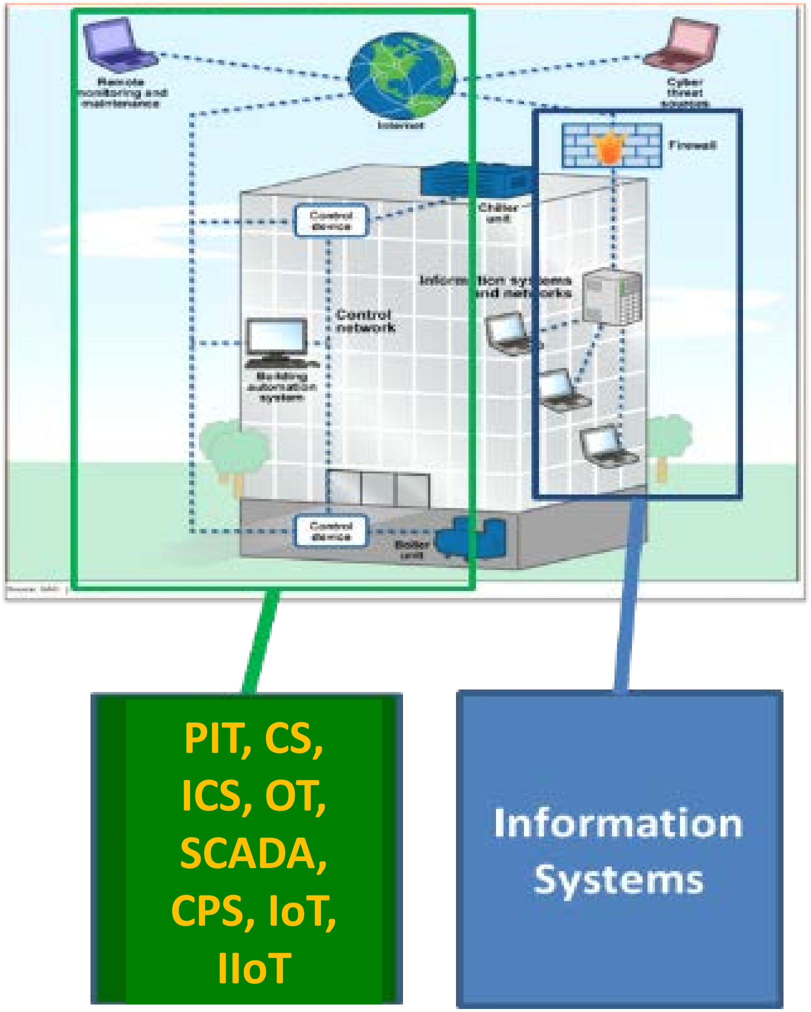
DoD Terminology Decision In Progress:

PIT, CS, PIT-CS, ICS,OT, SCADA, CPS, IoT, IIoT

- **PIT = Platform Information Technology**
- **CS = Control Systems**
- **PIT-CS = PIT Control Systems**
- **ICS = Industrial Control Systems**
- **OT = Operational Technology**
- **SCADA = Supervisory Control And Data Acquisition**
- **CPS = Cyber Physical Systems**
- **IoT = Internet of Things**
- **IIoT = Industrial IoT**



PIT, CS, ICS, OT, SCADA, CPS, IoT, IIoT

Information Systems

Typically Lack Any Cyber Defenses; ~75% Use WIN XP

UNCLASSIFIED

>500 Installations
>250K Buildings
>200K Structures

Buildings

Weapon Platforms

Operational Energy

Electrical and HVAC

Pumps and Motors

Nuclear

Typical Controller

Vehicles/Charging

Medical

Manufacturing

Same Commercial Devices Installed Across DoD Enterprise

Top 20 Attacks from Least to Most Sophisticated

Sophistication Level

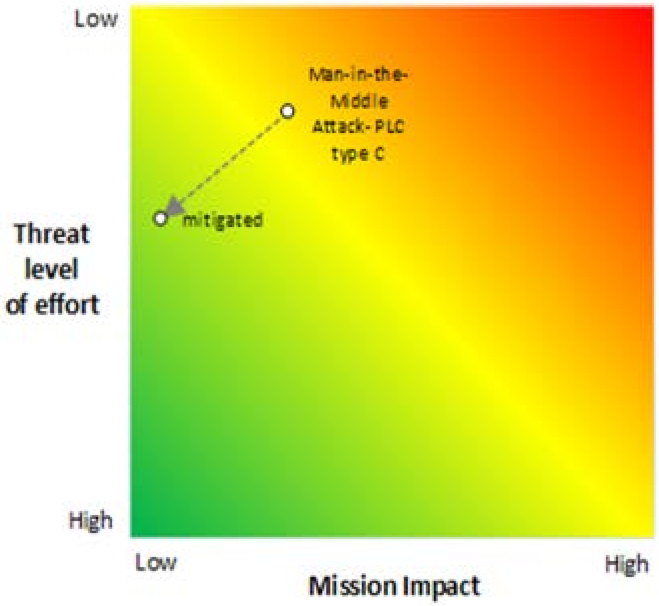
1. ICS Insider
2. IT Insider
3. Common Ransomware
4. Target Ransomware
5. Zero-Day Ransomware

6. Ukrainian Attack
7. Sophisticated Ukrainian Attack
8. Market Manipulation
9. Sophisticated Market Manipulation

10. Cell-phone WIFI
11. Hijacked Two-Factor
12. IIoT Pivot
13. Malicious Outsourcing

14.Compromised Vendor Website
15.Compromised Remote Site
16. Vendor Back Door
17. Stuxnet
18. Hardware Supply Chain

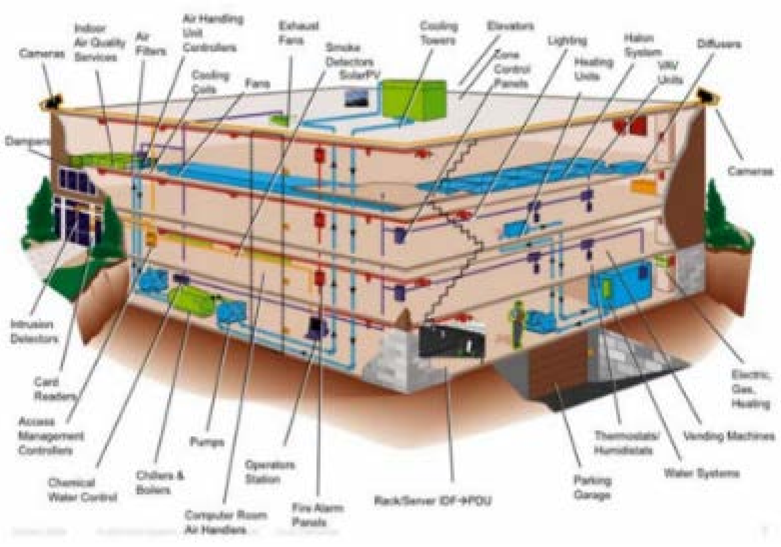
19. Nation-State Crypto Compromise
20.Sophisticated Credentialed ICS Insider



https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf

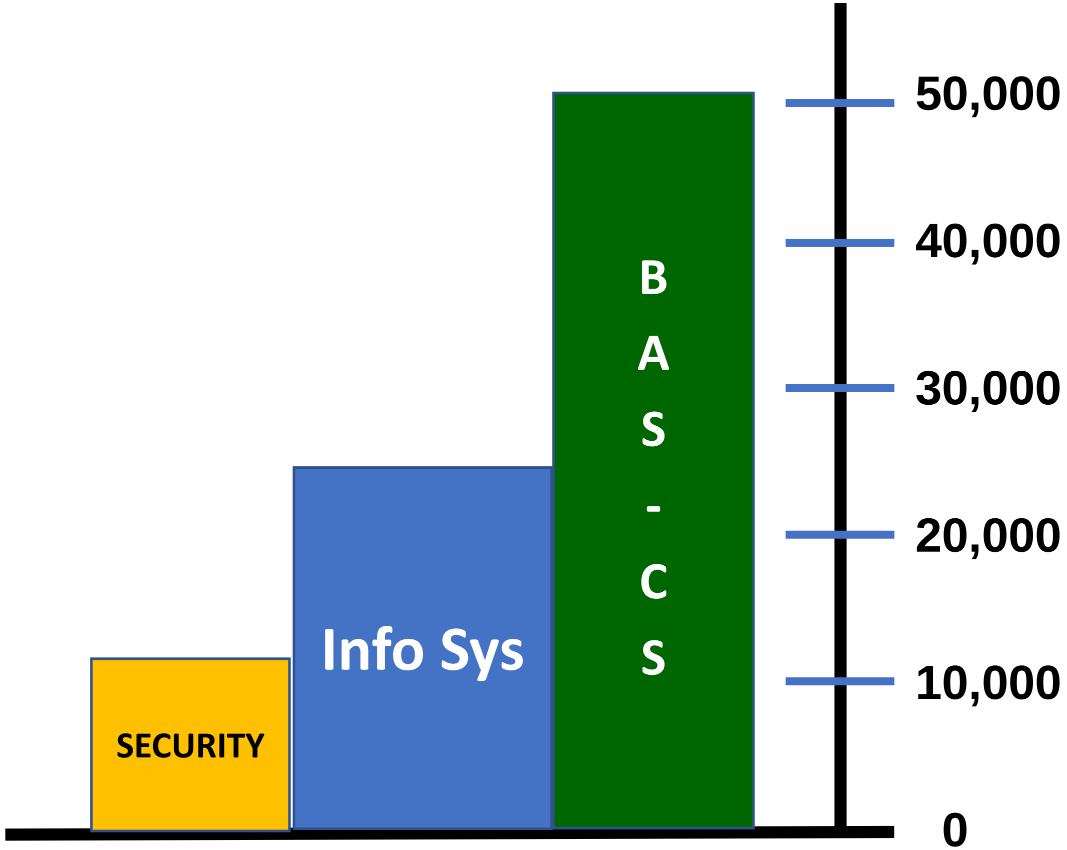
What's in Your 'Smart Building?'

