AECOM Imagine it. Delivered.

Understanding and Mitigating Risk of Internet-connected Industrial Systems (IIoT/ICS)

Joel Langill

Director – Industrial Security Services
Mission Engineering & Resilience
Management Services (MS)

January 23, 2020

Phase 0 – Current Situation

- Remote Site – unmanned, remotely monitored and managed
- Attractive Site – owned by “recognized” critical infrastructure (CI) entity
- Monitoring and Control – site process and safety parameters
- Configuration – modification of schematics and PLC configuration to support changing local conditions

- Industrial equipment supplied as part of a standard packaged unit for automation and control
- Unrelated national cyber security exercise took place between national government and key infrastructure providers …

Packaged Equipment – Third-Party Supply

ESD Web2Water®

Control Platform

A Web Based, Wireless, Remote Monitoring, Telemetry & Control PLC Platform

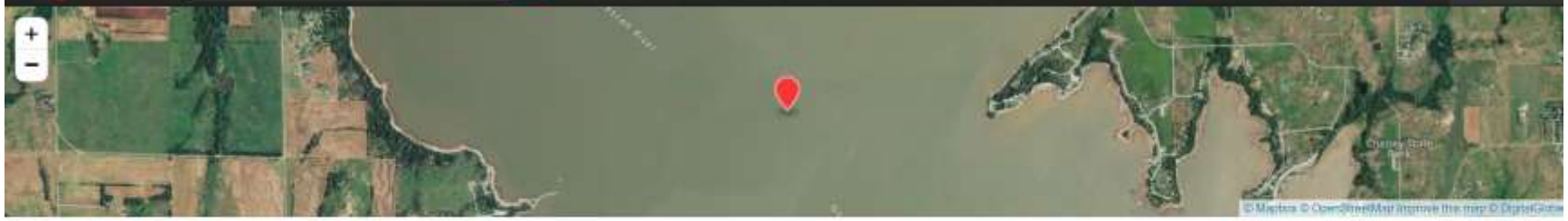
The ESD "Web2Water®" (W2W) Control Platform is designed to both operate and control all types of Industrial process systems including wastewater treatment and soil and groundwater remediation systems.

W2W is designed to provide the most economical, stable and interactive remote monitoring, telemetry & system control platform available on the market today. ESD has configured the platform with the intent of providing the system operator the most user friendly and intuitive interface experience available, without sacrificing cost or uptime dependability.

W2W utilizes an Allen Bradley MicroLogix PLC, C-More color touch screen operator interface terminal (OIT) with built-in FTP server, e-mail client, and Web server, and a wireless 3G high speed modem supporting major carriers such as AT&T and Verizon Wireless at up to 7.2 Mbps. One simple compact economical platform provides local PLC control, remote control, remote alarming, automatic system status updates, remote interactive control (start / stop / modify) data-logging and trending, and can ship with all wireless communications fully established and operational prior to shipping.

Internet Accessible + Target Attractiveness

SHODAN | Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us | My Account | Help Center



[redacted] myvzw.com View Raw Data

Industrial Control System

Country	United States
Organization	Verizon Wireless
ISP	Verizon Wireless
Last Update	2018-05-19T15:33:19.918311
Hostnames	[redacted] myvzw.com
ASN	AS22394

Web Technologies

jQuery

Ports

21 | 80 | 2332 | 9191 | 9443 | 44818

Services

A very large Energy company name!

21 / tcp / ftp

```
220 [redacted] FTP Service (WS_FTP Server Ver4.81.0.0).
502 Invalid command.
502 Invalid command.
```

80 / tcp / http

```
HTTP/1.1 401
Server: EA-HTTP/1.0
Date: Sun, 29 Apr 2018 11:16:27 GMT
WWW-Authenticate: Basic realm="Panel :"
Content-Type: text/html
Content-Length: 53
```

44818 / tcp / ethernetip

Rockwell Automation/Allen-Bradley Version: 1766-L32BXB B/15.00

```
Product name: 1766-L32BXB B/15.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60005408
Device type: Programmable Logic Controller
Device IP: 192.168.13.1
```

“Black Box” Enumeration

```
$ sudo hping3 -S -i u1000 --scan 1-65535 [redacted] | grep .A
Scanning [redacted] port 1-65535
65535 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A... 102 53762 32120    46
 9999            : .S..A... 102 27815 33232    46
10900            : .S..A... 101 48553 33232    46
11102            : .S..A... 102 45121 33232    46
11110            : .S..A... 101 28330 33232    46
44818            : .S..A... 101 11066  2000    48
All replies received. Done.
```

Phase 1 – Data Collection

Purpose:

