IOWA STATE UNIVERSITY College of Engineering

ADSICS

Anomaly Detection System for Industrial Control Systems

SDMay22-38 : Alex Nicolellis, Muhamed Stilic, Pallavi Santhosh, Jung Ho Suh Client : Dr. Manimaran Govindarasu

Advisors : Dr. Manimaran Govindarasu, Moataz Abdelkhalek

Problem Statement

- Cyber attacks on power distribution companies are debilitating and are now more common due to the increased use of IoT devices and the inadequate security on power grid systems
- To feel as secure in how our power is protected, our security measures must continue to advance with the constantly developing technology of cybercriminals.

College of Engineering

Cybersecurity Threats

• Domestic terrorists have developed "credible, specific plans" to attack the U.S. power grid and view it as a "particularly attractive target given its interdependency with other infrastructure sectors," according to a security briefing issued in January by Department of Homeland Security

• Past Attacks Globally:

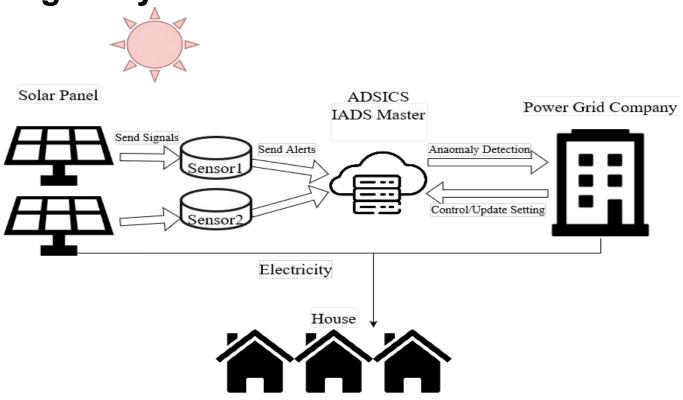
• The European Network of Transmission System Operators for Electricity (2020)

College of Engineering

- Russian power grid (2019)
- Saudi Aramco petrochemical plants (2017)

Solution Statement

ADSICS is a surveillance program that detects cyber attacks using machine learning analysis.



IOWA STATE UNIVERSITY

Solution Statement

- Traditional security measures easily disabled by user error; spear phishing
- Machine Learning Anomaly Detection System is needed
- Building our own ML ADS will cost a lot, use existing platform



IOWA STATE UNIVERSITY

Elastics Stack

- Elastic Stack is an open source tool
- Modification to features is like a black box
- Three Projects that make the Elastic Stack
 - Elasticsearch Search and Analytics Engine
 - Logstash(Beats) Data ingestion Pipeline
 - Kibana Data Dashboard and Visualizer



IOWA STATE UNIVERSITY

College of Engineering

elastic

Project Description

- The end goal is described as **a detailed visual output** of temporal anomaly detection, tracking alert information, and performing **machine learning analysis** quickly and efficiently **using the desired platforms (Elastic Stack)**.
- Additionally, we built our own, **local machine learning model** to compare with the outputs from Elastic to determine whether or not this relatively "new"platform could be **relied upon solely** as a valid solution to **detect and analyze** various cyberattacks on the grid.

College of Engineering

Requirements & Constraints

Functional Requirements:

- Use machine learning to detect network anomalies
- Verify incoming alerts and detect false positives
- Display alerts for easy human understanding
- Present temporal and spatial details for each alert
- Users should be able to add or remove data visualizations on the dashboard
- Alerts should be distinguishable from each other and labled

Non-Functional Requirements:

- Alerts should be presented intuitively
- Alerts should be color coded by severity
- The system should be able to handle a large volume of alerts
- The system should be reliable and consistent with analysis
- System should have an **accuracy of >95%** for detecting each alert

Constraints:

• One branch of the project must use Elastic Stack tools (specifically Elasticsearch, Kibana, and Logstash)

IOWA STATE UNIVERSITY

Datasets

- The main datasets we used for different types of attacks such as DoS, Brute Force, and XSS from https://www.unb.ca/cic/datasets/ids-2017.html (University of New Brunswick 2017).
 - Chosen for: variety of attacks and the length of an entire workday with network traffic
- Modbus dataset which includes Modbus query flood, ping flood, tcp SYN flood attacks from https://github.com/tjcruz-dei/ICS_PCAPS/releases (Frazão, I.)

