Next Gen Innovation

Your Automation Systems are Under Attack

12 February 2020

Project Team

- Integrated Control Systems (ICS) & Operational Information Technology (OIT) SATOC: Turn Key solution provides design, install, protect & defend, and onsite support for system operations, turnover, and training.

- **Tribal One Construction** (T1 Construction, LLC) is a 100% Tribally owned, SBA certified 8(a) firm that serves government and commercial clients from its North Bend, OR corporate office and from its satellite offices in Eugene, OR; Centennial, CO; and Colorado Springs, CO. Tribal One businesses fulfill contracts in the construction and communications technology sectors.

- **Goliath Solutions Group**, LLC is a Cyber Security and Managed Services company providing services across several market sectors to include Department of Defense (DoD), Department of Energy (DoE), Department of Homeland Security (DHS) other Federal Agencies, Oil & Gas, manufacturing, energy, healthcare and finance.

- **Tetra Tech**, based in Pasadena, CA, is a full-service consulting and engineering firm with a substantial global presence. We help our clients conceptualize and execute innovative solutions to their most difficult problems. From front-end science and planning to design, construction management, and operations, Tetra Tech's global service network provides best-in-class experts with worldwide project experience.

Overview

- Defining the problem / why we care
- Why ICS is different than IT
- Traditional approaches
- Machine learning
- Protecting to Level 0
- Defensible Plug-and-Play Network Backbone Concept

What are the issues

- Pervasive Problems
  1. Supply chain issues, inherently insecure COTS, insider threats
  2. Highly automated and skilled adversaries
  3. There are no secure enclaves - breach after breach after breach…
  4. “Air Gaps” can’t secure a system – see Stuxnet and Ukraine attacks…

- Pervasive Needs
  1. Must have 100% network situational awareness
  2. Must have data assurance and integrity
  3. Must be able to detect network anomalies at the source
  4. Must preserve mission critical functions in spite of pervasive problems
  5. Must be able to operate without perfect trust
  6. Must be able to establish, maintain and restore trust in cyber systems

- Continuous Trust Restoration: Resilient Technology
  - ✓ A concept to overcome pervasive problems
  - ✓ A concept to preserve mission critical functions
  - ✓ A concept to establish, maintain and restore trust in cyber systems
  - ✓ Start Secure, Stay Secure, Return Secure

The Problem: Critical Infrastructure & Industrial Control Systems

- Critical Infrastructure operations rely on critical infrastructure and ICS
- Electric power, fuel, water, waste water, building automation, HVAC
- Cyber protection of ICS at DoD installations is lacking
- No way to replicate a facility’s ICS to conduct R&D and testing of ICS defense

A Cybersecurity Approach with Machine Learning for ICS – In the beginning…..

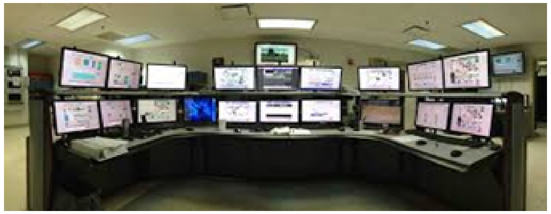
- ICS security was much simpler before the web or before it became the “buzz”
- Vendors designed control systems with automation and reliability in mind not security
- Then the internet creeped in, and with it, the threat of connectivity-enabled attacks that don’t require physical access to plants or their systems
- A.I.C vs C.I.A

Playing Catchup

- Let’s be honest, I.T. Cybersecurity has a tremendous head start on ICS/O.T. Cybersecurity
- Because of this, ICS/O.T. security must adapt quicker and come up with better solutions from the start
- Not only do we need to worry about I.T. related threats but O.T. specific threats

We All Know The Challenges of OT Security

- Industry never designed legacy systems for the Information Age
- Cyber security not considered at install and adding on old tech is difficult
- Vendor software often runs on unpatched or unsupported operating systems (Windows 95, 98, XP…etc)
- Industry engineers are not trained to be cyber security experts.
- Cyber security experts are not industrial engineers….hard to find both
- Information overload
  - Industry operators have exponentially more information to monitor.
  - Too much data.



Current Solutions for Critical Infrastructures Industries

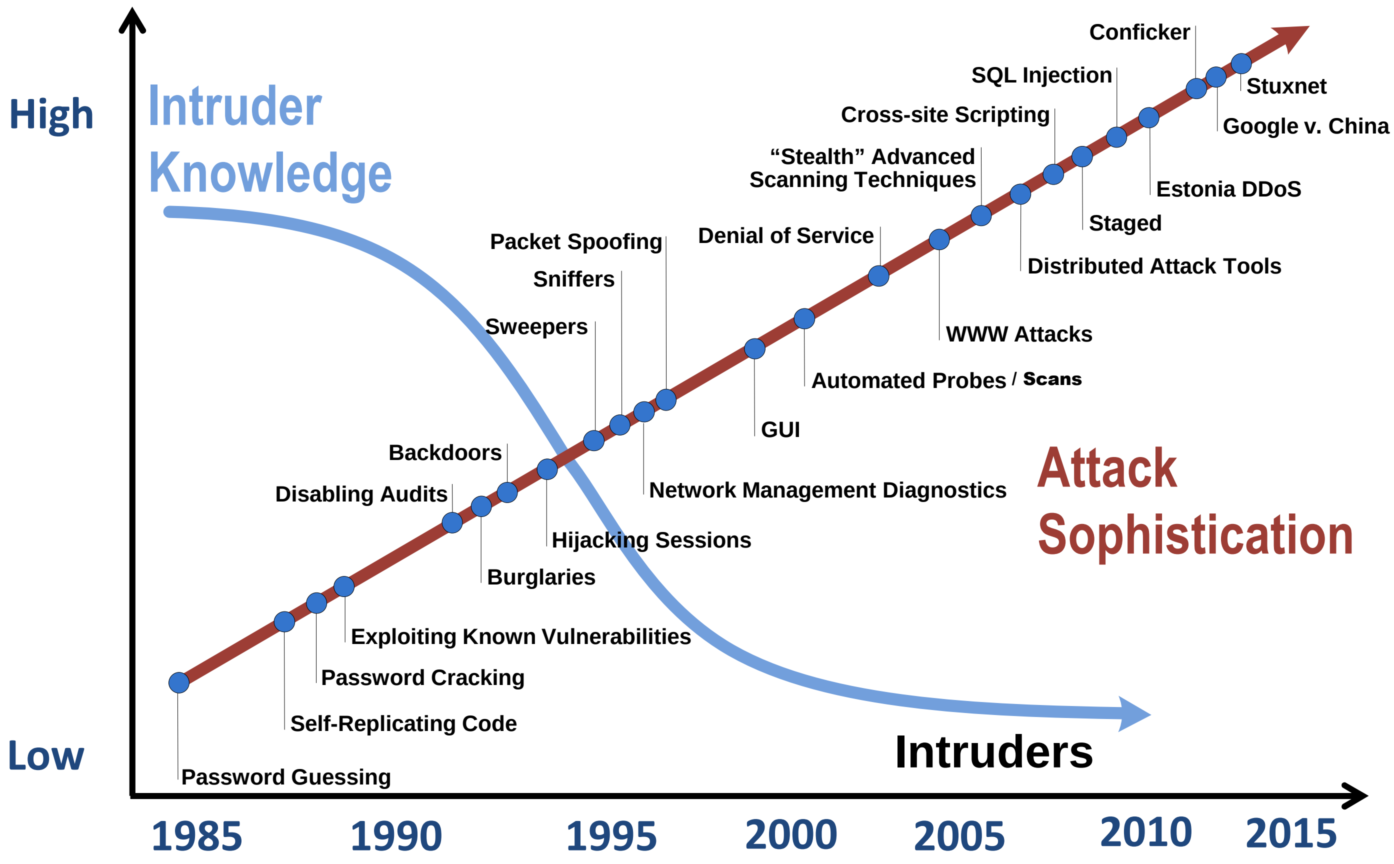
- Retread of IT capabilities for OT/ICS → Proven it doesn't work
- Traditionally, cyber security relied on rules-based or signature-based pattern matching.
  - Find malware and generate signatures
  - Only detects malware that is known – it has to match a virus definition or signature
- "AI"-powered cyber attacks are on the rise
  - Such attacks hide definitive characteristics and signatures
  - We will lose if we stick with the same defensive game plan
- ML will be the alternative to traditional cybersecurity solutions.
  - Algorithms analyze the behavior of the program, characterize it using machine learning, and identify that behavior is predictive of malicious code
  - Statistical & behavioral analysis

