INL/CON-23-75833-Revision-1

Malcolm slides for NSPA workshop

February 2024

Seth D Grover

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-23-75833-Revision-1

Malcolm slides for NSPA workshop

Seth D Grover

February 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

EFFICIENT.EFFECTIVE.RESPONSIVE.

Malcolm

LOWERING THE BARRIER TO ENTRY FOR ESTABLISHING A SECURE CYBERSECURITY POSTURE

Critical Infrastructure Cybersecurity Workshop

Seth Grover, Cyber Security R&D

February 6, 2024

NATO
OTAN

NATO Support and
Procurement Agency
(NSPA)

INL

NATO UNCLASSIFIED

Malcolm

A POWERFUL 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 visualisation. 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

- Analyses 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.

FREE AND OPEN-SOURCE

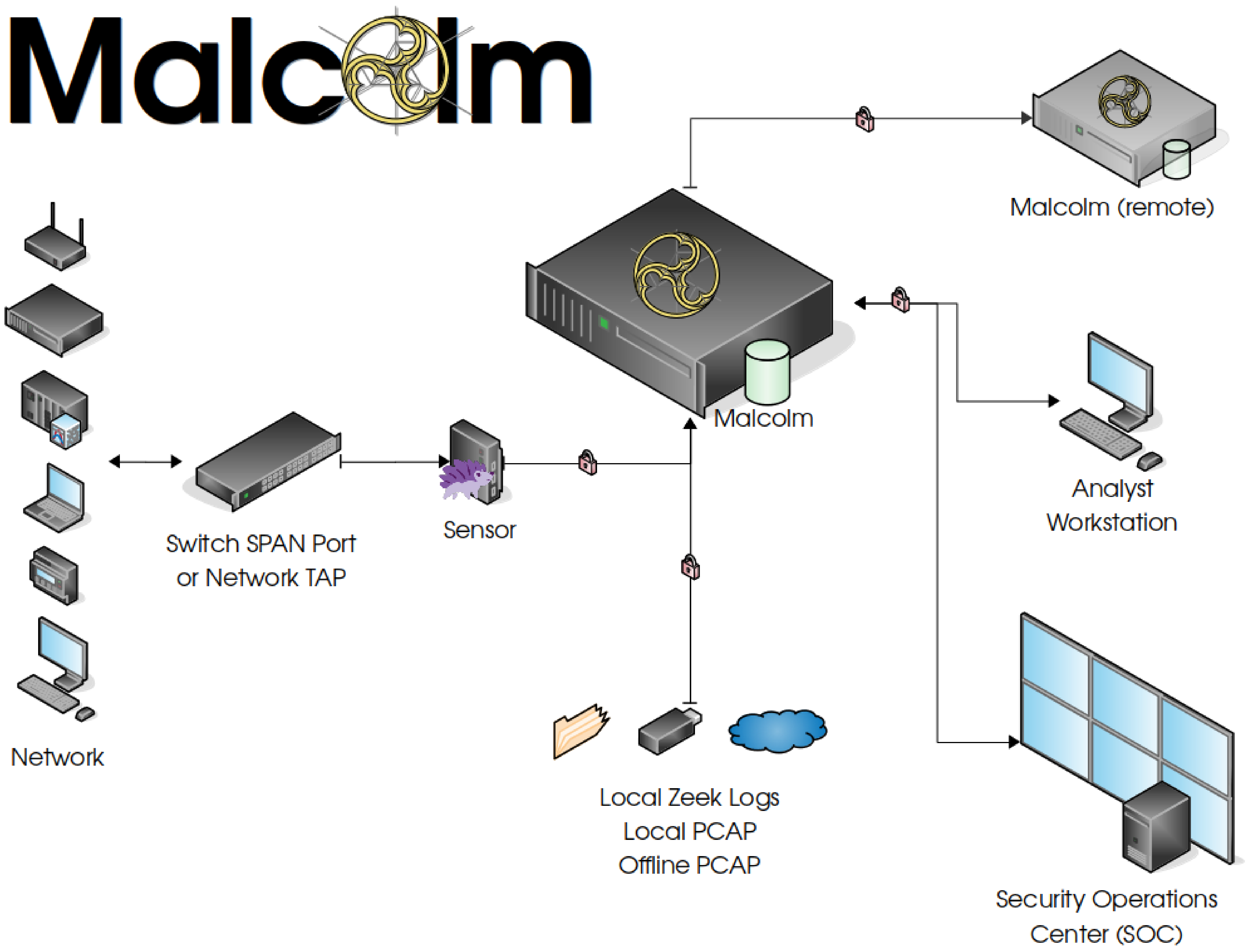
ORIGINS AND MILESTONES

- 2018.Q2 – Development begins on project (later dubbed "Malcolm") under CISA work agreement
- 2018.Q3 to 2019.Q2 – Field testing at USBR facilities
- 2019.Q2 – Initial public release
- 2020 – Collaboration begins with Germany's Federal Office for Information Security
- 2021.Q1 – First thousand 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 modelling and asset interaction analysis
- 2023.Q1 – Kali announces "Purple" bundling Malcolm
- 2023.Q2 – Cloud deployable with K8s

WHAT CAN IT DO FOR ME?

- Get to know your network: Malcolm **characterises** 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.

SIMPLIFIED NETWORK DIAGRAM



SUPPORTED 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)

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.)