- "Smart" / High Performance Green Buildings
  - Since 2005 ~7,000+
  - Example: 5,000 desks, 20 floors, ~2M sqft



- *Fire Sprinkler System*
- *Interior Lighting Control*
- *Intrusion Detection*
- *Land Mobile Radios*
- *Renewable Energy Photo Voltaic Systems*
- *Shade Control System*
- *Smoke and Purge*
- *Physical Access Control*
- *Vertical Transport System (Elevators and Escalators)*

- *Advanced Metering Infrastructure*
- *Building Automation System*
- *Building Management Control*
- *CCTV Surveillance System*
- *CO2 Monitoring*
- *Digital Signage Systems*
- *Electronic Security System*
- *Emergency Management System*
- *Energy Management System*
- *Exterior Lighting Control Systems*
- *Fire Alarm System*



3 Networks Independently Managed

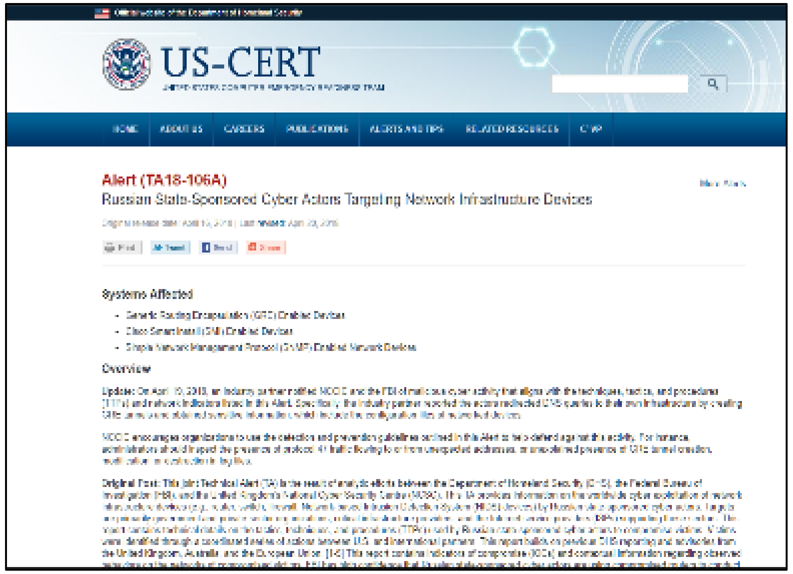
Significant Impacts; Tools Easily Accessible and Unsophisticated

- **WannaCry** *(May'17)* – ransomware affecting Microsoft Windows millions of computers across 150 countries, halting manufacturing, transportation and telecommunications systems; many medical systems inoperable affecting health & safety
- **NotPetya** *(Jun'17)* – malware infected 10,000's of internet connected systems across 65 countries [Maersk shipping company halted operations in most of its 76 port terminals; loses exceeded $300M, 4,000 new servers, 45,000 new PCs, 2,500 new apps]
- **Trisis** *(Aug'17)* – virus sabotaging physical safety mechanisms of Saudi Arabian oil, gas facility control systems [coding error prevented potential catastrophe]

Number Targeted Attacks Almost Doubled Since 2013;
Urgent Need to Understand Your "Connectedness"

Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

- 16 April 2018 – DHS US CERT, FBI & UK's National Cyber Security Centre – Alert – **Russian State-sponsored actors establishing worldwide cyber exploitation of network devices**
- Targets primarily **government and private-sector orgs, critical infrastructure providers & internet service providers**.



Alert (TA18-106A)

Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

Original release date: April 16, 2018 | Last revised: April 20, 2018

Systems Affected

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

Overview

Update: On April 19, 2018, an industry partner notified NCCIC and the FBI of malicious cyber activity that aligns with the techniques, tactics, and procedures (TTPs) and network indicators listed in this Alert. Specifically, the industry partner reported the actors redirected DNS queries to their own infrastructure by creating GRE tunnels and obtained sensitive information, which include the configuration files of networked devices.

NCCIC encourages organizations to use the detection and prevention guidelines outlined in this Alert to help defend against this activity. For instance, administrators should inspect the presence of protocol 47 traffic flowing to or from unexpected addresses, or unexplained presence of GRE tunnel creation, modification, or destruction in log files.

Original Post: This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC). This TA provides information on the worldwide cyber exploitation of network infrastructure devices (e.g., router, switch, firewall, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and the Internet service providers (ISPs) supporting these sectors. This report contains technical details on the tactics, techniques, and procedures (TTPs) used by Russian state-sponsored cyber actors to compromise victims. Victims were identified through a coordinated series of actions between U.S. and international partners. This report builds on previous DHS reporting and advisories from the United Kingdom, Australia, and the European Union. [1-5] This report contains indicators of compromise (IOCs) and contextual information regarding observed behaviors on the networks of compromised victims. FBI has high confidence that Russian state-sponsored cyber actors are using compromised routers to conduct

FBI - actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

Exploiting:

Routers

Switches

Firewalls

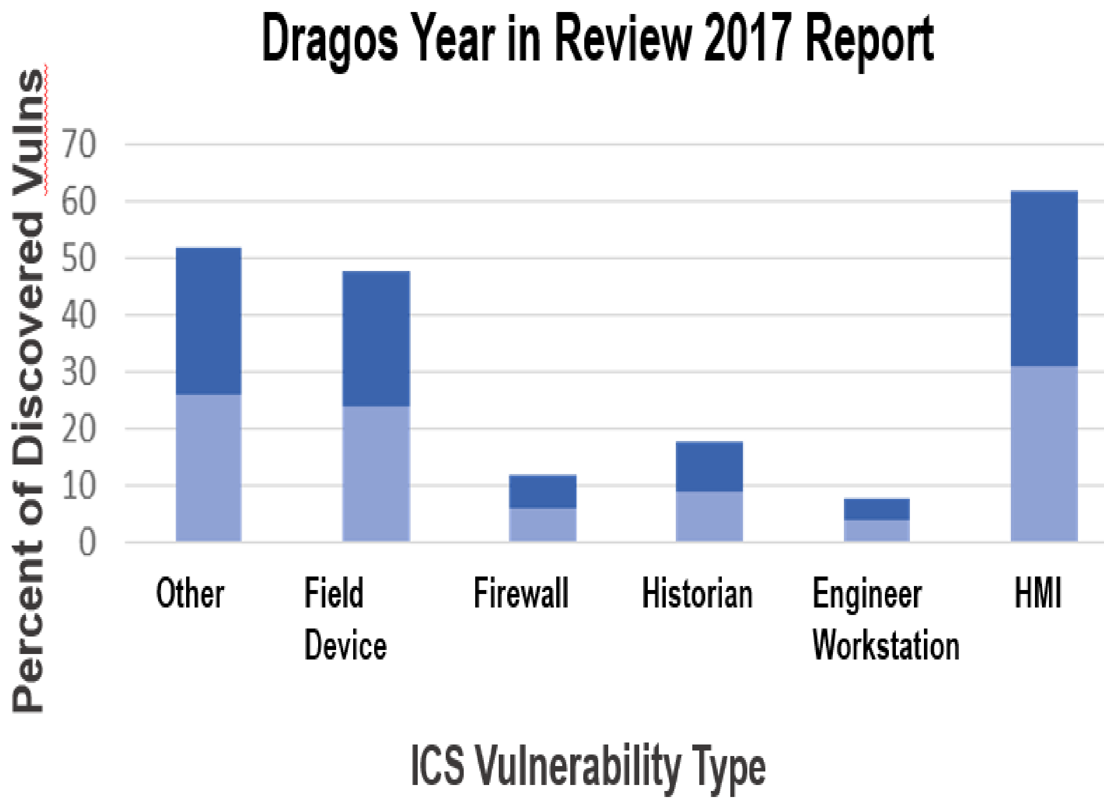
Network-based Intrusion Detection Systems

Russian "Trolling" Activity

Up 2,000% After Syrian Strike

Make sure that your router software is up-to-date and its password is secure

Cyber Threat to ICS Highest Yet – CS Threats



72%	Of Vulnerabilities Could Cause a Loss of View/Control
63%	Of Vulnerabilities from Late in Kill Chain Indicating Prolonged Presence, Pivot from Other Systems
63%	Of Vulnerabilities Could Be Leveraged to Gain Initial Access Into Control Network

"We regrettably expect ICS operational losses and likely safety events to continue into 2018 and the foreseeable future"

UNCLASSIFIED

April 2018 Report

Key findings over past 3 yrs:

- 90% of targeted attack groups are motivated by intelligence gathering
- Most active groups compromised an average of 42 organizations
- 71% of groups use spear-phishing emails as primary infection vector
- 29 % increase of recorded ICS vulnerabilities
- U.S. accounts for 27% of all targeted attack activity (most)