The old IT way security does not protect ICS devices!

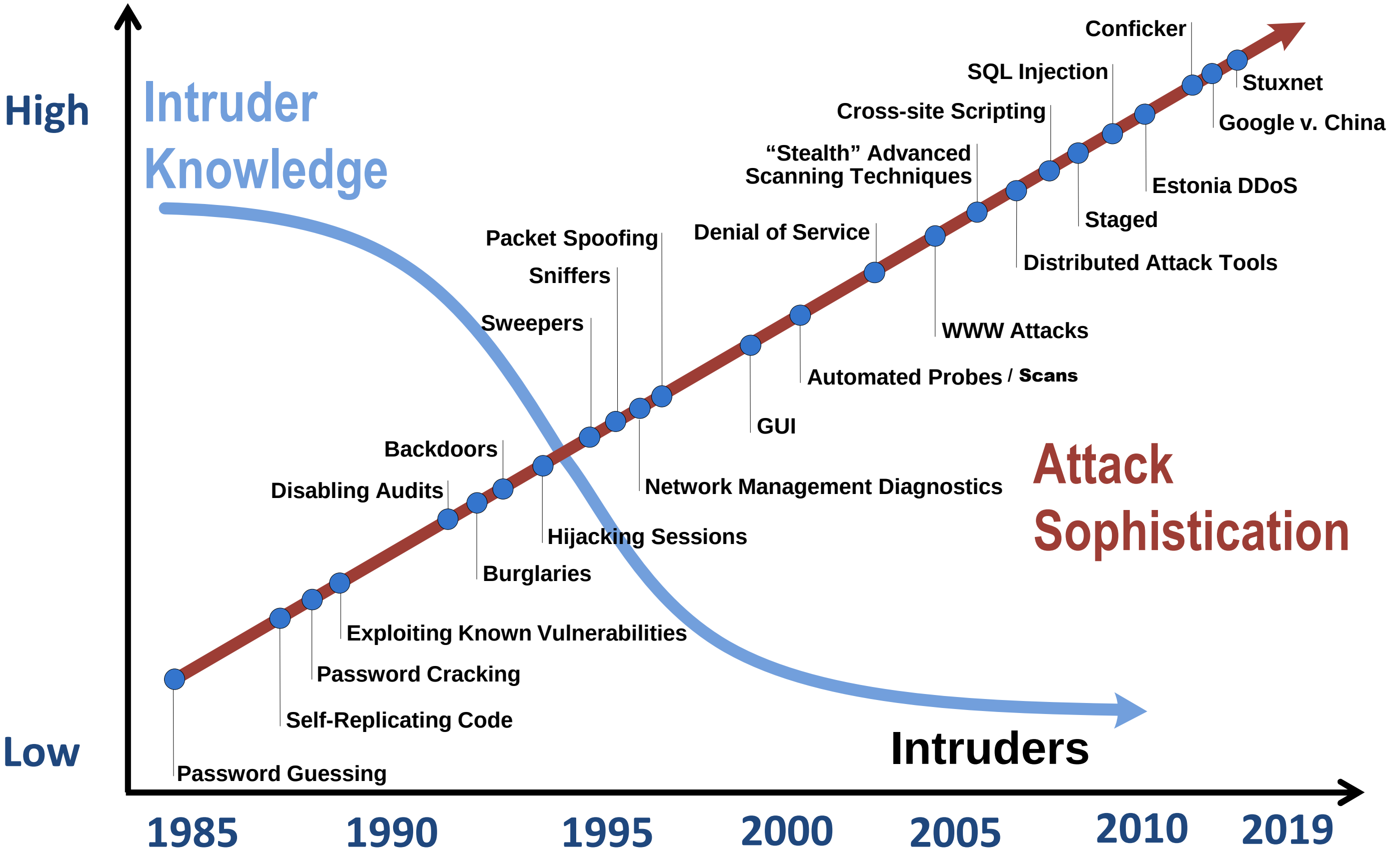
Things I’ve been told on Assessments

- **It’s a “closed network”**
  - In 2011 I demonstrated that I could shut down a power system by hacking the GPS. Imagine what I can do now.
- **Why would anyone want to attack me?**
  - Pizza plot attack
- **I could tell if we were hacked because I watch my HMI**
  - Ask the guys in Iran about spoofing attacks
- **We don’t have any modems on our networks**
  - I found 78 on a fuel management systems that was connected to their corporate network for billing
- **I don’t care who’s on my network, as long as I can get my product from point “A” to point “B”**