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

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

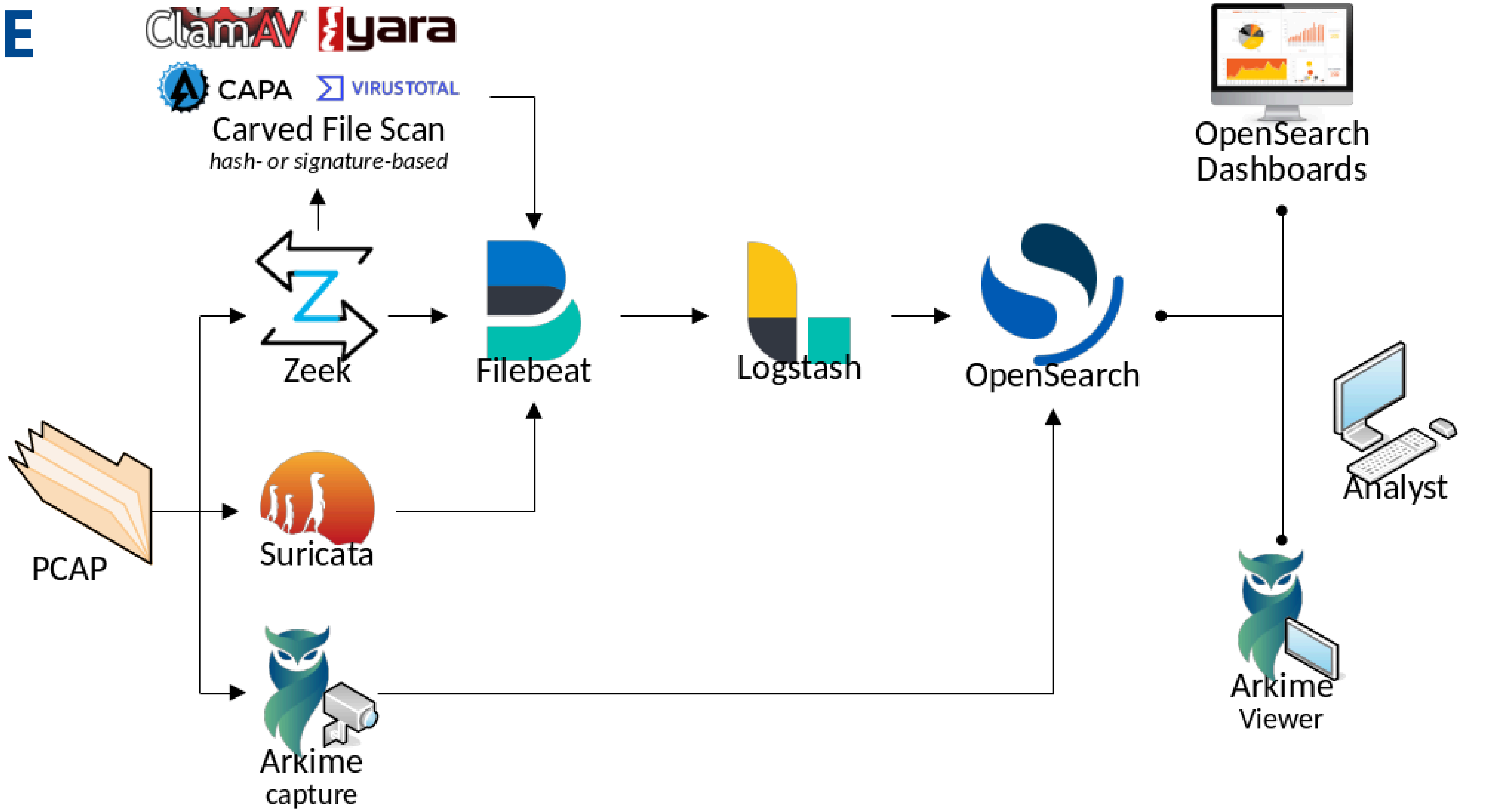
Payload Analysis

- CyberChef
- Arkime session PCAP export to WIRESHARK

Framework

- docker
- NGINX
- kubernetes

DATA PIPELINE



Traffic is collected passively by sensor device running Hedgehog Linux

Logs are securely forwarded to Malcolm

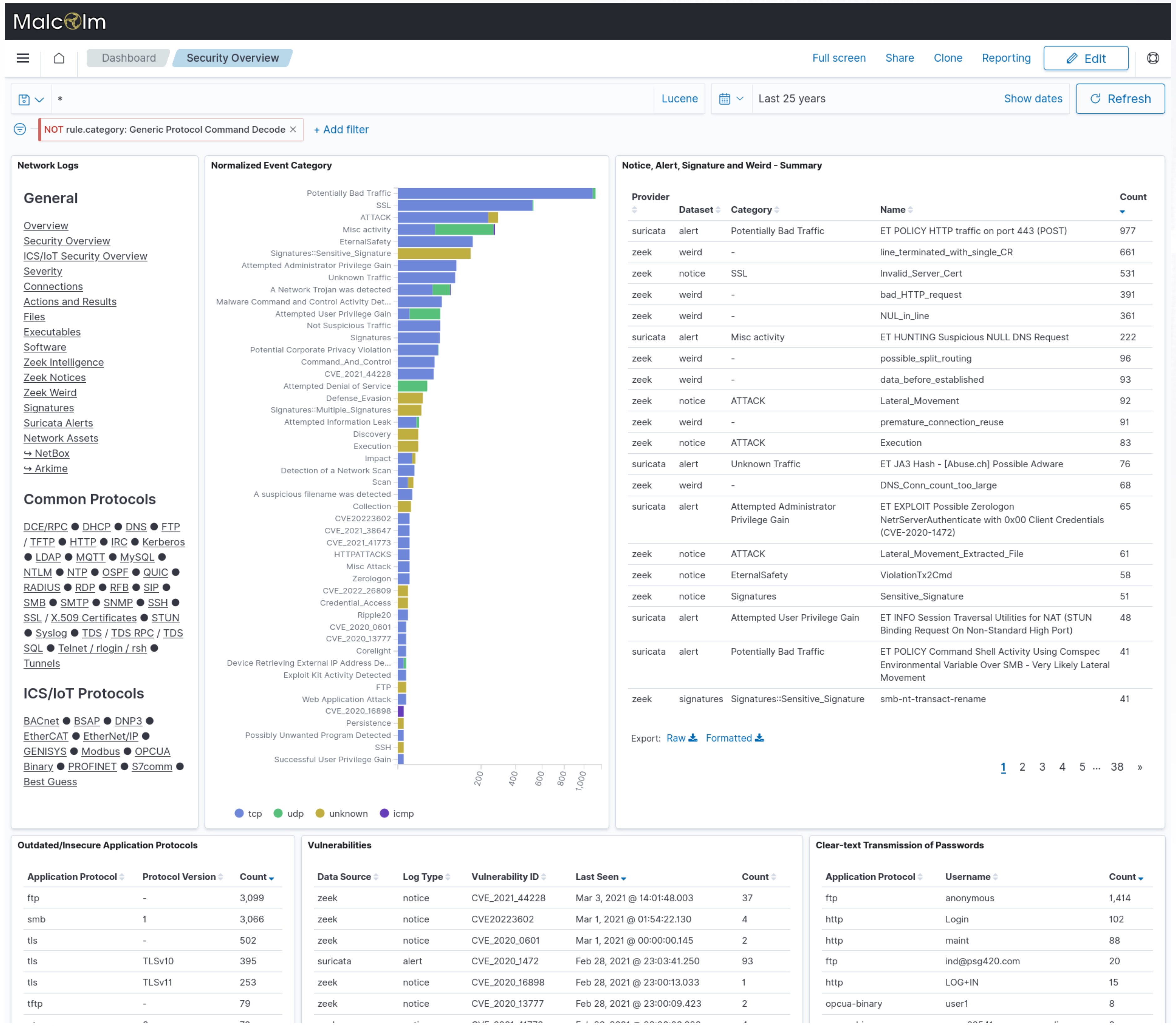
Logs are enriched and stored in OpenSearch