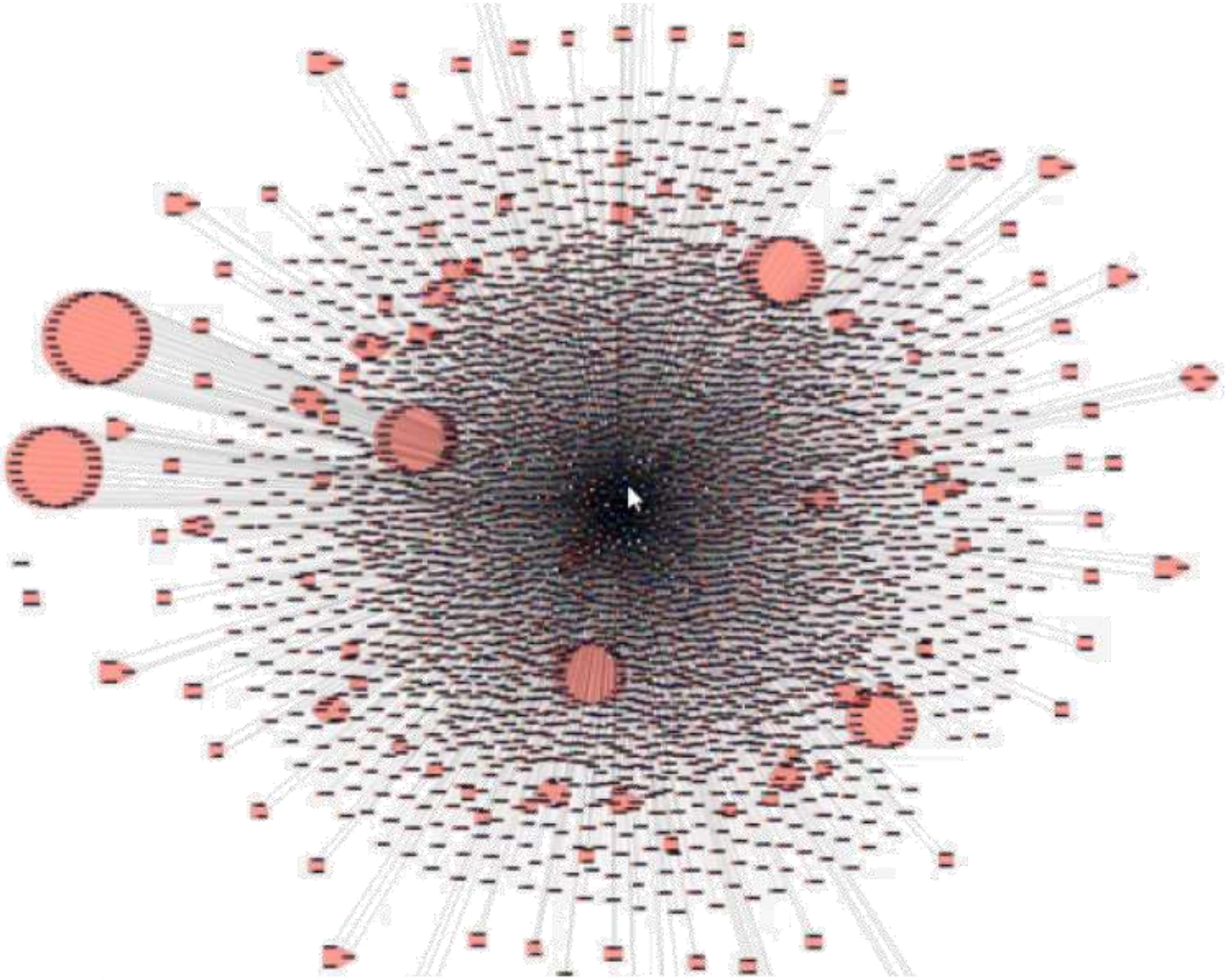
- Understand current security posture
- Collect attribution data of “unauthorized” access (~1 week)

Technique:

- Inline collection of all network traffic
- Utilized “bridged” network interfaces
- Record all data via `tcpdump` throughout collection period

```
$ sudo tcpdump -i <interface> -G <seconds> -w <filename.pcap>
```

Potential Adversaries (Complete Source Attribution)



More than 3100 source addresses over 7 day period

Phase 2 – Data Analysis

Purpose:

- Extract attribution of potential actors
- Leverage threat intelligence in evaluating actors
- Evaluate capability of actors (determine intent)
- Evaluate extent of any breach