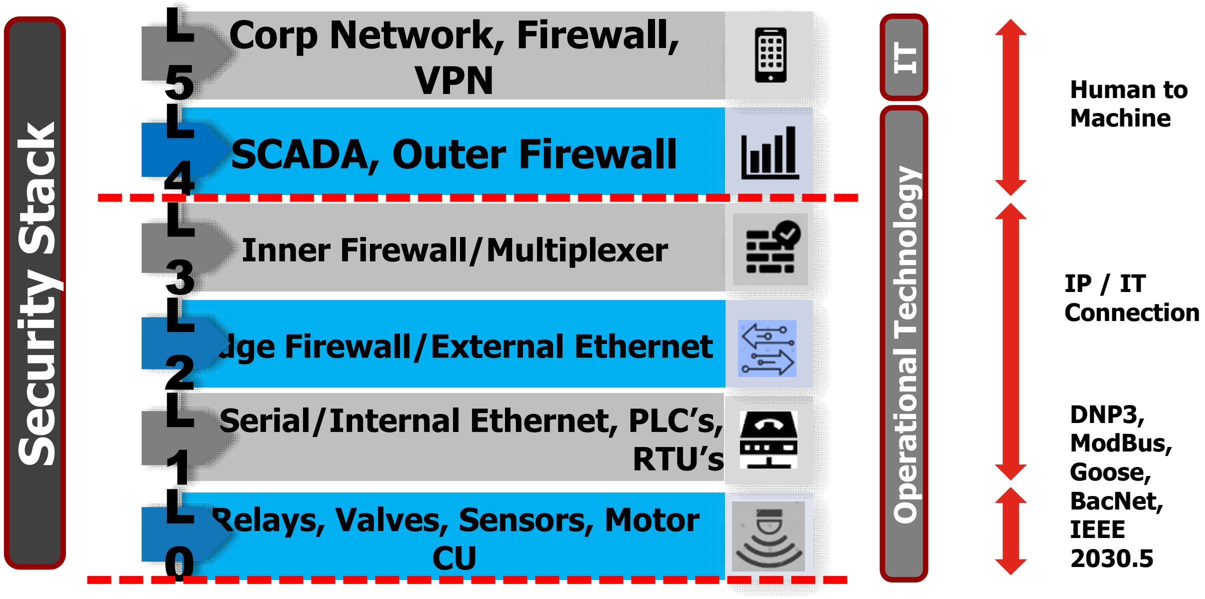
Why should you care



Why should you care

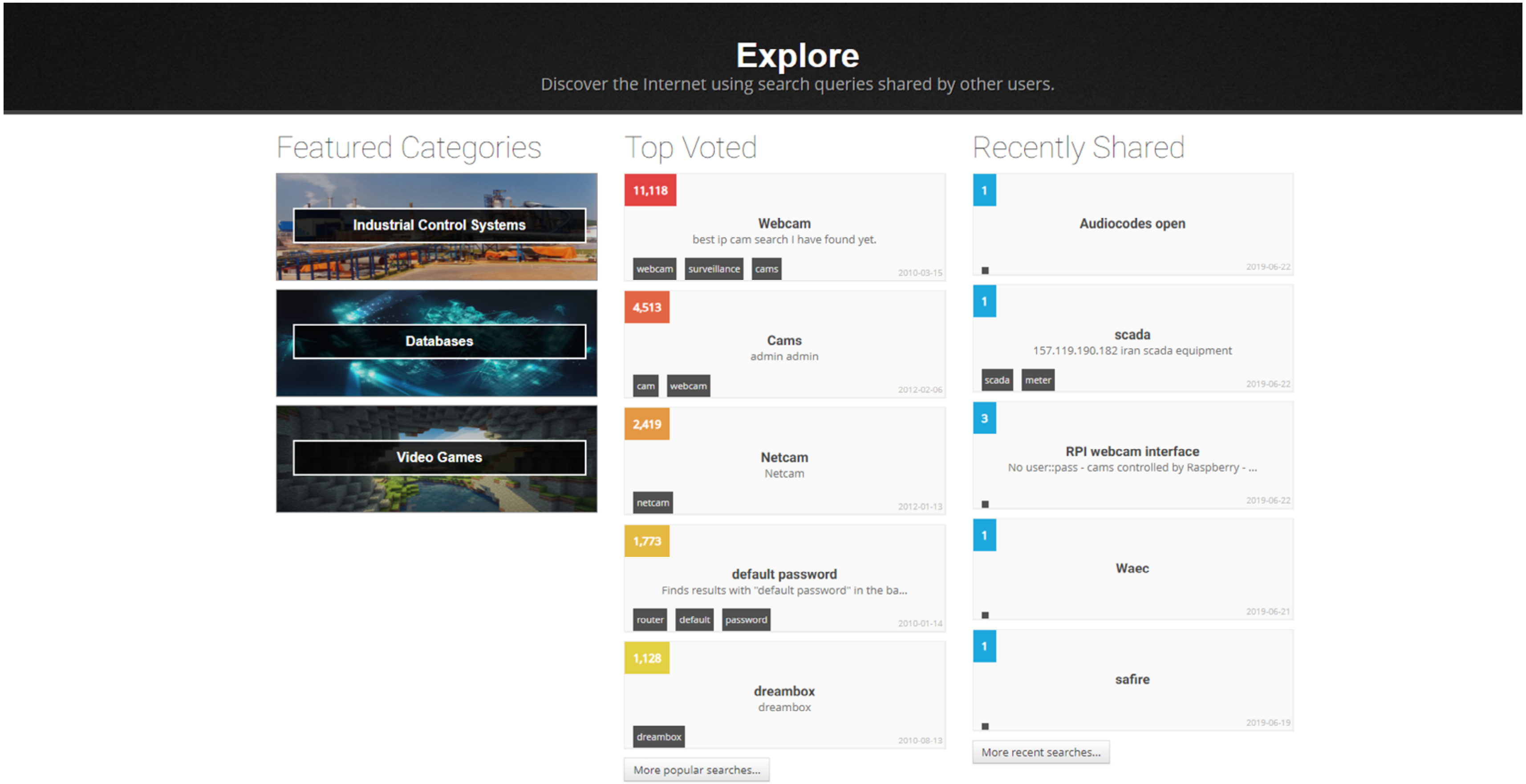


We need to protect Protects where others don’t


Security Stack
L5
Corp Network, Firewall, VPN
L4
SCADA, Outer Firewall
L3
Inner Firewall/Multiplexer
L2
dge Firewall/External Ethernet
L1
Serial/Internal Ethernet, PLC’s, RTU’s
L0
Relays, Valves, Sensors, Motor CU
IT
Operational Technology
Human to Machine
IP / IT Connection
DNP3, ModBus, Goose, BacNet, IEEE 2030.5

Protection is focused at the top…proven threats also exist at the bottom

Shodan makes life easy – An Example



Explore

Discover the Internet using search queries shared by other users.

Featured Categories

Industrial Control Systems

Databases

Video Games

Top Voted

11,118
Webcam
best ip cam search I have found yet.
webcam surveillance cams 2010-03-15

4,513
Cams
admin admin
cam webcam 2012-02-06

2,419
Netcam
Netcam
netcam 2012-01-13

1,773
default password
Finds results with "default password" in the ba...
router default password 2010-01-14

1,128
dreambox
dreambox
dreambox 2010-08-13

More popular searches...