Machine learning algorithms identify anomalies

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

Traffic is visualised in OpenSearch Dashboards and Arkime Viewer

DASHBOARDS: FOCUS ON SECURITY



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
Network Assets
↪ NetBox
↪ 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
SSL
ATTACK
Misc activity
EternalSafety
Signatures::Sensitive_Signature
Attempted Administrator Privilege Gain
Unknown Traffic
A Network Trojan was detected
Malware Command and Control Activity Det...
Attempted User Privilege Gain
Not Suspicious Traffic
Signatures
Potential Corporate Privacy Violation
Command_And_Control
CVE_2021_44228
Attempted Denial of Service
Defense_Evasion
Signatures::Multiple_Signatures
Attempted Information Leak
Discovery
Execution
Impact
Detection of a Network Scan
Scan
A suspicious filename was detected
Collection
CVE20223602
CVE_2021_38647
CVE_2021_41773
HTTPATTACKS
Misc Attack
Zerologon
CVE_2022_26809
Credential_Access
Ripple20
CVE_2020_0601
CVE_2020_13777
Corelight
Device Retrieving External IP Address De...
Exploit Kit Activity Detected
FTP
Web Application Attack
CVE_2020_16898
Persistence
Possibly Unwanted Program Detected
SSH
Successful User Privilege Gain
200
400
600
800
1,000
tcp
udp
unknown
icmp

Notice, Alert, Signature and Weird - Summary

Provider	Dataset	Category	Name	Count
suricata	alert	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)	977
zeek	weird	-	line_terminated_with_single_CR	661
zeek	notice	SSL	Invalid_Server_Cert	531
zeek	weird	-	bad_HTTP_request	391
zeek	weird	-	NUL_in_line	361
suricata	alert	Misc activity	ET HUNTING Suspicious NULL DNS Request	222
zeek	weird	-	possible_split_routing	96
zeek	weird	-	data_before_established	93
zeek	notice	ATTACK	Lateral_Movement	92
zeek	weird	-	premature_connection_reuse	91
zeek	notice	ATTACK	Execution	83
suricata	alert	Unknown Traffic	ET JA3 Hash - [Abuse.ch] Possible Adware	76
zeek	weird	-	DNS_Conn_count_too_large	68
suricata	alert	Attempted Administrator Privilege Gain	ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)	65
zeek	notice	ATTACK	Lateral_Movement_Extracted_File	61
zeek	notice	EternalSafety	ViolationTx2Cmd	58
zeek	notice	Signatures	Sensitive_Signature	51
suricata	alert	Attempted User Privilege Gain	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)	48
suricata	alert	Potentially Bad Traffic	ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement	41
zeek	signatures	Signatures::Sensitive_Signature	smb-nt-transact-rename	41

Export: Raw Formatted

1 2 3 4 5 ... 38 »

Outdated/Insecure Application Protocols

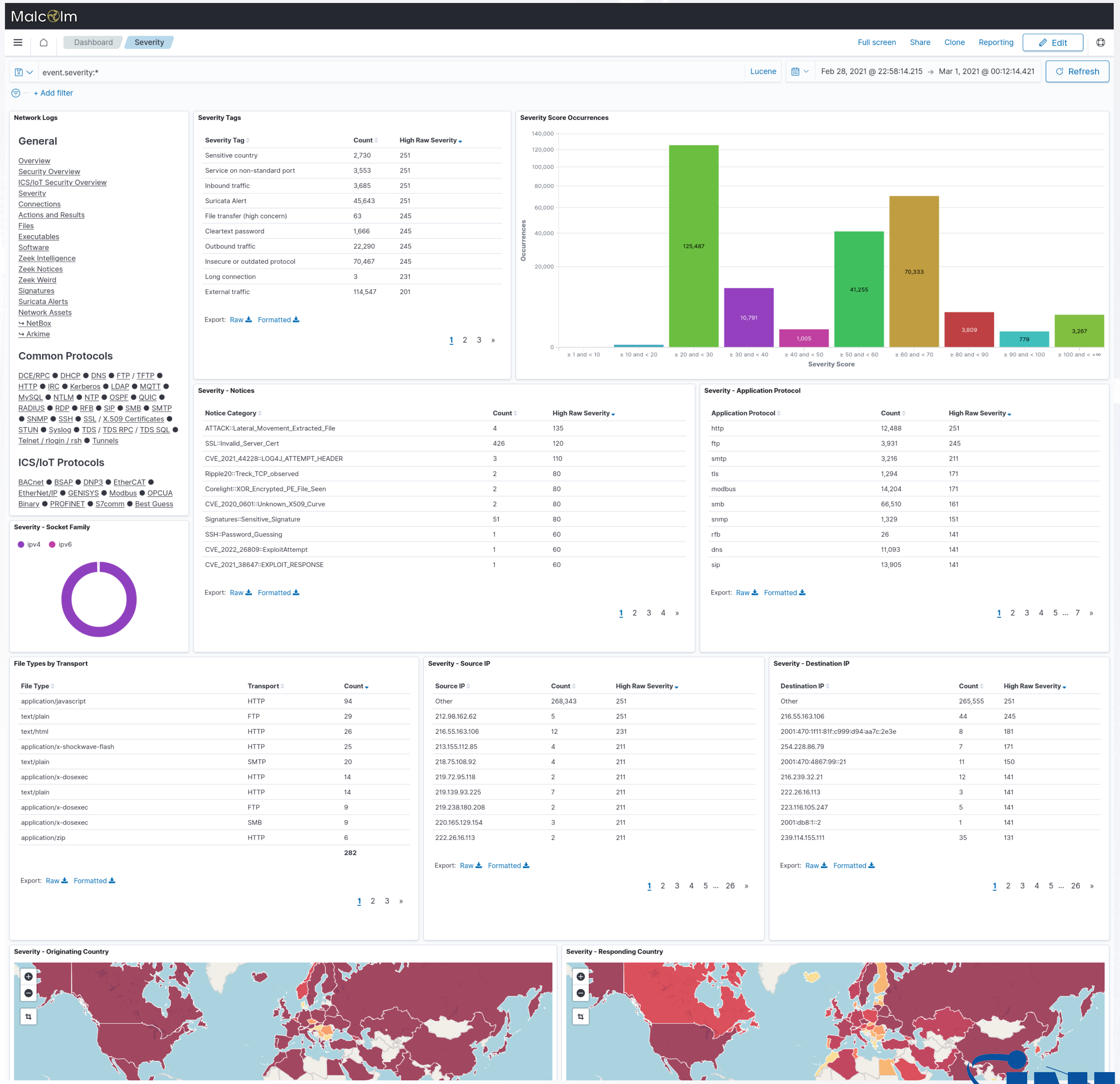
Application Protocol	Protocol Version	Count
ftp	-	3,099
smb	1	3,066
tls	-	502
tls	TLSv10	395
tls	TLSv11	253
tftp	-	79