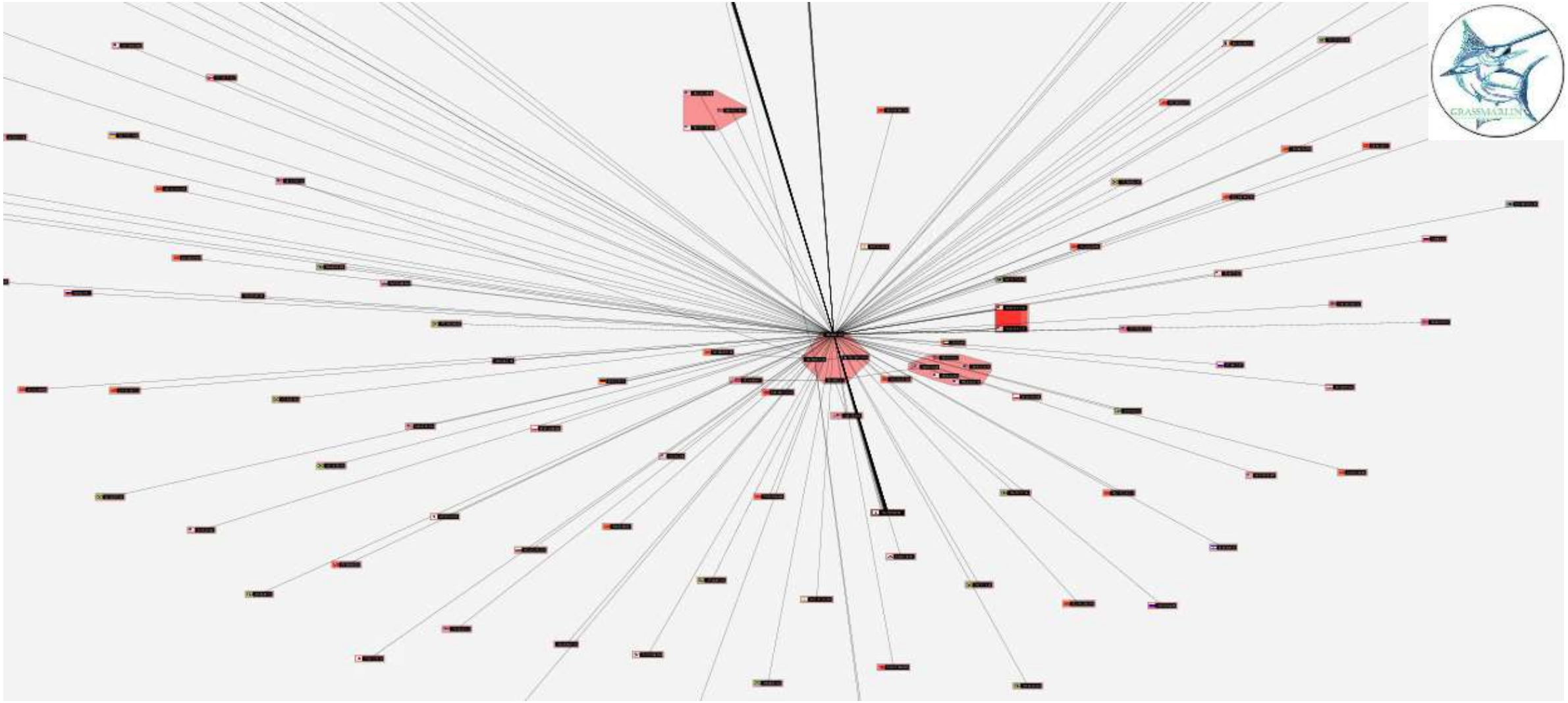
Technique:

- Evaluate network packet captures across multiple tools
  - Flow Data - GeoLocation
  - Session Data - Credentials + Files
  - Application Data – Source Attribution + Deep Packet Inspection

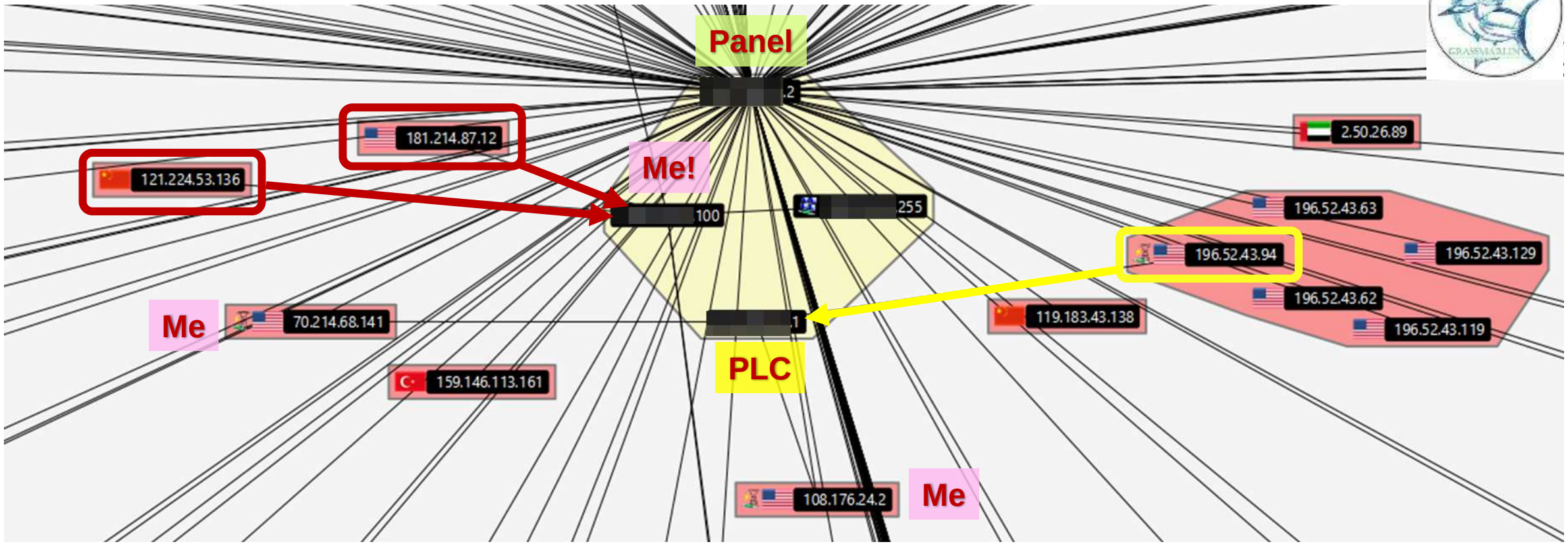
Potential Adversaries (Complete Source Attribution)