Recently Shared

1
Audiocodes open
2019-06-22

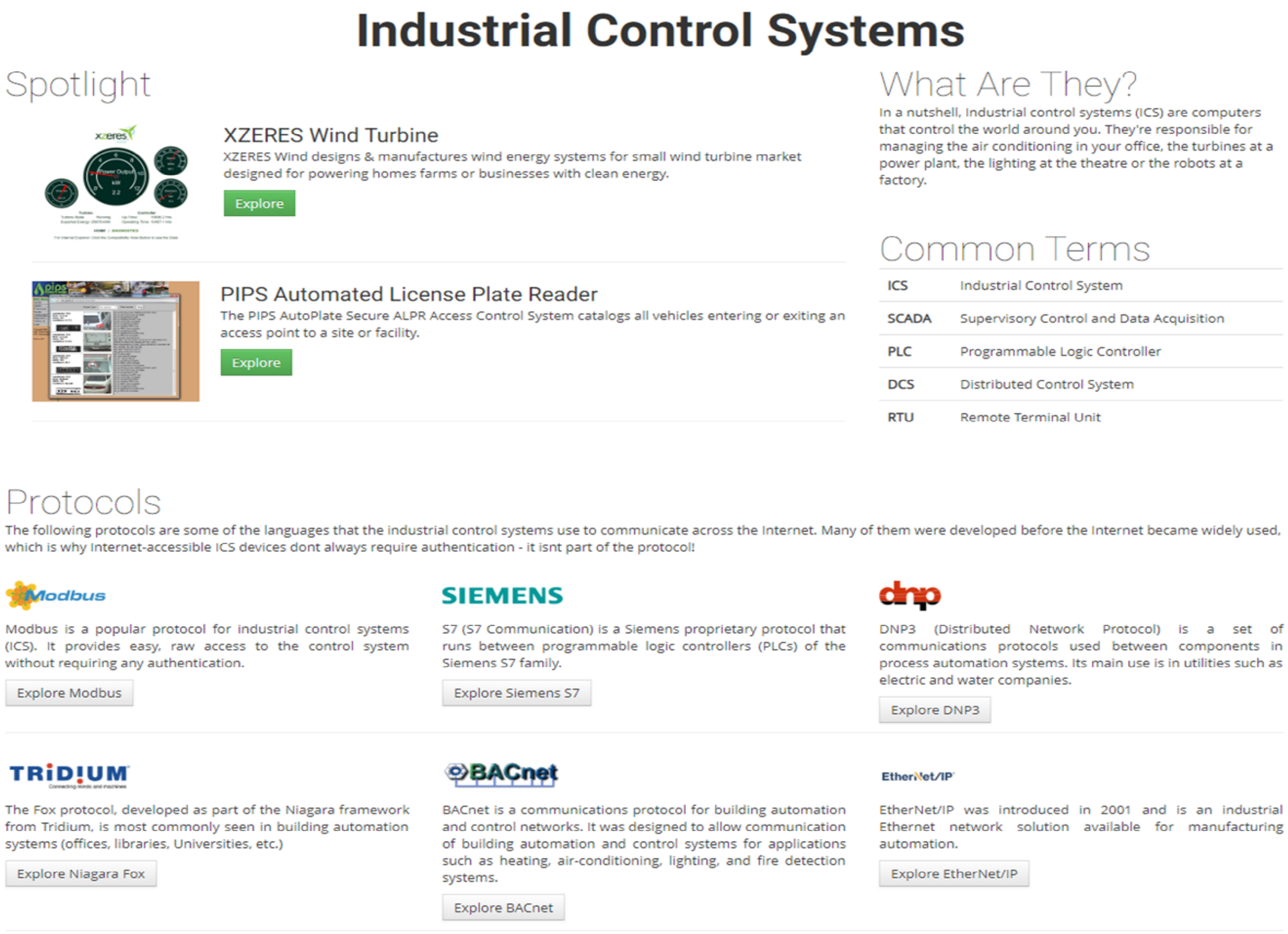
1
scada
157.119.190.182 iran scada equipment
scada meter 2019-06-22

3
RPI webcam interface
No user::pass - cams controlled by Raspberry - ...
2019-06-22

1
Waec
2019-06-21

1
safire
2019-06-19

More recent searches...



Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore

PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

Explore

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit

Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TRIDIUM

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet

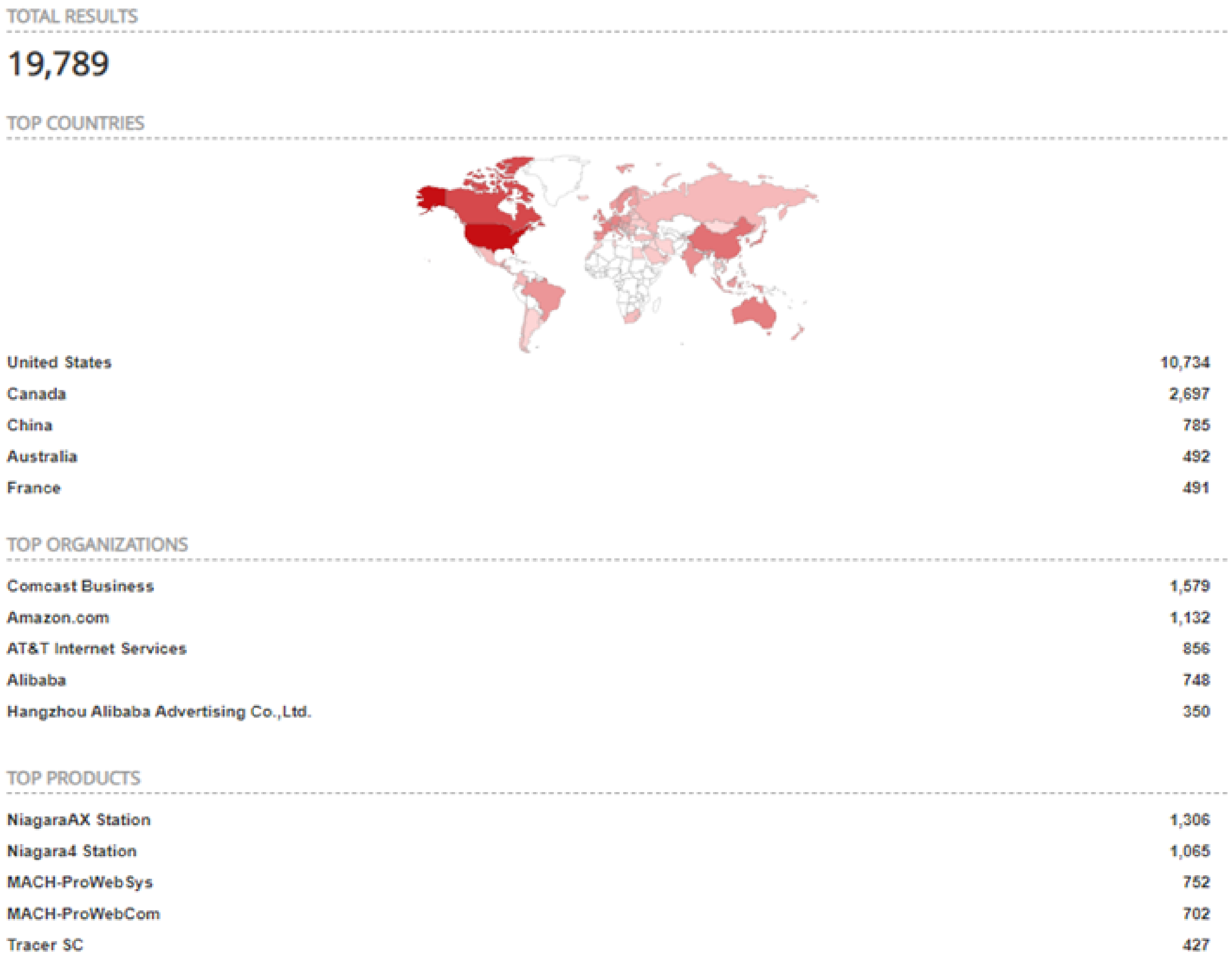
BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP



