

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

November 2023

Seth D Grover



hanging the World's Energy Future

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

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.

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

MOICOIM Lowering the Barrier to Entry for **Establishing a Secure Cybersecurity Posture**



Molecon Malcolm A Powerful Network Traffic Analysis

Streamlined deployment

000000

. . .

. . .

. . .

• 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.

Malcel Morigins 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











Malc@ImWhat 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.





Malc@ImSupported 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**

Malcomponents



Malc@ImData Pipeline

Traffic is collected passively by sensor device running Hedgehog Linux

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 Logs are securely forwarded to Malcolm

- •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.

Logs are

enriched and

stored in

OpenSearch

- •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

- Machine learning algorithms identify anomalies
- •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 are sent over email, webhooks, Slack or Amazon Chime

•Alerts may be triggered

thresholds, anomalies

detected. custom

by exceeded

queries, etc.

Traffic is visualized in OpenSearch Dashboards and Arkime Viewer

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

NCCONTRACTOR Dashboards: Focus on Security

102

88

20

15

Malc ∂lm																
Dashboard Se	curity Overview								Full screen	Share	Clone	Repo	rting	Ø E	dit	0
₿∨ *					Lu	icene (. ~ .	Last 25 ye	ars			ş	Show dat	es 🛛	ර Refre	sh
NOT rule.category: Generic Protoco	I Command Decode × + Add filter															
Network Logs	Normalized Event Category				Notice, Aler	rt, Signature	and We	eird - Summ	ary							
General	Potentially Bad Traff SS	ic - iL -			Provider	Dataset 🗘	Categ	iory 🗢		Name 🗘					Cou	nt
Overview	ATTAC Mice activit	к –					0.44		40 -	ET DOUI		<i>w</i>	-1.40 /00	OT)	077	
Security Overview	EternalSafe	y -			suricata	alert	Poten	tially Bad Tra	iffic	ETPOLIC	JT HITP trai	me on po	rt 443 (PU	51)	977	
ICS/IoT Security Overview	Signatures::Sensitive_Signature	e -			zeek	weird	-			line_term	ninated_with	_single_Cl	R		661	
Severity	Attempted Administrator Privilege Ga	in -			zook	notice	991			Invalid S	Conver Cert				521	
Connections	Unknown Traff	C			2008	Hotice	331			Invalia_5	erver_oert					
Actions and Results	Malware Command and Control Activity Det				zeek	weird	-			bad_HT1	(P_request				391	
Files	Attempted User Privilege Ga	n –			zeek	weird				NUL in I	line				361	
Executables	Not Suspicious Traff	IC -														
Software	Signature	IS -			suricata	alert	Misc a	activity		ET HUN	TING Suspici	ous NULL	DNS Req	uest	222	
Zeek Intelligence	Command_And_Contr	pl –			zeek	weird	-			possible.	_split_routing	g			96	
Zeek Notices	CVE_2021_4422	8 -			70.0k	waird				data hef	fore establis	had			02	
