INL/MIS-23-75752-Revision-0

Malcolm: Lowering the Barrier to Entry for Establishing a Secure Cybersecurity Posture

November 2023

Seth D Grover

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-23-75752-Revision-0

Malcolm: Lowering the Barrier to Entry for Establishing a Secure Cybersecurity Posture

Seth D Grover

November 2023

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

November 7, 2023

Seth Grover
Malcolm Project Lead
Cybersecurity R&D

Malcolm

Lowering the Barrier to Entry for Establishing a Secure Cybersecurity Posture

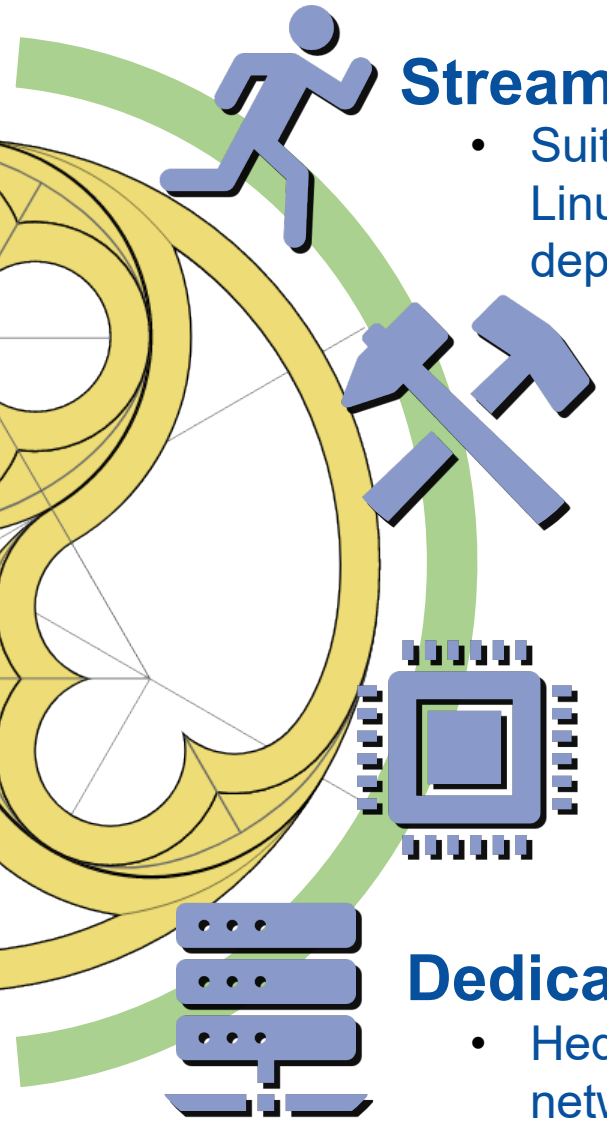
Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

INL Idaho National Laboratory

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 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.