College of Engineering

• Chosen for: OT protocol (common for power grid)

Datasets

• We used the **PCAP files to replay the network flow** along with attacks inside it and used **CSV files to classify attacks** with our VM ML model.

- The CSV datasets are each compiled of a data flow in the PCAP which was grouped together by CICFlowMeter.
 - These data flows consist of **78 features** ranging from Destination Port to Flow ID

• By analyzing the alert data of the PCAP files, a "Label" column was created and input with the various "attack" types associated with each data flow.

College of Engineering

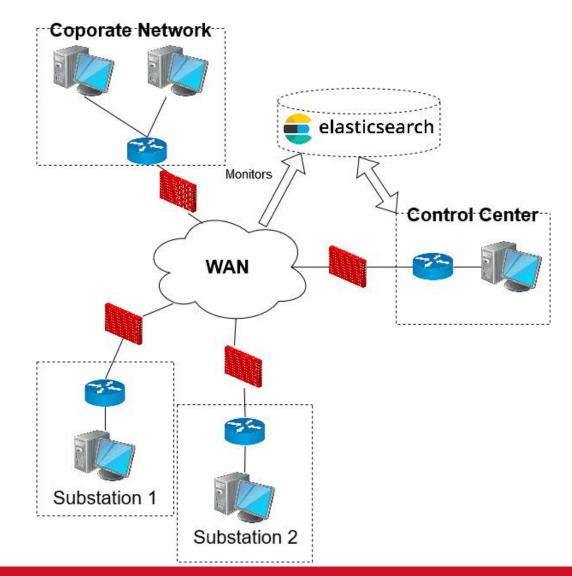
Datasets: Wednesday

Wednesday_Workingday dataset is the largest dataset with **13 gigabytes** and has four classified DoS attacks: **DoS slowloris, DoS Slowhttptest, DoS Hulk, DoS GoldenEye**.

Wednesday_Work	kingday		
DoS / DDoS			
Network Traffic from 9:0	00 A.M. to 5:00 P.M.		
	os	IP	Local IP
Attacker	Kali	205.174.165.73	
Victim DDoS	WebServer Ubuntu	205.174.165.68	192.168.10.50
Victim Heartbleed	Ubuntu12	205.174.165.66	192.168.10.51
Type of Attack		Start	End
DoS Slowloris		9:47	10:10
DoS Slowhttptest		10:14	10:35
DoS Hulk		10:43	11:00
DoS GoldenEye		11:10	11:23

IOWA STATE UNIVERSITY

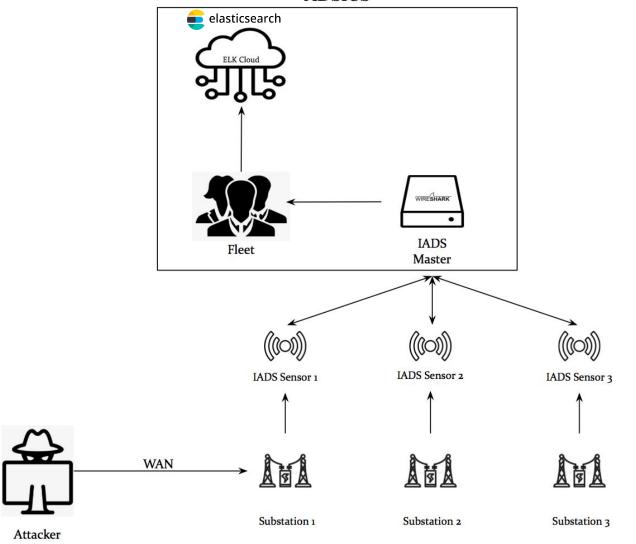
Elastic: Theoretical Design



IOWA STATE UNIVERSITY

Elastic: Practical Design

ADSICS



IOWA STATE UNIVERSITY

Elastic: System Architecture

Functional Decomposition - Operating Systems:

- Attacker Kali Linux
- ELK_Agent, IADS_Sensor, IADS_MASTER - Linux
- Victim Windows XP