Vulnerabilities

Data Source	Log Type	Vulnerability ID	Last Seen	Count
zeek	notice	CVE_2021_44228	Mar 3, 2021 @ 14:01:48.003	37
zeek	notice	CVE20223602	Mar 1, 2021 @ 01:54:22.130	4
zeek	notice	CVE_2020_0601	Mar 1, 2021 @ 00:00:00.145	2
suricata	alert	CVE_2020_1472	Feb 28, 2021 @ 23:03:41.250	93
zeek	notice	CVE_2020_16898	Feb 28, 2021 @ 23:00:13.033	1
zeek	notice	CVE_2020_13777	Feb 28, 2021 @ 23:00:09.423	2

Clear-text Transmission of Passwords

Application Protocol	Username	Count
ftp	anonymous	1,414
http	Login	102
http	maint	88
ftp	ind@psg420.com	20
http	LOG+IN	15
opcua-binary	user1	8



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
Network Assets
↪ NetBox
↪ 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

Severity Tags

Severity Tag	Count	High Raw Severity
Sensitive country	2,730	251
Service on non-standard port	3,553	251
Inbound traffic	3,685	251
Suricata Alert	45,643	251
File transfer (high concern)	63	245
Cleartext password	1,666	245
Outbound traffic	22,290	245
Insecure or outdated protocol	70,467	245
Long connection	3	231
External traffic	114,547	201

Export: Raw Formatted

1 2 3 »

Severity Score Occurrences

Severity - Socket Family

Severity - Notices

Notice Category	Count	High Raw Severity
ATTACK::Lateral_Movement_Extracted_File	4	135
SSL::Invalid_Server_Cert	426	120
CVE_2021_44228::LOG4J_ATTEMPT_HEADER	3	110
Ripple20::Treck_TCP_observed	2	80
Corelight::XOR_Encrypted_PE_File_Seen	2	80
CVE_2020_0601::Unknown_X509_Curve	2	80
Signatures::Sensitive_Signature	51	80
SSH::Password_Guessing	1	60
CVE_2022_26809::ExploitAttempt	1	60
CVE_2021_38647::EXPLOIT_RESPONSE	1	60

Export: Raw Formatted

1 2 3 4 »

Severity - Application Protocol

Application Protocol	Count	High Raw Severity
http	12,488	251
ftp	3,931	245
smtp	3,216	211
tls	1,294	171
modbus	14,204	171
smb	66,510	161
snmp	1,329	151
rfb	26	141
dns	11,093	141
sip	13,905	141

Export: Raw Formatted

1 2 3 4 5 ... 7 »

File Types by Transport

File Type	Transport	Count
application/javascript	HTTP	94
text/plain	FTP	29
text/html	HTTP	26
application/x-shockwave-flash	HTTP	25
text/plain	SMTP	20
application/x-dosexec	HTTP	14
text/plain	HTTP	14
application/x-dosexec	FTP	9
application/x-dosexec	SMB	9
application/zip	HTTP	6
		282

Export: Raw Formatted

1 2 3 »

Severity - Source IP

Source IP	Count	High Raw Severity
Other	268,343	251
212.98.162.62	5	251
216.55.163.106	12	231
213.155.112.85	4	211
218.75.108.92	4	211
219.72.95.118	2	211
219.139.93.225	7	211
219.238.180.208	2	211
220.165.129.154	3	211
222.26.16.113	2	211

Export: Raw Formatted

1 2 3 4 5 ... 26 »

Severity - Destination IP

Destination IP	Count	High Raw Severity
Other	265,555	251
216.55.163.106	44	245
2001:470:1f11:81f:c999:d94:aa7c:2e3e	8	181
254.228.86.79	7	171
2001:470:4867:99::21	11	150
216.239.32.21	12	141
222.26.16.113	3	141
223.116.105.247	5	141
2001:db8:1::2	1	141
239.114.155.111	35	131