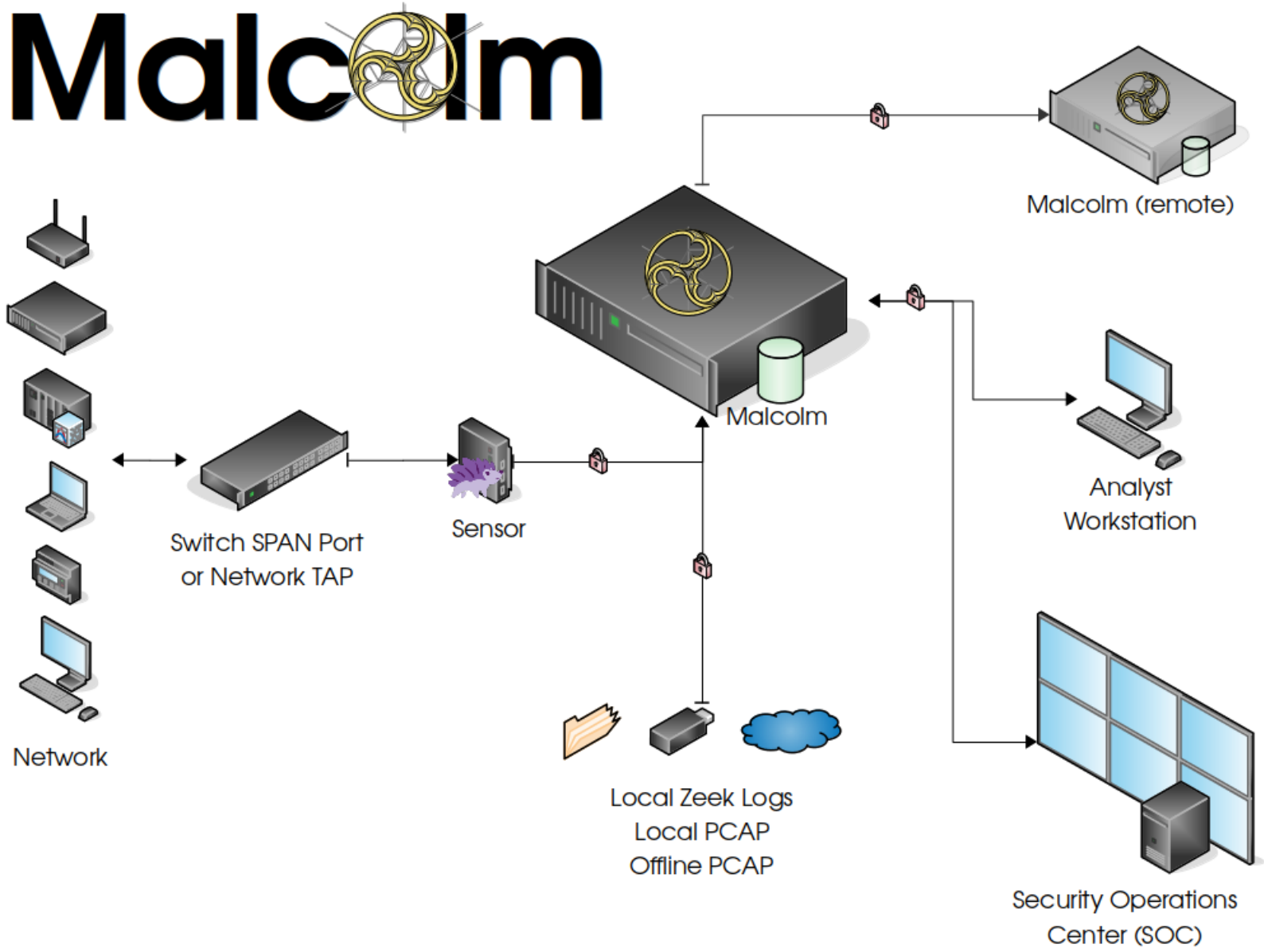
Malcolm Origins and Milestones

- 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 modelling 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


Malcolm (remote)
Malcolm
Analyst
Workstation
Switch SPAN Port
or Network TAP
Sensor
Network
Local Zeek Logs
Local PCAP
Offline PCAP
Security Operations
Center (SOC)

Malcolm 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***

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

Network Modelling

- netbox

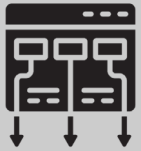
Visualization

- OpenSearch Dashboards
- Arkime

Payload Analysis

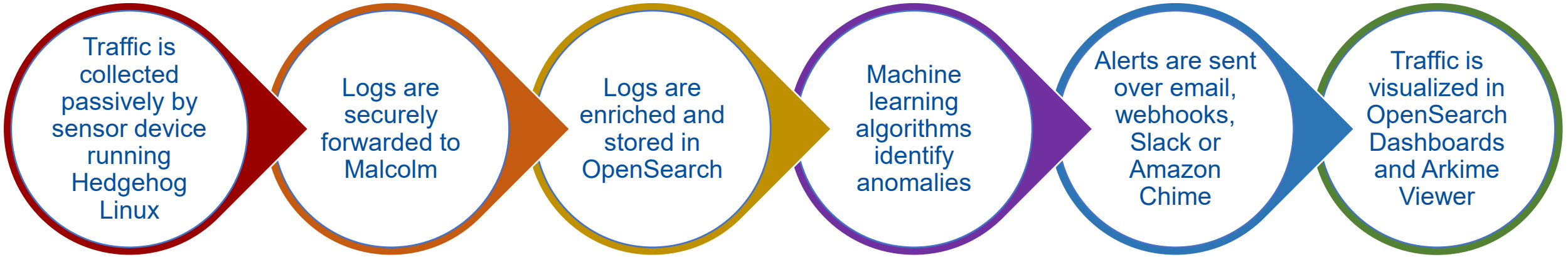
- CyberChef
- Arkime session PCAP export to WIRESHARK