Zeek Weird	Attempted Denial of Service	e -			2008	wonu				uata_bei	ore_catabilat	neu				
Signatures	Signatures::Multiple_Signature	n			zeek	notice	ATTAC	CK		Lateral_M	vlovement				92	
Suricata Alerts	Attempted Information Lea	ik –			zeek	weird	-			prematu	.re_connectic	on_reuse			91	
Network Assets	Discove	y														
↔ NetBox	Executio	n			zeek	notice	ATTAC	JK		Executio	n				83	
⇔ Arkime	Impa Detection of a Notwork Ser	et -			suricata	alert	Unkno	own Traffic		ET JA3 H	-lash - [Abus	e.ch] Pos	sible Adw	are	76	
	Sciences	n -			zeek	weird				DNS Cor	nn count tor	o large			68	
Common Protocols	A suspicious filename was detected	d -			LUUN	Weird				5110_00	in_coount_coo	2_iaigo			00	
DCE/RPC ● DHCP ● DNS ● FTP	Collectic CVE2022360 CVE_2021_3864	n			suricata	alert	Attem Privile	ipted Admini ege Gain	strator	NetrServ (CVE-20	VerAuthentica J20-1472)	Zerologo ate with C	in 0x00 Client	t Credenti	65 ials	
/ <u>TFTP</u> ● <u>HTTP</u> ● <u>IRC</u> ● <u>Kerberos</u>	CVE_2021_4177	3 -					ATTAC	21/		Laboral B			F 11-		01	
● <u>LDAP</u> ● <u>MQTT</u> ● <u>MySQL</u> ●	HI IPAT IACK Misc Attac	S -			zeek	notice	ATTAC	JK		Lateral_r	viovement_E	xtracted_	"L-lie		01	
<u>NTLM</u> ● <u>NTP</u> ● <u>OSPF</u> ● <u>QUIC</u> ●	Zerologo	n -			zeek	notice	Eterna	alSafety		Violation	Tx2Cmd				58	
$\underline{RADIUS} \bullet \underline{RDP} \bullet \underline{RFB} \bullet \underline{SIP} \bullet$	CVE_2022_2680	9 -			zeek	notice	Signat	tures		Sensitive	e Signature				51	
$\underline{SMB} \bullet \underline{SMTP} \bullet \underline{SNMP} \bullet \underline{SSH} \bullet$	Credential_Acces	is -														
SSL / X.509 Certificates • STUN	CVE_2020_060	01-			suricata	alert	Attem	ipted User Pi	rivilege Gain	ET INFO Binding I	Session Trav Request On I	versal Util	lities for Na dard High	AT (STUN Port)	48	
• Syslog • IDS / IDS RPC / IDS	CVE_2020_1377	7								binding r	request on i	NOTI-Starr	uaru nigri	FOID		
<u>SQL</u> ● <u>Telnet / rlogin / rsh</u> ● <u>Tunnels</u>	Coreligi Device Retrieving External IP Address De	nt			suricata	alert	Poten	tially Bad Tra	affic	ET POLIC Environn	CY Command nental Variab	d Shell Ac ble Over S	tivity Usin MB - Very	g Comspe Likely La	ec 41 teral	
ICS/IoT Protocols	FT Web Application Attac	Р			zeek	signatures	Signat	tures∷Sensit	ive_Signature	smb-nt-1	transact-ren	ame			41	
BACnet BSAP DNP3	CVE_2020_1689 Deceletary	8 -														
EtherCAT EtherNet/IP	Possibly Unwanted Program Detected	d -			Export: D	aw + For	natted									
GENISYS Modbus OPCUA	ss	H-			Export. N		natteur	-								
Binary	Successful User Privilege Ga	in -										1	2 3	4 5		35
Best Guess			200 400 600	000'1								1	2 0	4 0		
	🔵 tcp 🕚 udp 😑 unknown 🌘	icmp														
Outdated/Insecure Application Protocols	Vulnerabilities								Clear-text Tr	ansmissio	n of Passwo	ords				
Application Protocol 🗧 Protocol Vers	sion ≎ Count - Data Source ≎	Log Type 🗘	Vulnerability ID 🗘	Last See	n .		Cou	unt ‡	Application	n Protocol	Userr	name ≑			Count	•
fto	3 000 Took	notico	CVE 2021 44229	Mar 2, 20	121 @ 14:01:48	8.003	37		ftn		9000	umoure			1.414	