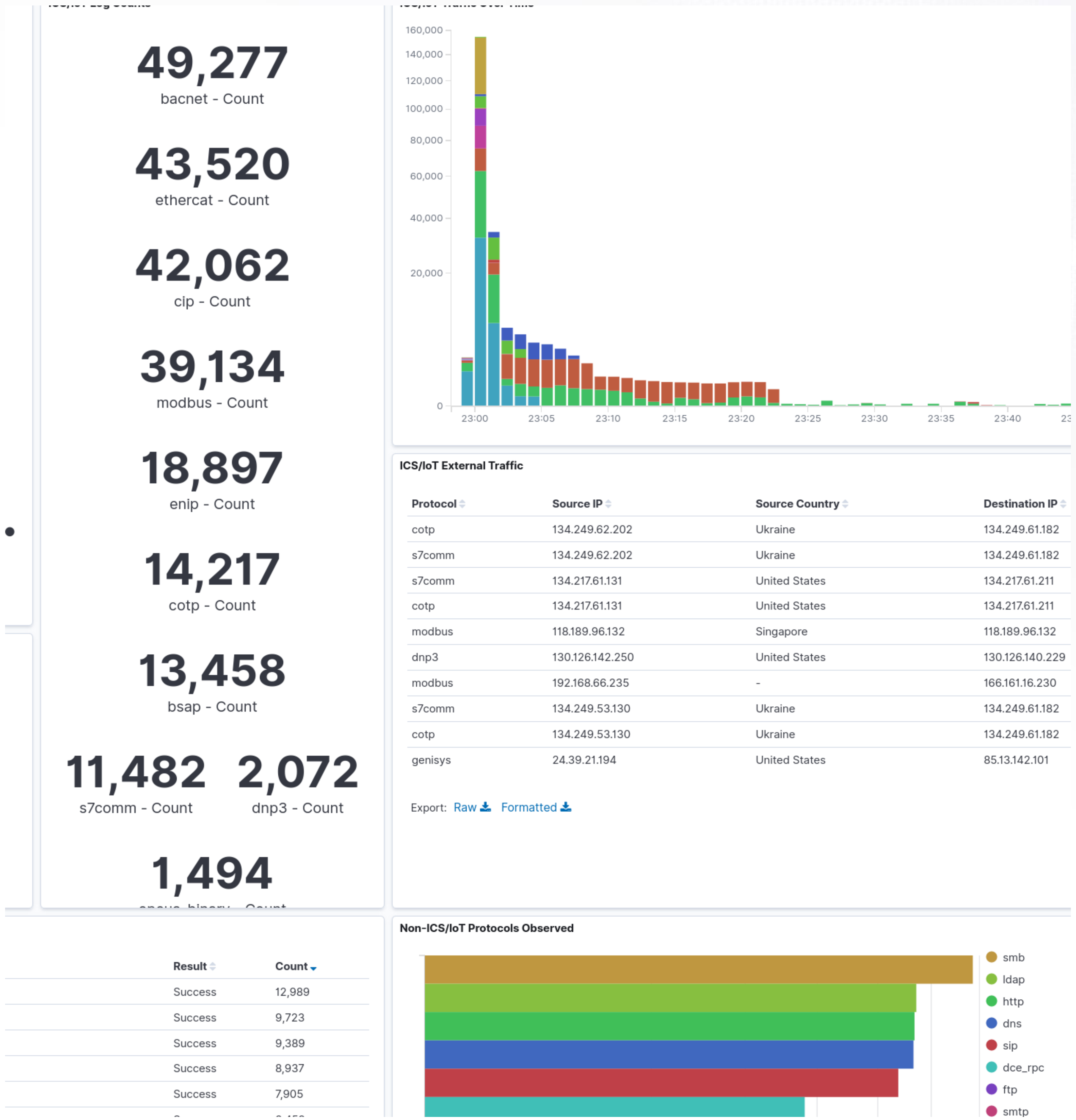
Export: Raw Formatted

1 2 3 4 5 ... 26 »

Severity - Originating Country

Severity - Responding Country

DASHBOARDS: FOCUS ON OT



49,277
bacnet - Count

43,520
ethercat - Count

42,062
cip - Count

39,134
modbus - Count

18,897
enip - Count

14,217
cotp - Count

13,458
bsap - Count

11,482
s7comm - Count

2,072
dnp3 - Count

1,494

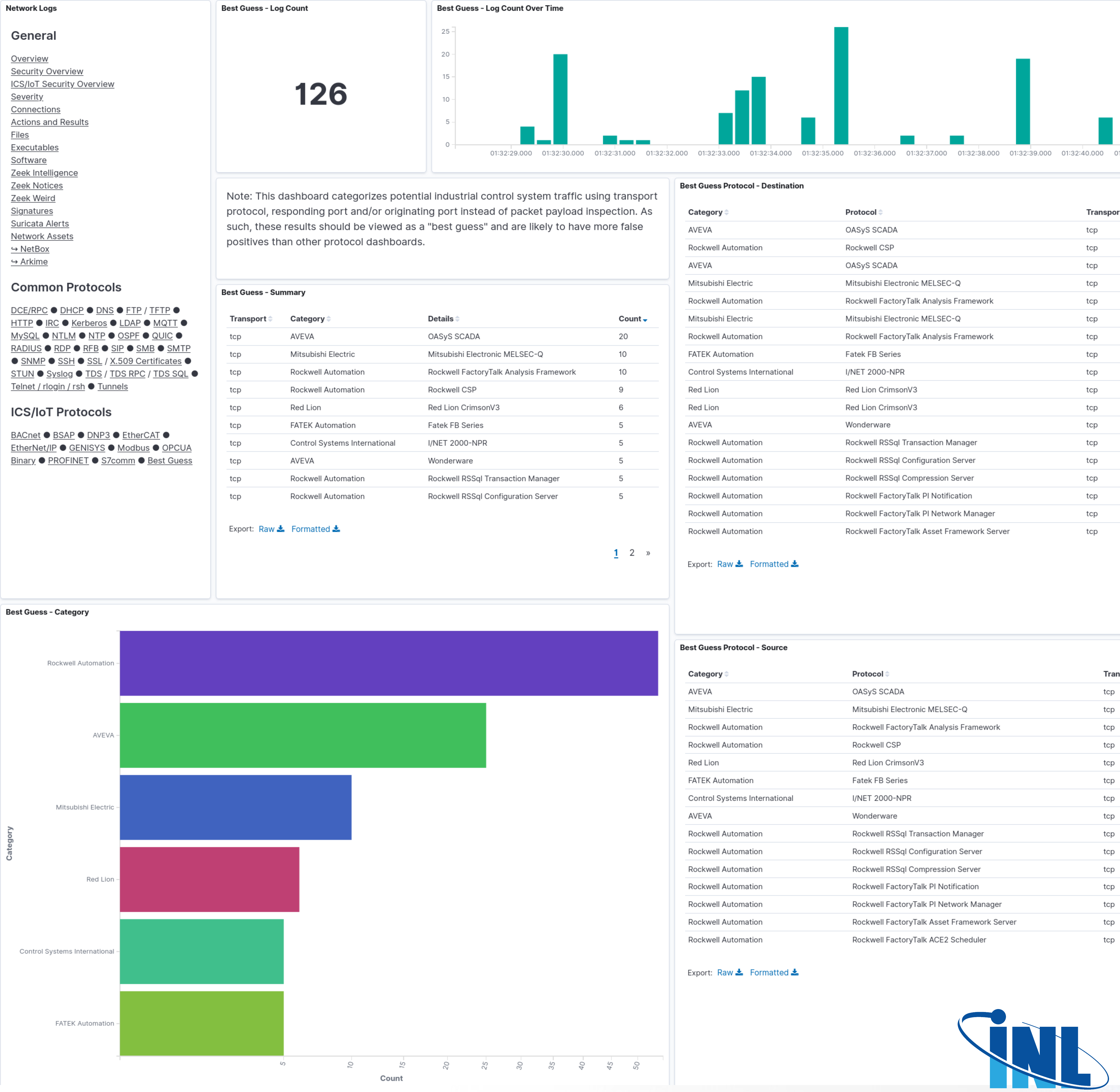
ICS/IoT External Traffic

Protocol	Source IP	Source Country	Destination IP
cotp	134.249.62.202	Ukraine	134.249.61.182
s7comm	134.249.62.202	Ukraine	134.249.61.182
s7comm	134.217.61.131	United States	134.217.61.211
cotp	134.217.61.131	United States	134.217.61.211
modbus	118.189.96.132	Singapore	118.189.96.132
dnp3	130.126.142.250	United States	130.126.140.229
modbus	192.168.66.235	-	166.161.16.230
s7comm	134.249.53.130	Ukraine	134.249.61.182
cotp	134.249.53.130	Ukraine	134.249.61.182
genisys	24.39.21.194	United States	85.13.142.101

Export: Raw Formatted

Result	Count
Success	12,989
Success	9,723
Success	9,389
Success	8,937
Success	7,905

Non-ICS/IoT Protocols Observed



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
Network Assets
↪ NetBox
↪ 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

Best Guess - Log Count

126

Best Guess - Log Count Over Time

Note: This dashboard categorizes potential industrial control system traffic using transport protocol, responding port and/or originating port instead of packet payload inspection. As such, these results should be viewed as a "best guess" and are likely to have more false positives than other protocol dashboards.