Software Architecture:

- vSphere VM Platform
- SIEM
 - Elastic Stack
 - Elastic Search
 - Logstash(Beats)
 - Kibana
- Tools
 - TCPReplay
 - Wireshark
 - Editcap



IOWA STATE UNIVERSITY

Elastic: Integrations

- Integrations
 - Fleet
 - Agents

Q Search			Namespace 🗸	Add integration
Name 🛧	Integration	Namespace		Actions
ZEEK-AGENT	Zeek Logs v1.6.0	default		000
auditd-1	Auditd v2.1.2	default		
end_point_security_new 🔘	Endpoint Security v8.2.0	default		
network_packet_capture 🔘	Network Packet Capture v0.8.1	default		
security_detection_engine-1	Prebuilt Security Detection Rules	default		
system-1	⊿⊷ System v1.6.4	default		

College of Engineering

- Packet beat(Data ingestion)
- Network Packet Capture
- Security Integrations(Jobs)

Elastic: Kibana



- Machine Learning Anomaly Detection
 - High Count Jobs
 - Rare Processes
- Machine Learning Data Frame Analytics



(Sorted by max anomaly score)						ID 个	Description	Memory status	Source index
Annotations	E1 0	п			~	benign_then_atta	c test	ok	test_benign_th
Overall					~	heart_disease		ok	heart_2020
					~	mitm_15h_6h_tes	t test	ok	mitm_15m_6h
kibana-logs-ui-default-def					~	modbusqueryfloo	test	ok	modbusqueryfl
high_count_network_events					~	no_header_thurso	test	ok	no_headers_th
xss_bruteforce_attackspa					~	pingfloodddos_1	5 test	ok	pingfloodddos
authentic_v2_linux_anom authentic_v2_rare_proces					~	tcpsynfloodddos	: test	ok	tcpsynflooddd
authentic_v2_linux_anom					~	test_attack_then_	t test	ok	test_attack_be
xss_bruteforce_attackspa					~	test_dos_first_try	test	ok	test_dos_first
authentic_v2_linux_anom					~	test_dos_last_try	test	ok	test_dos_last
2022-03-26	2022-04-02	2022-04-09	2022-04-16	2022-04-23					

IOWA STATE UNIVERSITY

Elastic/Network Issues

- No modbus port integrations
 - Cannot edit Network Packet Capture
- Near real time analytics
 - Data ingested in real time but analyzed in near-real time
- TCPReplay
 - MTU Size

powercyber@powercyber-testbed-ELK:~/Downloads\$ sudo tcpreplay -i ens160 Wednesday-WorkingHours.pcap Warning in send packets.c:send packets() line 644:	
Unable to send packet: Error with PF_PACKET send() [10208]: Message too long (errno = 90) Actual: 10207 packets (10298644 bytes) sent in 29.98 seconds	
Rated: 343511.7 Bps, 2.74 Mbps, 340.45 pps	
Statistics for network device: ens160	
Successful packets: 10207	
Failed packets: 1	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	