Actual Adversaries

Flow Data: Target + GeoLocation



Flow Data: Target + GeoLocation + Capability



AECOM

Flow Data: Target + GeoLocation + Capability + Intent

Timestamp	Source IP	Source Port	Destination IP	Destination Port	PCAP File	Frame	Protocol	Size
1969-12-23T15:47:52.345Z	[redacted].1	44818	108.176.24.2	2221	[redacted]Network_Capture_consolidated.pcap	6552	TCP	0
1969-12-23T15:49:15.060Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6583	TCP	0
1969-12-23T15:49:15.076Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6595	TCP	0
1969-12-23T15:49:15.088Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6601	TCP	0
1969-12-23T15:49:15.468Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6604	TCP	0
1969-12-23T15:49:15.982Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6605	TCP	0
1969-12-23T15:49:17.983Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6608	TCP	0
1969-12-23T15:49:21.984Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6615	TCP	0
1969-12-23T15:49:29.988Z	[redacted].1	44818	108.176.24.2	1695	[redacted]Network_Capture_consolidated.pcap	6623	TCP	0
1969-12-23T16:11:16.556Z	196.52.43.94	6712	[redacted].1	44818	[redacted]Network_Capture_consolidated.pcap	6759	UDP	24
1969-12-23T16:11:16.557Z	[redacted].1	44818	196.52.43.94	6712	[redacted]Network_Capture_consolidated.pcap	6760	UDP	83

Me

???

Session Data: Client/Server Relationship, Files, Credentials

Hosts (3192) | Browsers (31) | Files (133) | Images (2) | Messages | Credentials (20) | Sessions (8844) | DNS (61) | Parameters (2226) | Keywords | Anomalies

Sort Hosts On: IP Address (ascending) | Sort and Refresh

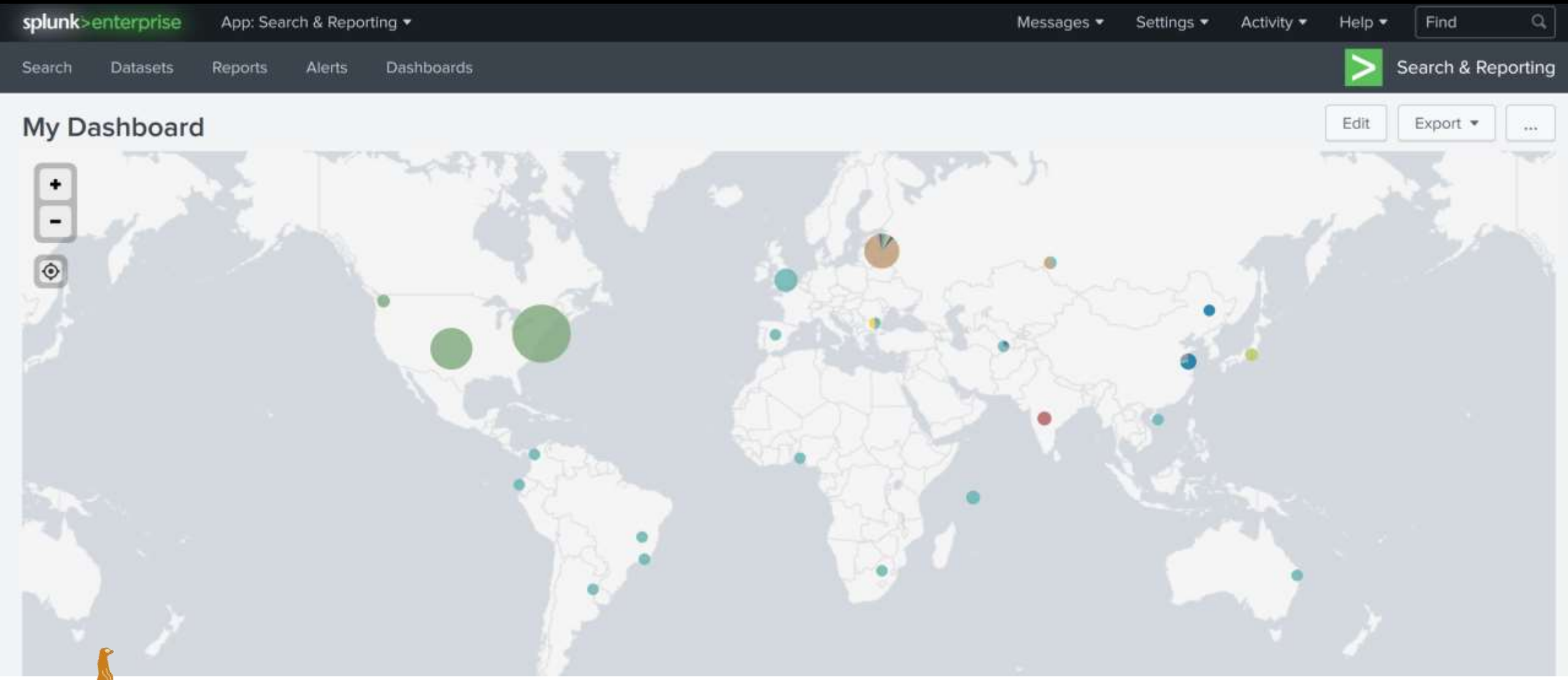
- 70.187.149.166
- 70.187.154.173
- 70.214.68.141
  - IP: 70.214.68.141
  - MAC: 00143E198218
  - NIC Vendor: AirLink Communications, Inc.
  - Hostname:
  - GeoIP: US United States
  - OS: Unknown
  - TTL: 51 (distance: 13)
  - Open TCP Ports:
  - Sent: 76 packets (4,911 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Received: 53 packets (7,661 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Incoming sessions: 0
  - Outgoing sessions: 9
    - Server: [redacted].2 [[redacted]] [Panel :] [[redacted].myvzw.com] [[redacted]:80] (Windows) TCP 80
  - Host Details
- 71.6.135.131
- 71.6.142.80
- 71.6.142.87
- 71.6.146.130
- 71.6.146.185
- 71.6.146.186
- 71.6.158.166
- 71.6.167.142
- 71.6.202.198