Framework



- NGINX
- docker
- kubernetes

Malcolm Data Pipeline



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

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

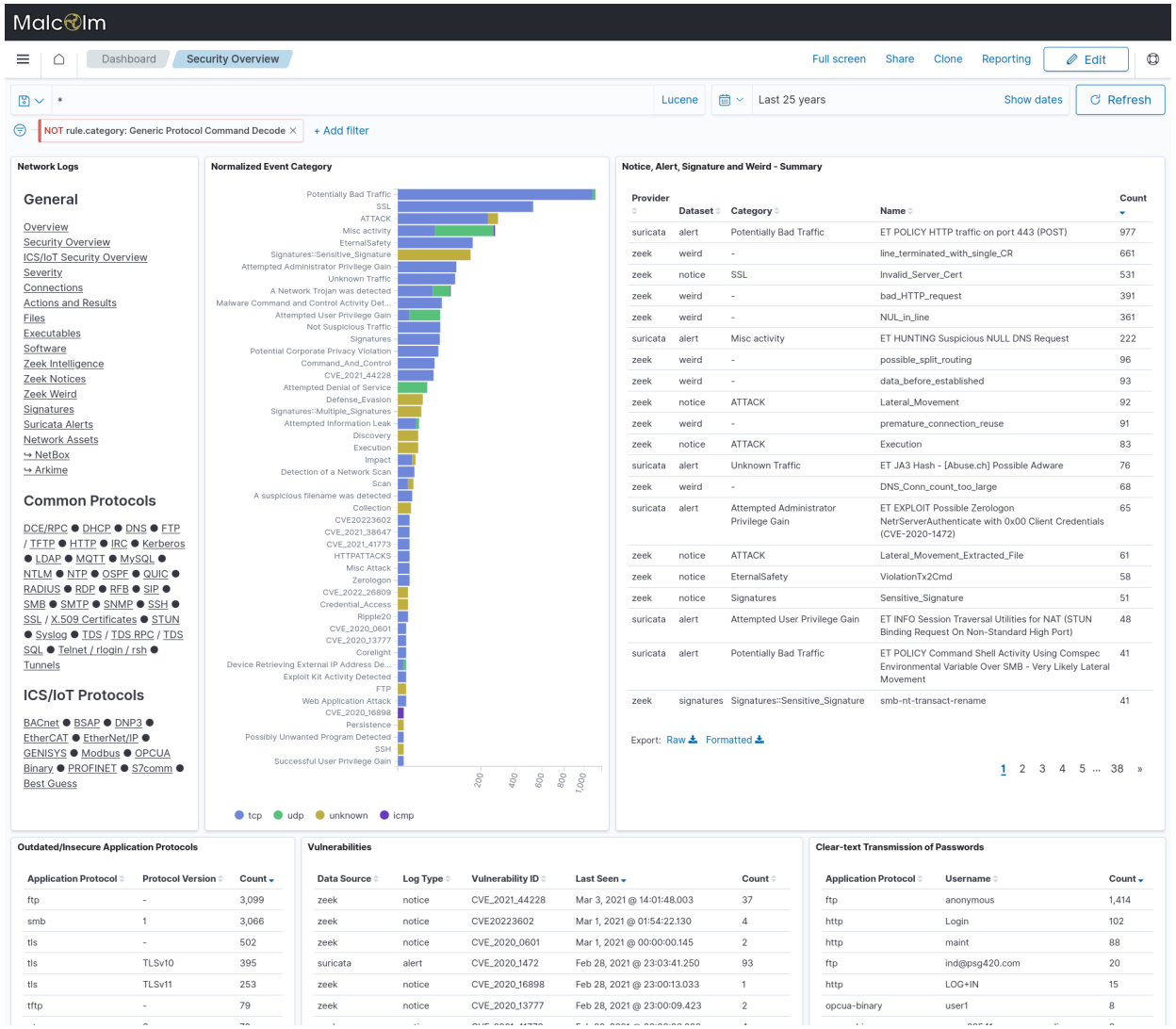
- Lookups are performed for GeoIP, ASN, MAC-to-vendor, community ID, domain name entropy, etc.
- Network events are normalized across protocols and data sources
- Best-guess techniques are applied to identify obscure OT traffic
- Enriched metadata may be forwarded to higher-tiered Malcolm instance

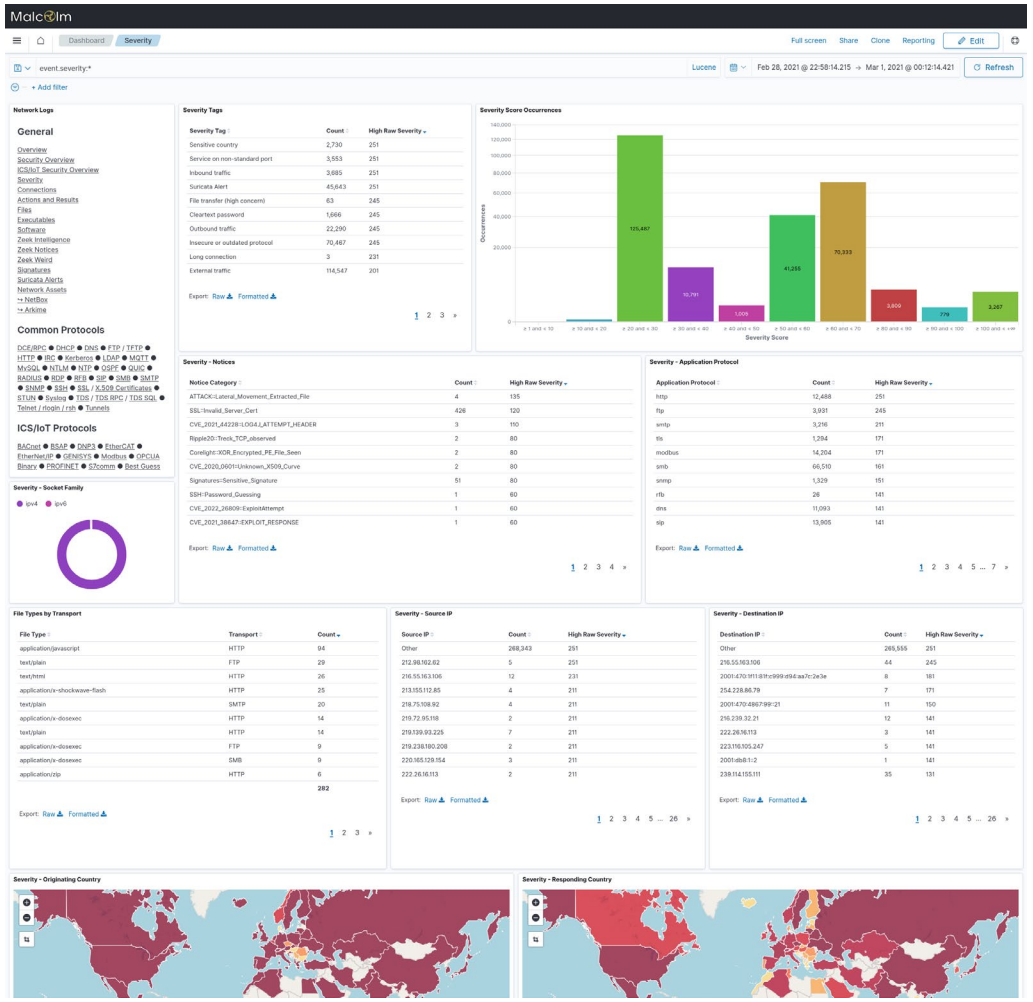
- Default detectors are provided for action and result, flow size, and MIME types of file transfers
- Custom detectors may be created for any aspect of any supported protocol