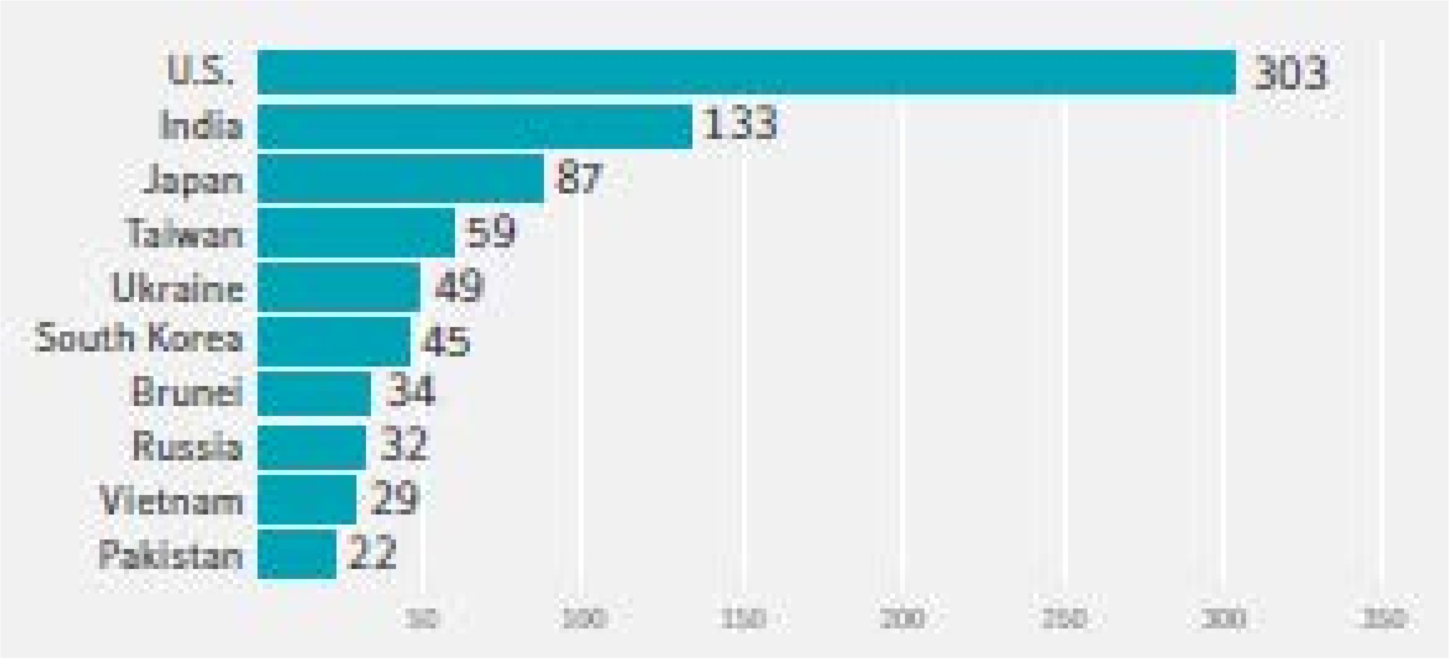
ISTR

Internet Security Threat Report

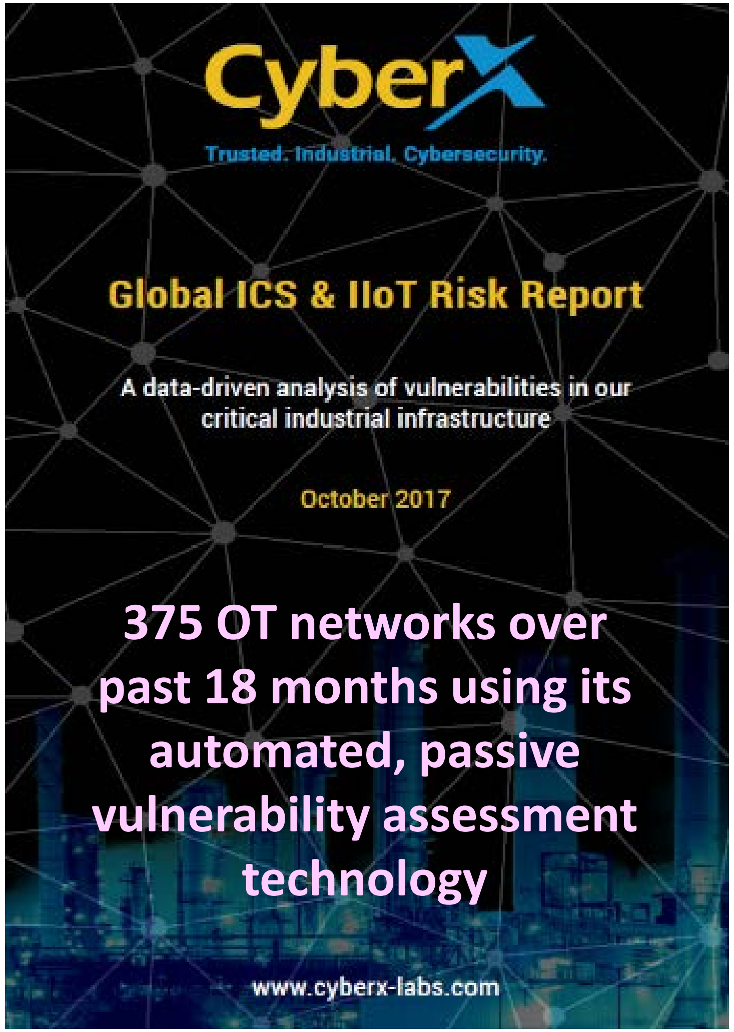
Volume

23

Symantec.



- 60% have plain-text passwords traversing their control networks
- 50% aren’t running any AV protection
- Nearly 50% have at least one unknown or rogue device
- 20% have wireless access points
- 28% of all devices in each site are vulnerable
- 82% of industrial sites are running remote management protocols



CyberX

Trusted. Industrial. Cybersecurity.

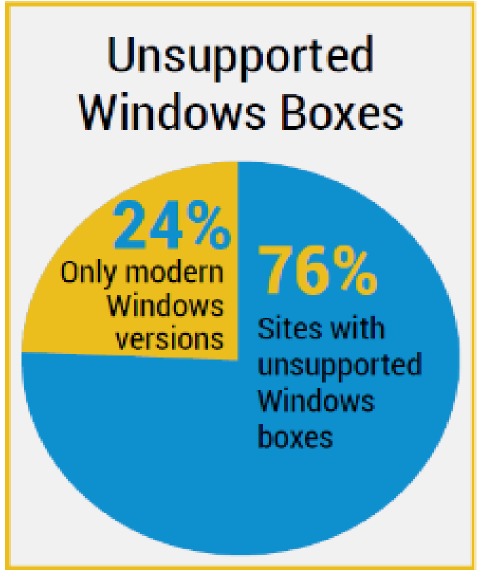
Global ICS & IIoT Risk Report

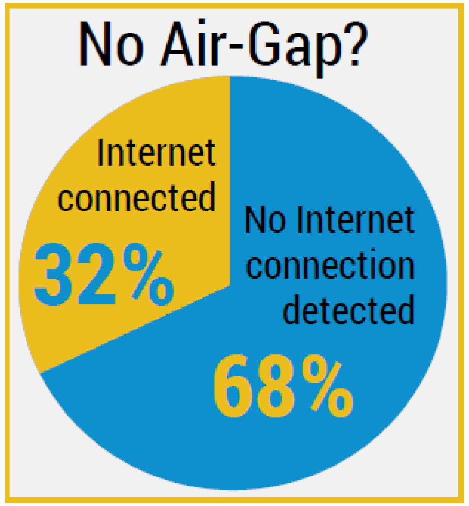
A data-driven analysis of vulnerabilities in our critical industrial infrastructure

October 2017

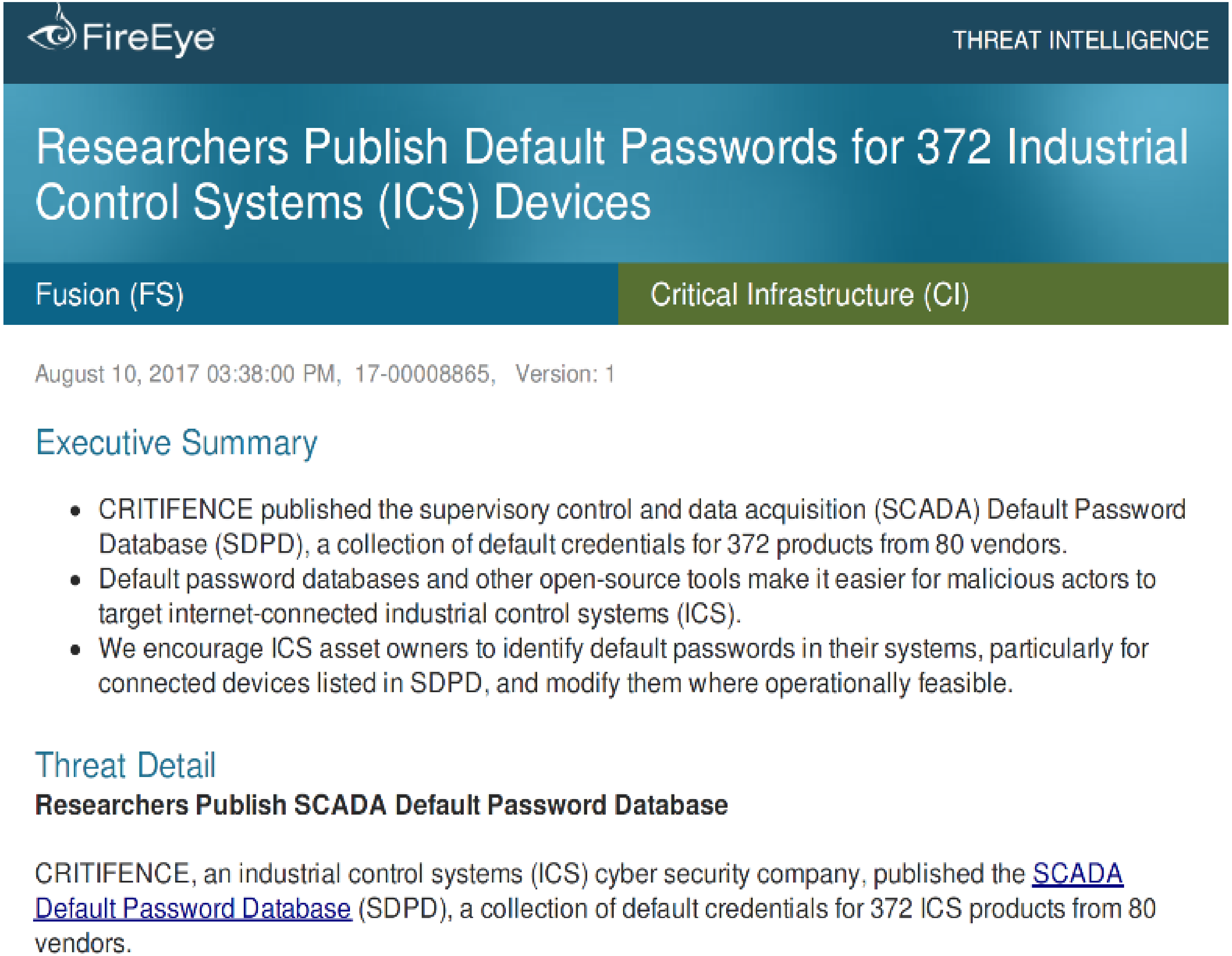
375 OT networks over past 18 months using its automated, passive vulnerability assessment technology

www.cyberx-labs.com





“They’re testing out red lines, what they can get away with. You push and see if you’re pushed back. If not, you try the next step.” *Thomas Rid, Professor of War Studies at King’s College London*



FireEye THREAT INTELLIGENCE

Researchers Publish Default Passwords for 372 Industrial Control Systems (ICS) Devices

Fusion (FS) | Critical Infrastructure (CI)

August 10, 2017 03:38:00 PM, 17-00008865, Version: 1

Executive Summary

- CRITIFENCE published the supervisory control and data acquisition (SCADA) Default Password Database (SDPD), a collection of default credentials for 372 products from 80 vendors.
- Default password databases and other open-source tools make it easier for malicious actors to target internet-connected industrial control systems (ICS).
- We encourage ICS asset owners to identify default passwords in their systems, particularly for connected devices listed in SDPD, and modify them where operationally feasible.