Best Guess - Summary

Transport	Category	Details	Count
tcp	AVEVA	OASyS SCADA	20
tcp	Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	10
tcp	Rockwell Automation	Rockwell FactoryTalk Analysis Framework	10
tcp	Rockwell Automation	Rockwell CSP	9
tcp	Red Lion	Red Lion CrimsonV3	6
tcp	FATEK Automation	Fatek FB Series	5
tcp	Control Systems International	I/NET 2000-NPR	5
tcp	AVEVA	Wonderware	5
tcp	Rockwell Automation	Rockwell RSSql Transaction Manager	5
tcp	Rockwell Automation	Rockwell RSSql Configuration Server	5

Export: Raw Formatted

1 2 »

Best Guess Protocol - Destination

Category	Protocol	Transpor
AVEVA	OASyS SCADA	tcp
Rockwell Automation	Rockwell CSP	tcp
AVEVA	OASyS SCADA	tcp
Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	tcp
Rockwell Automation	Rockwell FactoryTalk Analysis Framework	tcp
Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	tcp
Rockwell Automation	Rockwell FactoryTalk Analysis Framework	tcp
FATEK Automation	Fatek FB Series	tcp
Control Systems International	I/NET 2000-NPR	tcp
Red Lion	Red Lion CrimsonV3	tcp
Red Lion	Red Lion CrimsonV3	tcp
AVEVA	Wonderware	tcp
Rockwell Automation	Rockwell RSSql Transaction Manager	tcp
Rockwell Automation	Rockwell RSSql Configuration Server	tcp
Rockwell Automation	Rockwell RSSql Compression Server	tcp
Rockwell Automation	Rockwell FactoryTalk PI Notification	tcp
Rockwell Automation	Rockwell FactoryTalk PI Network Manager	tcp
Rockwell Automation	Rockwell FactoryTalk Asset Framework Server	tcp

Export: Raw Formatted

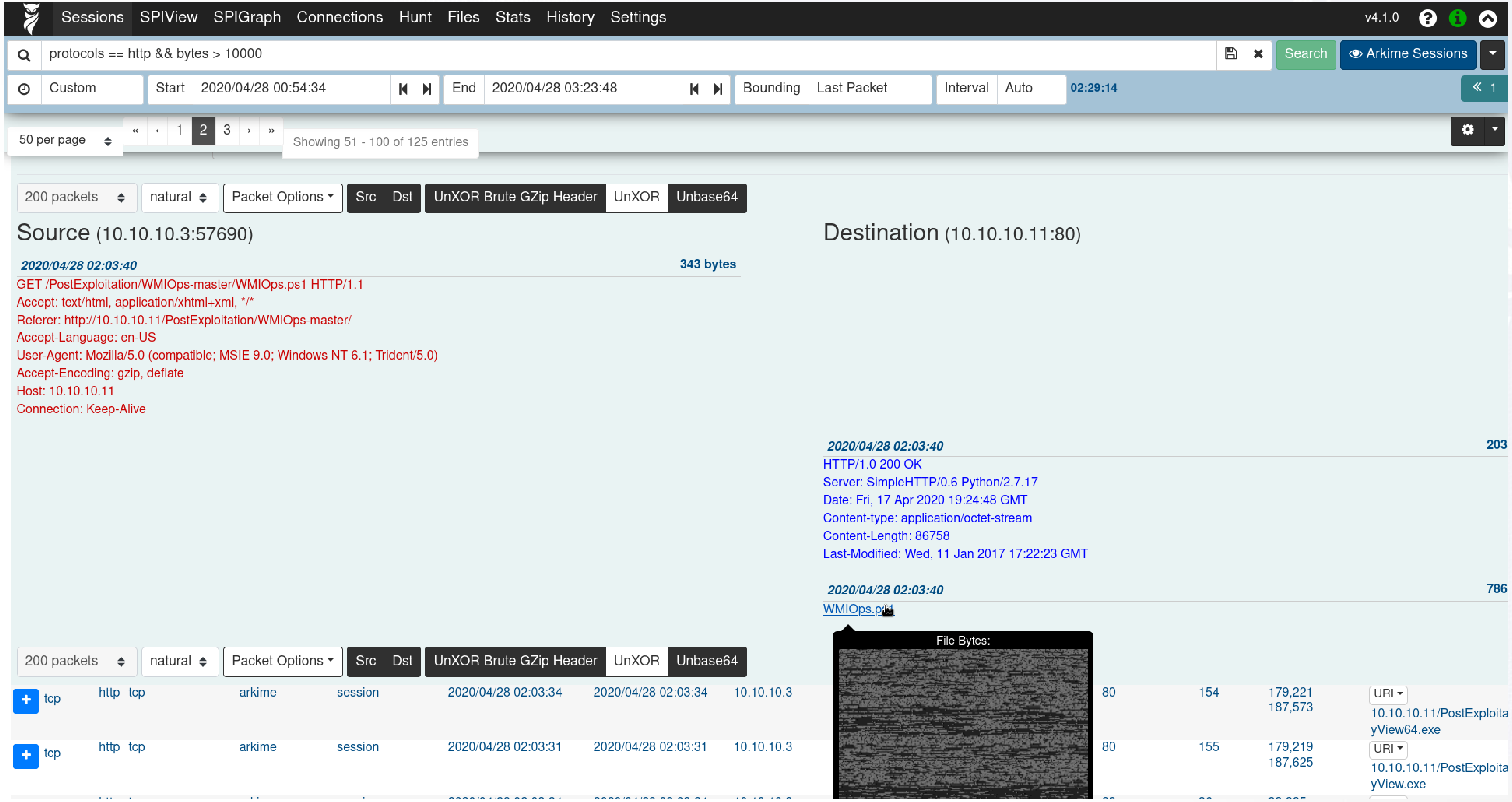
Best Guess - Category

Best Guess Protocol - Source

Category	Protocol	Tran
AVEVA	OASyS SCADA	tcp
Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	tcp
Rockwell Automation	Rockwell FactoryTalk Analysis Framework	tcp
Rockwell Automation	Rockwell CSP	tcp
Red Lion	Red Lion CrimsonV3	tcp
FATEK Automation	Fatek FB Series	tcp
Control Systems International	I/NET 2000-NPR	tcp
AVEVA	Wonderware	tcp
Rockwell Automation	Rockwell RSSql Transaction Manager	tcp
Rockwell Automation	Rockwell RSSql Configuration Server	tcp
Rockwell Automation	Rockwell RSSql Compression Server	tcp
Rockwell Automation	Rockwell FactoryTalk PI Notification	tcp
Rockwell Automation	Rockwell FactoryTalk PI Network Manager	tcp
Rockwell Automation	Rockwell FactoryTalk Asset Framework Server	tcp
Rockwell Automation	Rockwell FactoryTalk ACE2 Scheduler	tcp