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

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

Malcolm Dashboards: Focus on Security





IDAHO NATIONAL LABORATORY

Malcolm Dashboards: Focus on OT

49,277
bacnet - Count

43,520
ethercat - Count

42,062
cip - Count

39,134
modbus - Count

18,897
enip - Count

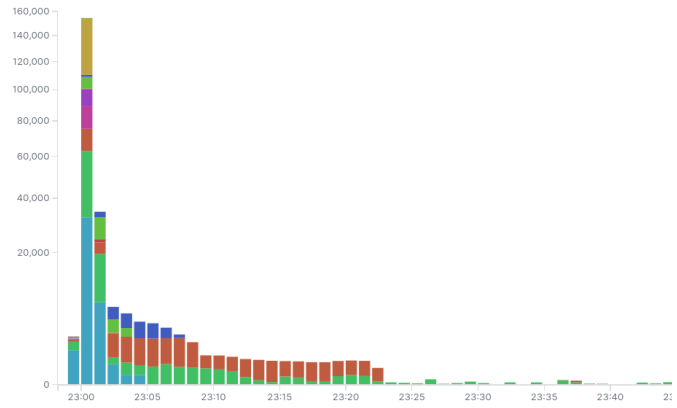
14,217
cotp - Count

13,458
bsap - Count

11,482
s7comm - Count

2,072
dnp3 - Count

1,494



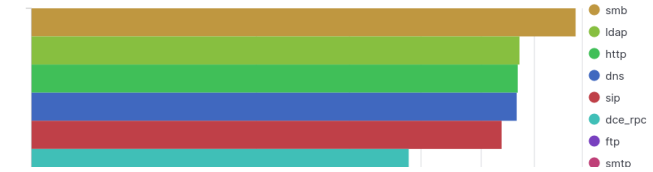
ICS/IoT External Traffic

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



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

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 »

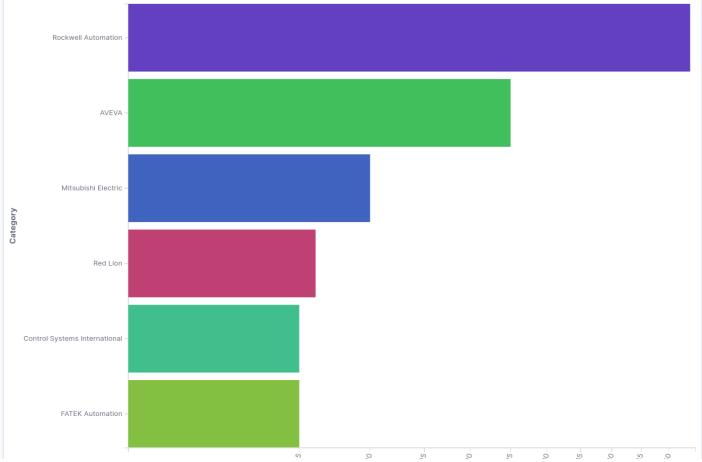
Best Guess Protocol - Destination

Category	Protocol	Transport	Destination	Count
AVEVA	OASyS SCADA	tcp	10.10.20.10	12
Rockwell Automation	Rockwell CSP	tcp	10.10.20.11	9
AVEVA	OASyS SCADA	tcp	10.10.20.11	8
Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	tcp	10.10.20.10	6
Rockwell Automation	Rockwell FactoryTalk Analysis Framework	tcp	10.10.20.10	6
Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	tcp	10.10.20.11	4
Rockwell Automation	Rockwell FactoryTalk Analysis Framework	tcp	10.10.20.11	4
FATEK Automation	Fatek FB Series	tcp	10.10.20.10	3
Control Systems International	I/NET 2000-NPR	tcp	10.10.20.10	3
Red Lion	Red Lion CrimsonV3	tcp	10.10.20.11	3
Red Lion	Red Lion CrimsonV3	tcp	10.10.20.10	3
AVEVA	Wonderware	tcp	10.10.20.10	3
Rockwell Automation	Rockwell RSSql Transaction Manager	tcp	10.10.20.10	3
Rockwell Automation	Rockwell RSSql Configuration Server	tcp	10.10.20.10	3
Rockwell Automation	Rockwell RSSql Compression Server	tcp	10.10.20.10	3
Rockwell Automation	Rockwell FactoryTalk PI Notification	tcp	10.10.20.10	3
Rockwell Automation	Rockwell FactoryTalk PI Network Manager	tcp	10.10.20.10	3
Rockwell Automation	Rockwell FactoryTalk Asset Framework Server	tcp	10.10.20.10	3