				File <u>E</u> dit <u>Vi</u> ew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>Wi</u> reless <u>T</u> ools <u>H</u> elp
d) Observability	Stream	Details for log entry sF3mtH8Bqvhq4v581nZh	Investigate	📶 🔳 🦽 🐵 🔚 🗋 X 🖸 🍳 🗰 🗯 🗮 🐺 💆 🔜 🗮 🔍 🔍 🕮
		From index .ds-logs-network_traffic.flow-default-2022.03.15-000001		l traport == 502 66 ip.addr == 127.0.01
Overview		N. MILLON M.		No. Time Source Destination Protocol Length Info
Alerts	Q source.port : 502	host.os.codename		5206 192.7238365151 35.193.143.25 192.168.15.132 TCP 02.466 AppLication Data
Cases		host.os.family	🗇 debian	5207 1027 /23097/104 35. 103. 143. 25 192. 168. 15. 1.22 TCP 62. 443 = 53322 (AK) 5eg=13764 Acx129726 Min=64240 Len=0 5208 1027. 23097/245 5. 103. 143. 25 192. 168. 15. 1.22 TCP 62. 443 = -5332 (AK) 5eg=13764 Acx129391 Min=64240 Len=0 5209 1027. 23097/345 35. 103. 143. 25 192. 168. 15. 1.32 TCP 62. 443 = -5332 (AK) 5eg=13764 Acx1243931 Min=64240 Len=0 5209 1097. 2309970 35. 103. 143. 25 192. 168. 15. 1.32 TCP 62. 443 = -5332 (AK) 5eg=13764 Acx1243931 Min=64240 Len=0
Logs	⊕ Customize ♥ Highlights	host.os.kernel	5.13.0-37-generic	5211 102.723925629 192.108.15.132 35.103.143.25 TL5V1.2 4181 Application Data 5212 102.723956553 192.108.15.132 35.103.143.25 TL5V1.2 8306 Application Data
Stream Anomalies	Mar 22, 2022 event.dataset Message	host.os.name	🗇 Ubuntu	
Categories	22:51:00.336 network_traffic.flow failed to find message	host.os.name.text	🗇 Ubuntu	5211 092,723991000 35,193,143,25 192,106,15,122 TCP 02.443 - 53322 [ACK] 5ee;13704 Acx1437281 Min=64240 Lenn0 5217 1027,72309523 35,193,143,25 192,106,15,132 TCP 02.443 - 53322 [ACK] 5ee;13704 Acx1438741 Min=64240 Lenn0 5218 1027,74008559 102,180,15,132 T5,132 TCP 02.443 - 53322 [ACK] 5ee;13704 Acx1438741 Min=64240 Lenn0
Metrics	22:51:10.336 network_traffic.flow failed to find message 22:51:20.336 network_traffic.flow failed to find message	host.os.platform	🗇 ubuntu	2022 002 / 2003074 0 210 121 - 20 2 102 101 13 - 12 170 0 0 443 - 0332 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1994 A 1 - 1032 / ACX 9 0 - 1040 / A
Inventory Metrics Explorer	22:51:30.337 network_traffic.flow failed to find message 22:51:38.337 network_traffic.flow failed to find message	host.os.type	🗇 linux	922 192 / 5009219 92 / 103 / 432 / 52 / 102 / 103 / 103 / 102 / 103 / 103 / 103 / 102 / 103 / 10
	22:51:40.336 network_traffic.flow failed to find message	host.os.version	② 20.04.4 LTS (Focal Fossa)	2022 027 /2020000 29.103.131.25 /25 102.103.151.27 TCP 03 743 - 3332 /AC 504.37430000 201-0420 2000 2000 2000 2000 2000 2000 2000
АРМ	22:51:40.336 network_traffic.flow failed to find message 22:51:50.336 network_traffic.flow failed to find message	network.bytes	798799	5229 102.81438053 95.193.149.25 102.108.15.132 TLSVI.2 B13.Application Data 5230 102.81438061 95.108.15.132 St.131.93.143.25 TCP 56 5332 - 4.43 [Ack] Seq-1452326 Ack=38259 Min=65535 Len=0
Services Traces	22:51:50.336 network_traffic.flow failed to find message 22:52:00.336 network_traffic.flow failed to find message	network.community_id	I:2LMrecjBkrZeAncPpPn9POJ2Eok=	r Frame 4455; 62 bytes on wire (409 bits), 62 bytes captured (409 bits) on interface any, 1d 0 Internet Process Version 4, sec 12.07.22.02.22.02.1051 127.2.7.22.42.500
Dependencies	22:52:00.336 network_traffic.flow failed to find message	network.packets	I1039	Transmission control. Protocol, Src. Port: 80/08, Ott Fort: 90/08, Ott Fo
Service Map	22:52:10.337 network_traffic.flow failed to find message 22:52:10.337 network_traffic.flow failed to find message	network.transport	⊙ tcp	
Uptime Monitors	22:52:20.336 network_traffic.flow failed to find message 22:52:30.336 network_traffic.flow failed to find message	network.type	ipv4	00000 00 04 00 01 00 06 48 bb 39 64 40 79 97 88 60 00 ····· Hf 9969v····
TLS Certificates	22:52:40.336 network_traffic.flow failed to find message	source.bytes	③ 320831	
User Experience	22:52:50.336 network_traffic.flow failed to find message 22:53:00.336 network_traffic.flow failed to find message	source.ip	T172.27.224.250	
Dashboard	22:53:10.337 network_traffic.flow failed to find message 22:53:20.337 network_traffic.flow failed to find message	source.packets	③ 3688	Wireshark - Display Filter Expression
	22:53:30.336 network_traffic.flow failed to find message	source.port		Field Name Relation
	22:53:40.336 network_traffic.flow failed to find message 22:53:50.336 network_traffic.flow failed to find message	type	low flow	> GSM SMS - GSM SMS - FDPU (GSM 03.40) is present > GSM SMS U- OSM SMS - Brows Service User Data is > gsup - Character SME Application is > gsup - Character SME Application is

