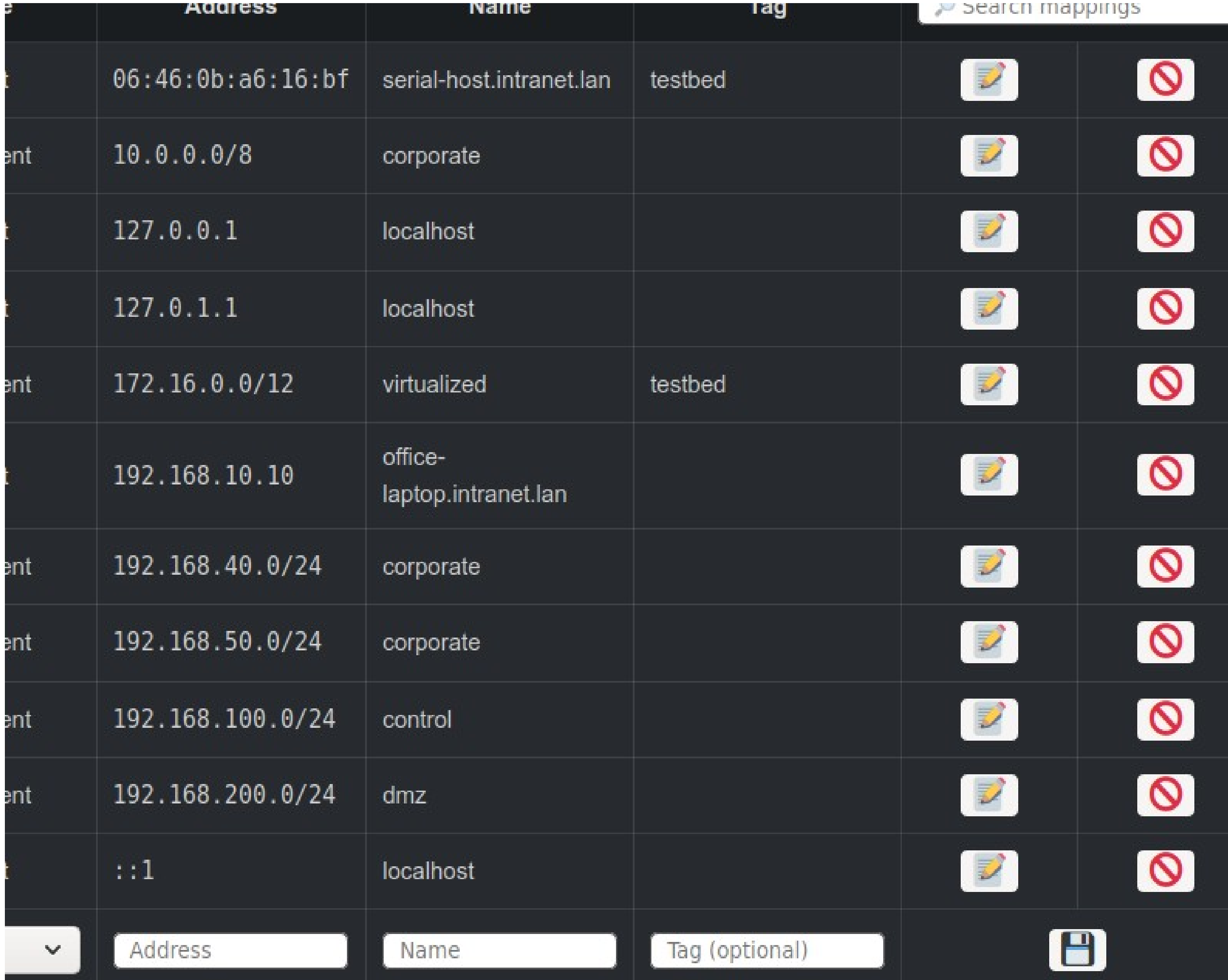
Configuring and Running Malcolm

- Runs natively in Docker or in a Virtual Machine
- 16+GB RAM, 4+ cores, “enough” disk for PCAP and logs suggested
- Documentation and source code on GitHub: github.com/idaholab/Malcolm
- Walkthroughs on YouTube: search “Malcolm Network Traffic Analysis”



Identifying Network Hosts and Subnets

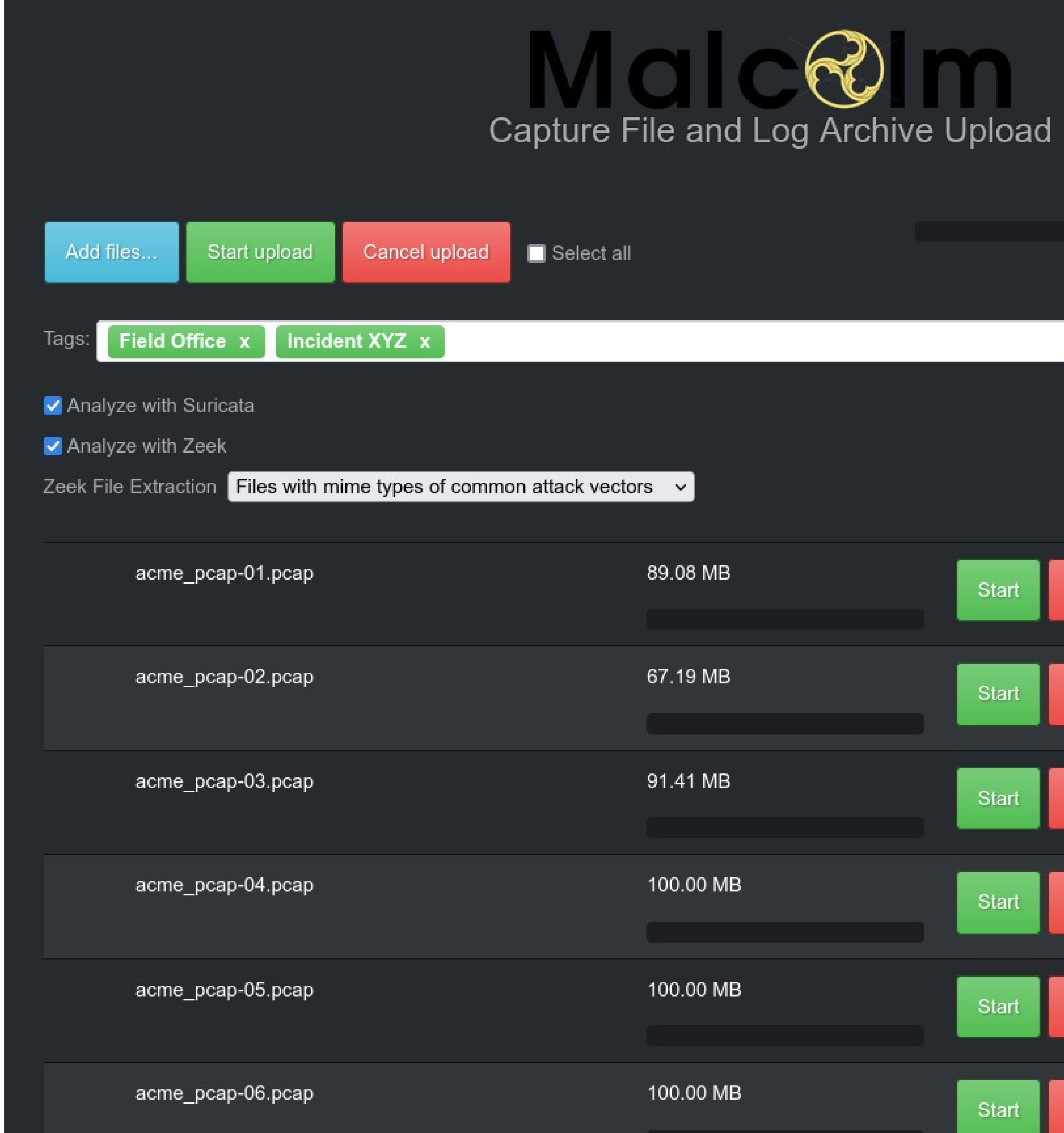
- Assign custom names to network hosts and subnets prior to PCAP import
- Allows identification of cross-segment traffic and name-based search and filter
- Define in text file(s) or via web interface
- https://localhost/name-map-ui



e	Address	Name	Tag	Search mappings	
t	06:46:0b:a6:16:bf	serial-host.intranet.lan	testbed	✎	🚫
ent	10.0.0.0/8	corporate		✎	🚫
t	127.0.0.1	localhost		✎	🚫
t	127.0.1.1	localhost		✎	🚫
ent	172.16.0.0/12	virtualized	testbed	✎	🚫
t	192.168.10.10	office-laptop.intranet.lan		✎	🚫
ent	192.168.40.0/24	corporate		✎	🚫
ent	192.168.50.0/24	corporate		✎	🚫
ent	192.168.100.0/24	control		✎	🚫
ent	192.168.200.0/24	dmz		✎	🚫
t	::1	localhost		✎	🚫
	Address	Name	Tag (optional)	💾	

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://localhost/upload



Malcolm
Capture File and Log Archive Upload

Tags: Field Office x Incident XYZ x

✓ Analyze with Suricata

✓ Analyze with Zeek

Zeek File Extraction: Files with mime types of common attack vectors

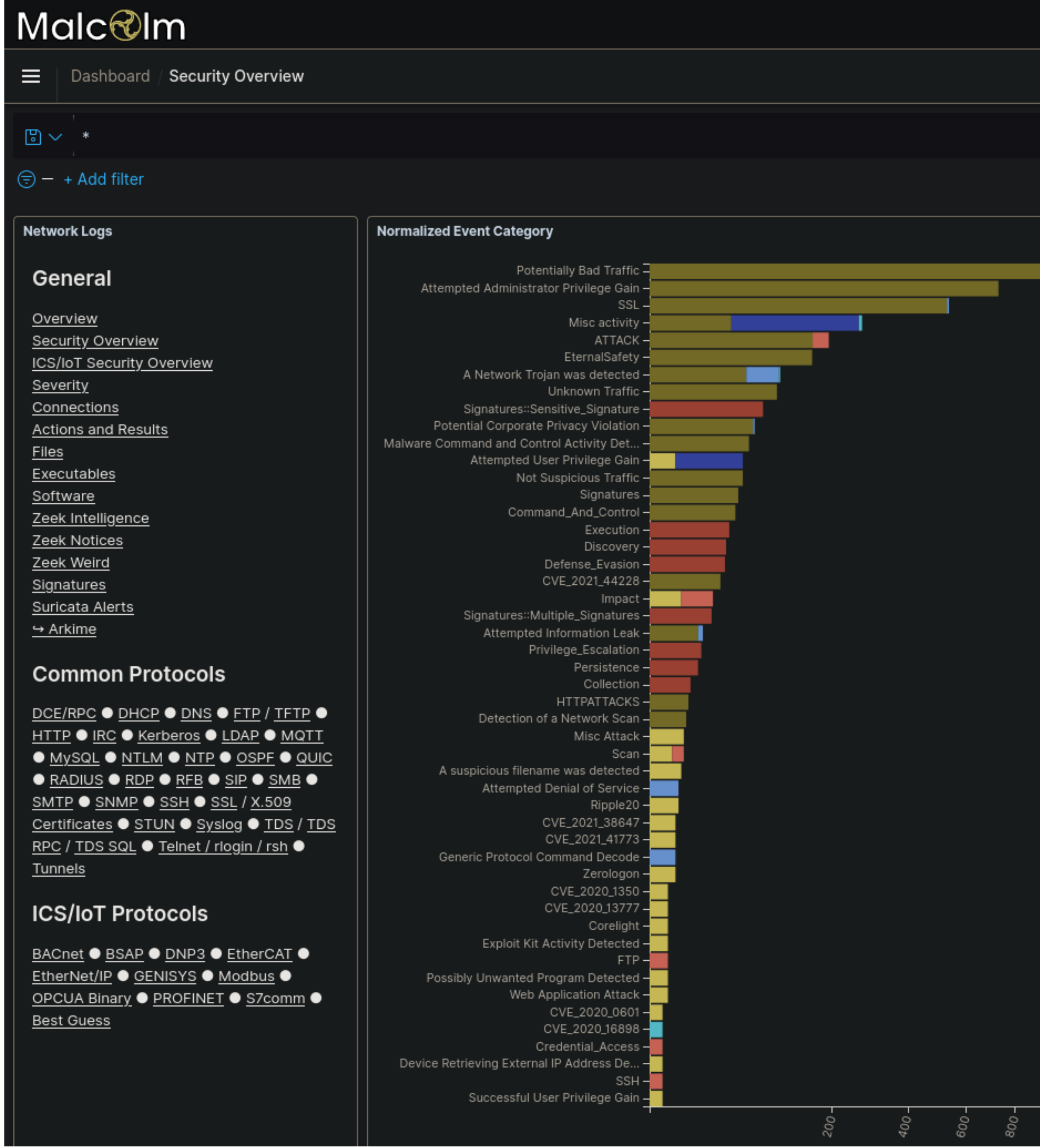
acme_pcap-01.pcap	89.08 MB	Start
acme_pcap-02.pcap	67.19 MB	Start
acme_pcap-03.pcap	91.41 MB	Start
acme_pcap-04.pcap	100.00 MB	Start
acme_pcap-05.pcap	100.00 MB	Start
acme_pcap-06.pcap	100.00 MB	Start