Hosts (3192) | Browsers (31) | Files (133) | Images (2) | Messages | Credentials (20) | Sessions (8844) | DNS (61) | Parameters (2226) | Keywords | Anomalies

☑ Show Cookies ☑ Show NTLM challenge-response ☐ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
70.214.68.141	[redacted].2 [[redacted]] [Panel :]	HTTP	user	1234	Unknown	2/26/2018 1:56:44 PM
108.176.24.2	[redacted].2 [[redacted]] [Panel :] (Windows)	FTP	anonymous	mozilla@example.com	Unknown	2/26/2018 7:09:07 PM
108.176.24.2 (Windows)	[redacted].2 [[redacted]] [Panel :] (Windows)	FTP	anonymous	User@	Unknown	2/26/2018 7:11:50 PM
108.176.24.2 (Windows)	[redacted].2 [[redacted]] [Panel :] (Windows)	FTP			Unknown	2/26/2018 7:15:11 PM
108.176.24.2 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	HTTP	user	1234	Unknown	2/26/2018 8:12:07 PM
108.176.24.2 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	chrome@example.com	Unknown	2/27/2018 9:02:03 AM
100.46.50.195 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	User@	Unknown	2/27/2018 11:43:59 AM
100.46.50.195 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	anonymous@example.com	Unknown	2/27/2018 11:46:13 AM
108.176.24.2 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	jfangill		Unknown	2/27/2018 11:57:40 AM
37.215.156.231 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	admin	pass	Unknown	2/27/2018 5:23:51 PM
195.88.112.213 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	devry	Unknown	2/28/2018 12:55:13 PM
212.96.79.17 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	qwerty	Unknown	2/28/2018 10:05:09 PM
212.112.124.174	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	test	qazwsxedc	Unknown	3/1/2018 4:02:19 AM
31.211.102.129	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	bot@filemare.com	Unknown	3/2/2018 2:24:40 AM
164.132.91.13	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	mozilla@example.com	Unknown	3/2/2018 7:49:23 AM
62.190.148.115	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	proxy@	Unknown	3/2/2018 8:27:38 AM
106.77.24.77 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	derok010101	Unknown	3/3/2018 2:25:51 AM
159.65.62.20	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	ftp@	Unknown	3/3/2018 6:27:11 PM
46.228.8.228 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	1234567890	Unknown	3/5/2018 12:40:35 AM
103.68.55.4 (Windows)	[redacted].2 [[redacted]] [Panel :] [redacted]	FTP	anonymous	cjmasterinf	Unknown	3/5/2018 4:52:16 AM

Application Data: Converting Data to Intelligence



Basic Attribution – Authorized versus Unauthorized Access

Source IP

sourceip	count	Country	City	Region
108.176.24.2	1523	United States	New York	New York
65.240.194.232	947	United States		
23.194.140.36	198	United States	Cambridge	Massachusetts
5.188.9.25	198	Russia	Saint Petersburg	St.-Petersburg
5.188.11.25	196	Russia	Saint Petersburg	St.-Petersburg
190.7.62.162	164	Argentina	Federal	Entre Rios
62.190.148.115	152	United Kingdom	Solihull	Solihull
100.46.50.195	97	United States		
46.55.209.53	95	Bulgaria	Kavarna	Oblast Dobrich
195.88.112.213	83	Russia		
37.215.156.231	83	Belarus	Maladzyechna	Minsk
185.2.196.196	71	United Kingdom	Wimbledon	Merton