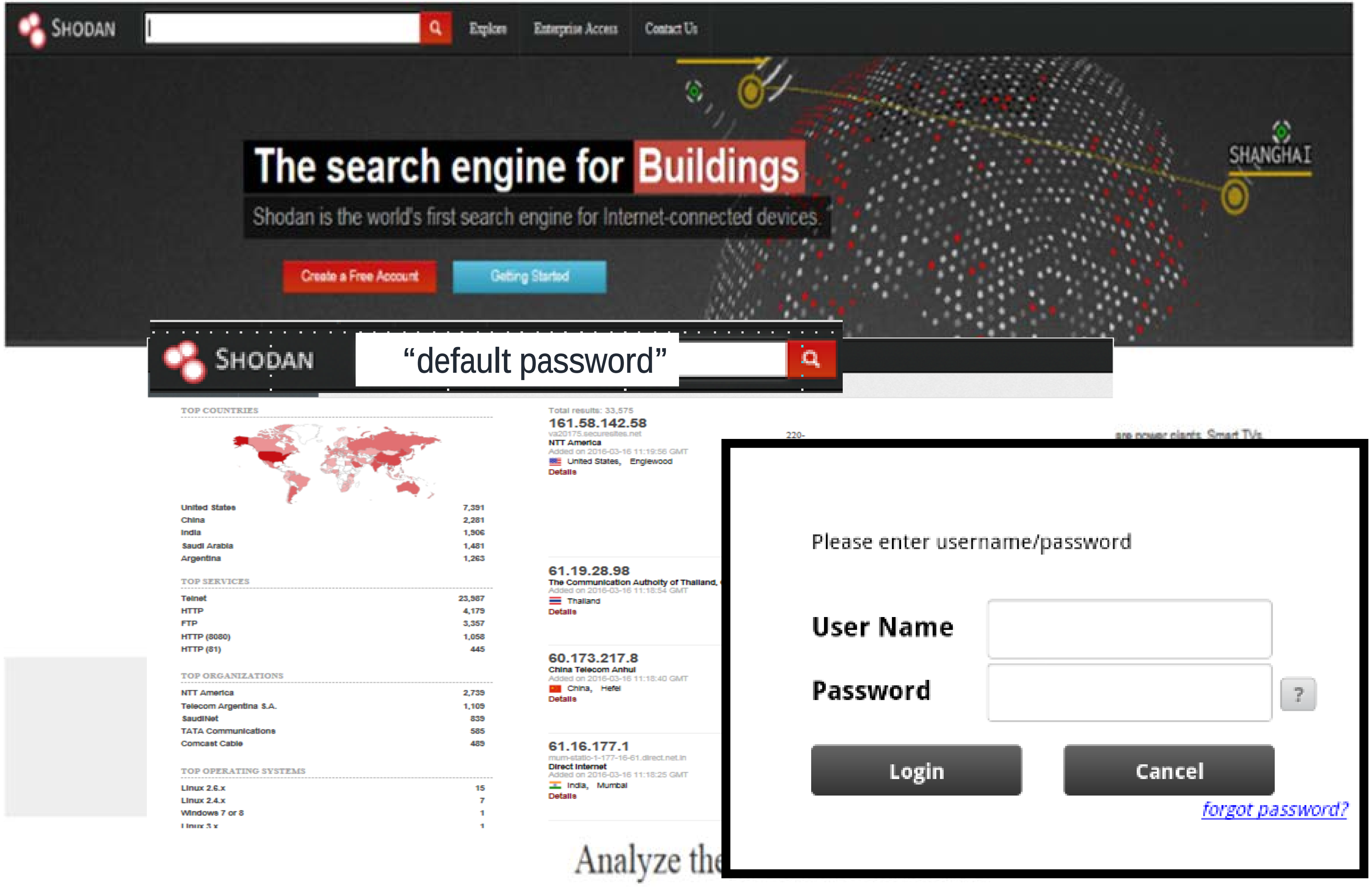
Threat Detail

Researchers Publish SCADA Default Password Database

CRITIFENCE, an industrial control systems (ICS) cyber security company, published the SCADA Default Password Database (SDPD), a collection of default credentials for 372 ICS products from 80 vendors.

Default Passwords Found … Again: 370 Products / 80 Vendors

Shodan



The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

"default password"

TOP COUNTRIES

United States	7,391
China	2,281
India	1,906
Saudi Arabia	1,481
Argentina	1,263

TOP SERVICES

Telnet	23,987
HTTP	4,179
FTP	3,357
HTTP (8080)	1,058
HTTP (81)	445

TOP ORGANIZATIONS

NTT America	2,739
Telecom Argentina S.A.	1,109
SaudiNet	839
TATA Communications	585
Comcast Cable	489

TOP OPERATING SYSTEMS

Linux 2.6.x	15
Linux 2.4.x	7
Windows 7 or 8	1
Linux 3.x	1

Total results: 33,575

161.58.142.58
va20175.securesites.net
NTT America
Added on 2016-03-16 11:19:56 GMT
United States, Englewood

220-

61.19.28.98
The Communication Authoity of Thailand,
Added on 2016-03-16 11:18:54 GMT
Thailand

60.173.217.8
China Telecom Anhui
Added on 2016-03-16 11:18:40 GMT
China, Hefei

61.16.177.1
mum-static-1-177-16-61.direct.net.in
Direct Internet
Added on 2016-03-16 11:18:25 GMT
India, Mumbai

Analyze the

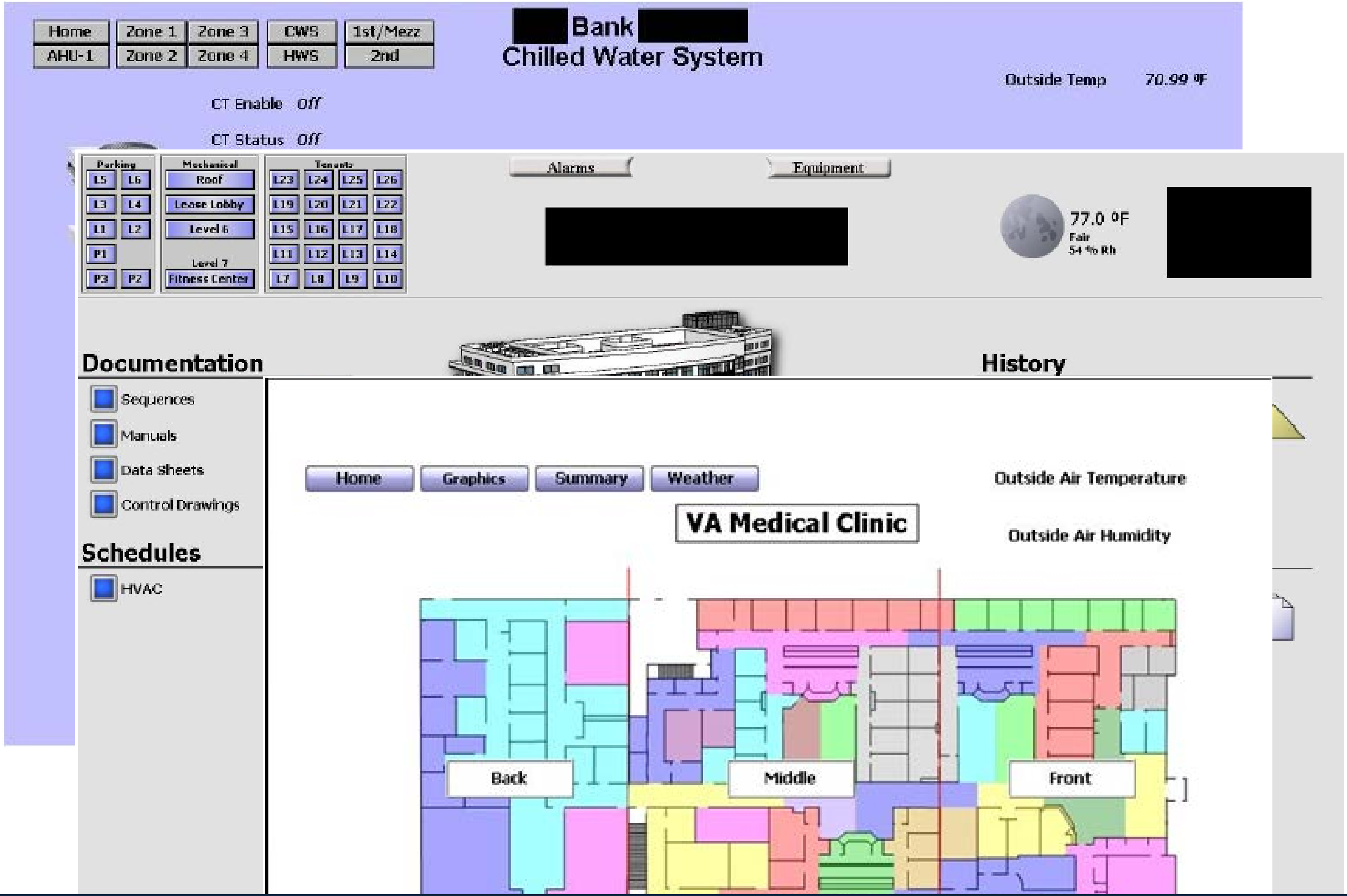
are power plants, Smart TVs

Please enter username/password

User Name

Password

UNCLASSIFIED



[redacted] Bank [redacted]
Chilled Water System

CT Enable Off

CT Status Off

Outside Temp 70.99 °F

[redacted]

77.0 °F
Fair
54 % Rh

[redacted]

Documentation

History

Schedules

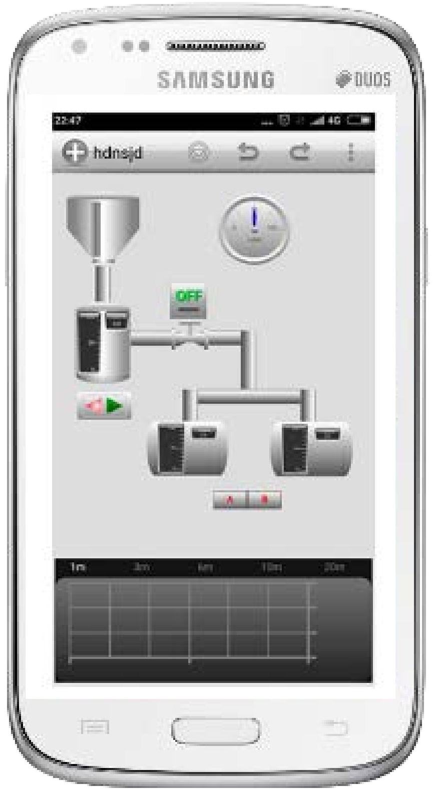
VA Medical Clinic

Outside Air Temperature

Outside Air Humidity

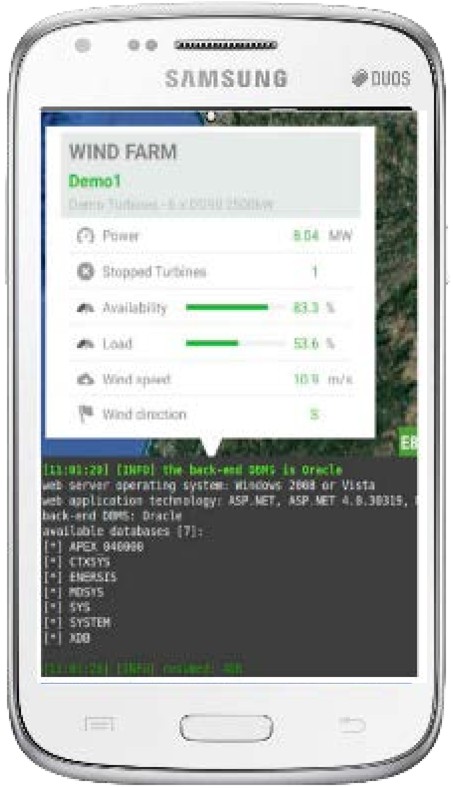
Never Attribute Evil When Stupid is Still Available

Just Because You Can Control via Mobile Devices…..