IOWA STATE UNIVERSITY

Elastic: Dashboard Ul



IOWA STATE UNIVERSITY

Elastic: Machine Learning - Anomaly Detection





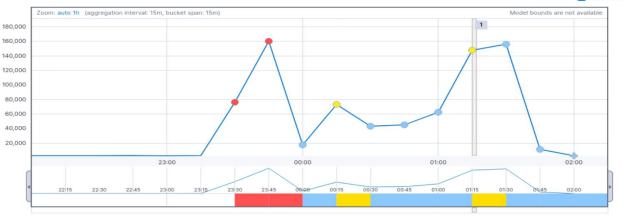
high_count @

550,000

500,000 450,000

400,000

300.000



IOWA STATE UNIVERSITY

Elastic: Machine Learning Data Frame Analytics

Actual class	~	BENIGN ~	DoS Hulk ~	DoS Slowhttptest \checkmark	DoS slowloris \checkmark
	BENIGN	99%	1%	0%	0%
	DoS Hulk	0%	100%	0%	0%
	DoS Slowhttptest	1%	0%	99%	1%
	DoS slowloris	0%	0%	0%	100%

Evaluation quality metrics

0.998 0.994

Overall accuracy ⁽²⁾ Mean recall ⁽²⁾

Per class recall and accuracy

Class	Accuracy	Recall	
BENIGN	0.998	0.993	
DoS Hulk	0.998	1	
DoS Slowhttptest	1	0.985	
DoS slowloris	1	0.996	

Model evaluation

stopped 170366

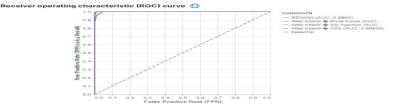
Normalized confusion matrix for entire dataset 🗔

	Predicted class				
	le Columns				
Actual class	~	BENIGN	Web Attack � Brute F 🗸	Web Attack � Sql Inje 🗸	Web Attack � XSS 🛛 🗸
	BENIGN	100%	0%	0%	0%
	Web Attack � Brute Force	1%	19%	0%	80%
	Web Attack � Sql Injection	0%	43%	0%	57%
	Web Attack & XSS	5%	0.36	0.36	95%

Evaluation quality metrics

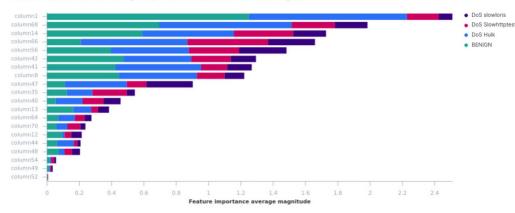
0.99		0.534	
Overall accuracy	O	Mean recall	Ð

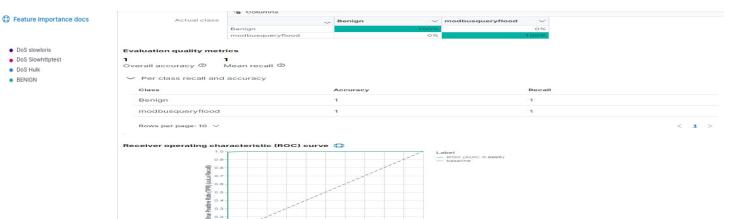
> Per class recall and accuracy



Total feature importance 🔿

Total feature importance values indicate how significantly a field affects the predictions across all the training data.