Mar 1. 2021 @ 01:54:22.130

Mar 1. 2021 @ 00:00:00.145

Feb 28. 2021 @ 23:03:41.250

Feb 28 2021 @ 23:00:13.033

Feb 28, 2021 @ 23:00:09.423

3.066

502

395

253

79

zeek

zeek

suricata

zeek

notice

notice

notice

notice

CVE20223602

CVE 2020 0601

CVE_2020_1472

CVE 2020 16898

CVE 2020 13777

1

TLSv10

TLSv11

http

http

ftp

http

opcua-binary

1

Login

maint

LOG+IN

user1

ind@psg420.con

							Lucene 🔮 ~ Feb 28, 24	021 @ 22:58:14.215 →	Mar 1, 2021 @ 00:12:14.421 C I
+ Add filter									
work Logs	Severity Tags			Seve	rity Score Occurrences				
eneral	Severity Tag :	Count	High Raw Severity -		40.000				
	Sensitive country	2,730	251		20,000				
curity Overview	Service on non-standard port	3,553	251		00,000				
S/IoT Security Overview	Inbound traffic	3,685	251		80,000				
Internations	Suricata Alert	45,643	251						
tions and Results	File transfer (high concern)	63	245	-	50,000				
les	Cleartext password	1,666	245	inces	10,000			_	
oftware	Outbound traffic	22,290	245	curre		125,487			
eek Intelligence	Insecure or outdated protocol	70,467	245	8	20.000				
vek Weird	Long connection	3	231					70,833	
anatures aricata Alerts	External traffic	114,547	201				41	255	
rtwork Assets NetBox Arkime	Export: Raw & Formatted &					52	201		3,809
ommon Protocols			1 2 3		0 z 1 and 4 10 z 10 and 4 20	e 20 and 4 30 e 30 a	nd < 40 × 40 and < 50 × 50 a Severity Score	na < 60 2 60 ana < 70	01 \$ 001 > bits 01 \$ 00 > bits 08 \$
LE/RPC DHCP DNS FTP / TFTP TTP IRC Kerberos LDAP MGTT	Severity - Notices					Severity - Apr	dication Protocol		
YSQL NTLM NTP OSPF QUIC ACULS RDP RFB SIP SIP SMB SMTP									
SNMP • SSH • SSL / X.509 Certificates •	Notice Category :			Count	High Raw Severity -	Application	Protocol	Count	High Raw Severity -
TUN Syslog TDS / TDS RPC / TDS SQL	ATTACK::Lateral_Movement_Extracted,	File		4	135	http		12,488	251
snet / nogin / rsn	SSL=Invalid_Server_Cert			426	120	ftp		3,931	245
CS/IoT Protocols	CVE_2021_44228:LOG4J_ATTEMPT_H	ADER		3	110	smtp		3,216	211
Cnet BSAP DNP3 EtherGAT	Ripple20::Treck_TCP_observed			2	80	tis		1,294	171
herNetJIP GENISYS Modbus OPCUA	Corelight=XOR_Encrypted_PE_File_See			2	80	modbus		14,204	171
nary PROFINET S7comm Best Guess	CVE_2020_0601=Unknown_X509_Curv			2	80	smb		66,510	161
erity - Socket Family	Signatures=Sensitive_Signature			51	80	snmp		1,329	151
iov4 😑 iov6	SSH:Password_Guessing			1	60	rfb		26	141
	CVE_2022_26809:ExploitAttempt			1	60	dns		11,093	143
					1 2 3	4 *			12345
Types by Transport			Severity - Source IP				Severity - Destination IP		
ile Type :	Transport :	Count -	Source IP :		Count : High Raw Seve	erity -	Destination IP :		Count : High Raw Severity -
pplication/isvascript	HTTP	94	Other		268.343 251		Other		265,555 251
ext/plain	FTP	29	212.98.102.62		5 251		216.55.163.106		44 245
ext/html	HTTP	26	216.55.163.105		12 231		2001:470:1111:811:e999:d	34:aa7c:2e3e	8 181
pplication/x-shockwave-flash	HTTP	25	213.155.112.85		4 211		254.228.86.79		7 171
ext/plain	SMTP	20	218.75.108.92		4 211		2001:470:4867:98::21		11 150
pplication/x-dosexec	HTTP	54	219.72.95.118		2 211		216.239.32.21		12 141
ast/plain	HTTP	14	219.139.93.225		7 211		222.26.16.113		3 141
pplication/x-dosexec	FTP	9	219.238.180.208		2 211		223.116.105.247		5 141
pplication/x-dosexec	SMB	9	220.165.129.154		3 211		2001:db8:1:2		1 141
	HTTP	6 282	222.26.16.113		2 211		239.114.155.111		35 131
ppscasorizip			Export: Raw 📥 F	ormatted 🛦			Export: Raw 🛦 Format	ted &	
cort: Ray & Formatted &		1 2 3	×		1	2 3 4 5 26 3			12345
xport: Raw ▲ Formatted ▲									
oport: Raw & Formatted &					1 Annal Annal Annal	-			