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
  - `internal_source`, `internal_destination`, `external_source`, `external_destination`, `cross_segment`

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://localhost/dashboards



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

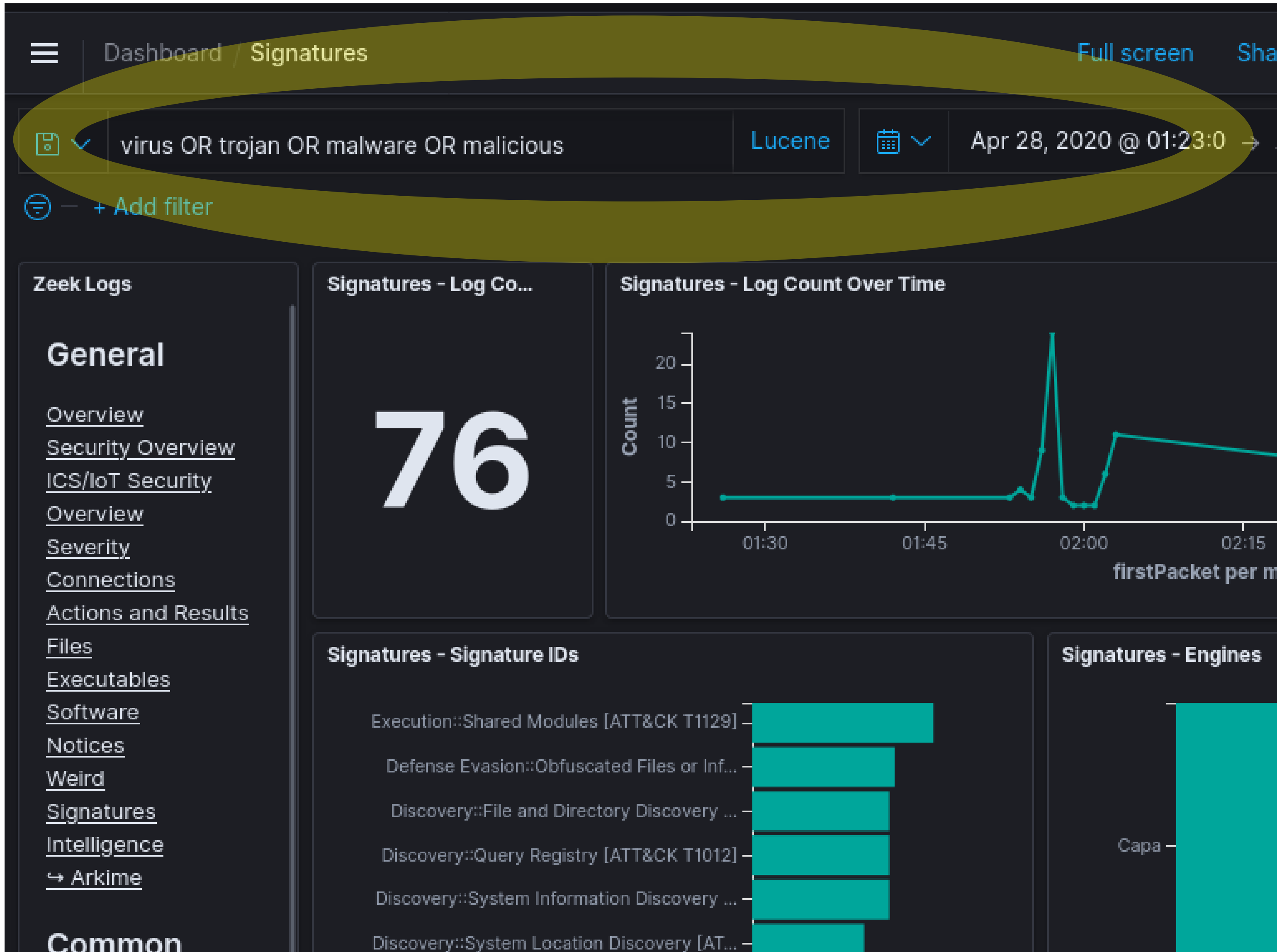
BACnet ● BSAP ● DNP3 ● EtherCAT ● EtherNet/IP ● GENISYS ● Modbus ● OPCUA Binary ● PROFINET ● S7comm ● Best Guess

Normalized Event Category

Potentially Bad Traffic
Attempted Administrator Privilege Gain
SSL
Misc activity
ATTACK
EternalSafety
A Network Trojan was detected
Unknown Traffic
Signatures::Sensitive_Signature
Potential Corporate Privacy Violation
Malware Command and Control Activity Det...
Attempted User Privilege Gain
Not Suspicious Traffic
Signatures
Command_And_Control
Execution
Discovery
Defense_Evasion
CVE_2021_44228
Impact
Signatures::Multiple_Signatures
Attempted Information Leak
Privilege_Escalation
Persistence
Collection
HTTPATTACKS
Detection of a Network Scan
Misc Attack
Scan
A suspicious filename was detected
Attempted Denial of Service
Ripple20
CVE_2021_38647
CVE_2021_41773
Generic Protocol Command Decode
Zerologon
CVE_2020_1350
CVE_2020_13777
Corelight
Exploit Kit Activity Detected
FTP
Possibly Unwanted Program Detected
Web Application Attack
CVE_2020_0601
CVE_2020_16898
Credential_Access
Device Retrieving External IP Address De...
SSH
Successful User Privilege Gain
200
400
600
800

Dashboards Filters and Search

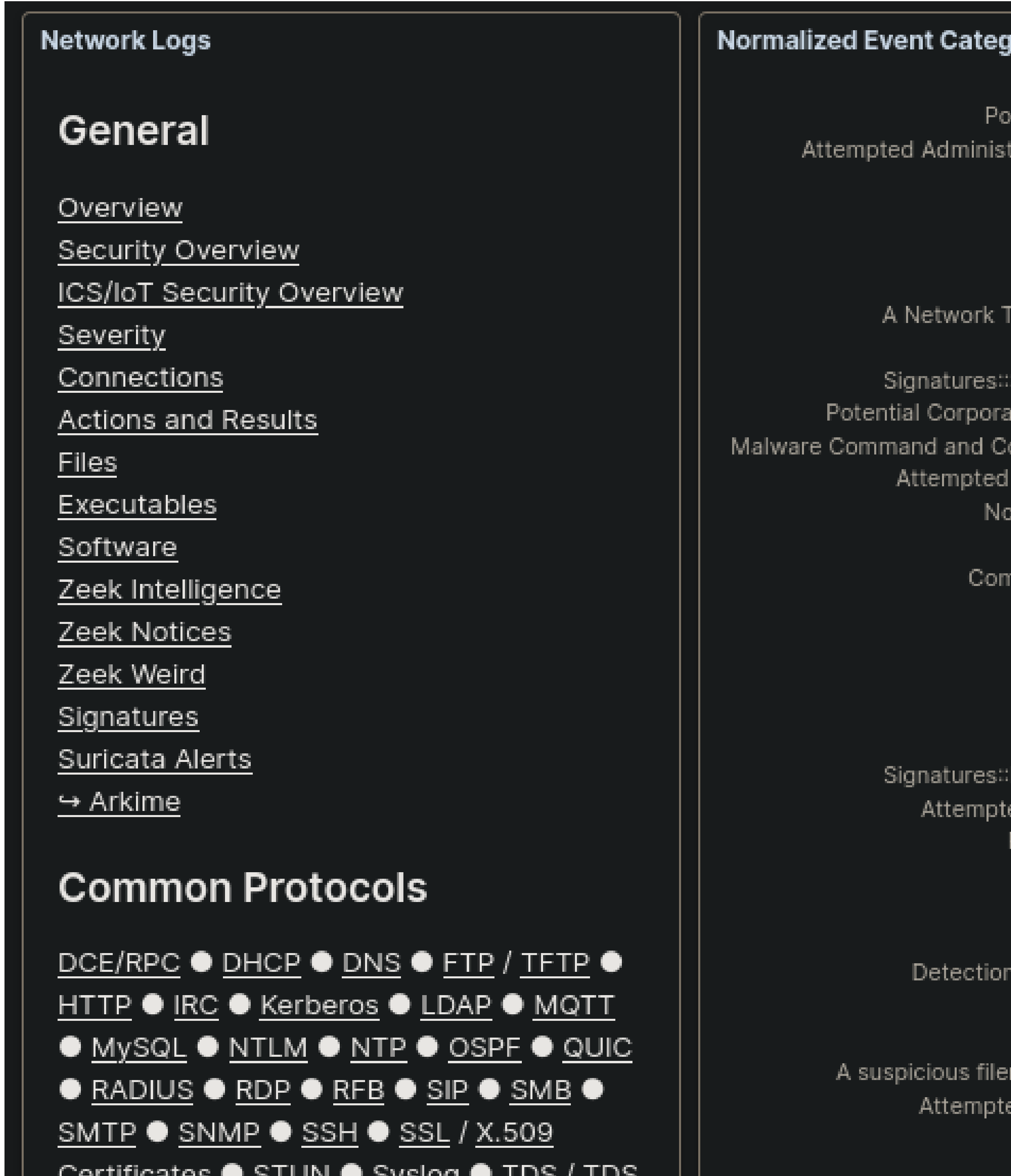
- Time filter: define search time frame
- Query bar: write queries in Lucene syntax or DQL (Dashboards Query Language)
- Filter bar: define filters using a UI
  - Pin filters as you move across dashboards
- Save queries and filters for reuse



Dashboard / Signatures
Full screen
Sha
virus OR trojan OR malware OR malicious
Lucene
Apr 28, 2020 @ 01:23:0
+ Add filter
Zeek Logs
General
Overview
Security Overview
ICS/IoT Security Overview
Severity
Connections
Actions and Results
Files
Executables
Software
Notices
Weird
Signatures
Intelligence
↪ Arkime
Common
Signatures - Log Co...
76
Signatures - Log Count Over Time
Count
20
15
10
5
0
01:30
01:45
02:00
02:15
firstPacket per m
Signatures - Signature IDs
Execution::Shared Modules [ATT&CK T1129]
Defense Evasion::Obfuscated Files or Inf...
Discovery::File and Directory Discovery ...
Discovery::Query Registry [ATT&CK T1012]
Discovery::System Information Discovery ...
Discovery::System Location Discovery [AT...
Signatures - Engines
Capa