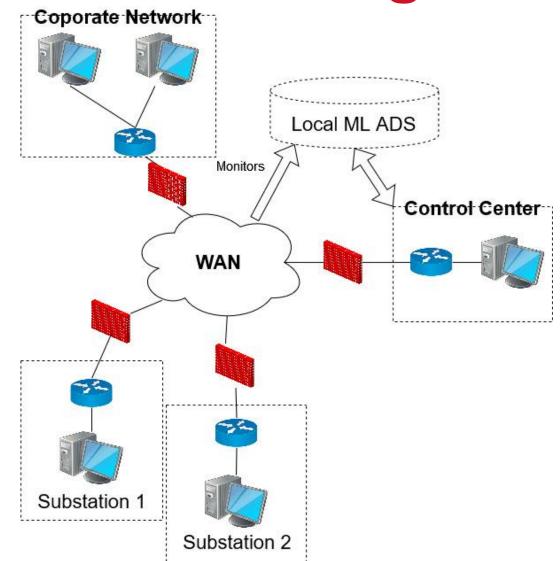




0.3 0.4 0.5 0.6 0.7 0.8 0.9 1.0 Fatse Positive Pate (FPP)

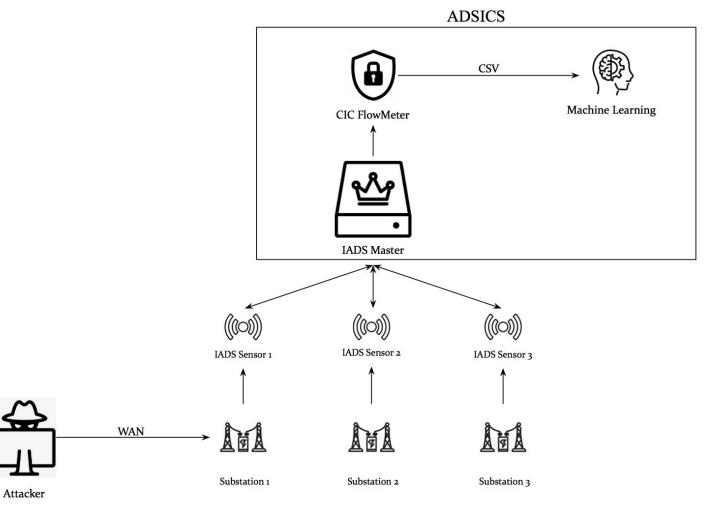
IOWA STATE UNIVERSITY

Local: Theoretical Design



IOWA STATE UNIVERSITY

Local: Practical Design



IOWA STATE UNIVERSITY

Local: SMOTE/Undersampling

	Benign (Normal)	DoS Slowloris	DoS Slowhttptest	DoS Hulk	Dos GoldenEye
Before SMOTE	440042	5796	5499	231073	10293
Distribution	63.53%	0.84%	0.79%	33.36%	<mark>1.49%</mark>
After SMOTE	231073	115536	115536	231073	115536
Distribution	28.57%	14.29%	14.29%	28.57%	14.29%

College of Engineering

• Imbalanced dataset

Synthetic Minority Oversampling Technique (SMOTE)

Random undersampling

- Undersampling amount = $\frac{1}{2}$ the largest alert count (ie. the BENIGN count).
- Oversampling amount = $\frac{1}{2}$ of the undersampling amount

Local: Cross Validation

- Reduced feature count from 78 to 29 features from Thursday dataset.
- Forward model selection is used to select the features.
- Evaluated by least MSE, applied greedy algorithm to get the best combination of the features
- Set the number of features to 29, so no other criterion is used (such as AIC, BIC, Mallows CP, adjusted R squared)