Export: Raw Formatted

ARKIME: PACKET-LEVEL FORENSICS



protocols == http && bytes > 10000

Custom | Start 2020/04/28 00:54:34 | End 2020/04/28 03:23:48 | Bounding Last Packet | Interval Auto | 02:29:14

50 per page « ‹ 1 2 3 › » Showing 51 - 100 of 125 entries

200 packets | natural

Source (10.10.10.3:57690)

2020/04/28 02:03:40 **343 bytes**

```
GET /PostExploitation/WMIOps-master/WMIOps.ps1 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://10.10.10.11/PostExploitation/WMIOps-master/
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 (10.10.10.11:80)

2020/04/28 02:03:40 **203**

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.17
Date: Fri, 17 Apr 2020 19:24:48 GMT
Content-type: application/octet-stream
Content-Length: 86758
Last-Modified: Wed, 11 Jan 2017 17:22:23 GMT
```

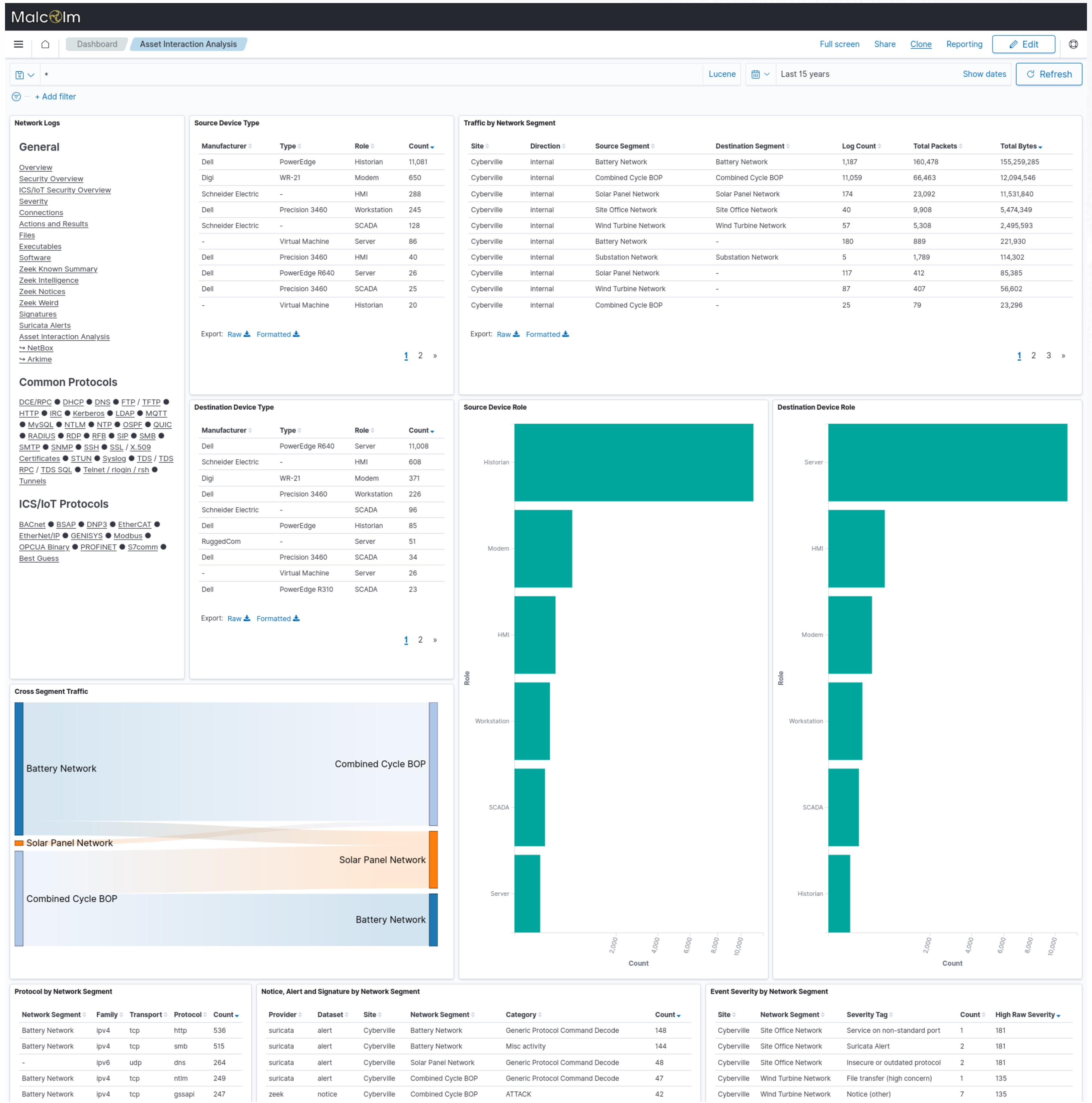
2020/04/28 02:03:40 **786**

WMIOps.ps1

200 packets | natural

+ tcp	http tcp	arkime	session	2020/04/28 02:03:34	2020/04/28 02:03:34	10.10.10.3	80	154	179,221 187,573	URI 10.10.10.11/PostExploitayView64.exe
+ tcp	http tcp	arkime	session	2020/04/28 02:03:31	2020/04/28 02:03:31	10.10.10.3	80	155	179,219 187,625	URI 10.10.10.11/PostExploitayView.exe

ASSET INTERACTION ANALYSIS



Network Logs

General

Overview
Security Overview
ICS/IoT Security Overview
Severity
Connections
Actions and Results
Files
Executables
Software
Zeek Known Summary
Zeek Intelligence
Zeek Notices
Zeek Weird
Signatures
Suricata Alerts
Asset Interaction Analysis
↪ NetBox
↪ 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

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 »

Destination Device Type

Manufacturer	Type	Role	Count
Dell	PowerEdge R640	Server	11,008
Schneider Electric	-	HMI	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 »