Source Country

Country	count
United States	3350
Russia	864
United Kingdom	475
Argentina	167
China	164
India	103
Bulgaria	100
Belarus	83
Seychelles	83
Republic of Korea	50
France	47
Germany	45
Hong Kong	45
Netherlands	44
Japan	41

Threat Intelligence – Source Address Reputation

SID

sid	count	percent	sid-msg
2402000	509	39.827856	ET DROP Dshield Block Listed Source group 1
2403303	121	9.467919	ET CINS Active Threat Intelligence Poor Reputation IP group 4
2403304	104	8.137715	ET CINS Active Threat Intelligence Poor Reputation IP group 5
2101411	36	2.816901	GPL SNMP public access udp
2403367	20	1.564945	ET CINS Active Threat Intelligence Poor Reputation IP group 68
2403361	20	1.564945	ET CINS Active Threat Intelligence Poor Reputation IP group 62
2403380	18	1.408451	ET CINS Active Threat Intelligence Poor Reputation IP group 81
2221014	18	1.408451	SURICATA HTTP missing Host header
2403384	16	1.251956	ET CINS Active Threat Intelligence Poor Reputation IP group 85
2403397	14	1.095462	ET CINS Active Threat Intelligence Poor Reputation IP group 98
2500046	13	1.017214	ET COMPROMISED Known Compromised or Hostile Host Traffic

SID by Source IP

sid	sourceip
2001219	108.176.24.2
2006402	108.176.24.2
2006402	70.214.68.141
2010935	121.224.53.136
2010939	70.187.149.166
2012936	46.183.219.132
2017174	42.202.133.28
2017616	203.162.13.243
2018317	108.176.24.2
2018489	108.176.24.2
2023753	188.230.73.37
2023753	212.92.115.77
2023753	212.92.124.11
2023753	5.101.40.8
2023753	62.102.148.173
2101280	173.249.22.112

Threat Intelligence – Source Address Reputation

"Block Listed Source Group" [SID 2402000]

sourceip	count	Country
5.188.9.25	99	Russia
5.188.11.25	98	Russia
77.72.82.101	39	Russia
5.188.11.111	35	Russia
191.101.167.167	18	United States
85.93.20.34	18	Germany
77.72.82.98	17	Russia
77.72.82.222	14	Russia
92.63.197.40	14	Russia
5.188.10.108	13	Russia
89.248.168.14	10	Seychelles
77.72.82.11	9	Russia
80.82.77.33	9	Seychelles
5.188.11.20	7	Russia
181.214.87.230	6	United States

>50%

"Active Threat Intelligence Poor Reputation IP Group 4" [SID 2403303]

sourceip	count	Country
5.188.11.25	98	Russia
5.188.10.108	13	Russia
5.188.11.20	7	Russia
5.101.40.10	1	Russia
5.188.10.4	1	Russia
5.188.11.22	1	Russia
	121	

100%

"Active Threat Intelligence Poor Reputation IP Group 5" [SID 2403304]