Export: Raw Formatted

1 2 »

Best Guess - Category



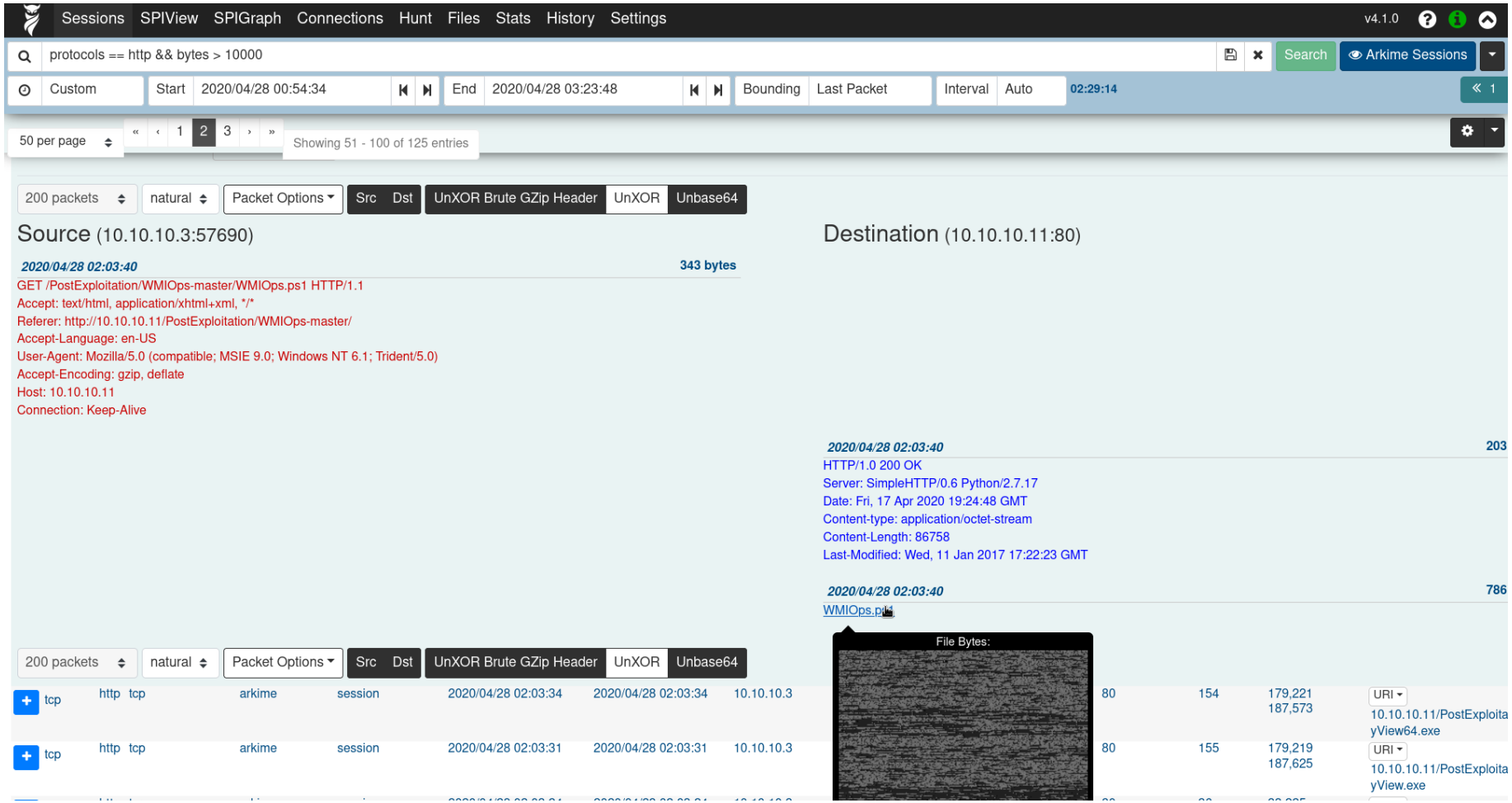
Best Guess Protocol - Source

Category	Protocol	Tranport	Source	Count
AVEVA	OASyS SCADA	tcp	10.10.20.5	20
Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	tcp	10.10.20.5	10
Rockwell Automation	Rockwell FactoryTalk Analysis Framework	tcp	10.10.20.5	10
Rockwell Automation	Rockwell CSP	tcp	10.10.20.5	9
Red Lion	Red Lion CrimsonV3	tcp	10.10.20.5	6
FATEK Automation	Fatek FB Series	tcp	10.10.20.5	5
Control Systems International	I/NET 2000-NPR	tcp	10.10.20.5	5
AVEVA	Wonderware	tcp	10.10.20.5	5
Rockwell Automation	Rockwell RSSql Transaction Manager	tcp	10.10.20.5	5
Rockwell Automation	Rockwell RSSql Configuration Server	tcp	10.10.20.5	5
Rockwell Automation	Rockwell RSSql Compression Server	tcp	10.10.20.5	5
Rockwell Automation	Rockwell FactoryTalk PI Notification	tcp	10.10.20.5	5
Rockwell Automation	Rockwell FactoryTalk PI Network Manager	tcp	10.10.20.5	5
Rockwell Automation	Rockwell FactoryTalk Asset Framework Server	tcp	10.10.20.5	5
Rockwell Automation	Rockwell FactoryTalk ACE2 Scheduler	tcp	10.10.20.5	5