TOTAL RESULTS

19,789

TOP COUNTRIES

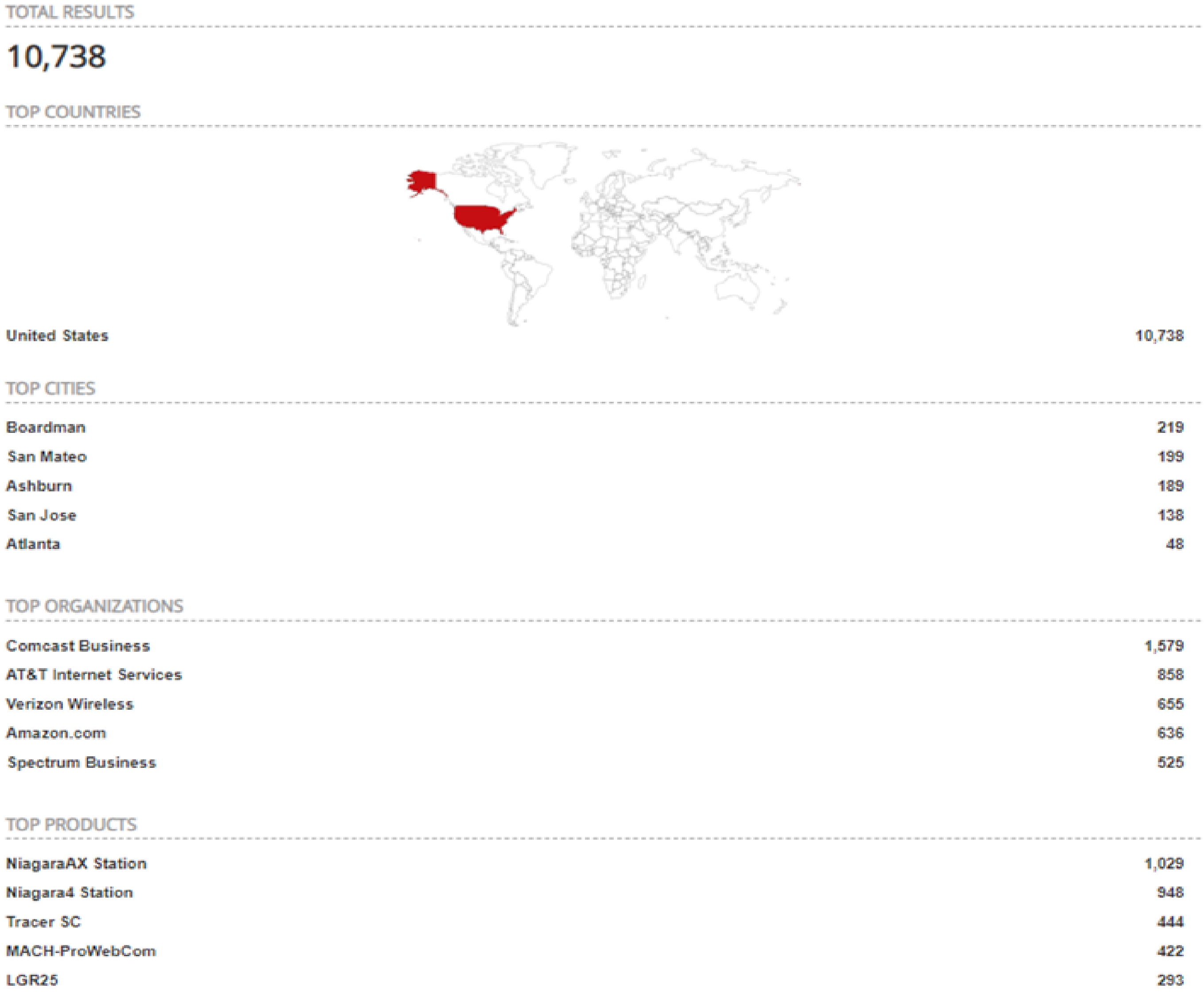
United States	10,734
Canada	2,697
China	785
Australia	492
France	491

TOP ORGANIZATIONS

Comcast Business	1,579
Amazon.com	1,132
AT&T Internet Services	856
Alibaba	748
Hangzhou Alibaba Advertising Co.,Ltd.	350

TOP PRODUCTS

NiagaraAX Station	1,306
Niagara4 Station	1,065
MACH-ProWebSys	752
MACH-ProWebCom	702
Tracer SC	427