Top 5 security weaknesses:

- 94% code tampering
- 59% insecure authorization
- 53% reverse engineering
- 47% insecure data storage
- 38% insecure communication



WIND FARM

Demo1

[illegible]

Power 8.04 MW

Stopped Turbines 1

Availability 83.3 %

Load 53.6 %

Wind speed 10.9 m/s

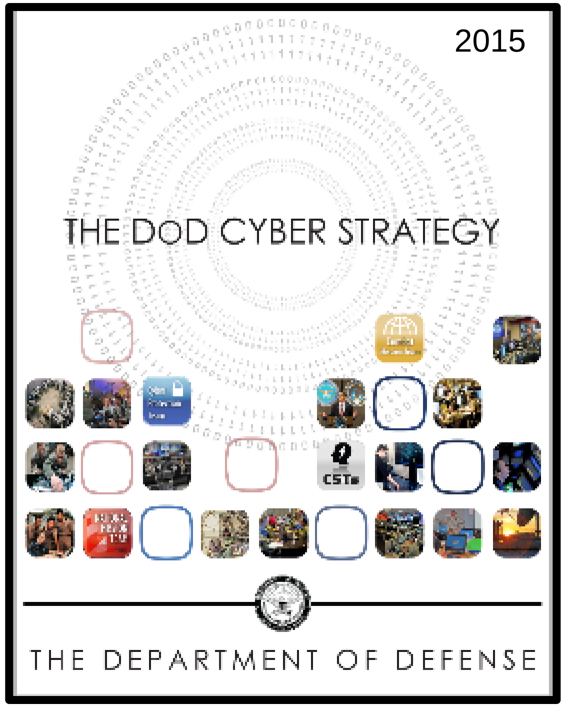
Wind direction S

```
[11:01:29] [INFO] the back-end DBMS is Oracle
web server operating system: Windows 2008 or Vista
web application technology: ASP.NET, ASP.NET 4.0.30319,
back-end DBMS: Oracle
available databases [7]:
[*] APEX_040000
[*] CTXSYS
[*] ENERSIS
[*] MDSYS
[*] SYS
[*] SYSTEM
[*] XDB

[11:01:29] [INFO] [illegible]
```

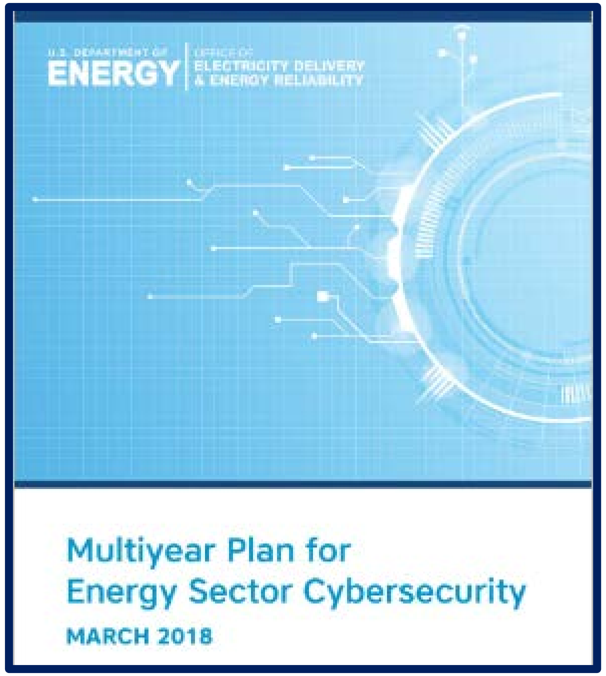
> *"Why should anyone have the power to control a 2 GW power plant, or the entire production line of an automobile factory, from a cell phone, while stopped at a traffic light?"*
>
> *– Andrew Ginter, VP Industrial Security Waterfall Security Solutions*

Strategies… Good for the Long Term


2015

THE DOD CYBER STRATEGY

THE DEPARTMENT OF DEFENSE


U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for Energy Sector Cybersecurity

MARCH 2018

U.S. DEPARTMENT OF HOMELAND SECURITY

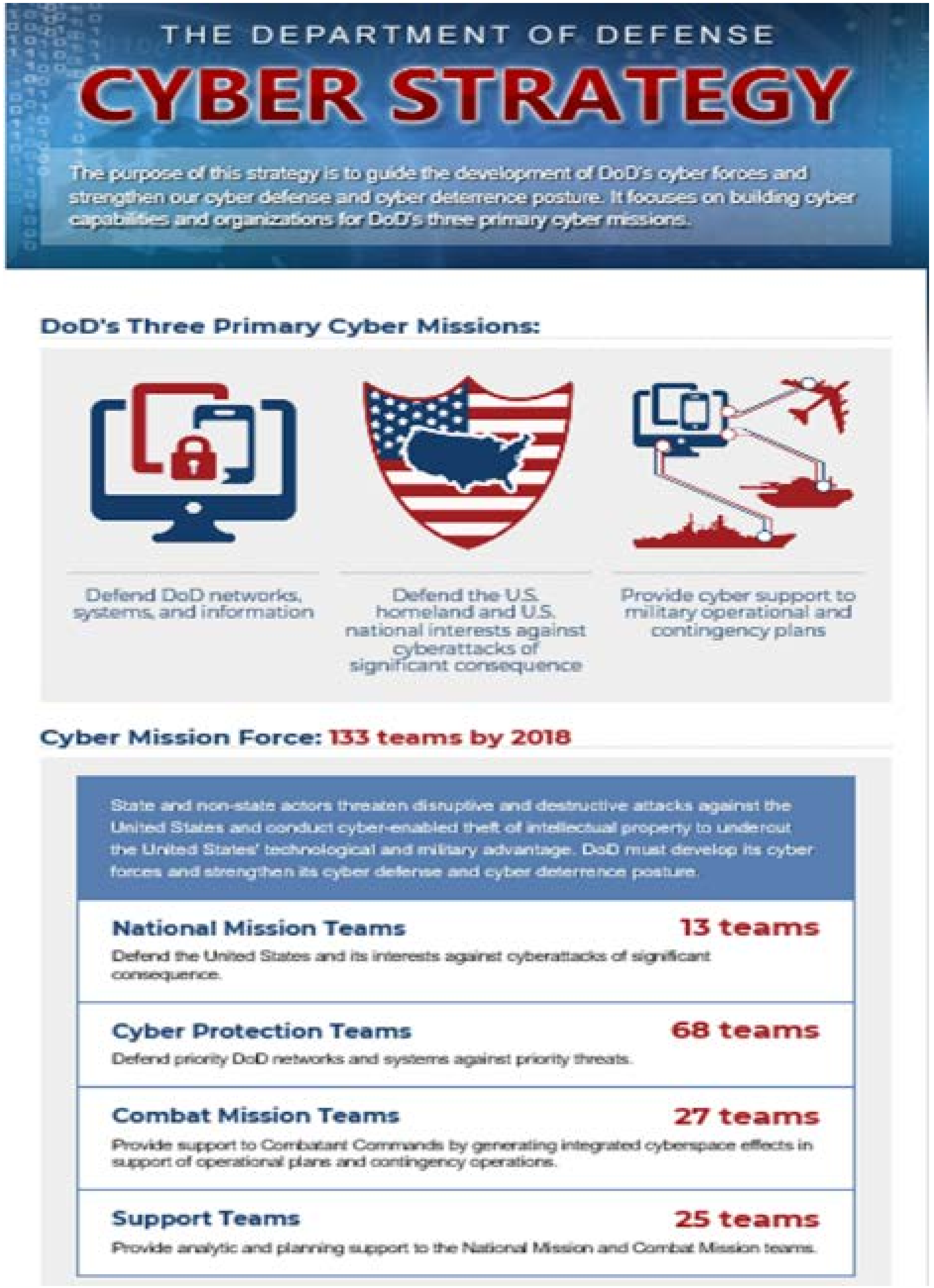
CYBERSECURITY STRATEGY

May 15, 2018

Vision: By **2023**, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.

UNCLASSIFIED

Who Defends FRCS?



THE DEPARTMENT OF DEFENSE

CYBER STRATEGY

The purpose of this strategy is to guide the development of DoD's cyber forces and strengthen our cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DoD's three primary cyber missions.

DoD's Three Primary Cyber Missions:

Defend DoD networks, systems, and information

Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence

Provide cyber support to military operational and contingency plans

Cyber Mission Force: 133 teams by 2018

State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States' technological and military advantage. DoD must develop its cyber forces and strengthen its cyber defense and cyber deterrence posture.

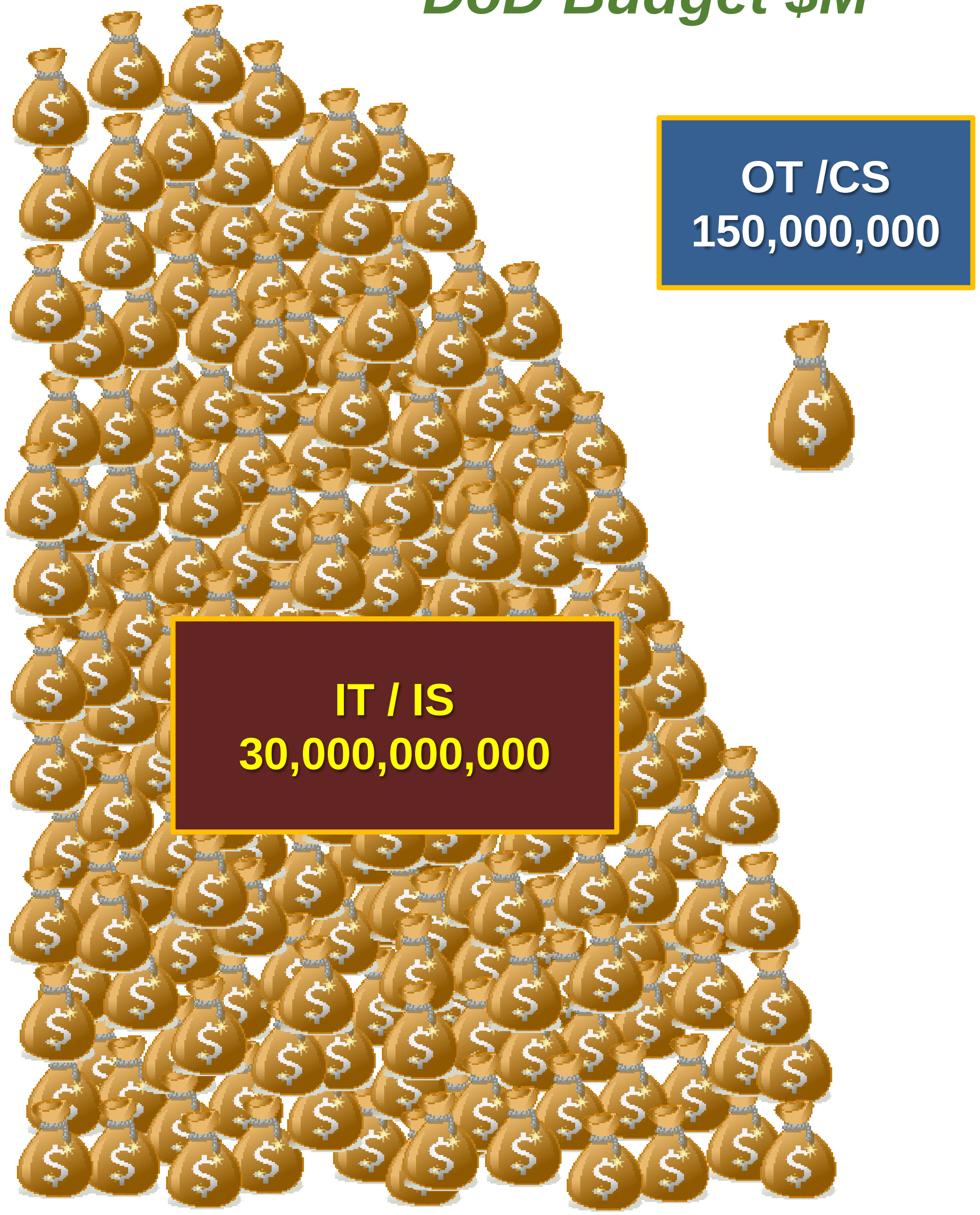
National Mission Teams Defend the United States and its interests against cyberattacks of significant consequence.	**13 teams**
Cyber Protection Teams Defend priority DoD networks and systems against priority threats.	**68 teams**
Combat Mission Teams Provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations.	**27 teams**
Support Teams Provide analytic and planning support to the National Mission and Combat Mission teams.	**25 teams**