Export: Raw Formatted

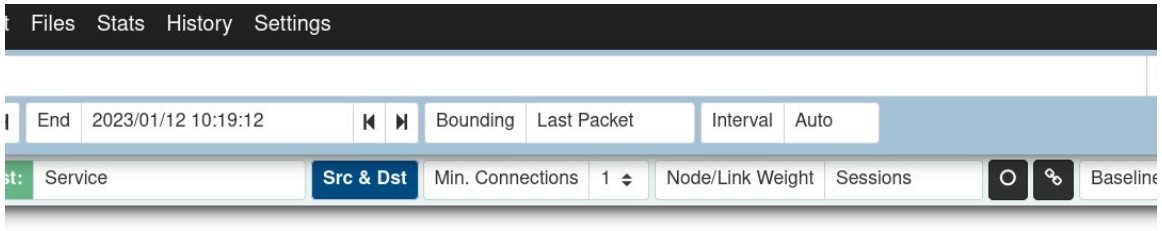
Malcolm

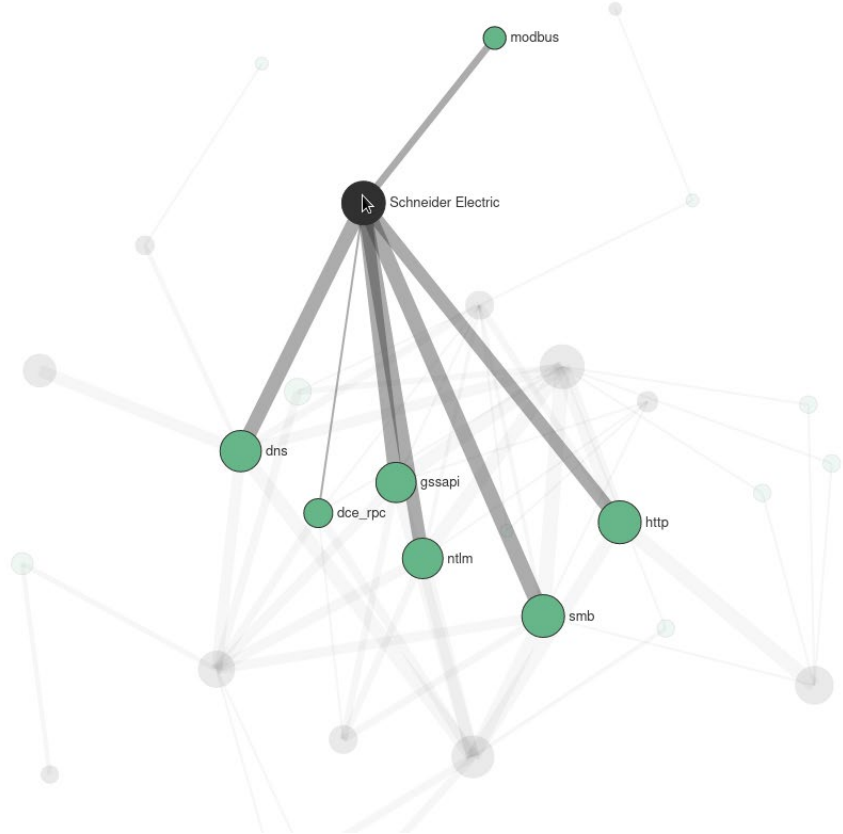
Arkime: Packet-level Forensics

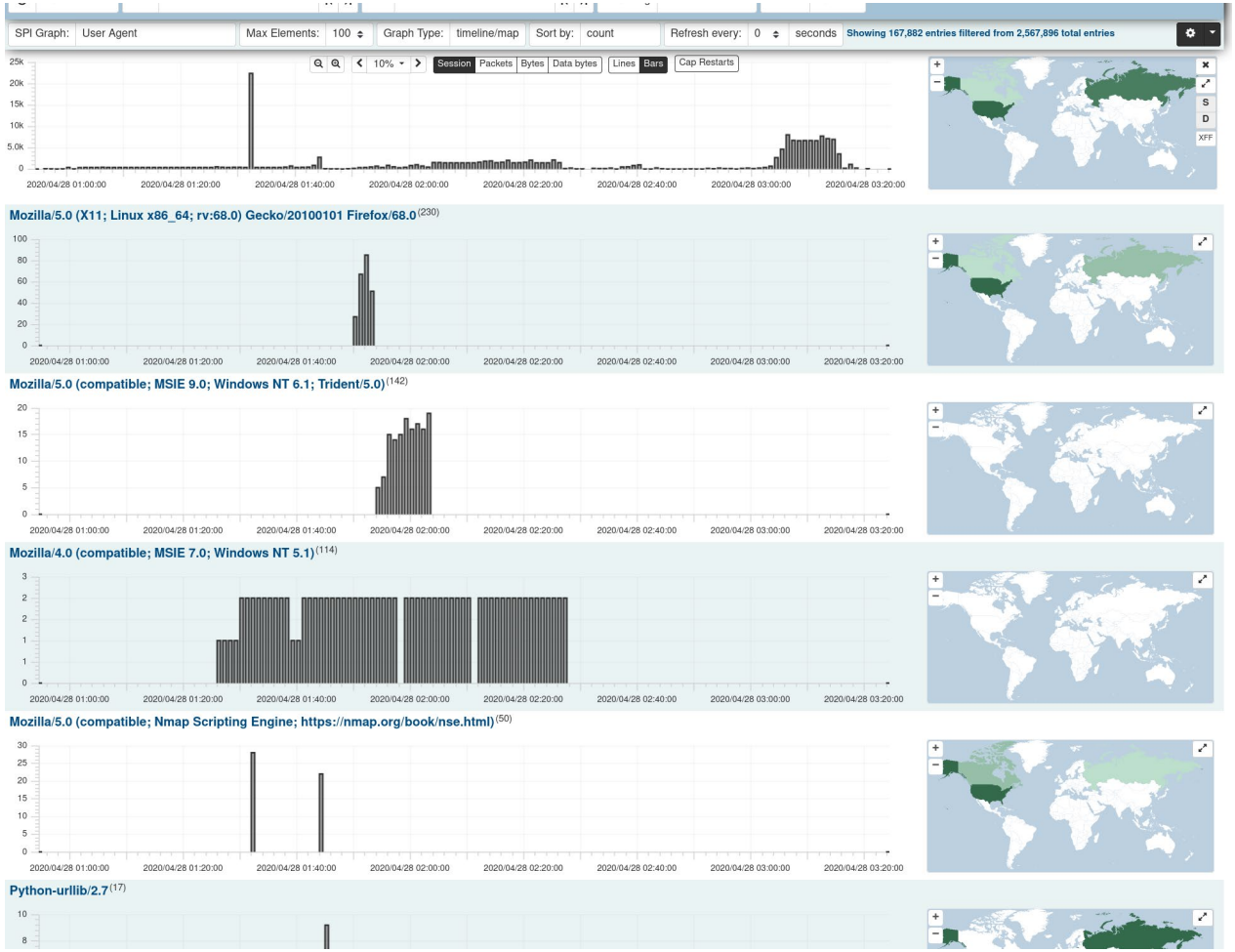


Malcolm

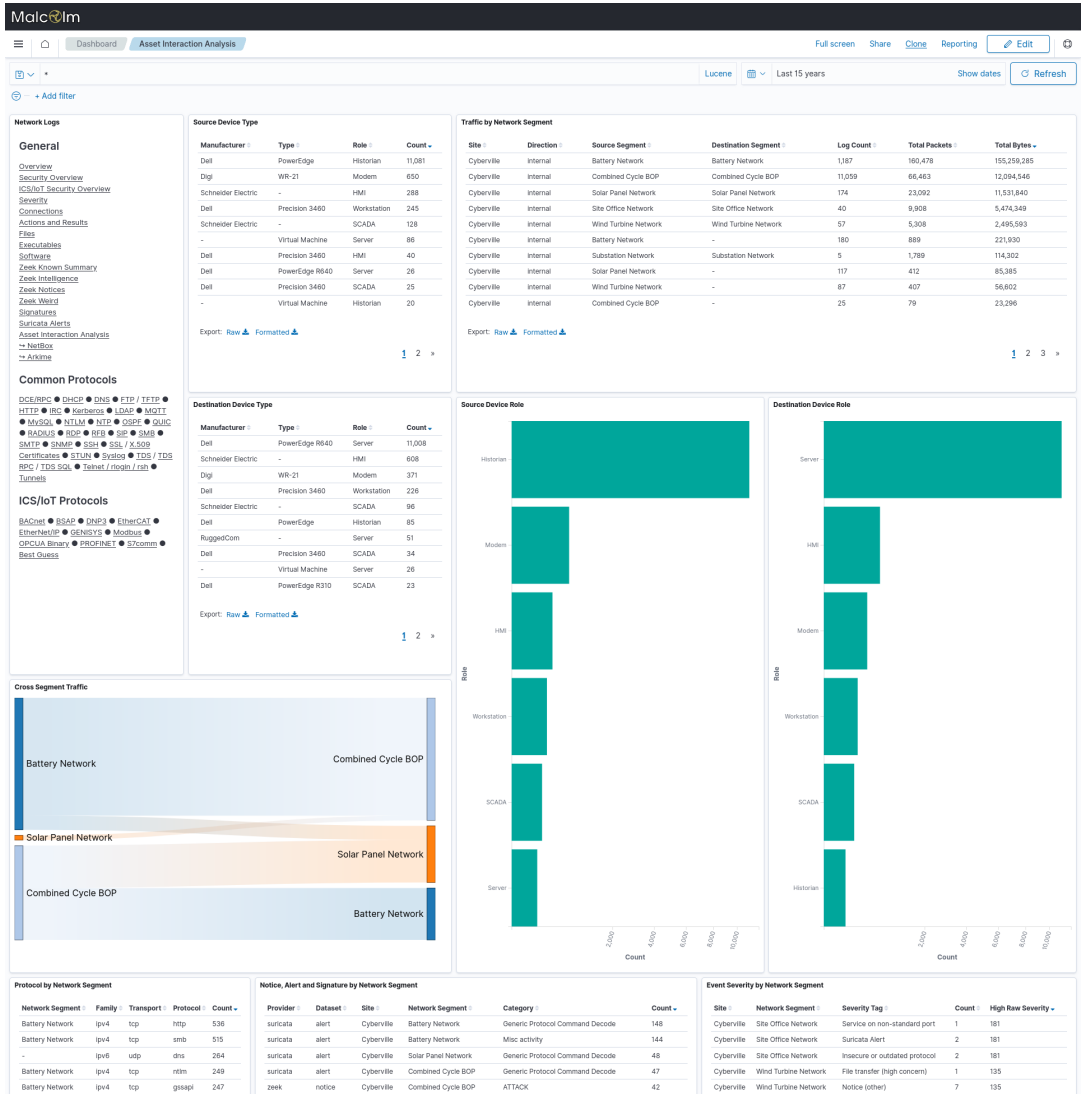
Arkime: Traffic Visualization