TOTAL RESULTS

10,738

TOP COUNTRIES

United States	10,738

TOP CITIES

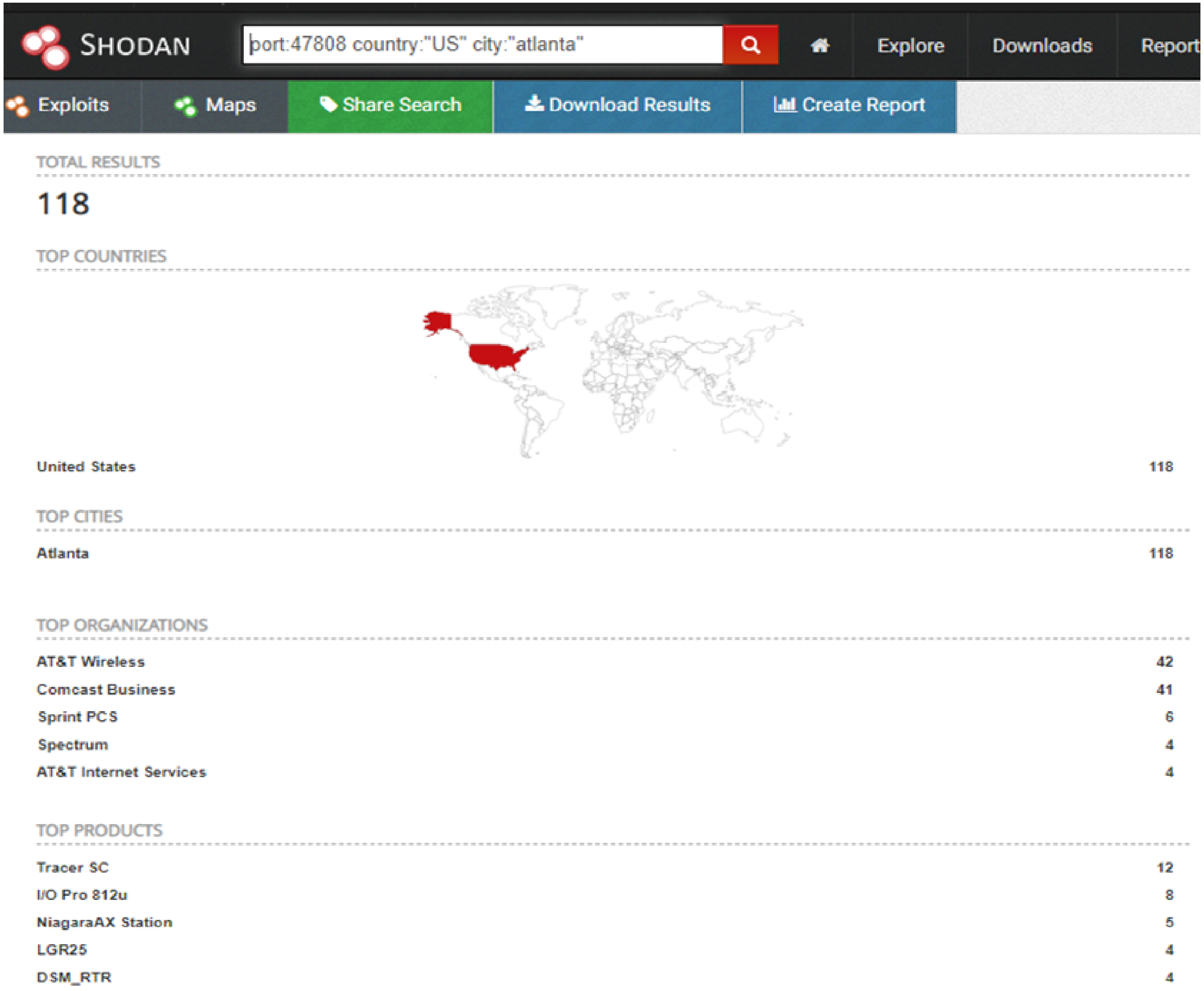
Boardman	219
San Mateo	199
Ashburn	189
San Jose	138
Atlanta	48

TOP ORGANIZATIONS

Comcast Business	1,579
AT&T Internet Services	858
Verizon Wireless	655
Amazon.com	636
Spectrum Business	525

TOP PRODUCTS

NiagaraAX Station	1,029
Niagara4 Station	948
Tracer SC	444
MACH-ProWebCom	422
LGR25	293



port:47808 country:"US" city:"atlanta"

TOTAL RESULTS

118

TOP COUNTRIES

United States	118

TOP CITIES

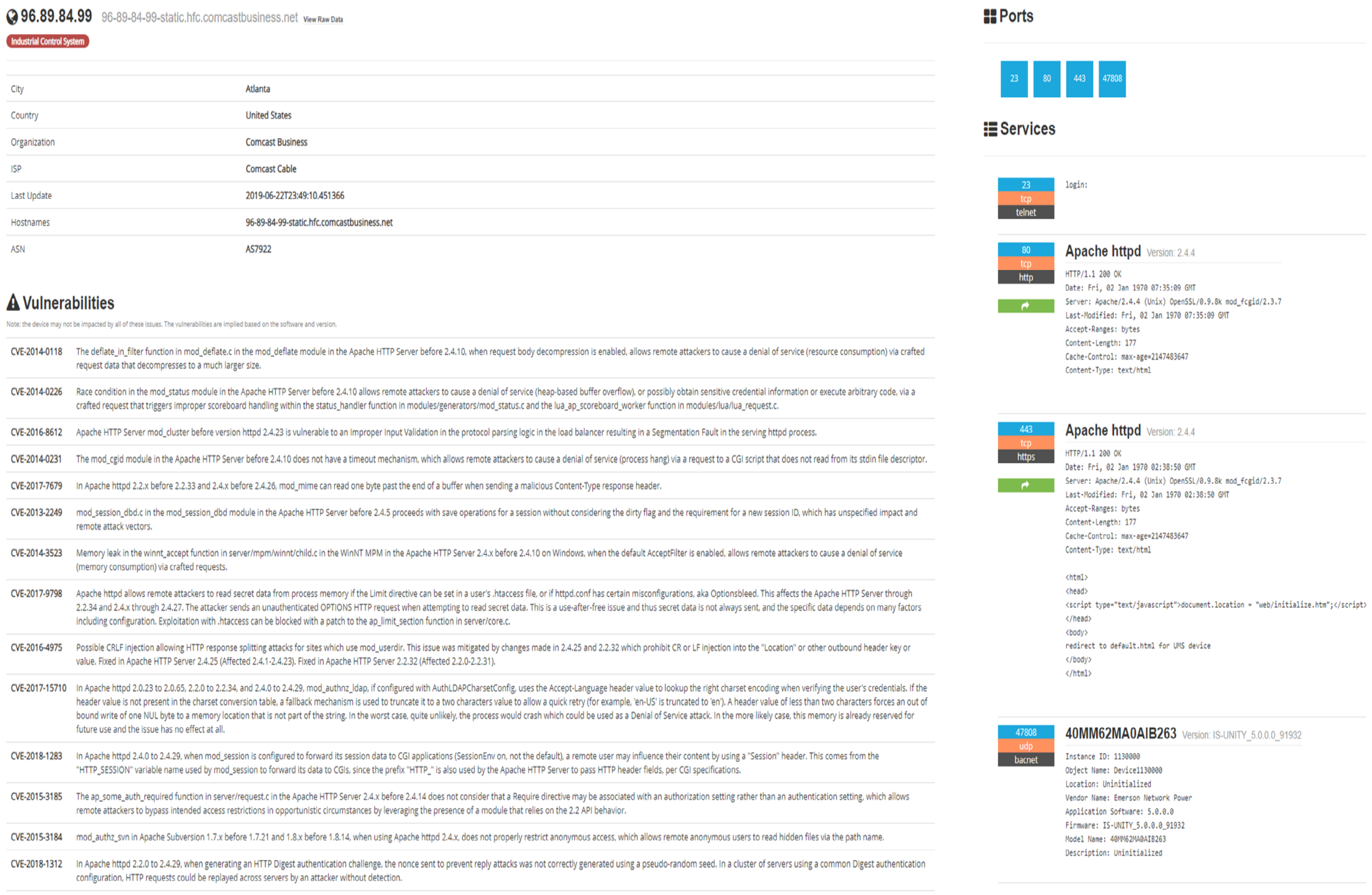
Atlanta	118

TOP ORGANIZATIONS

AT&T Wireless	42
Comcast Business	41
Sprint PCS	6
Spectrum	4
AT&T Internet Services	4