MCICOM Dashboards: Focus on OT

Software

Zeek Intelligenc

Zeek Notices



Source IP

134.249.62.202

134.249.62.202

134.217.61.131

134 217 61 131

118.189.96.132

192.168.66.235

134.249.53.130

134.249.53.130

24.39.21.194

130.126.142.250

Source Country

Ukraine

Ukraine

United States

United States

United States

Singapore

Ukraine

Ukraine

United States

ICS/IoT External Traffic

Protocol

cotp

s7comm

s7comm

cotp

modbus

dnp3

modbus

s7comm

genisys

cotp

enip - Count

14,217 cotp - Count

13,458 bsap - Count

11,482 2,072 s7comm - Count dnp3 - Count

Result

Success

Success

Success

Success

Success

Export: Raw 📥 Formatted 📥



Zeek Weird Signatures	sing transport nspection. As	Category ≎										
Suricata Alerts Network Assets	such, the	more false	AVEVA									
SetBox	etBox positives than other protocol dashboards.											
					AVEVA							
Common Protocols					Mitsubishi Electric							
	Best Guess -	summary			Rockwell Automation							
HTTP IRC Kerberos LDAP	MQTT Transport	Category 0	Details 🗘	Count 🗸	Mitsubishi Electric							
MySQL ● NTLM ● NTP ● OSPF ●	QUIC tcp	AVEVA	OASyS SCADA	20	Rockwell Automation							
RADIUS RDP RFB SIP SMB	S SMTP top	Mitsubishi Electric	Mitsubishi Electronic MELSEC-Q	10	FATEK Automation							
STUN Syslog TDS / TDS RPC /	TDS SQL top	Rockwell Automation	Rockwell FactoryTalk Analysis Framework	10	Control Systems International							
Telnet / rlogin / rsh Tunnels	tcp	Rockwell Automation	Rockwell CSP	9	Red Lion							
ICS/IoT Protocols	tcp	Red Lion	Red Lion CrimsonV3	6	Red Lion							
	top	FATEK Automation	Fatek FB Series	5	AVEVA							
EtherNet/IP GENISYS Modbus	OPCUA top	Control Systems International	I/NET 2000-NPR	5	Rockwell Automation							
Binary PROFINET S7comm	est Guess top	AVEVA	Wonderware	5	Rockwell Automation							
	tcp	Rockwell Automation	Rockwell RSSql Transaction Manager	5	Rockwell Automation							
	top	Rockwell Automation	Rockwell RSSql Configuration Server	5	Rockwell Automation							
					Rockwell Automation							
	Export: Ray	v 🛓 Formatted 🛓			Rockwell Automation							
Best Guess - Category				-	Expert: Raw 🕹 Formatted 🛓							
Rockwell Automation –					Best Guess Protocol - Source							
					AVEVA							
					Mitsubishi Electric							
AVEVA -					Rockwell Automation							
					Rockwell Automation							
					Red Lion							
					FATEK Automation							
Mitsubishi Electric -					Control Systems International							
					AVEVA							
Č 0 5					Rockwell Automation							
Cat					Rockwell Automation							
Red Lion -					Dockwell Automation							
TOTAL STORE					Rockwell Addoniation							
					Rockwell Automation							
					Rockwell Automation Rockwell Automation							

Best Guess Protocol - Destination				
Category	Protocol 0	Transport 🕀	Destination 0	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

01:32:30.000 01:32:31.000 01:32:32.000 01:32:33.000 01:32:34.000 01:32:36.000 01:32:37.000 01:32:38.000 01:32:38.000 01:32:40.000 01:32:41.000 01:32:42.000 01:32:40.000 01:32:

Protocol

OASyS SCADA

Rockwell CSP

Red Lion CrimsonV2

Eatek EB Series

I/NET 2000-NPR

Wonderware

Mitsubishi Electronic MELSEC-G

Rockwell FactoryTalk Analysis Fr

Rockwell RSSgl Transaction Manage

Rockwell RSSal Configuration Serv

ockwell EactoryTalk PI Notificatio

Rockwell FactoryTalk ACE2 Schedule

Rockwell FactoryTalk PI Network Manage

Rockwell FactoryTalk Asset Framework Serve

Destination IP

134.249.61.182

134.249.61.182

134.217.61.211

134 217 61 211

118.189.96.132

130.126.140.229

166.161.16.230

134.249.61.182

134.249.61.182

85.13.142.101



2

IDAHO NATIONAL LABORATORY

<u>1</u> 2 »