- “U.S. Cyber Command is not “optimized” today to combat information operations orchestrated by foreign powers”

- “NSA we’re focused externally, Cyber Command we’re largely focused externally. So I will monitor bots, infrastructure external to the U.S., but one of the phenomenon we’re beginning to see is a migration of capabilities from external infrastructure — that we’ve been aware of and observing for some time — the way this is going to go next in my mind is you’re going to see this in domestic manipulation. And that is a part now that no, I am not really involved with,” Rogers said.
16 May 2017 SASC Hearing

USCC’s Role Does NOT Include Securing ALL Control Systems

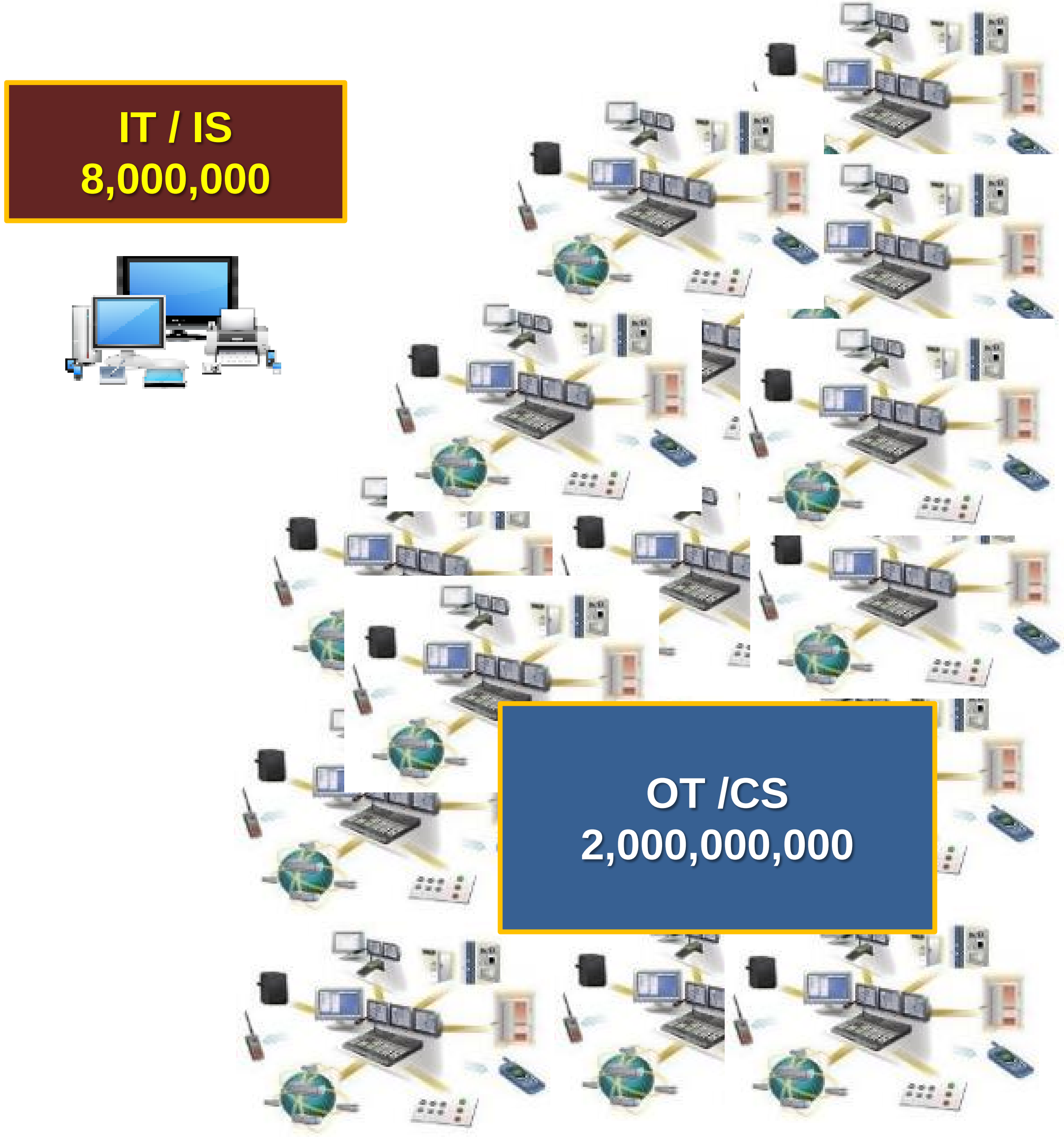
DoD Budget $M



OT /CS
150,000,000

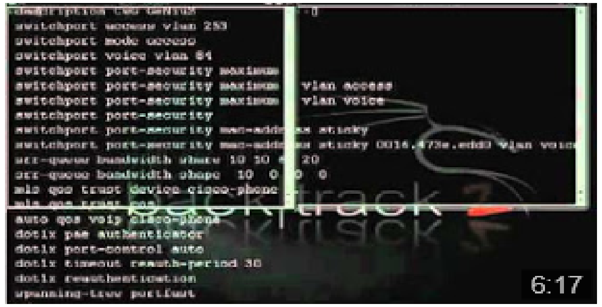
IT / IS
30,000,000,000

DoD # of Devices



IT / IS
8,000,000

OT /CS
2,000,000,000



```
description [illegible]
switchport access vlan 253
switchport mode access
switchport voice vlan 84
switchport port-security maximum
switchport port-security maximum  vlan access
switchport port-security maximum  vlan voice
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0014.[illegible].edd3 vlan voice
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape  10  0  0  0
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
dot1x pae authenticator
dot1x port-control auto
dot1x timeout reauth-period 30
dot1x reauthentication
spanning-tree portfast
```

anonymous vice vlan hacking

rhanem youssef
5 years ago • 348 views

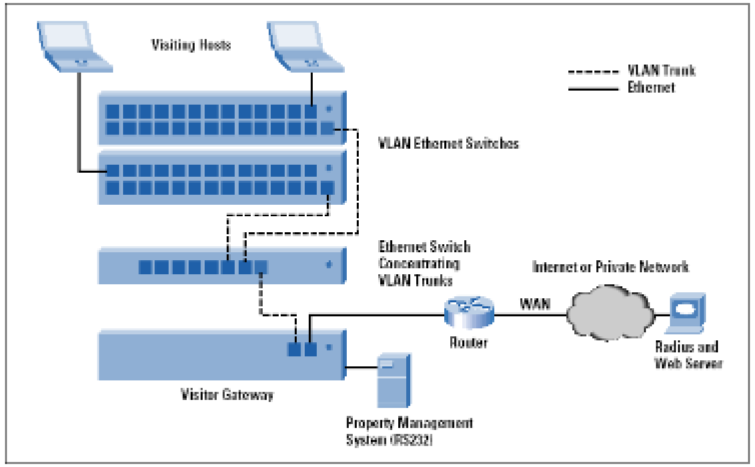
Mix - VLAN Hopping - Switch Spoofing Attack and Mitigation Tutorial

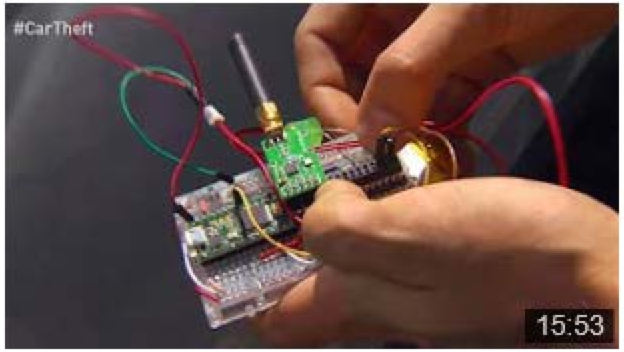
YouTube

VLAN Hopping - Switch Spoofing Attack and Mitigation Tutorial 2:10

MicroNugget: CAM Table Overflow Attack and How To Prevent It 8:49

Figure 3: VLAN Configuration





High-tech car theft: How to hack a car (CBC Marketplace)

CBC News ✓
2 years ago • 1,355,391 views

We go on the hunt for the mysterious device police believe those thieves are using to steal your car. To read more: http://www.cbc.ca