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

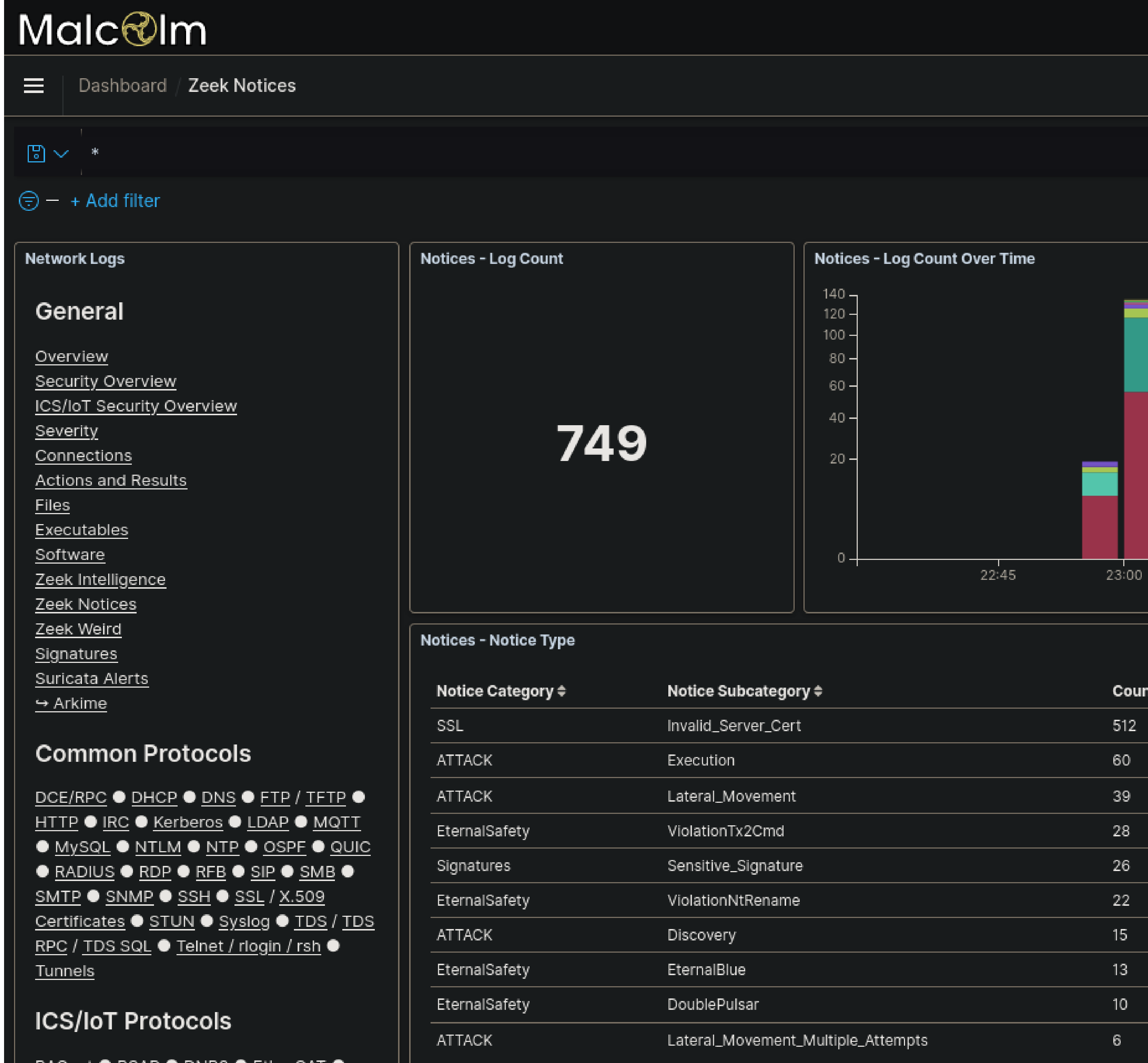
DCE/RPC ● DHCP ● DNS ● FTP / TFTP ● HTTP ● IRC ● Kerberos ● LDAP ● MQTT ● MySQL ● NTLM ● NTP ● OSPF ● QUIC ● RADIUS ● RDP ● RFB ● SIP ● SMB ● SMTP ● SNMP ● SSH ● SSL / X.509 Certificates ● STUN ● Syslog ● TDS / TDS

Normalized Event Categ

Po
Attempted Administ
A Network T
Signatures::
Potential Corpora
Malware Command and C
Attempted
No
Com
Signatures::
Attempte
Detection
A suspicious file
Attempte

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

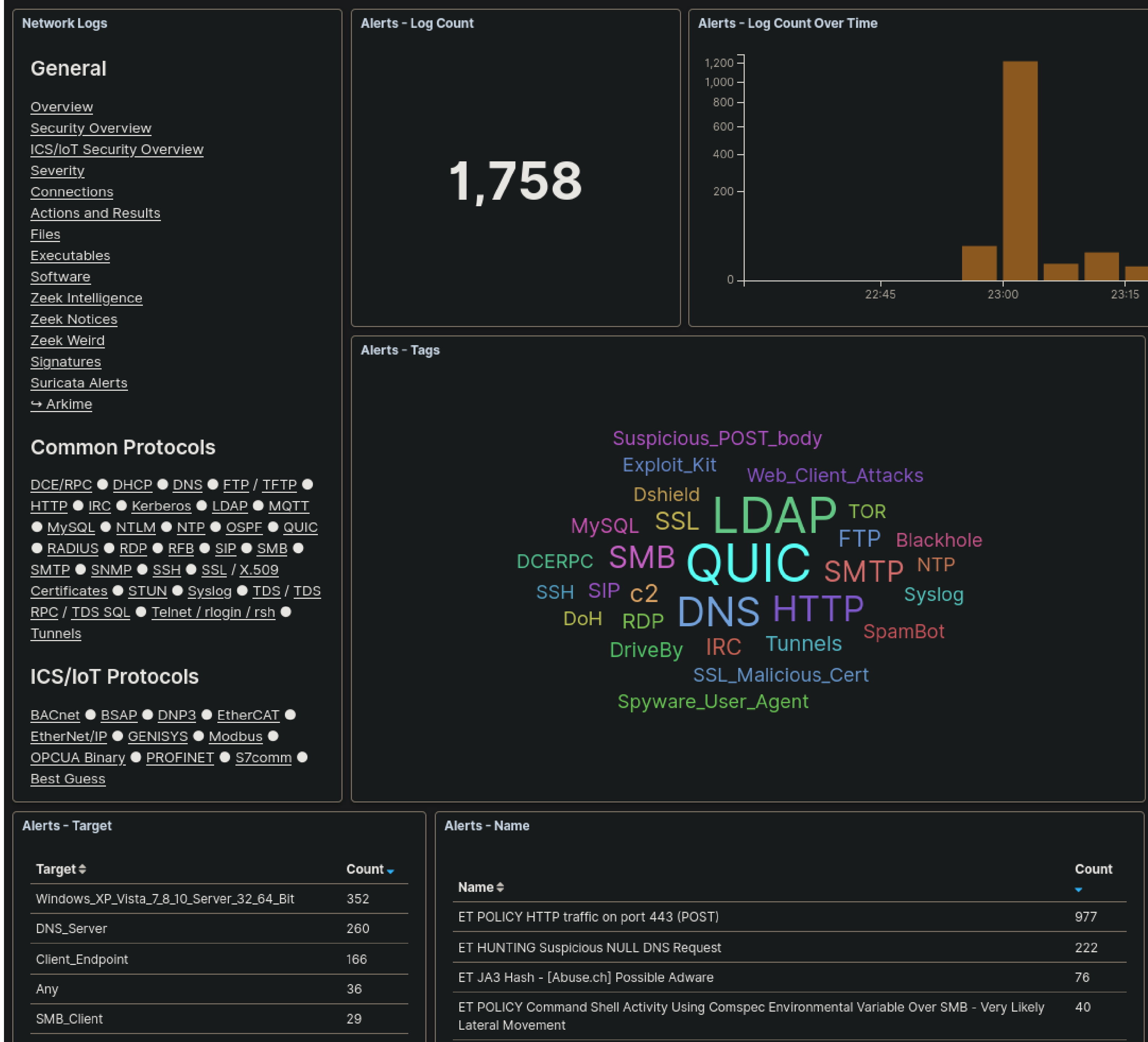
Notices - Log Count Over Time

Notices - Notice Type

Notice Category	Notice Subcategory	Cour
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



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

BACnet ● BSAP ● DNP3 ● EtherCAT ● EtherNet/IP ● GENISYS ● Modbus ● OPCUA Binary ● PROFINET ● S7comm ● Best Guess

Alerts - Log Count

1,758

Alerts - Log Count Over Time

Alerts - Tags

Suspicious_POST_body
Exploit_Kit
Web_Client_Attacks
Dshield
MySQL
SSL
LDAP
TOR
FTP
Blackhole
DCERPC
SMB
QUIC
SMTP
NTP
SSH
SIP
c2
DNS
HTTP
Syslog
DoH
RDP
SpamBot
DriveBy
IRC
Tunnels
SSL_Malicious_Cert
Spyware_User_Agent

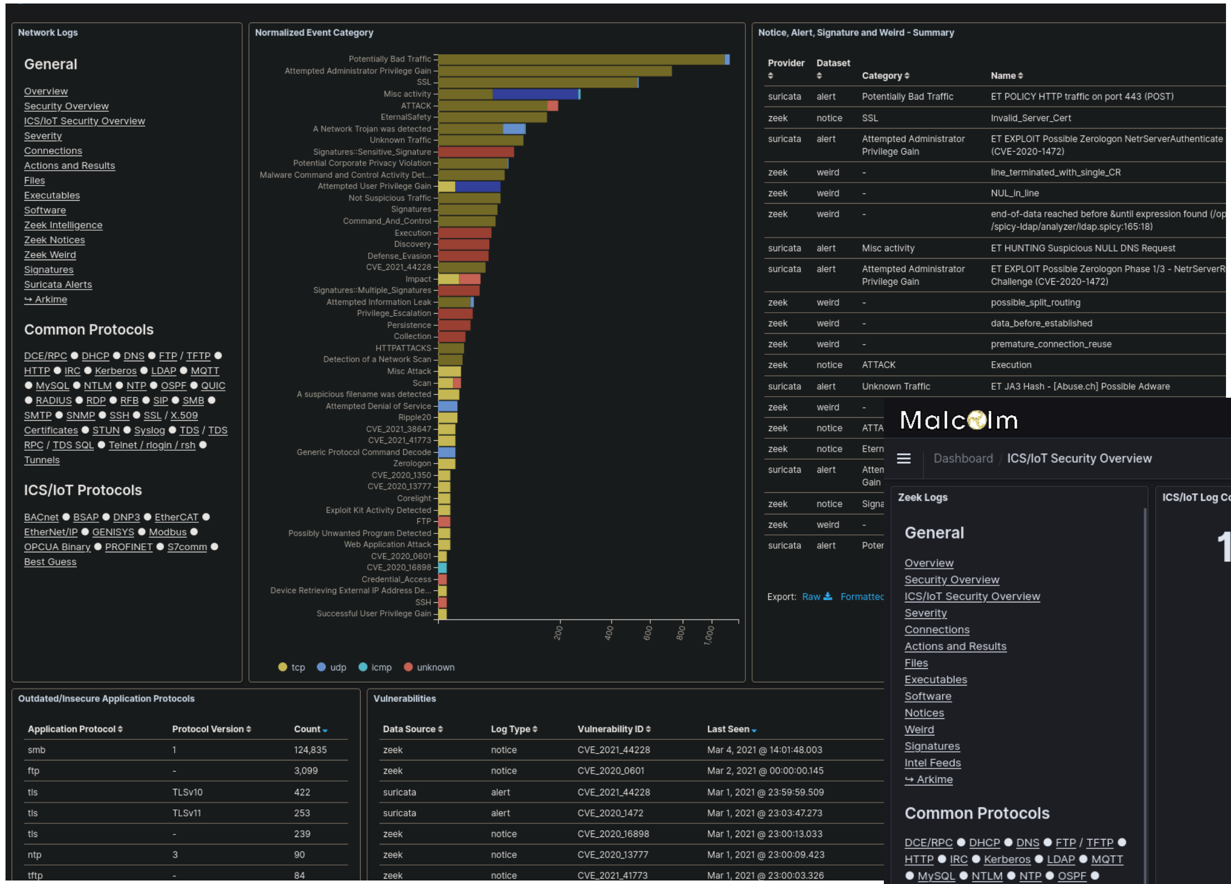
Alerts - Target

Target	Count
Windows_XP_Vista_7_8_10_Server_32_64_Bit	352
DNS_Server	260
Client_Endpoint	166
Any	36
SMB_Client	29

Alerts - Name

Name	Count
ET POLICY HTTP traffic on port 443 (POST)	977
ET HUNTING Suspicious NULL DNS Request	222
ET JA3 Hash - [Abuse.ch] Possible Adware	76
ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement	40

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 ● 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

Normalized Event Category

Potentially Bad Traffic
Attempted Administrator Privilege Gain
SSL
Misc activity
ATTACK
EternalSafety
A Network Trojan was detected
Unknown Traffic
Signatures::Sensitive_Signature
Potential Corporate Privacy Violation
Malware Command and Control Activity Det...
Attempted User Privilege Gain
Not Suspicious Traffic
Signatures
Command_And_Control
Execution
Discovery
Defense_Evasion
CVE_2021_44228
Impact
Signatures::Multiple_Signatures
Attempted Information Leak
Privilege_Escalation
Persistence
Collection
HTTPATTACKS
Detection of a Network Scan
Misc Attack
Scan
A suspicious filename was detected
Attempted Denial of Service
Ripple20
CVE_2021_38647
CVE_2021_41773
Generic Protocol Command Decode
Zerologon
CVE_2020_1350
CVE_2020_13777
Corelight
Exploit Kit Activity Detected
FTP
Possibly Unwanted Program Detected
Web Application Attack
CVE_2020_0601
CVE_2020_16898
Credential_Access
Device Retrieving External IP Address De...
SSH
Successful User Privilege Gain
200
400
600
800
1,000
● tcp ● udp ● icmp ● unknown