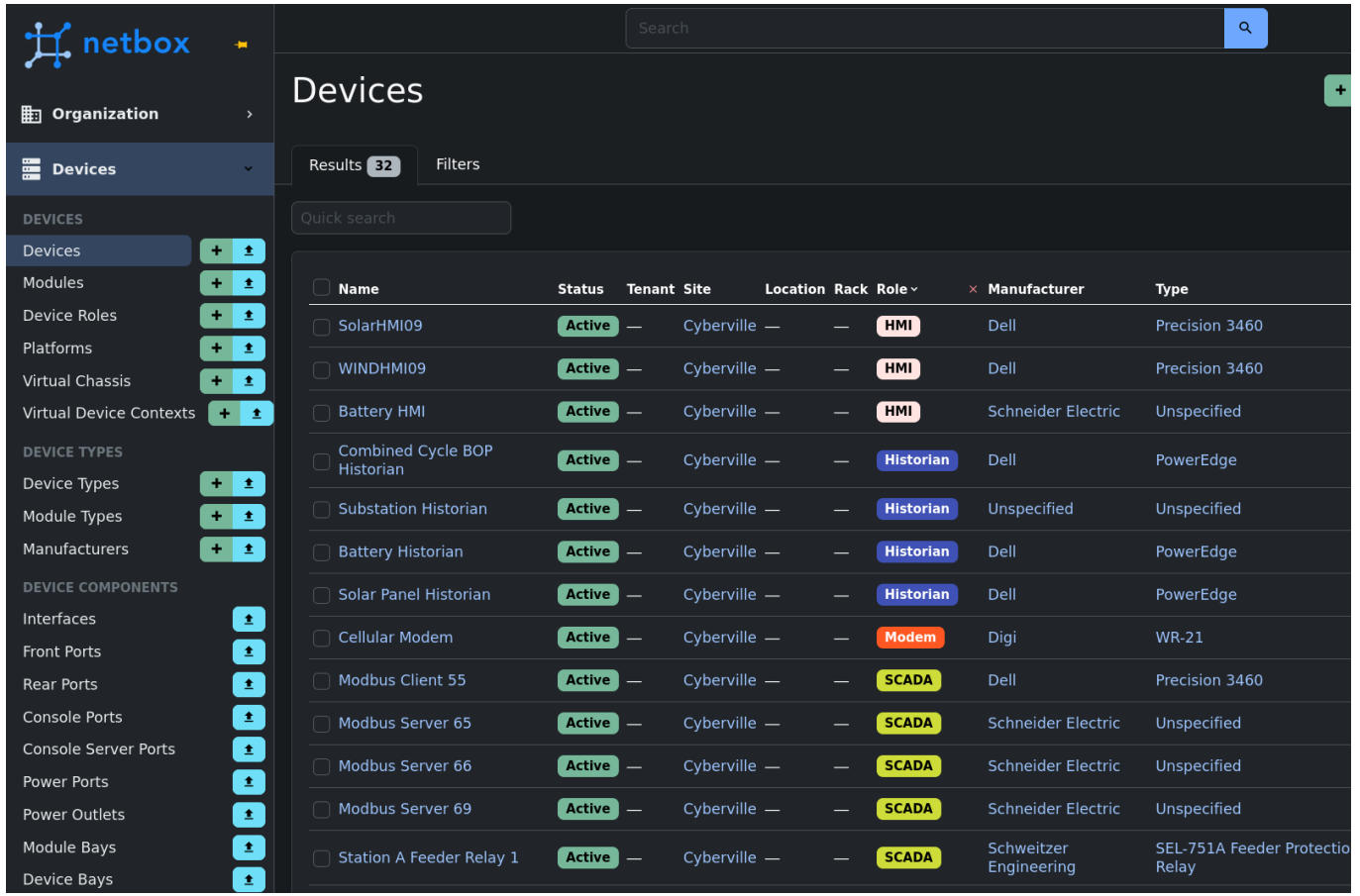






Malcolm Asset Interaction Analysis





Malcolm 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)
- Improve Asset Inventory Capabilities for OT and IT
  - Passive auto-population
  - Active scanning
- Support Generic (Sigma) Rules
- 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 https://idaholab.github.io/Malcolm for documentation, tutorials, project status, issue tracker and more.

St★r to show your support!

Email: malcolm@inl.gov

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.