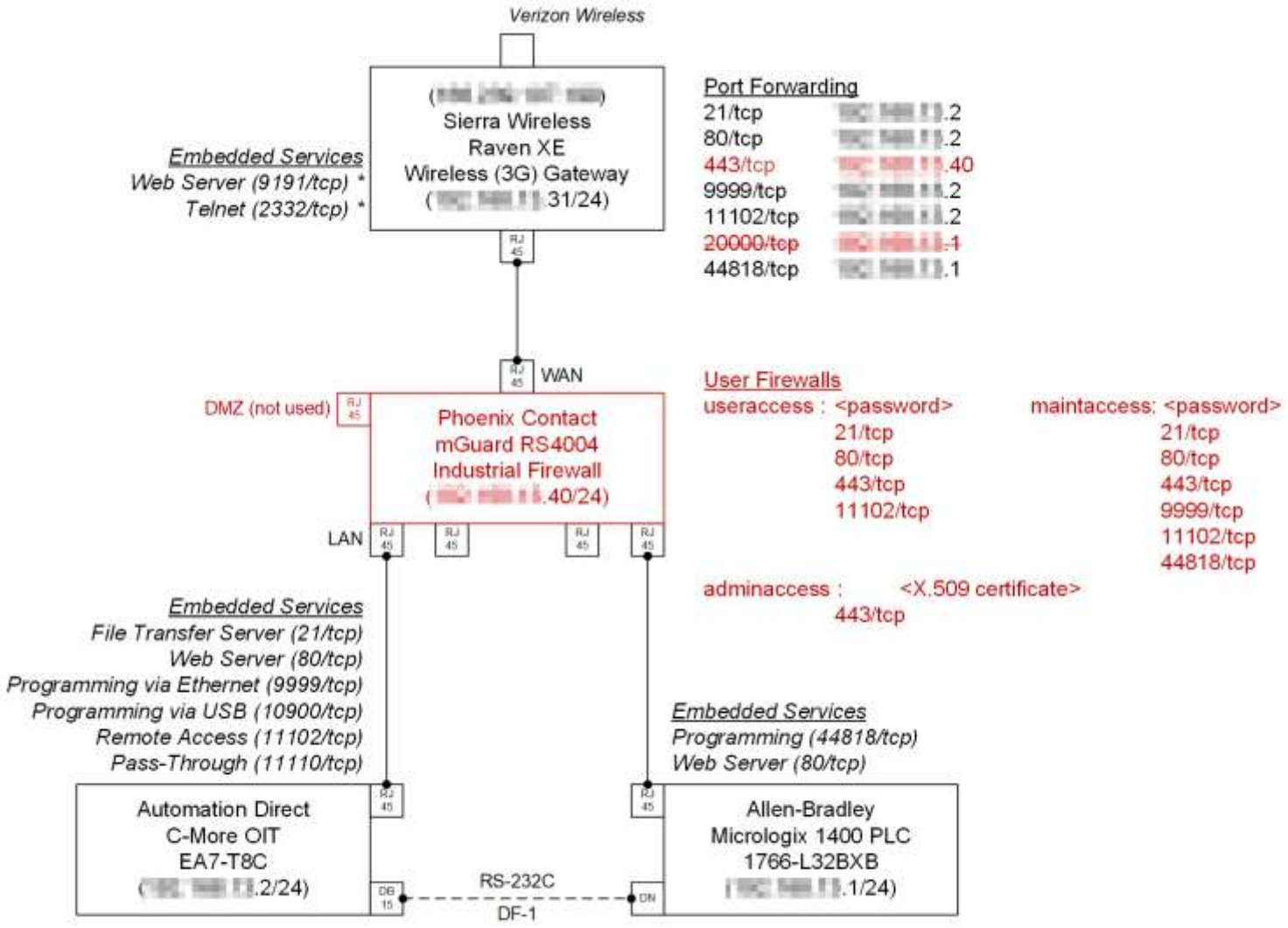
sourceip	count	Country
5.188.9.25	98	Russia
5.188.203.40	5	Russia
5.188.86.140	1	Russia
	104	

100%

Phase 3 – Risk Reduction and Remediation

- Replace existing switch with multi-port firewall (approx. 2” of rail space available)
- Use existing 24VDC power supply
- Basic stateful shallow-packet inspection firewall (deep-packet inspection not necessary)
- Establish role-based rules/policy
  - “user” = schematics, logs
  - “maintenance” = configuration
- Utilize digital certificates for authentication to firewall for sensitive configuration and support

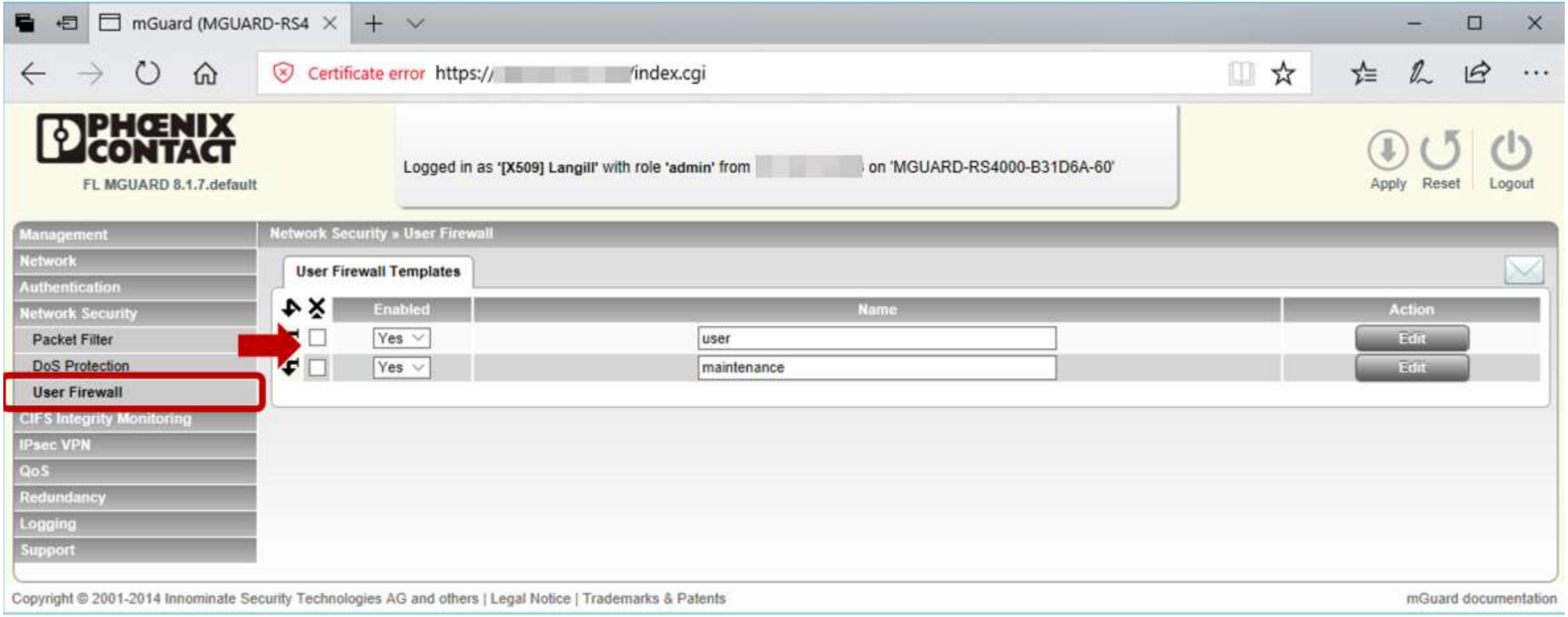
Basic Architecture ("Secured")