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 NetrServerAuthenticate (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-ldap/analyzer/ldap.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 - NetrServerR Challenge (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	ATTA	
zeek	notice	Etern	
suricata	alert	Atten Gain	
zeek	notice	Signa	
zeek	weird	-	
suricata	alert	Poter	

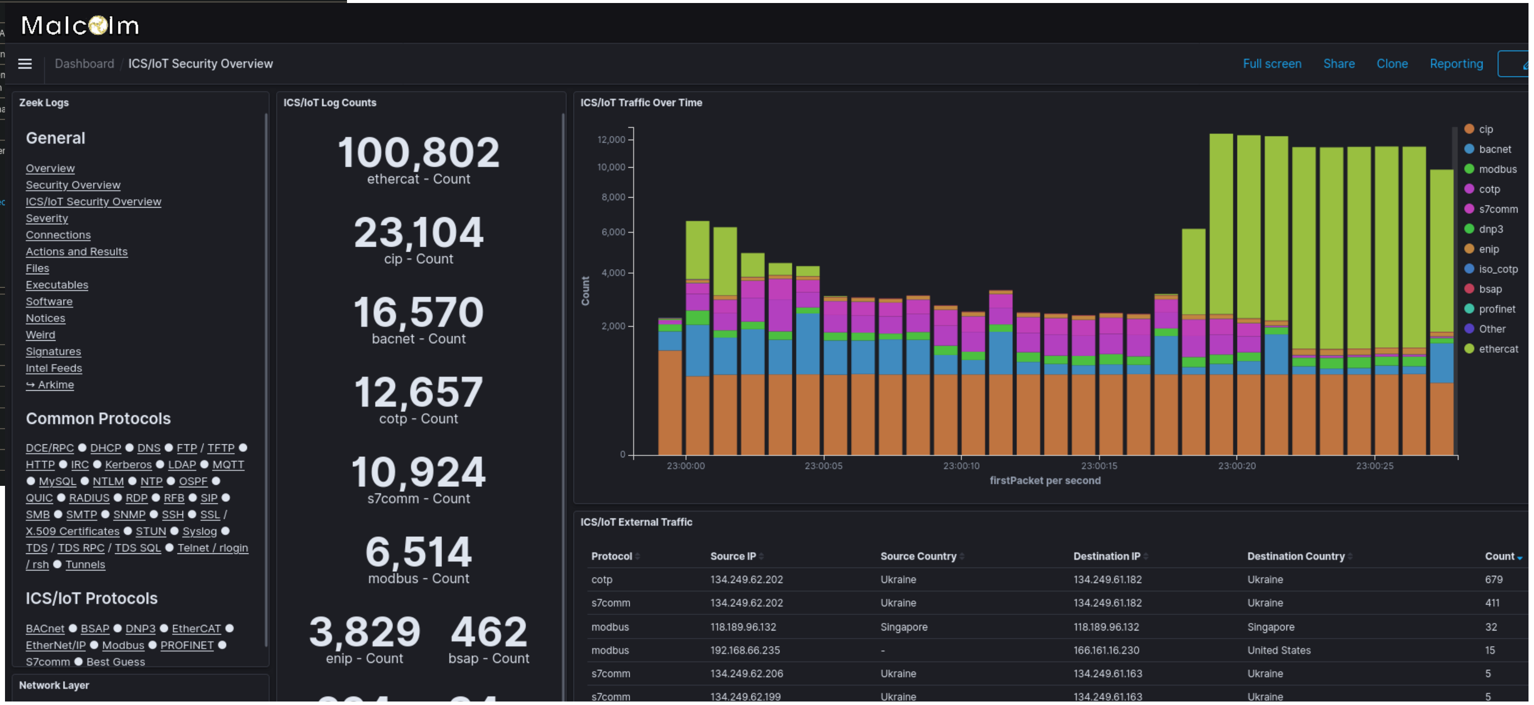
Export: Raw Formattec

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

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



Zeek Logs

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 ● 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 ● Modbus ● PROFINET ● S7comm ● Best Guess

Network Layer

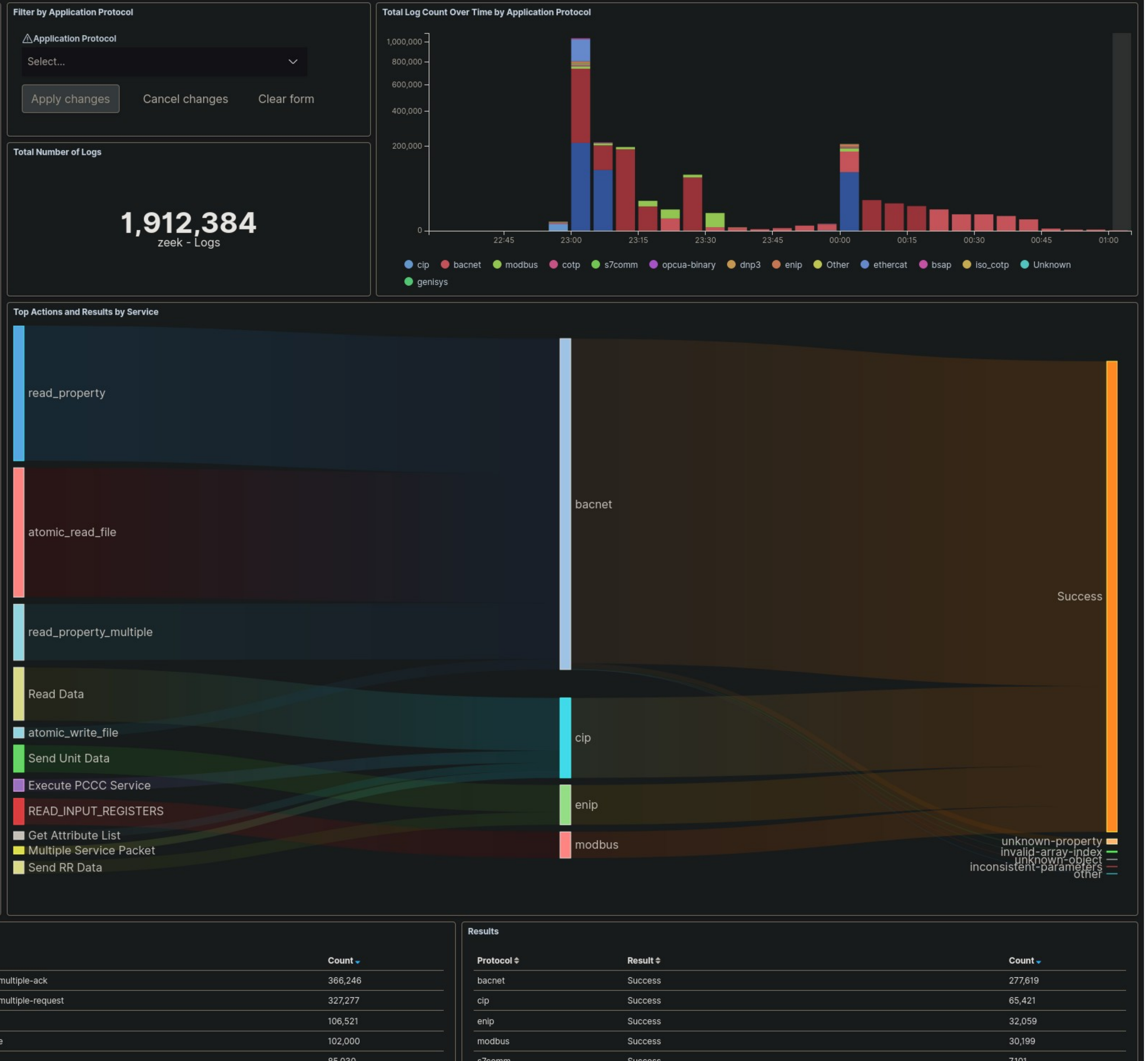
ICS/IoT Log Counts

100,802 ethercat - Count
23,104 cip - Count
16,570 bacnet - Count
12,657 cotp - Count
10,924 s7comm - Count
6,514 modbus - Count
3,829 enip - Count
462 bsap - Count

ICS/IoT Traffic Over Time

ICS/IoT External Traffic

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



	Count
multiple-ack	366,246
multiple-request	327,277
	106,521
e	102,000
	85,030

Results

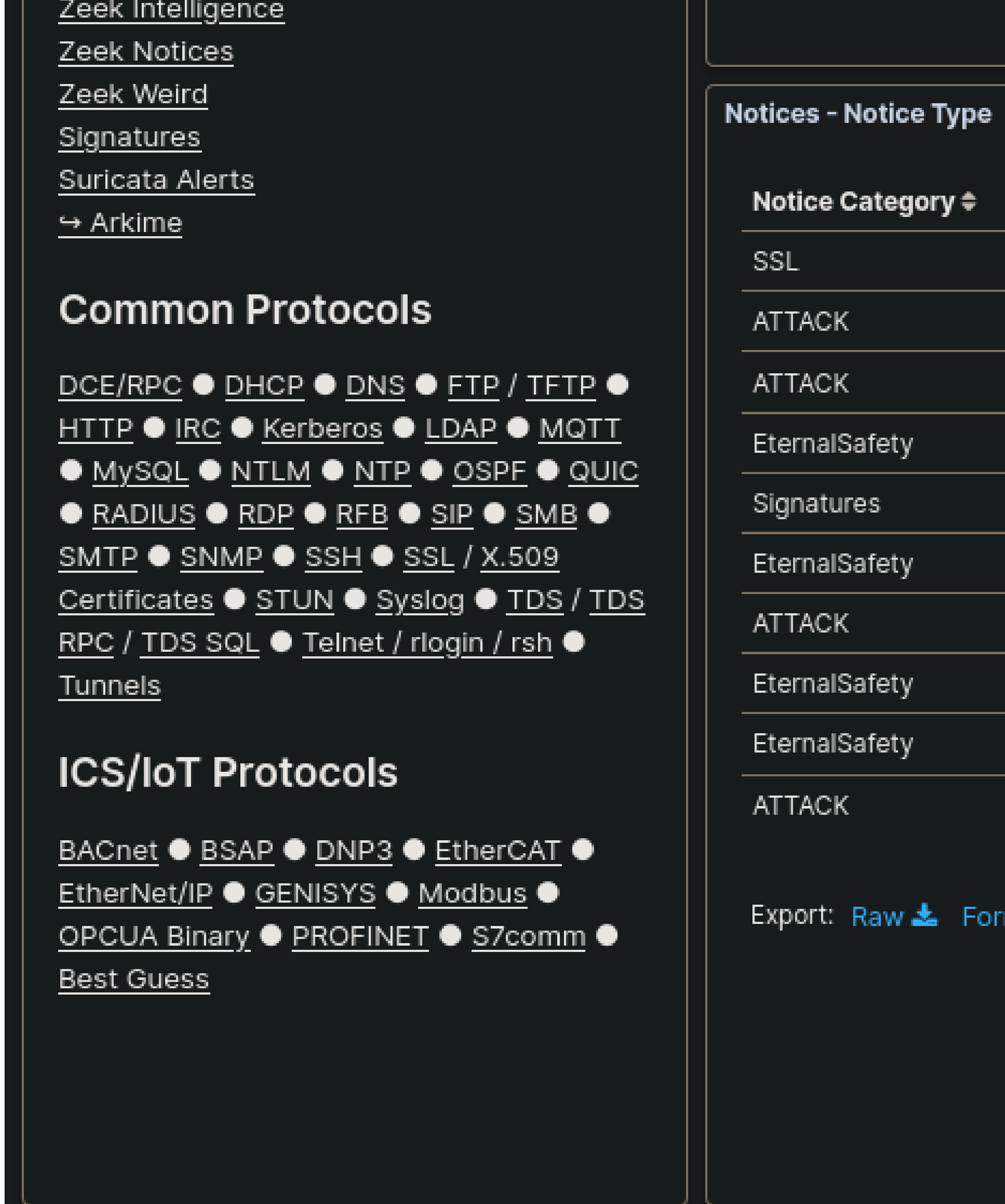
Protocol	Result	Count
bacnet	Success	277,619
cip	Success	65,421
enip	Success	32,059
modbus	Success	30,199
s7comm	Success	7101