	Feature Name	Description						
1	Destination Port	Destination Port						
2	Total Length of Bwd Packets	Total size of packet in backward direction						
3	Fwd Packet Length Min	Minimum size of packet in forward direction Minimum size of packet in backward direction						
4	Bwd Packet Length Min							
5	Bwd Packet Length Mean	Mean size of packet in backward direction						
6	Bwd Packet Length Std	Standard deviation size of packet in backward direction						
7	Bwd PSH Flags	Number of times the PSH flag was set in packets travelling in the backward direction (0 for UDP)						
8	Fwd Header Length	Total bytes used for headers in the forward direction						
9	Max Packet Length	Maximum length of a packet						
10	Packet Length Mean	Mean length of a packet						
11	Packet Length Std	Standard deviation length of a packet						
12	FIN Flag Count	Number of packets with FIN						
13	PSH Flag Count	Number of packets with PSH						
14	ACK Flag Count	Number of packets with ACK						
15	URG Flag Count	Number of packets with URG						
16	CWE Flag Count	Number of packets with CWE						
17	ECE Flag Count	Number of packets with ECE						
18	Down/Up Ratio	Download and upload ratio						
19	Avg Fwd Segment Size	Average size observed in the forward direction						
20	Fwd Avg Bytes/Bulk	Average number of bytes bulk rate in the forward direction						
21	Fwd Avg Packets/Bulk	Average number of packets bulk rate in the forward direction						
22	Fwd Avg Bulk Rate	Average number of bulk rate in the forward direction						
23	Bwd Avg Bytes/Bulk	Average number of bytes bulk rate in the backward direction						
24	Bwd Avg Packes/Bulk	Average number of packets bulk rate in the backward direction						
25	Bwd Avg Bulk Rate	Average number of bulk rate in the backward direction						
26	Subflow Fwd Bytes	The average number of packets in a sub flow in the forward direction						
27	Subflow Bwd Bytes	The average number of packets in a sub flow in the backward direction						
28	Init_Win_bytes_backward	The total number of bytes sent in initial window in the backward direction						
29	min_seg_size_forward	Minimum segment size obeserved in the forward direction						
6								

IOWA STATE UNIVERSITY

Local: Decision Tree

DECI	ISTON	TREE	WEDNES	DAY TE	ST			DECI	SION T	REE TH	URSDAY			
[[17		8		26]				[[16	7541	48	533	64]		
r r	10	8902		16]]	2	220	1213	72]		
F	10		17760	14]				[22	0	629	1]		
L r	3	ø		6787]	1			Ī	0	0	0	21]]		
E.	2	Ŭ	precis	12 (19 (19 (19 (19 (19 (19 (19 (19 (19 (19	The second se	f1-score	support	1000		pro	ecision	recall	f1-score	support
		0.0	1	.00	0.97	0.99	17842			0	1.00	1.00	1.00	168186
		1.0		.00	1.00	1.00	8928			1	0.82	0.15	0.25	1507
		2.0		.87	1.00	0.93	17785			2	0.26	0.96	0.42	652
		3.0		.99	0.76	0.86	8910			3	0.13	1.00	0.23	21
	accu	nacy				0.95	53465		accura	icy			0.99	170366
		Sec. 2	0	.97	0.93	0.94	53465	п	lacro a	vg	0.55	0.78	0.47	170366
	nacro ghted	-		.96	0.95	0.95	53465	weig	hted a	ivg	1.00	0.99	0.99	170366

IOWA STATE UNIVERSITY

Local: Random Forest

RAND	OM FO	DREST	WEDNES	DAY TE	ST			RANDO	M FOR	EST TH	URSDAY			
[[17	400	2	421	19]				[[16]	7627	6	496	57]		
]	9	8903	0	16]				Ĩ	3	219	1213	72]		
Ε	9	1	17764	11]				ĩ	21	0	630	1]		
Γ	3	0	2120	6787]				Ĩ	1	0	0	20]]		
			precis	ion	recall	f1-score	support	70		pr	ecision		f1-score	support
		0.0	1	.00	0.98	0.99	17842			0	1.00	1.00	1.00	168186
		1.0	1	.00	1.00	1.00	8928			1	0.97	0.15	0.25	1507
		2.0	0	.87	1.00	0.93	17785			2	0.27	0.97	0.42	652
		3.0	0	.99	0.76	0.86	8910			3	0.13	0.95	0.23	21
	accu	acy				0.95	53465		accura	icy			0.99	170366
m	acro	avg	0	.97	0.93	0.95	53465		acro a	1	0.59	0.77	0.48	170366
weig	hted	avg	0	.96	0.95	0.95	53465		nted a		1.00	0.99	0.99	170366