Count

Source

10.10.20.5

10.10.20.5

10.10.20.5

10.10.20.5

10.10.20.5

10 10 20 5

10.10.20.5

10.10.20.5

10.10.20.5

10.10.20.5

10.10.20.5

10.10.20.5

10 10 20 5

10.10.20.5

10.10.20.5

Malc@Imarkime: Packet-level Forensics

	essions	SPIView S	SPIGraph Conr	nections Hun	t Files Stats Histo	ory Settings										v4.1.0 ? 🚺 🔿
Q prot	ocols == ht	tp && bytes >	10000										E	×		Arkime Sessions
⊘ Cus	tom	Start 20	20/04/28 00:54:34	H F	End 2020/04/28 03	3:23:48	нн	Bounding	Last Packet	Interval	Auto	02:29:14				« 1
50 per pa	ge 🗢 «	· 1 2	3 · » Showir	ng 51 - 100 of 125	entries		_									¢ -
200 pac	kets 🗢	natural 🗢	Packet Options	Src Dst	UnXOR Brute GZip Hea	der UnXOR Ur	nbase64									
Sourc	e (10.10	0.10.3:57	690)						Destination	1 (10.10 ו	.10.11:8	80)				
2020/04/2 GET /Post Accept: te: Referer: ht Accept-La User-Ager Accept-En Host: 10.1 Connectio	28 02:03:40 Exploitation/ (t/html, applii tp://10.10.10 gnuage: en-1 t: Mozilla/5. coding: gzip 0.10.11 n: Keep-Alive	WMIOps-mas cation/xhtml+> J.11/PostExplo JS 0 (compatible; , deflate	ter/WMIOps.ps1 HT (ml, */* iitation/WMIOps-max MSIE 9.0; Windows	TP/1.1 ster/ NT 6.1; Trident/5.0	0)	34	43 bytes		2020/04/28 02:03:4 HTTP/1.0 200 OK Server: SimpleHTTF Date: Fri, 17 Apr 20: Content-type: applic Content-Length: 867 Last-Modified: Wed,	10 7/0.6 Pythor 20 19:24:48 ation/octet-s 758 11 Jan 201	/2.7.17 GMT stream 7 17:22:23	GMT				203
									2020/04/28 02:03:4 WMIOps.ptf	10						786
200 pac	kets 🗢	natural 🗢	Packet Options	Src Dst	UnXOR Brute GZip Hea	der UnXOR Ur	nbase64			File Bytes:						
+ tcp	http tcp)	arkime	session	2020/04/28 02:03:34	2020/04/28 02:03	1:34 1	0.10.10.3				80	154	1	79,221 87,573	URI - 10.10.11/PostExploita yView64.exe
+ tcp	http top	0	arkime	session	2020/04/28 02:03:31	2020/04/28 02:03	:31 1	0.10.10.3				80	155	1	79,219 87,625	URI - 10.10.11/PostExploita yView.exe
									the second secon	and an an an and a second s						