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



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

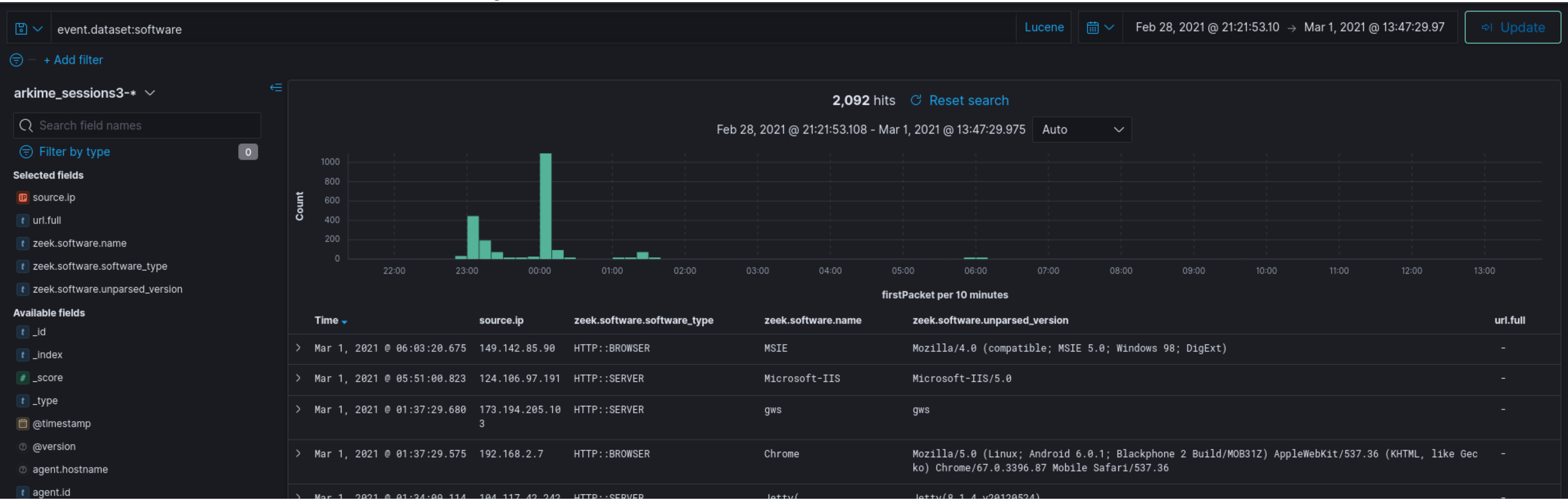
Notices - Notice Type

Notice Category ⇕
SSL
ATTACK
ATTACK
EternalSafety
Signatures
EternalSafety
ATTACK
EternalSafety
EternalSafety
ATTACK

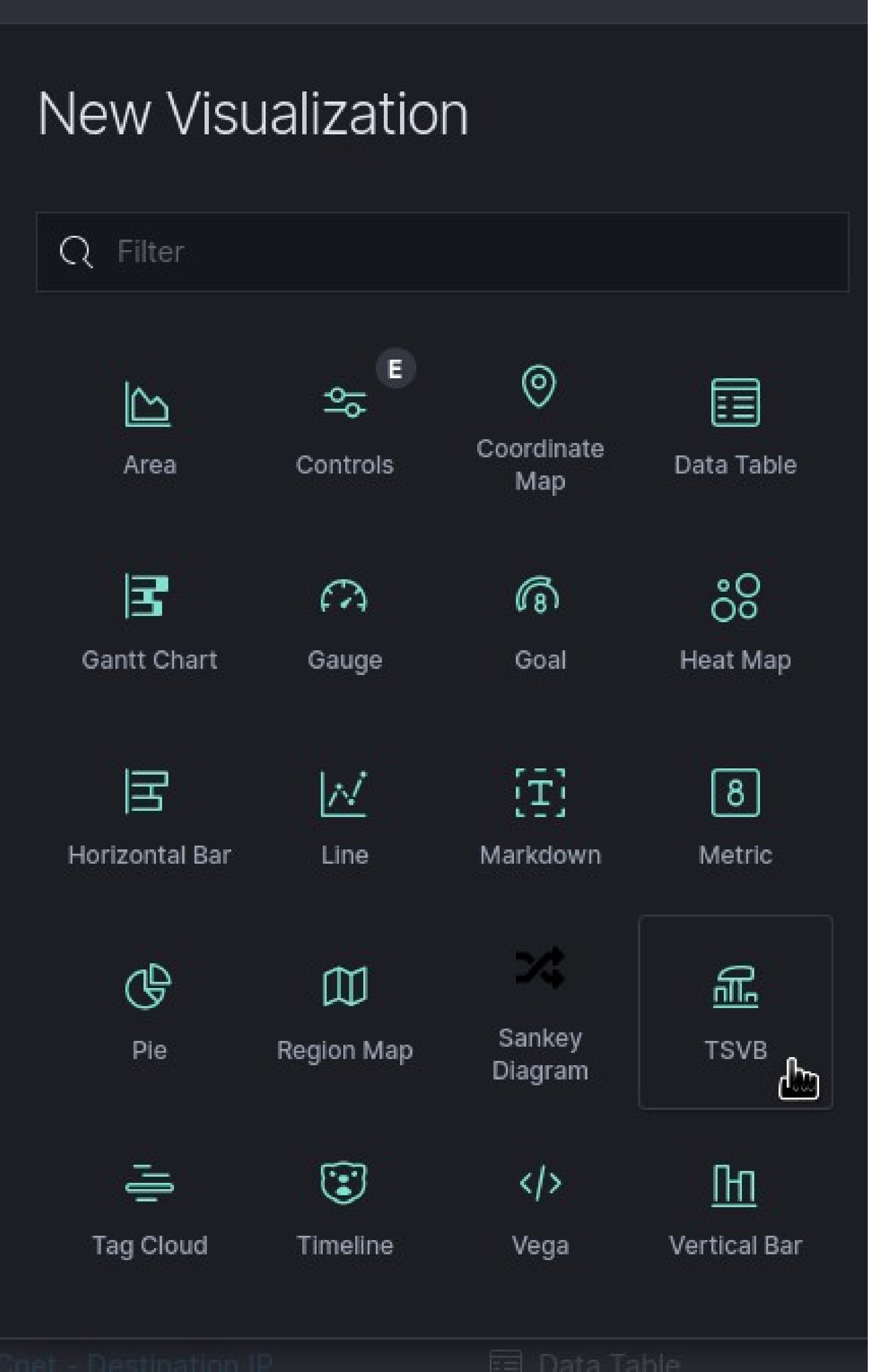
Export: Raw For

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



Time	source.ip	zeek.software.software_type	zeek.software.name	zeek.software.unparsed_version	url.full
Mar 1, 2021 @ 06:03:20.675	149.142.85.90	HTTP::BROWSER	MSIE	Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)	-
Mar 1, 2021 @ 05:51:00.823	124.106.97.191	HTTP::SERVER	Microsoft-IIS	Microsoft-IIS/5.0	-
Mar 1, 2021 @ 01:37:29.680	173.194.205.103	HTTP::SERVER	gws	gws	-
Mar 1, 2021 @ 01:37:29.575	192.168.2.7	HTTP::BROWSER	Chrome	Mozilla/5.0 (Linux; Android 6.0.1; Blackphone 2 Build/MOB31Z) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Mobile Safari/537.36	-
Mar 1, 2021 @ 01:34:09.114	104.117.42.242	HTTP::SERVER	Jetty(	Jetty(8.1.4.v20120524)	-



Custom Visualizations

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

Search Syntax Comparison

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

Search Syntax Comparison (cont.)

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

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.)

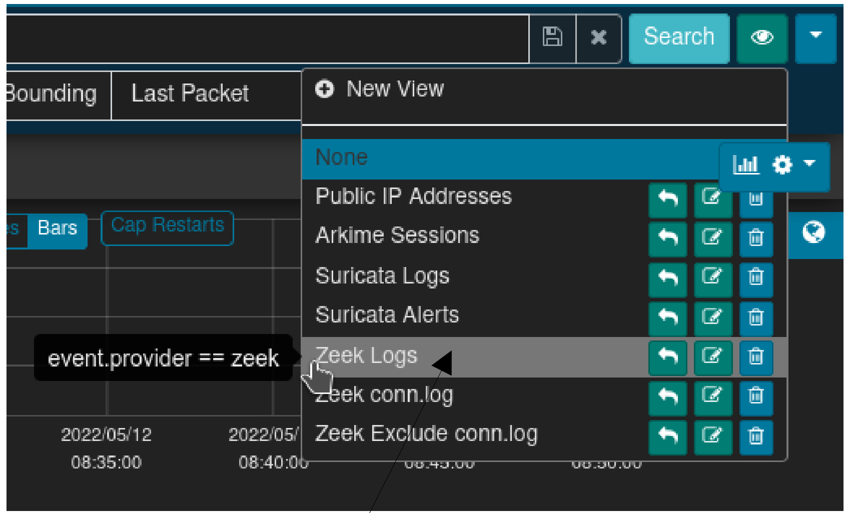
	Arkime	Dashboards (Lucene)	Dashboards (DQL)
GeoIP information available	`country == EXISTS!`	`_exists_:destination.geo OR _exists_:source.geo`	`destination.geo:* or source.geo:*`
Log type	`event.dataset == notice`	`event.dataset:notice`	`event.dataset:notice`
IP CIDR Subnets	`ip.src == 172.16.0.0/12`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

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



Search

Bounding | Last Packet

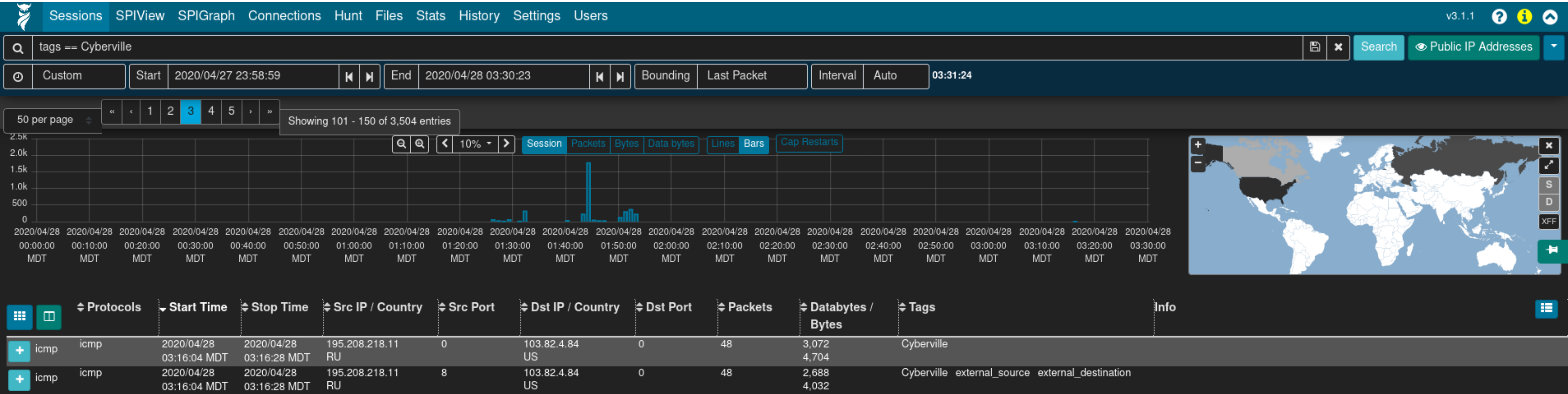
Bars | Cap Restarts

New View

None
Public IP Addresses
Arkime Sessions
Suricata Logs
Suricata Alerts
Zeek Logs
Zeek conn.log
Zeek Exclude conn.log