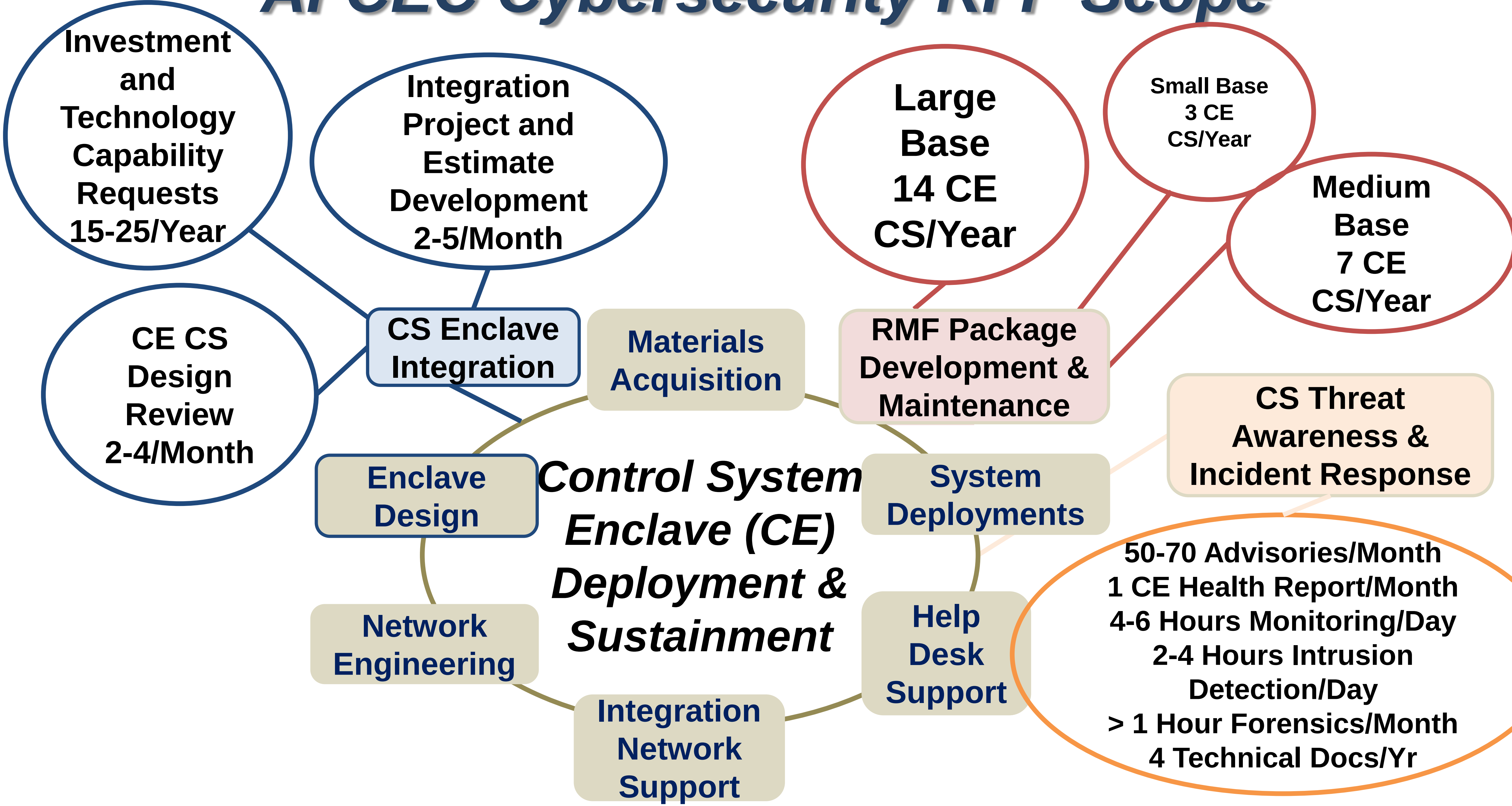
CC

Watch thieves steal car by hacking keyless tech

CNNMoney ✓
4 months ago • 112,327 views

Police in West Midlands, UK have released footage of criminals stealing a car by relaying a signal from the key inside the home, to

AFCEC Cybersecurity RFP Scope



Control System Enclave (CE) Deployment & Sustainment

CS Enclave Integration

Investment and Technology Capability Requests 15-25/Year

Integration Project and Estimate Development 2-5/Month

CE CS Design Review 2-4/Month

Materials Acquisition

RMF Package Development & Maintenance

Large Base 14 CE CS/Year

Small Base 3 CE CS/Year

Medium Base 7 CE CS/Year

CS Threat Awareness & Incident Response

System Deployments

50-70 Advisories/Month
1 CE Health Report/Month
4-6 Hours Monitoring/Day
2-4 Hours Intrusion Detection/Day
> 1 Hour Forensics/Month
4 Technical Docs/Yr

Help Desk Support

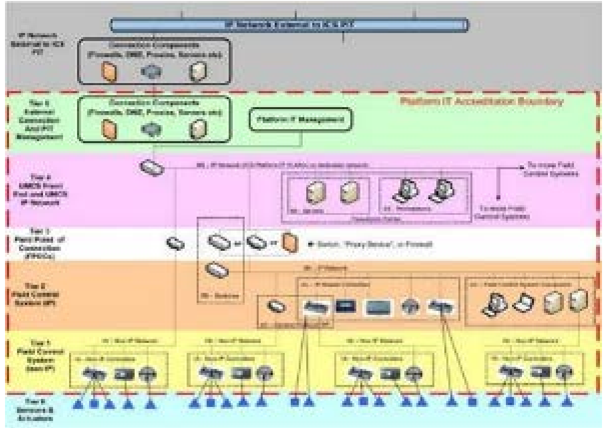
Integration Network Support

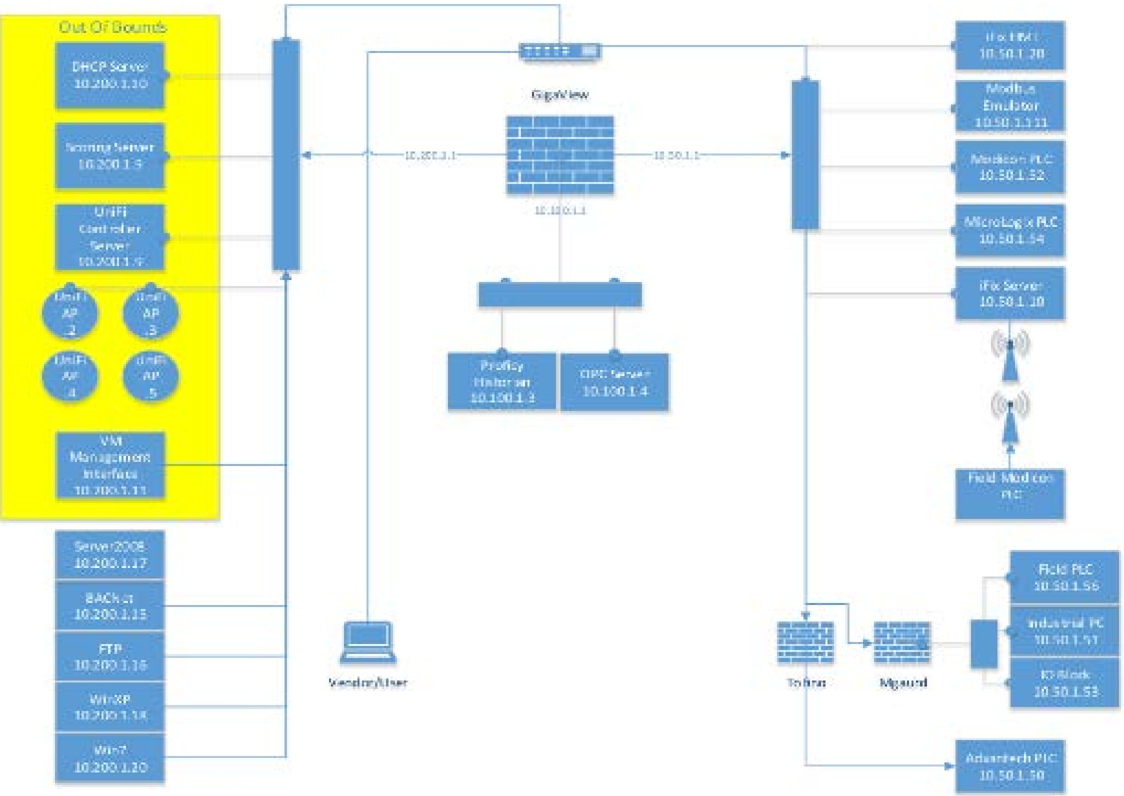
Network Engineering

Enclave Design

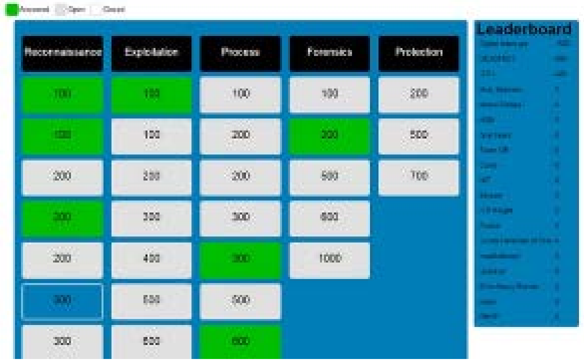
UNCLASSIFIED

SCADA Security Scientific Symposium (S4) Target Network


IP Network External to ICS PIT
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Platform IT Accreditation Boundary
Platform IT Management



- Corporate Zone
- Domain Controller
- FTP Server
- Windows 7 Workstation
- Windows XP Workstation
- BACnet Controller
- DMZ
- Advantech OPC Server
- Proficy Historian
- Control Zone
- iFix Server
- iFix HMI
- Schnider Electric Modicon PLCs
- Allen Bradley MicroLogix PLC
- ADAM Advantech PLC



🟩 [illegible] □ Open □ Closed

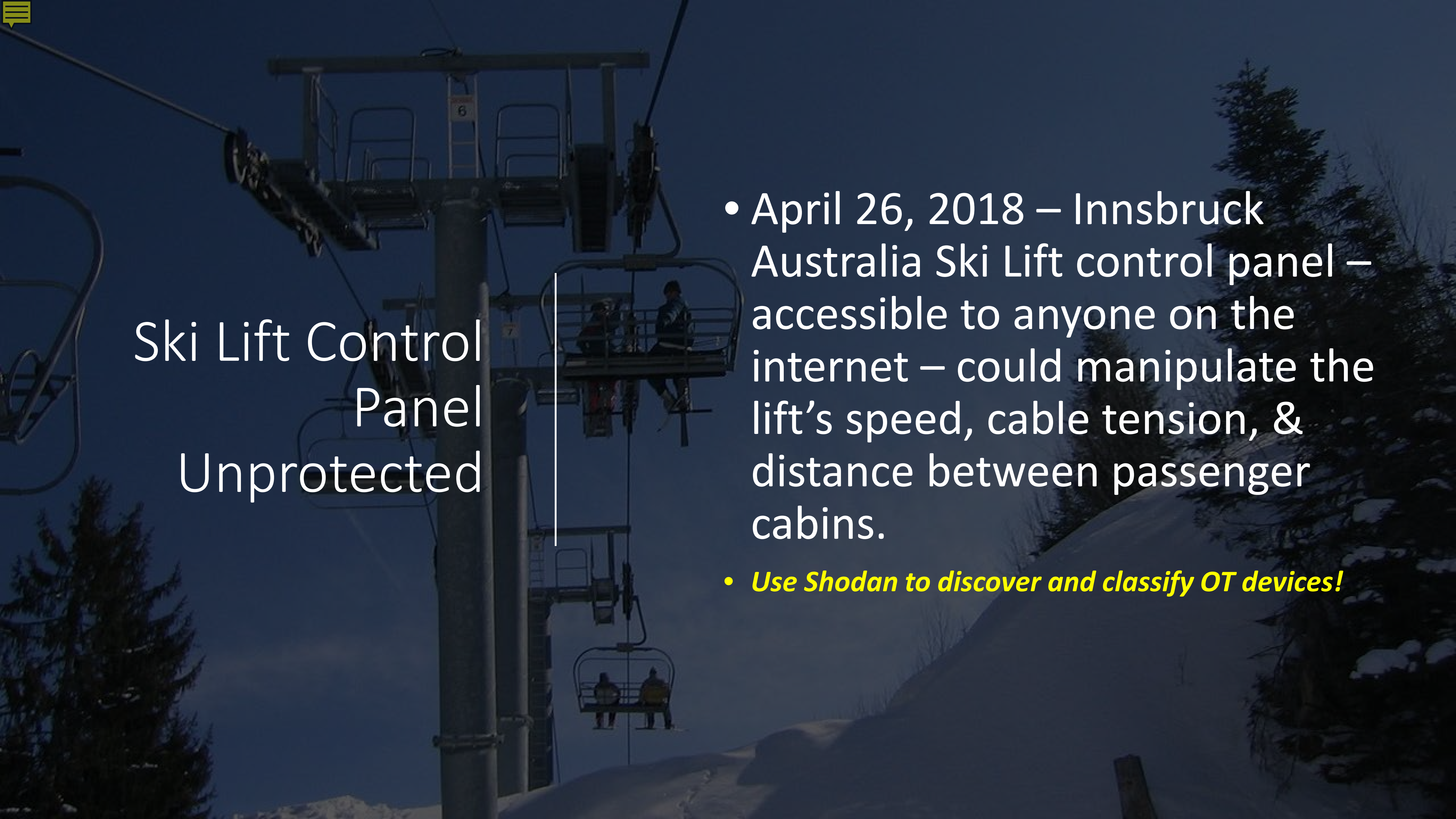
Reconnaissance	Exploitation	Process	Forensics	Protection
100	100	100	100	200
100	100	200	200	500
200	200	200	500	700
200	300	300	600	
200	400	300	1000	
300	500	500		
300	600	600		