TOP PRODUCTS

Tracer SC	12
I/O Pro 812u	8
NiagaraAX Station	5
LGR25	4
DSM_RTR	4



96.89.84.99 96-89-84-99-static.hfc.comcastbusiness.net View Raw Data

Industrial Control System

City	Atlanta
Country	United States
Organization	Comcast Business
ISP	Comcast Cable
Last Update	2019-06-22T23:49:10.451366
Hostnames	96-89-84-99-static.hfc.comcastbusiness.net
ASN	AS7922

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-0118	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.
CVE-2016-8612	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
CVE-2014-0231	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2013-2249	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.
CVE-2014-3523	Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2016-4975	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2018-1283	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2015-3185	The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.
CVE-2015-3184	mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Ports

23 80 443 47808

Services

23
tcp
telnet

```
login:
```

80
tcp
http

Apache httpd Version: 2.4.4

```
HTTP/1.1 200 OK
Date: Fri, 02 Jan 1970 07:35:09 GMT
Server: Apache/2.4.4 (Unix) OpenSSL/0.9.8k mod_fcgid/2.3.7
Last-Modified: Fri, 02 Jan 1970 07:35:09 GMT
Accept-Ranges: bytes
Content-Length: 177
Cache-Control: max-age=2147483647
Content-Type: text/html
```

443
tcp
https

Apache httpd Version: 2.4.4

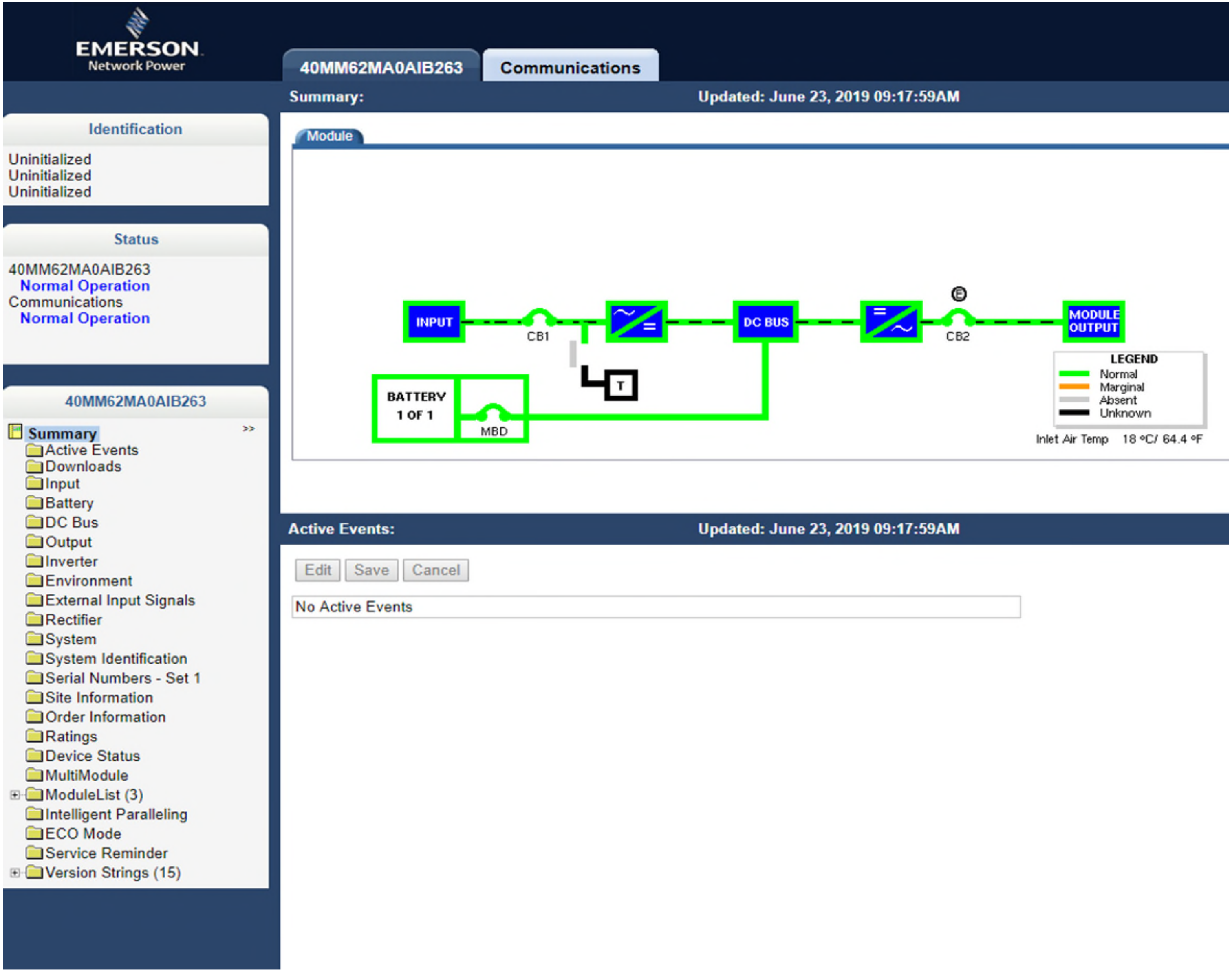
```
HTTP/1.1 200 OK
Date: Fri, 02 Jan 1970 02:38:50 GMT
Server: Apache/2.4.4 (Unix) OpenSSL/0.9.8k mod_fcgid/2.3.7
Last-Modified: Fri, 02 Jan 1970 02:38:50 GMT
Accept-Ranges: bytes
Content-Length: 177
Cache-Control: max-age=2147483647
Content-Type: text/html

<html>
<head>
<script type="text/javascript">document.location = "web/initialize.htm";</script>
</head>
<body>
redirect to default.html for UMS device
</body>
</html>
```

47808
udp
bacnet

40MM62MA0AIB263 Version: IS-UNITY_5.0.0.0_91932

```
Instance ID: 1130000
Object Name: Device1130000
Location: Uninitialized
Vendor Name: Emerson Network Power
Application Software: 5.0.0.0
Firmware: IS-UNITY_5.0.0.0_91932
Model Name: 40MM62MA0AIB263
Description: Uninitialized
```



Summary:

Updated: June 23, 2019 09:17:59AM

Identification

Uninitialized
Uninitialized
Uninitialized

Status

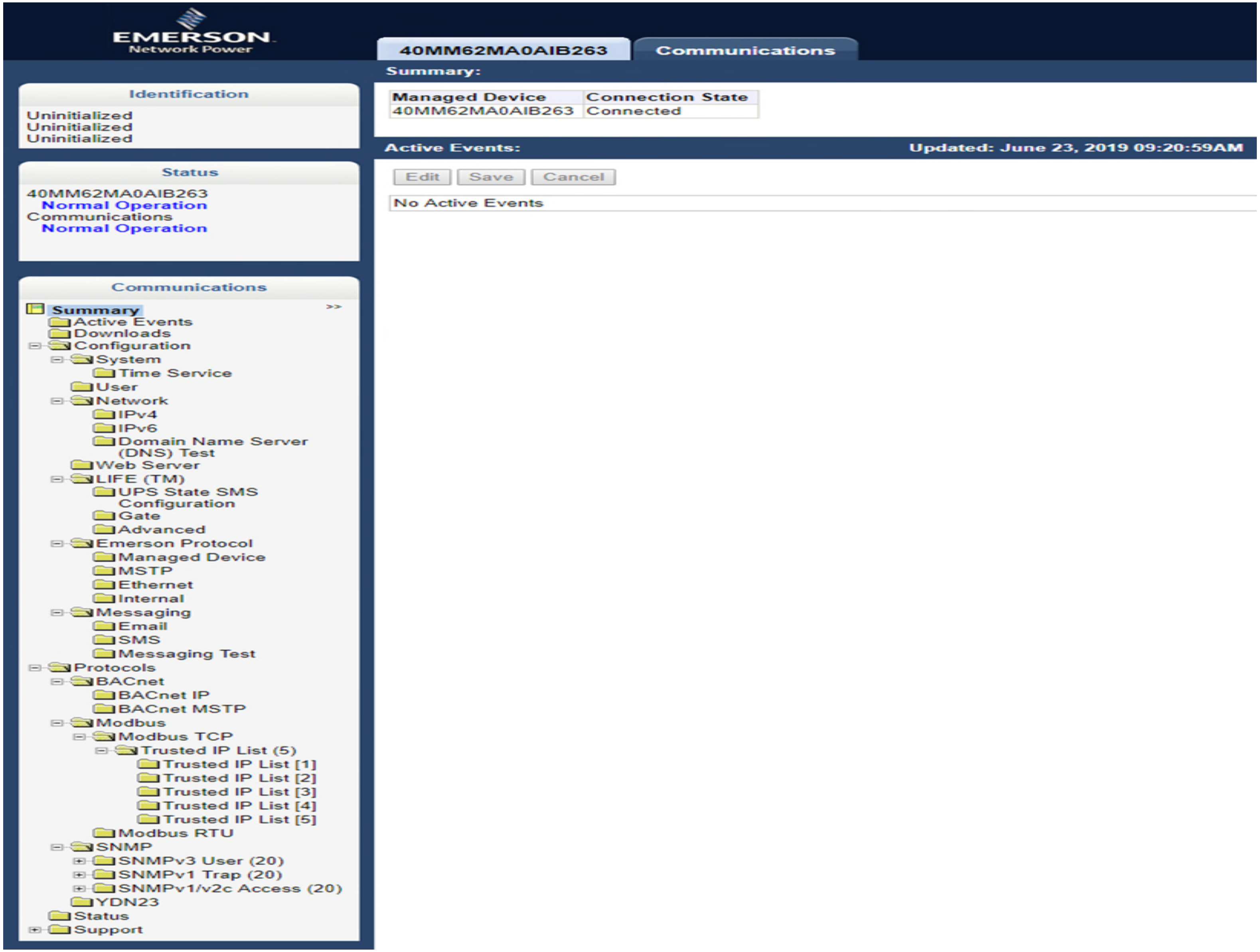
40MM62MA0AIB263
Normal Operation
Communications
Normal Operation

Inlet Air Temp 18 °C/ 64.4 °F

Active Events:

Updated: June 23, 2019 09:17:59AM

No Active Events



Uninitialized
Uninitialized
Uninitialized

40MM62MA0AIB263
Normal Operation
Communications
Normal Operation

Summary:

Managed Device	Connection State
40MM62MA0AIB263	Connected

Active Events:

Updated: June 23, 2019 09:20:59AM

No Active Events

Pretty Easy Right?

- This is the very first tool I use for Assessments
- People make mistakes
- People switch jobs – USAF example
- New systems get added
- Billing, maintenance, testing etc
- Acquisitions
- How many devices do I have…How many networks do I have?

I had no idea

- All of that was 100% in the clear and very easy to do
- BAS technician doesn’t have an IT background
- Every BAS out there has had security vulnerabilities and they will continue to in the future
- The reality is that people writing software are…. People
- BAS device shouldn’t be exposed to the Internet but they are

How Do We Protect

- IP-enabled industrial control systems should be isolated within a dedicated network segment and accessed over an encrypted, authenticated channel such as a VPN.
  - These systems typically have limited built-in security controls and need all the help they can get to operate in a secure manner.
- Strong passwords, detailed logging, and frequent security updates can help protect these systems from unauthorized tempering.
- The bad guys know and are trained on current defensive tools and strategies
- Must be better than they are
  - Faster, Outside the Box thinking and solutions
- **Understand your “Digital Footprint” and do things to minimize it**

Plug & Play Defensible Backbone Concept

- Approach proposed for Defense Critical Infrastructure Program assets at Cheyenne Mountain Air Force Station
- PWS called for:
  - Resilient, survivable, reliable, high-availability, defensible, recoverable, redundant, and secure
  - Where feasible, make it autonomous (to reduce man-hours for monitoring/defense)
  - End-to-end physical and cyber security with layered-defense/defense-in-depth methodologies
  - Strong segmentation between networks, enclaves, zones

Plug & Play Defensible Backbone Concept

- Key concepts in design:
  - Upgraded common network backbone for all ICS/FRCS/OT systems
    - Industrial area using NEMA-type enclosures and ruggedized switches
    - Normal comm closet/mechanical room using half-racks
    - Integrated through a pair of core switches with a firewall setup to manage traffic in/out of the system
  - Separate security overwatch system using ML type devices
    - Identify problems based upon behavior
    - Monitors to the true Level 0

Plug & Play Defensible Backbone Concept

- Benefits
  - Can integrate all subordinate systems onto the backbone through VLAN using VRF
  - Can be integrated using existing fiber pathways into highly resilient, redundant, reliable, highly-available network topologies based upon DCIP asset need
  - Real time threat monitoring (behavior changes, configuration changes, access attempts) and ability to isolate until threat eliminated
  - Gives Cyber Squadron MDT(s) the tools to remotely execute a tasked mission (e.g. analytics, forensics, find, characterize, track, target, engage, etc.) across the ICS/OT terrain using a specialized interface—interoperable with current MDT toolkit!

Contact Information

Erik Sell, P.E.

eriksell@tribal.one
(850) 625-0449
Construction Executive
Tribal 1 Construction

Jeramie Crabtree

jcrabtree@goliathsg.com
(303) 868-1954
Business Development
Goliath Solutions Group

Jason Cook, P.E., ATD

jason.cook2@tetratech.com
(719) 313-3114
Senior Project Manager
Tetra Tech