event.provider == zeek

2022/05/12 08:35:00 | 2022/05/ 08:40:00



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

tags == Cyberville

Search | Public IP Addresses

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

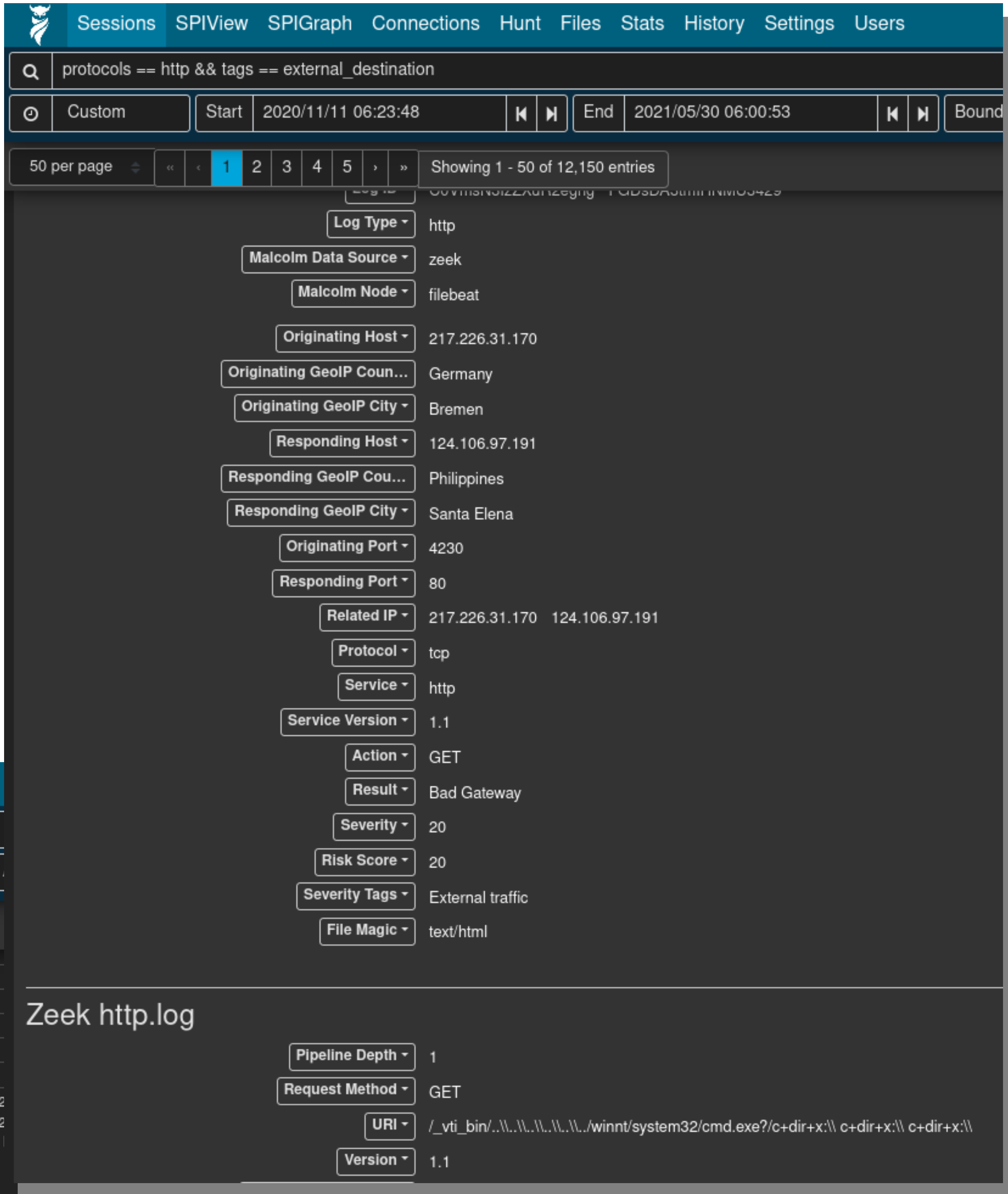
50 per page | « ‹ 1 2 3 4 5 › » | Showing 101 - 150 of 3,504 entries

10% | Session Packets Bytes Data bytes | Lines Bars | Cap Restarts

	Protocols	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Tags	Info
icmp	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	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


Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings Users

protocols == http && tags == external_destination

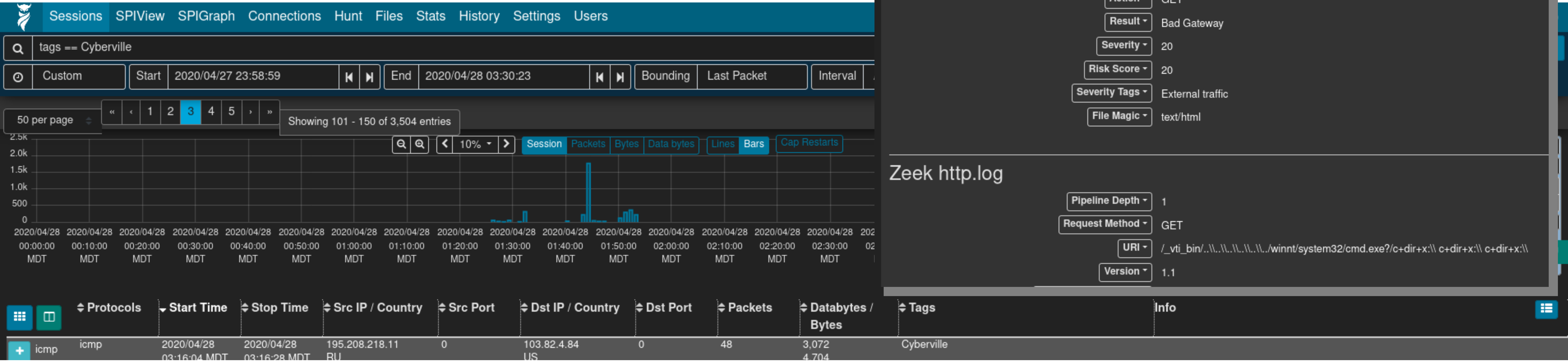
Custom | Start 2020/11/11 06:23:48 | End 2021/05/30 06:00:53 | Bound

50 per page « ‹ 1 2 3 4 5 › » Showing 1 - 50 of 12,150 entries

Log Type	http
Malcolm Data Source	zeek
Malcolm Node	filebeat
Originating Host	217.226.31.170
Originating GeoIP Coun...	Germany
Originating GeoIP City	Bremen
Responding Host	124.106.97.191
Responding GeoIP Cou...	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

Pipeline Depth	1
Request Method	GET
URI	/_vti_bin/..\\..\\..\\..\\..\\..\\../winnt/system32/cmd.exe?/c+dir+x:\\ c+dir+x:\\ c+dir+x:\\
Version	1.1



tags == Cyberville

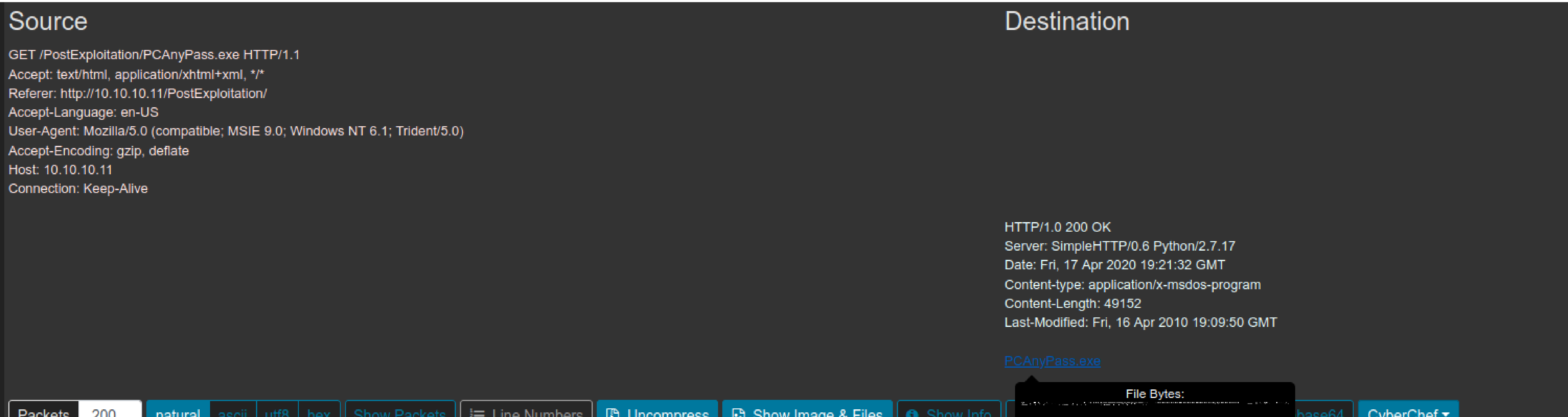
Custom | Start 2020/04/27 23:58:59 | End 2020/04/28 03:30:23 | Bounding Last Packet | Interval

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

	Protocols	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Tags	Info
icmp	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	

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

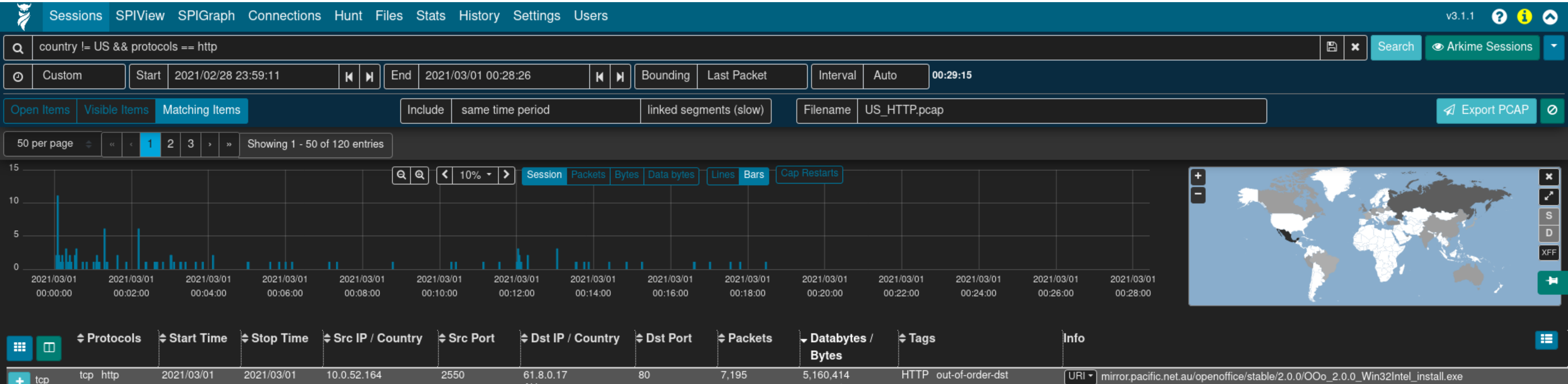
```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.17
Date: Fri, 17 Apr 2020 19:21:32 GMT
Content-type: application/x-msdos-program
Content-Length: 49152
Last-Modified: Fri, 16 Apr 2010 19:09:50 GMT
```

PCAnyPass.exe

File Bytes:

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)



country != US && protocols == http

Custom | Start 2021/02/28 23:59:11 | End 2021/03/01 00:28:26 | Bounding: Last Packet | Interval: Auto | 00:29:15