IOWA STATE UNIVERSITY

Local: Modbus

Modbus_Combined_Train										
Three different DDoS. Modbus query flood, Ping flood, tcpSYN flood										
Network Traffic	Network Traffic lasts 6,12,12 hours									
IP										
Attacker	172.27.224.50	172.27.224.70	70 172.27.224.80							
Victim	172.27.224.250									
Type of Attack			Description							
Modbus Query F	Flood		30 minute duration							
Ping Flood			30 minute duration							
TCP SYN Flood			30 minute duration							

- reference power grid data

IOWA STATE UNIVERSITY

Local: Modbus-Combined

[[60811 [5635	787] 92568]				
		precision	recall	f1-score	support
Category	0	0.92	0.99	0.95	61598
	1	0.99	0.94	0.97	98203
accu	iracy			0.96	159801
macro	avg	0.95	0.96	0.96	159801
weighted	l avg	0.96	0.96	0.96	159801

IOWA STATE UNIVERSITY

Local: Modbus-Separate

explain why we want to have this for anomaly detection	[[60809 ([0 26333 [5635 14883 [2 14896	3 21 0 2 5765 14988]			
		precision	recall	f1-score	support	
	BENIGN0MODBUS Query Flood1Ping Flood2TCP SYNFlood3	0.92 0.47 0.80 0.50	0.99 1.00 0.14 0.49	0.95 0.64 0.24 0.50	61598 26354 41270 30579	
	accuracy macro avg weighted avg	0.67 0.73	0.65 0.68	0.68 0.58 0.63	159801 159801 159801	

IOWA STATE UNIVERSITY

Comparison

	Elastics	earch	Local ML					
	Wednesday	Thursday	Wednesday	Thursday	Modbus			
					Combined	Separate		
Max Precision	100.0%	100.0%	100.0%	100.0%	99.0%	95.0%		
Min Precision	99.0%	0.0%	87.0%	23.0%	92.0%	24.0%		
Accuracy	99.8%	99.0%	95.0%	99.0%	96.0%	68.0%		
Macro Average	99.4%	53.4%	95.0%	48.0%	96.0%	67.0%		

IOWA STATE UNIVERSITY

Conclusion

- Elasticsearch worked well with IT attacks
- Local ML was able to capture Modbus attacks

REFERENCE POWER GRID

College of Engineering

- Refining ML model is needed to increase accuracy and provide additional information to the client
- *Elasticsearch may provide OT support later on? <- what do you think*

Recommendation:

Elasticsearch system could be used to detect IT attacks to the control system, however, it lacked OT protocol support. For OT network traffic, Local ML Anomaly detection can be used to supplement a company's anomaly detection system until this functionality is added to Elasticsearch.

Thank You For Your Time! Any Questions?

IOWA STATE UNIVERSITY

References

Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

https://www.linkedin.com/company/sqrrl

Intrusion Detection Evaluation Dataset (CIC-IDS2017). University of New Brunswick. https://www.unb.ca/cic/datasets/ids-2017.html

Applications - CICFlowMeter (formerly ISCXFlowMeter). University of New Brunswick. https://www.unb.ca/cic/research/applications.html#CICFlowMeter ahlashkari/CICFlowMeter. https://github.com/ahlashkari/CICFlowMeter

Frazão, I. and Pedro Henriques Abreu and Tiago Cruz and Araújo, H. and Simões, P., "Denial of Service Attacks: Detecting the frailties of machine learning algorithms in the Classication Process", in 13th International Conference on Critical Information Infrastructures Security (CRITIS 2018), ed. Springer, Kaunas, Lithuania, September 24-26, 2018, Springer series on Security and Cryptology , 2018. DOI: 10.1007/978-3-030-05849-4_19 modbus TCP SCADA #1. https://github.com/tjcruz-dei/ICS PCAPS/releases\

Network datasets, Overview of Network Forensic Tools and Datasets. Github. https://martinazembjakova.github.io/Network-forensic-tools-taxonomy/network-datasets.html

IOWA STATE UNIVERSITY

References

Extremists

https://www.utilitydive.com/news/extremists-have-developed-credible-specific-plans-to-attack-the-us-power/617741/

Global Threats

https://semiengineering.com/power-grids-under-attack/

IOWA STATE UNIVERSITY