NOTES:
* Service Exposed on Public Interface; cannot be disabled

AECOM

User Firewall – Assign Templates



User Firewall – Implement Role-based Policy/Rules

mGuard (MGUARD-RS4

Certificate error https://[redacted]/index.cgi

PHOENIX CONTACT

FL MGUARD 8.1.7.default

Logged in as '[X509] Langill' with role 'admin' from [redacted] on 'MGUARD-RS4000-B31D6A-60'

Apply Reset Logout

Management
Network
Authentication
Network Security
Packet Filter
DoS Protection
User Firewall
CIFS Integrity Monitoring
IPsec VPN
QoS
Redundancy
Logging
Support

Network Security » User Firewall » maintenance

General | Template users | Firewall rules

Firewall rules

Source IP %authorized_ip

Log ID: ufw-MAI0062384670-N°-05ca897d-9cad-13f4-9d6b-00a045b31d6a

N°	Protocol	From Port	To IP	To Port	Comment	Log
1	TCP	any	[redacted]2/32	80	Web	No
2	TCP	any	[redacted]2/32	11102	Panel Remote Access	No
3	TCP	any	[redacted]2/32	21	File Transfer	No
4	TCP	any	[redacted]2/32	9999	Panel Programming	No
5	TCP	any	[redacted]1/32	44818	PLC Programming	No

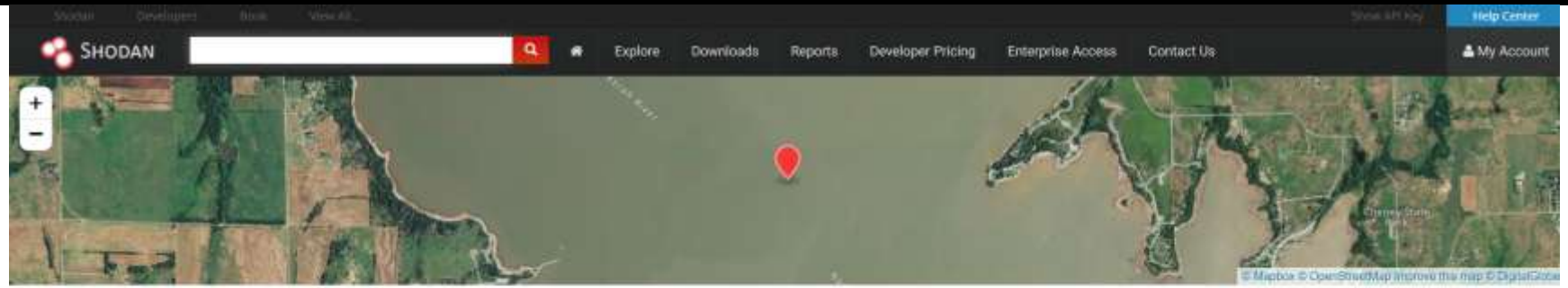
Please note: If the template is configured with dynamic timeout, the logout timer will be reset to its initial value, if TCP, UDP or any other network traffic except ICMP is passing the device due to a matching user firewall rule. For a more precise description of this feature please see the user manual.

Back

Copyright © 2001-2014 Innominate Security Technologies AG and others | Legal Notice | Trademarks & Patents

mGuard documentation

Improve Security, Increase Resilience, Descrease Attractiveness



[redacted] myvzw.com View Raw Data

Country	United States
Organization	Verizon Wireless
ISP	Verizon Wireless
Last Update	2018-05-14T12:52:37.912016
Hostnames	[redacted] myvzw.com
ASN	AS22394

Ports

443 2332 9191

Services

443
tcp
https

```
HTTP/1.1 200 OK
Server: mGuard
Date: Mon, 14 May 2018 07:51:13 UTC
X-Frame-Options: DENY
Content-Language: en
Set-Cookie: id=; Secure; HttpOnly; Max-Age=0
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Connection: close
```

AECOM Imagine it. Delivered.

Joel Langill
+1 (920) 594-0321
joel.langill@aecom.com