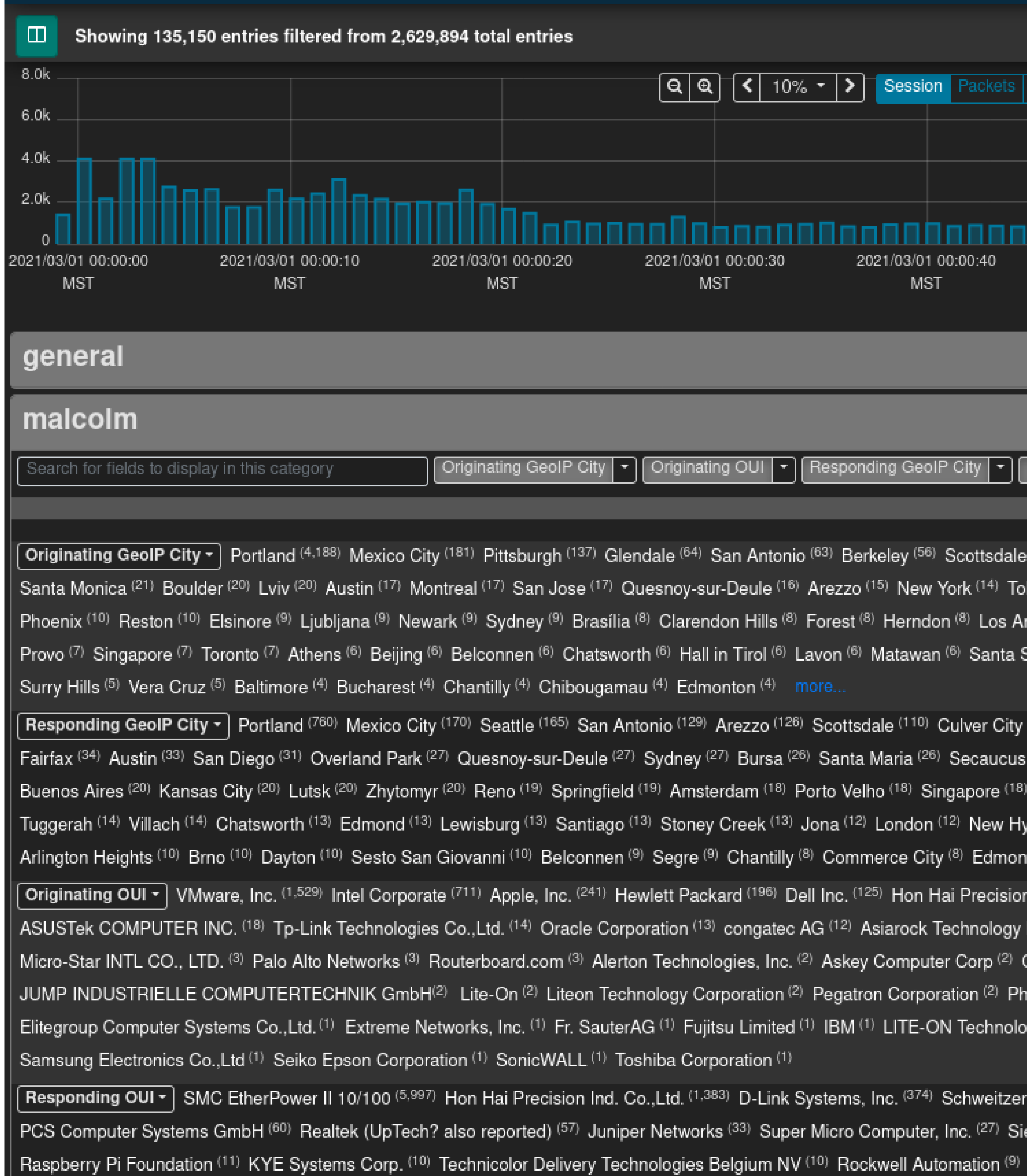
Include: same time period | linked segments (slow) | Filename: US_HTTP.pcap

Showing 1 - 50 of 120 entries

Protocols	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Tags	Info
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)



Showing 135,150 entries filtered from 2,629,894 total entries

general

malcolm

Search for fields to display in this category | Originating GeoIP City | Originating OUI | Responding GeoIP City

Originating GeoIP City: Portland (4,188) Mexico City (181) Pittsburgh (137) Glendale (64) San Antonio (63) Berkeley (56) Scottsdale
Santa Monica (21) Boulder (20) Lviv (20) Austin (17) Montreal (17) San Jose (17) Quesnoy-sur-Deule (16) Arezzo (15) New York (14) To
Phoenix (10) Reston (10) Elsinore (9) Ljubljana (9) Newark (9) Sydney (9) Brasília (8) Clarendon Hills (8) Forest (8) Herndon (8) Los A
Provo (7) Singapore (7) Toronto (7) Athens (6) Beijing (6) Belconnen (6) Chatsworth (6) Hall in Tirol (6) Lavon (6) Matawan (6) Santa
Surry Hills (5) Vera Cruz (5) Baltimore (4) Bucharest (4) Chantilly (4) Chibougamau (4) Edmonton (4) more...

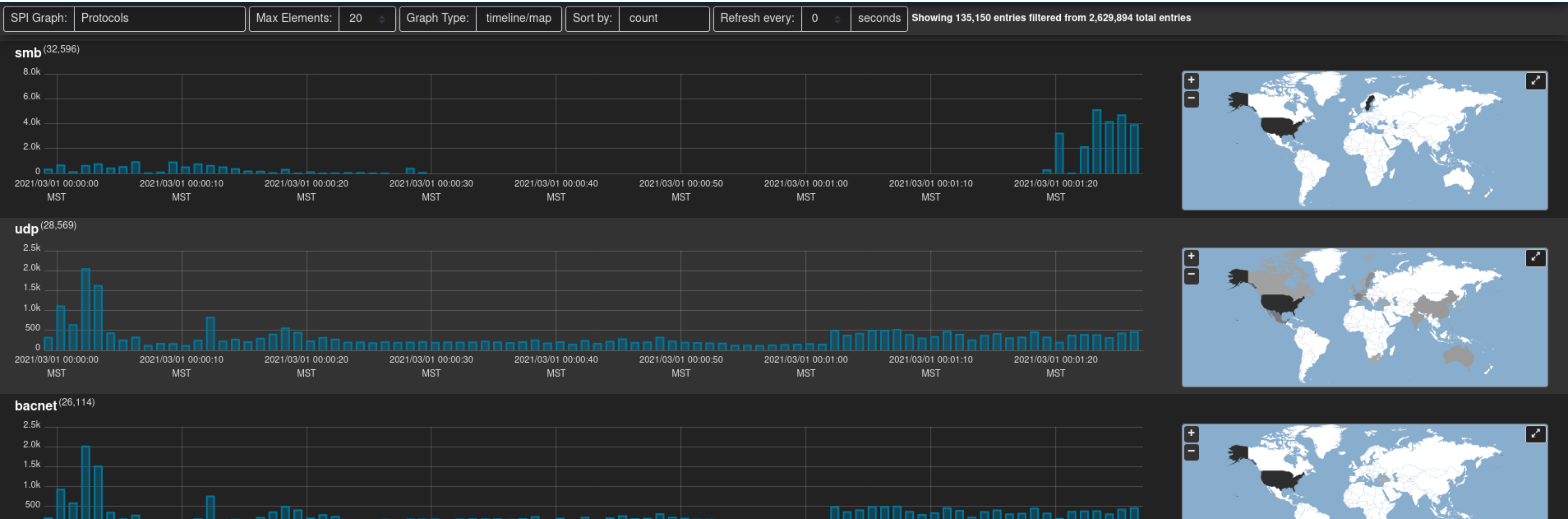
Responding GeoIP City: Portland (760) Mexico City (170) Seattle (165) San Antonio (129) Arezzo (126) Scottsdale (110) Culver City
Fairfax (34) Austin (33) San Diego (31) Overland Park (27) Quesnoy-sur-Deule (27) Sydney (27) Bursa (26) Santa Maria (26) Secaucus
Buenos Aires (20) Kansas City (20) Lutsk (20) Zhytomyr (20) Reno (19) Springfield (19) Amsterdam (18) Porto Velho (18) Singapore (18
Tuggerah (14) Villach (14) Chatsworth (13) Edmond (13) Lewisburg (13) Santiago (13) Stoney Creek (13) Jona (12) London (12) New Hy
Arlington Heights (10) Brno (10) Dayton (10) Sesto San Giovanni (10) Belconnen (9) Segre (9) Chantilly (8) Commerce City (8) Edmon

Originating OUI: VMware, Inc. (1,529) Intel Corporate (711) Apple, Inc. (241) Hewlett Packard (196) Dell Inc. (125) Hon Hai Precision
ASUSTek COMPUTER INC. (18) Tp-Link Technologies Co.,Ltd. (14) Oracle Corporation (13) congatec AG (12) Asiarock Technology
Micro-Star INTL CO., LTD. (3) Palo Alto Networks (3) Routerboard.com (3) Alerton Technologies, Inc. (2) Askey Computer Corp (2) C
JUMP INDUSTRIELLE COMPUTERTECHNIK GmbH (2) Lite-On (2) Liteon Technology Corporation (2) Pegatron Corporation (2) Ph
Elitegroup Computer Systems Co.,Ltd. (1) Extreme Networks, Inc. (1) Fr. SauterAG (1) Fujitsu Limited (1) IBM (1) LITE-ON Technolo
Samsung Electronics Co.,Ltd (1) Seiko Epson Corporation (1) SonicWALL (1) Toshiba Corporation (1)

Responding OUI: SMC EtherPower II 10/100 (5,997) Hon Hai Precision Ind. Co.,Ltd. (1,383) D-Link Systems, Inc. (374) Schweitzer
PCS Computer Systems GmbH (60) Realtek (UpTech? also reported) (57) Juniper Networks (33) Super Micro Computer, Inc. (27) Sie
Raspberry Pi Foundation (11) KYE Systems Corp. (10) Technicolor Delivery Technologies Belgium NV (10) Rockwell Automation (9)

SPIGraph

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


SPI Graph: Protocols | Max Elements: 20 | Graph Type: timeline/map | Sort by: count | Refresh every: 0 seconds | **Showing 135,150 entries filtered from 2,629,894 total entries**

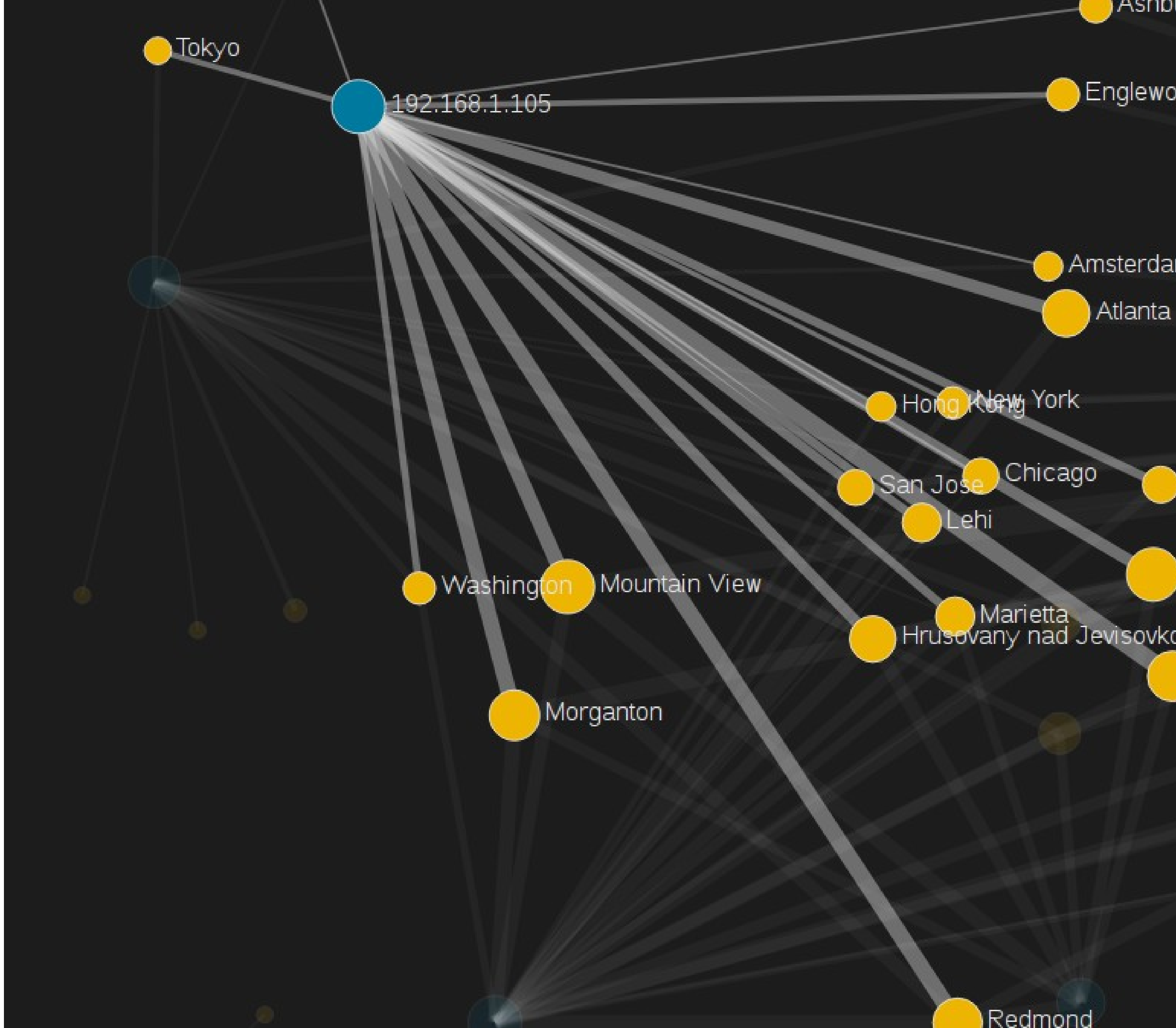
smb (32,596)

udp (28,569)

bacnet (26,114)