Malc@MArkime: Traffic Visualization





Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 (23







Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)⁽¹¹















2020/04/28 03:20:0





NCCOMMAsset Interaction Analysis

∎ o

Devi

Devi

Virtu Virtu

Devic Modu Manu

Inter

Rear Conse Conse Powe Powe Modu Devic

1alc €lm												
Dashboard Asset Intera	action Analysis								Ful	screen Share	Clone Reporting	Ø Edit
v *								Lucene	 Last 15 years 		Show o	lates C Refrest
+ Add filter												
work Logs	Source Device Type				Traffic by Netwo	rk Segment						
eneral	Manufacturer 0	Туре	Role 0	Count -	Site :	Direction 0	Source Segment	Destination Se	gment 0	Log Count	Total Packets	Total Bytes 🗸
rview	Dell	PowerEdge	Historian	11,081	Cyberville	Internal	Battery Network	Battery Netwo	rk	1,187	160,478	155,259,285
urity Overview	Digi	WR-21	Modern	650	Cyberville	Internal	Combined Cycle BOP	Combined Cyc	ie BOP	11,059	66,463	12,094,546
lioT Security Overview erity	Schneider Electric	-	HMI	288	Cyberville	internal	Solar Panel Network	Solar Panel Ne	twork	174	23,092	11,531,840
mections	Dell	Precision 3460	Workstation	245	Cyberville	Internal	Site Office Network	Site Office Net	work	40	9,908	5,474,349
s	Schneider Electric	-	SCADA	128	Cyberville	Internal	Wind Turbine Network	Wind Turbine I	Jetwork	57	5,308	2,495,593
cutables	- Dell	Precision 3460	HMI	40	Cyberville	Internal	Substation Network	- Substation Net	work	5	1789	114 302
sk Known Summary	Del	PowerEdge R640	Server	26	Cyberville	internal	Solar Panel Network	-		117	412	85.385
<u># Intelligence</u> # Notices	Dell	Precision 3460	SCADA	25	Cyberville	Internal	Wind Turbine Network			87	407	56,602
k Weird	-	Virtual Machine	Historian	20	Cyberville	internal	Combined Cycle BOP	-		25	79	23,296
natures cata Alerts												
et Interaction Analysis	Export: Raw 🛓 Fo	rmatted 📥			Export: Raw 🛓	Formatted &						
<u>letBox</u> Arkime				<u>1</u> 2 »								1 2 3 >
ommon Protocols												
E/RPC DHCP DNS FTP / TFTP TP Kerberos LDAP MQTT	Destination Device Ty	rpe			Source Device R	ole			Destination Devi	ce Role		
	Manufacturer 0	Type 🗧	Role 0	Count -					1			
TTP • SNMP • SSH • SSL / X.509	Dell	PowerEdge R640	Server	11,008								
tificates STUN Syslog TDS / TDS	Schneider Electric		HMI	608	Historian -				Server -			
inels	Digi	WR-21	Modem	371								
	Dell	Precision 3460	Workstation	226								
S/IOT Protocols	Schneider Electric		SCADA	96								
Cnet BSAP DNP3 EtherCAT Average of the second secon	Dell	PowerEdge	Historian	85								
CUA Binary PROFINET S7comm	RuggedCom	-	Server	51	Modem -				HMI -			
st Guess	Dell	Precision 3460	SCADA	34								
		Virtual Machine	Server	26								
	Dell	PowerEdge R310	SCADA	23								
	Export: Raw 📥 Fo	rmatted 📥										
					HMI -				Modern -			
				1 2 *								
					Role				Role			
is Segment Traffic												
					Worketation				Workstation			
					101838001				1011210201			
Battery Network		C	ombined Cyc	le BOP		_						
					SCADA -				SCADA -			
Solar Panel Network												
		s	Solar Panel N	stwork								
Combined Cycle BOP					Server -				Historian -			
			Battery N	etwork								
			,				6 6					
							-2.001 4.007	6.00X			2,00y	6.00 6.00
							Count				Count	
ocol by Network Segment	N	lotice, Alert and Signatu	re by Network Se	gment				Event Severity I	y Network Segment			
-	tocol Count -	Provider Dotorot	Site	Naturai Pa	ament Cut	egopy	Count	Site	Jetwork Sermert	Severity Ta~	Count	High Daw Savaria
ttery Network ipv4 tcp http	D 536	suricata alort	Cyberville	Battery Note	work Gon	eric Protocol Commany	1 Decode 148	Cyberylle	Site Office Network	Service on pon-s	tandard port 1	181
ttery Network ipv4 tcp sm	b 515	suricata alert	Cyberville	Battery Netv	work Miss	c activity	144	Cyberylle	Site Office Network	Suricata Alert	2	181
a construction of the second		and added	Concerning	Color Denald	Natural Car			Cohendle	The Office Methods	landaria contra	-	101

netbox	+			Searc	h					Q
ganization		Devices								E
vices	¥	Results 32 Filters								
s	+ ±									
es 💽	+ ±	Name	Status	Tenant	Site	Location	Rack	Role - ×	Manufacturer	Туре
Roles	+ ±	SolarHMI09	Active		Cyberville			нмі	Dell	Precision 3460
ms 🧧	+ ±		Active		Cyberyille			HMI	Dell	Precision 3460
Chassis	+ ±		Active		Cyberville					
Device Contexts	+ ±	Battery HMI	Active		Cyberville			НМІ	Schneider Electric	Unspecified
	+ +	Combined Cycle BOP Historian	Active		Cyberville			Historian	Dell	PowerEdge
e Types	+ ±	Substation Historian	Active		Cyberville			Historian	Unspecified	Unspecified
acturers	+ 1	Battery Historian	Active		Cyberville			Historian	Dell	PowerEdge
COMPONENTS		Solar Panel Historian	Active		Cyberville			Historian	Dell	PowerEdge
ces orts		Cellular Modem	Active		Cyberville			Modem	Digi	WR-21
orts	1	Modbus Client 55	Active		Cyberville			SCADA	Dell	Precision 3460
e Ports	1	Modbus Server 65	Active		Cyberville			SCADA	Schneider Electric	Unspecified
e Server Ports	±	Modbus Server 66	Active		Cyberville			SCADA	Schneider Electric	Unspecified
Ports Outlets		Modbus Server 69	Active		Cyberville			SCADA	Schneider Electric	Unspecified
e Bays	1	Station A Feeder Relay 1	Active		Cyberville			SCADA	Schweitzer Engineering	SEL-751A Feeder Protectio Relay
Bays	±								Engineering	- totaj

Nalcolm 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, ...





Thank you!

Visit https://idaholab.github.io/Malcolm for documentation, tutorials, project status, issue tracker and more. St \star r to show your support! Email: malcolm@inl.gov

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

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.

WWW.INL.GOV