Source Device Role

Destination Device Role

Cross Segment Traffic

Protocol by Network Segment

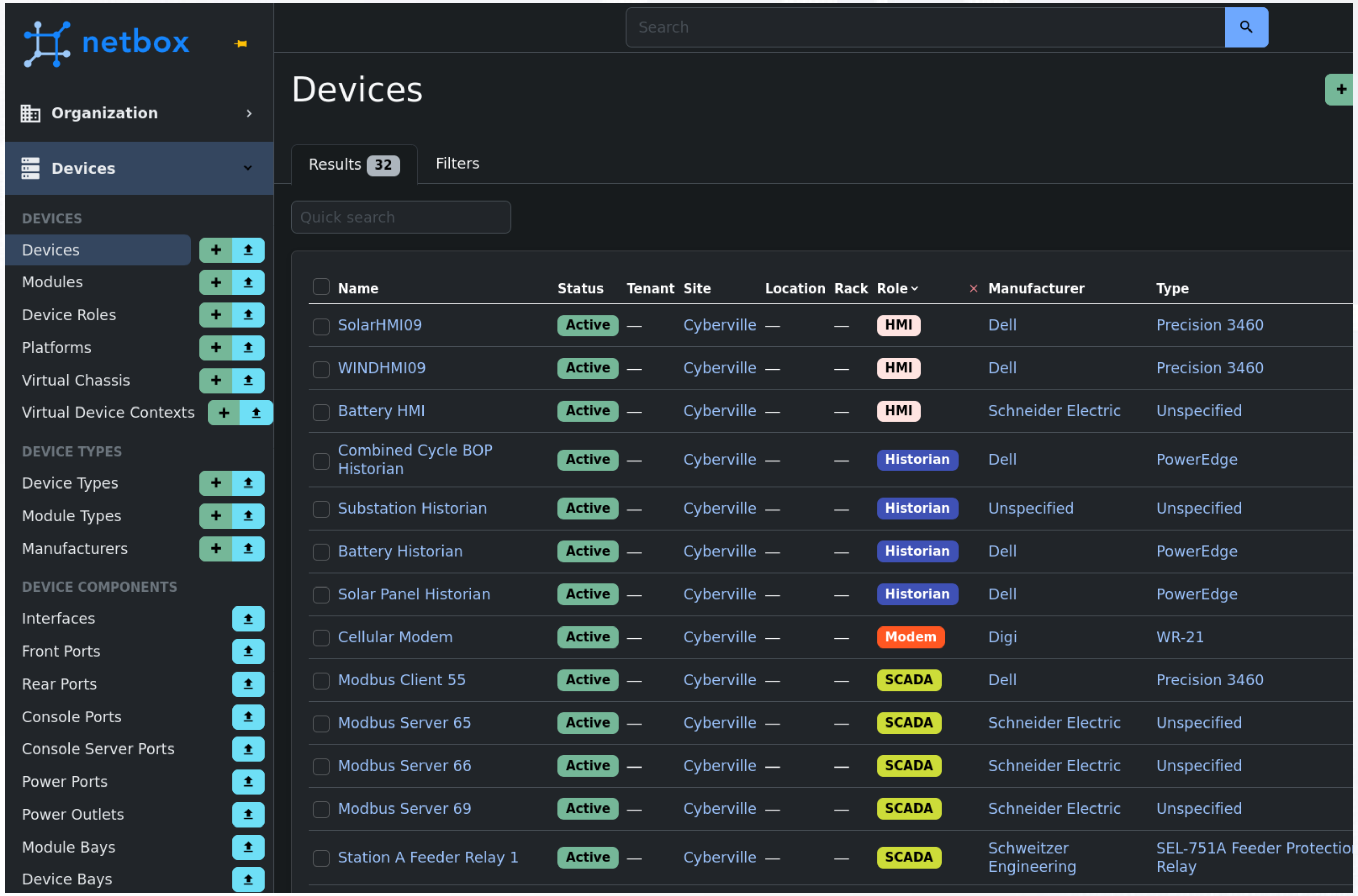
Network Segment	Family	Transport	Protocol	Count
Battery Network	ipv4	tcp	http	536
Battery Network	ipv4	tcp	smb	515
-	ipv6	udp	dns	264
Battery Network	ipv4	tcp	ntlm	249
Battery Network	ipv4	tcp	gssapi	247

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
zeek	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



Devices

Results 32   Filters

Quick search

Name	Status	Tenant	Site	Location	Rack	Role	Manufacturer	Type
SolarHMI09	Active	—	Cyberville	—	—	HMI	Dell	Precision 3460
WINDHMI09	Active	—	Cyberville	—	—	HMI	Dell	Precision 3460
Battery HMI	Active	—	Cyberville	—	—	HMI	Schneider Electric	Unspecified
Combined Cycle BOP Historian	Active	—	Cyberville	—	—	Historian	Dell	PowerEdge
Substation Historian	Active	—	Cyberville	—	—	Historian	Unspecified	Unspecified
Battery Historian	Active	—	Cyberville	—	—	Historian	Dell	PowerEdge
Solar Panel Historian	Active	—	Cyberville	—	—	Historian	Dell	PowerEdge
Cellular Modem	Active	—	Cyberville	—	—	Modem	Digi	WR-21
Modbus Client 55	Active	—	Cyberville	—	—	SCADA	Dell	Precision 3460
Modbus Server 65	Active	—	Cyberville	—	—	SCADA	Schneider Electric	Unspecified
Modbus Server 66	Active	—	Cyberville	—	—	SCADA	Schneider Electric	Unspecified
Modbus Server 69	Active	—	Cyberville	—	—	SCADA	Schneider Electric	Unspecified
Station A Feeder Relay 1	Active	—	Cyberville	—	—	SCADA	Schweitzer Engineering	SEL-751A Feeder Protectio Relay

TOWARDS THE FUTURE

- Community Building
  - Official DHS-hosted Slack channel
  - Prepackaged training modules
  - Additional tutorial videos on YouTube
- Vulnerability/IOC sharing, identification (CSAF), and exploitation visibility (KEV)
- Improve asset inventory capabilities
  - Passive auto-population
  - Active scanning
- Further analytics, rule, and ML development
- Improve cloud deployment
- Improve integration of 3rd party/host logs
- Increase OT/ICS protocol support
  - HART-IP, IEC 61850 GOOSE, ANSI C12.22, PROFINET-IO CM, ...

REACH OUT

https://idaholab.github.io/Malcolm

- downloads
- documentation and tutorials
- project status
- issue tracker
- … and more!

Email: malcolm@inl.gov