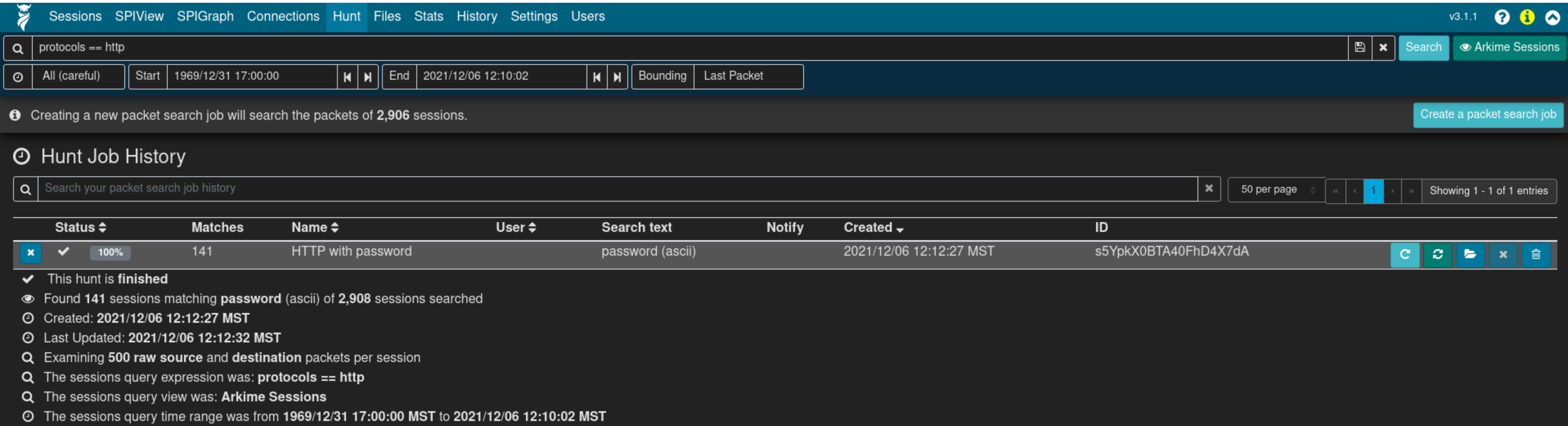
Connections

- 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
Search
Arkime Sessions
Create a packet search job

```
protocols == http
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.

Hunt Job History

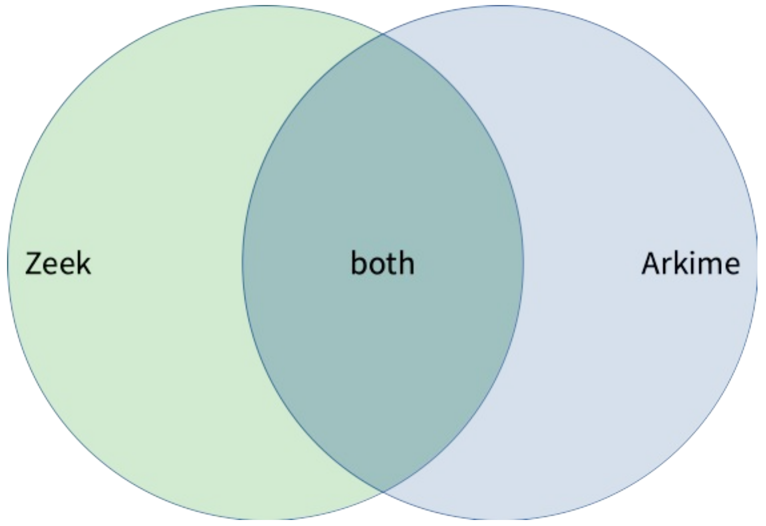
Search your packet search job history — 50 per page — Showing 1 - 1 of 1 entries

Status	Matches	Name	User	Search text	Notify	Created	ID
✓ 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

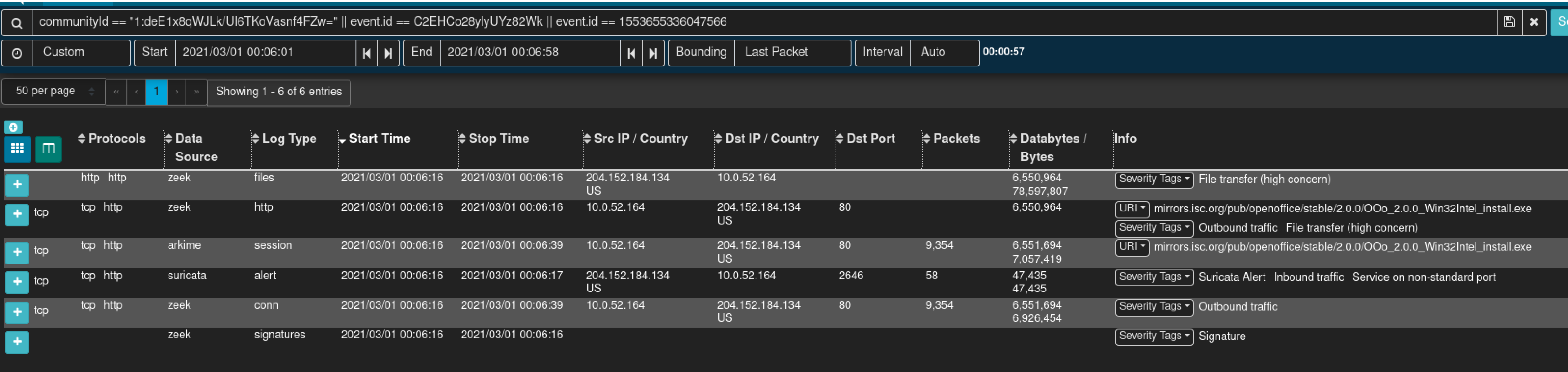
- Search syntax is different between Arkime and Dashboards (and in some cases, so are field names)
  - See search syntax comparison table, Malcolm and Arkime docs
- Despite considerable overlap, there are differences in protocol parser support among Zeek, Suricata and Arkime
  - Learning the strengths 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"
```



```
communityId == "1:deE1x8qWJLk/Ul6TKoVasnf4FZw=" || event.id == C2EHCo28ylyUYz82Wk || event.id == 1553655336047566
```

Custom | Start 2021/03/01 00:06:01 | End 2021/03/01 00:06:58 | Bounding Last Packet | Interval Auto | 00:00:57

50 per page | 1 | Showing 1 - 6 of 6 entries

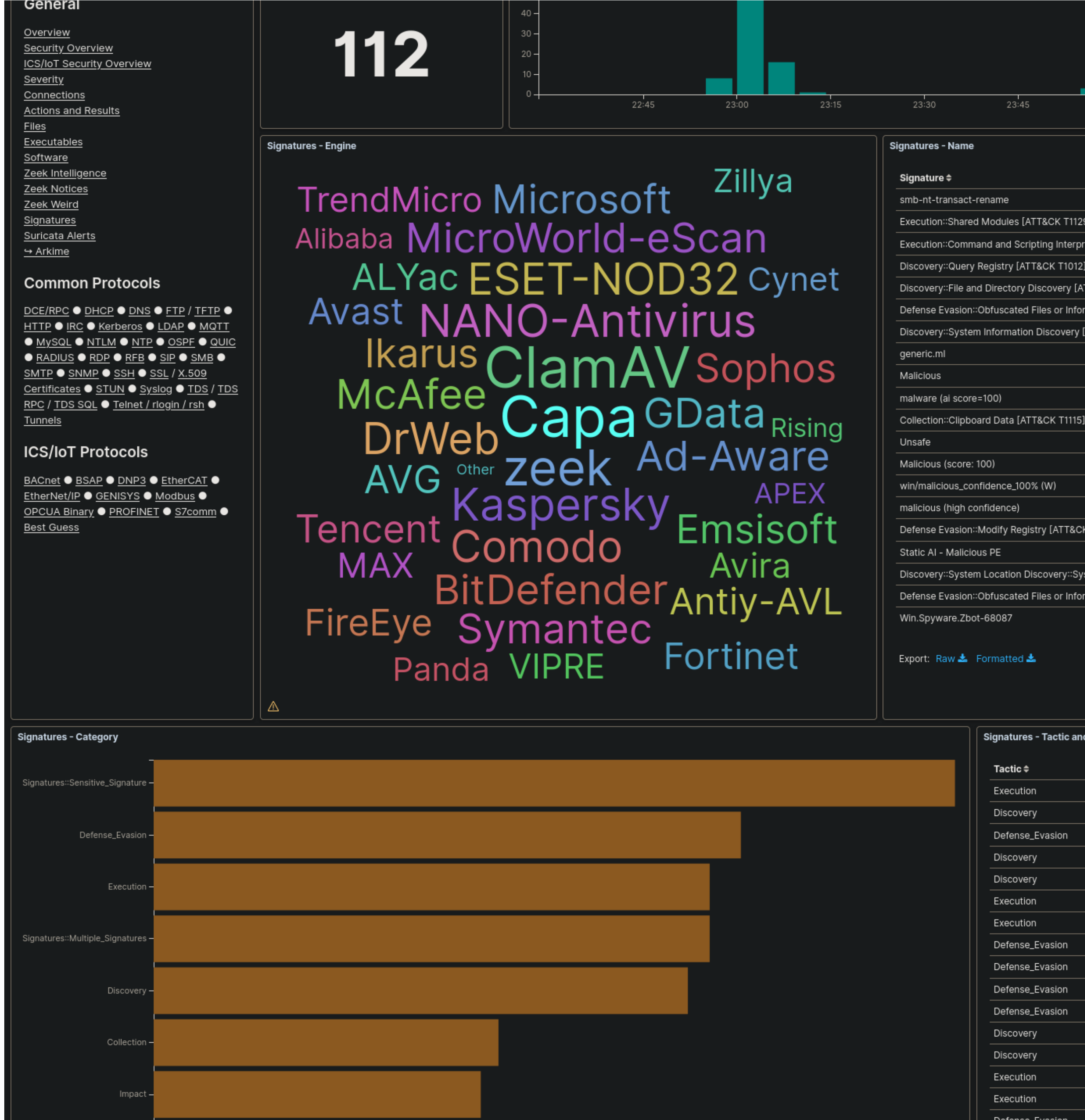
	Protocols	Data Source	Log Type	Start Time	Stop Time	Src IP / Country	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Info
	http http	zeek	files	2021/03/01 00:06:16	2021/03/01 00:06:16	204.152.184.134 US	10.0.52.164			6,550,964 78,597,807	Severity Tags File transfer (high concern)
tcp	tcp http	zeek	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	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	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	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
- Use `zeek.fuid` field in *Signatures – Logs* table to pivot to connection UID (`zeek.uid`) and other logs with pertinent session details



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

BACnet ● BSAP ● DNP3 ● EtherCAT ● EtherNet/IP ● GENISYS ● Modbus ● OPCUA Binary ● PROFINET ● S7comm ● Best Guess

112

Signatures - Engine

TrendMicro Microsoft Zillya Alibaba MicroWorld-eScan ALYac ESET-NOD32 Cynet Avast NANO-Antivirus Ikarus ClamAV Sophos McAfee Capa GData Rising DrWeb Ad-Aware AVG Other zeek Kaspersky APEX Tencent Emsisoft Comodo MAX Avira BitDefender Antiy-AVL FireEye Symantec Fortinet Panda VIPRE

Signatures - Name

Signature ⇕
smb-nt-transact-rename
Execution::Shared Modules [ATT&CK T112
Execution::Command and Scripting Interpr
Discovery::Query Registry [ATT&CK T1012]
Discovery::File and Directory Discovery [A
Defense Evasion::Obfuscated Files or Infor
Discovery::System Information Discovery [
generic.ml
Malicious
malware (ai score=100)
Collection::Clipboard Data [ATT&CK T1115]
Unsafe
Malicious (score: 100)
win/malicious_confidence_100% (W)
malicious (high confidence)
Defense Evasion::Modify Registry [ATT&C
Static AI - Malicious PE
Discovery::System Location Discovery::Sy
Defense Evasion::Obfuscated Files or Infor
Win.Spyware.Zbot-68087

Export: Raw Formatted

Signatures - Category

Signatures::Sensitive_Signature
Defense_Evasion
Execution
Signatures::Multiple_Signatures
Discovery
Collection
Impact

Signatures - Tactic an

Tactic ⇕
Execution
Discovery
Defense_Evasion
Discovery
Discovery
Execution
Execution
Defense_Evasion
Defense_Evasion
Defense_Evasion
Defense_Evasion
Discovery
Discovery
Execution
Execution

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 (2000+)
- 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

Malcolm

Thank you!

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