Leaderboard

Team Name

Casino Hacked Via Thermometer

Thermometer in lobby aquarium hacked to pull high roller database to the cloud



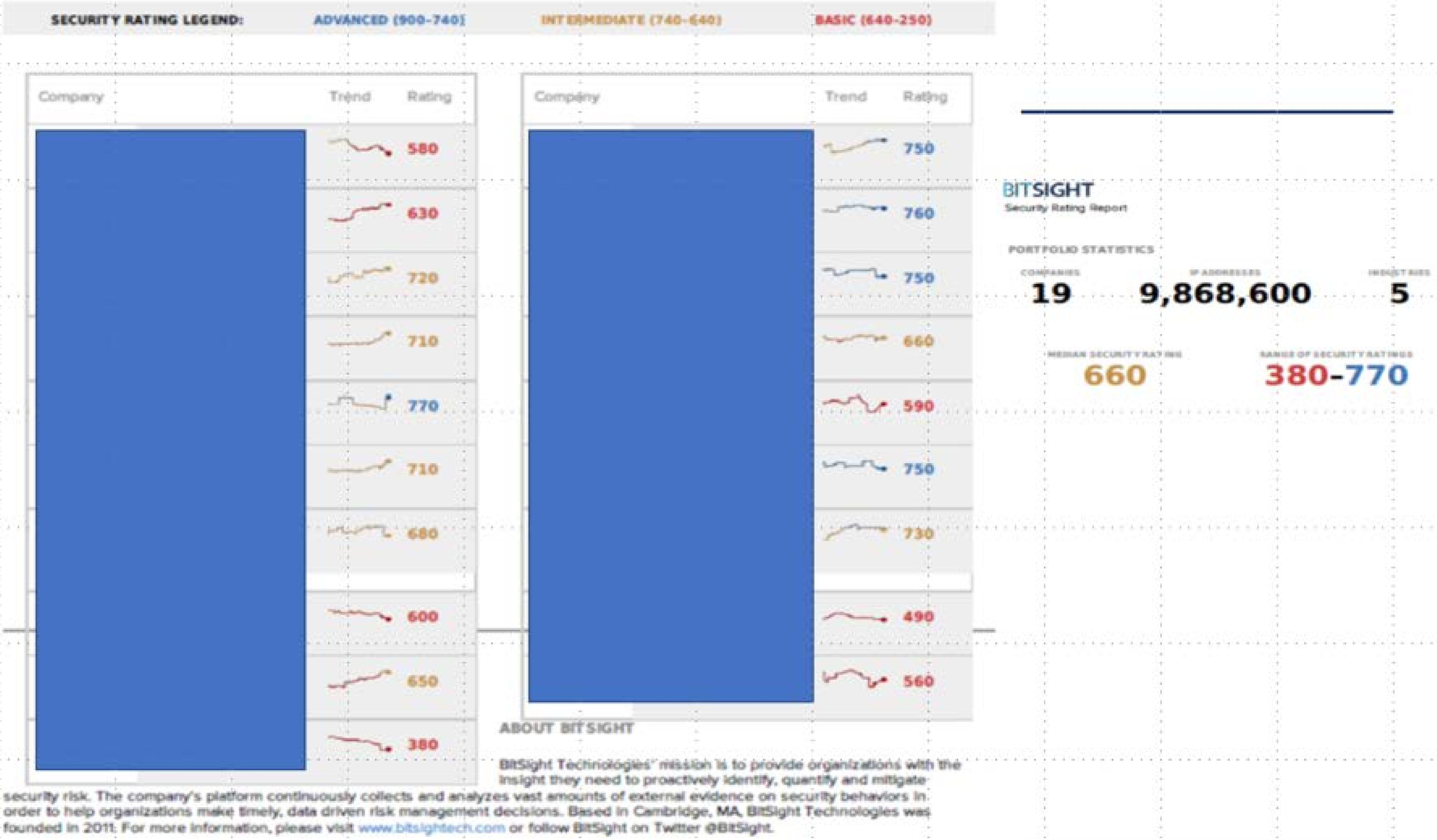
Ski Lift Control Panel Unprotected

- April 26, 2018 – Innsbruck Australia Ski Lift control panel – accessible to anyone on the internet – could manipulate the lift’s speed, cable tension, & distance between passenger cabins.
- *Use Shodan to discover and classify OT devices!*

What's Your Cyber 'Risk' or 'Trust' Score?

• **Bitsight**	bitsighttech.com
• **Risk Recon**	riskrecon.com
• **Security Scorecard**	securityscorecard.com
• **Upguard**	upguard.com
• **Others…**	

- ➢ All use public information & network signatures for FICO score-like rating approximating relative risk
- ➢ Enables intelligence for evaluation of critical suppliers, vendors, and others in the industry
- ➢ Augments Business Intelligence Unit and Security Operations Center; ques alerts to potential cyber or physical threats to our supply chains and internal infrastructure
- ➢ Each vendor's approach & scores roughly similar
- ➢ Need to verify accuracy – may detect one or more notables that were not really present in the enterprise under evaluation (e.g. a sub-domain or IP address not really associated with the target)
- ➢ **Benefit / Objectives**: Credibility when approaching supplier/partner with a security issue; avoid false positives & decrease time to investigate and mitigate



SECURITY RATING LEGEND: ADVANCED (900-740) INTERMEDIATE (740-640) BASIC (640-250)

Company	Trend	Rating
[redacted]		580
[redacted]		630
[redacted]		720
[redacted]		710
[redacted]		770
[redacted]		710
[redacted]		680
[redacted]		600
[redacted]		650
[redacted]		380

Company	Trend	Rating
[redacted]		750
[redacted]		760
[redacted]		750
[redacted]		660
[redacted]		590
[redacted]		750
[redacted]		730
[redacted]		490
[redacted]		560

BITSIGHT
Security Rating Report

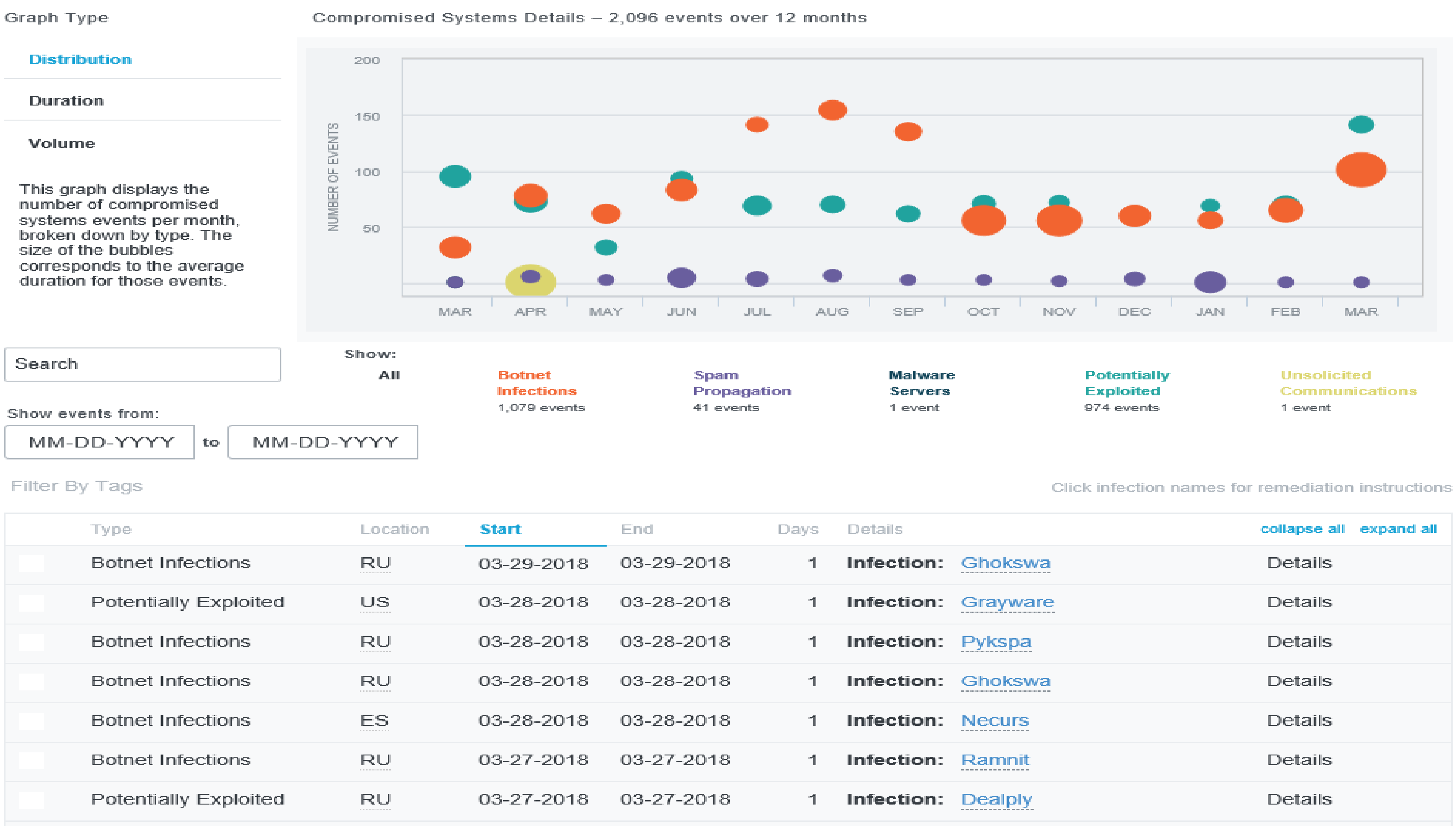
PORTFOLIO STATISTICS

COMPANIES	IP ADDRESSES	INDUSTRIES
19	9,868,600	5

MEDIAN SECURITY RATING	RANGE OF SECURITY RATINGS
660	380-770

ABOUT BITSIGHT

BitSight Technologies' mission is to provide organizations with the insight they need to proactively identify, quantify and mitigate security risk. The company's platform continuously collects and analyzes vast amounts of external evidence on security behaviors in order to help organizations make timely, data driven risk management decisions. Based in Cambridge, MA, BitSight Technologies was founded in 2011. For more information, please visit www.bitsightech.com or follow BitSight on Twitter @BitSight.



Graph Type

Distribution

Duration

Volume

This graph displays the number of compromised systems events per month, broken down by type. The size of the bubbles corresponds to the average duration for those events.

Compromised Systems Details – 2,096 events over 12 months

Search

Show events from:

MM-DD-YYYY to MM-DD-YYYY

Show:

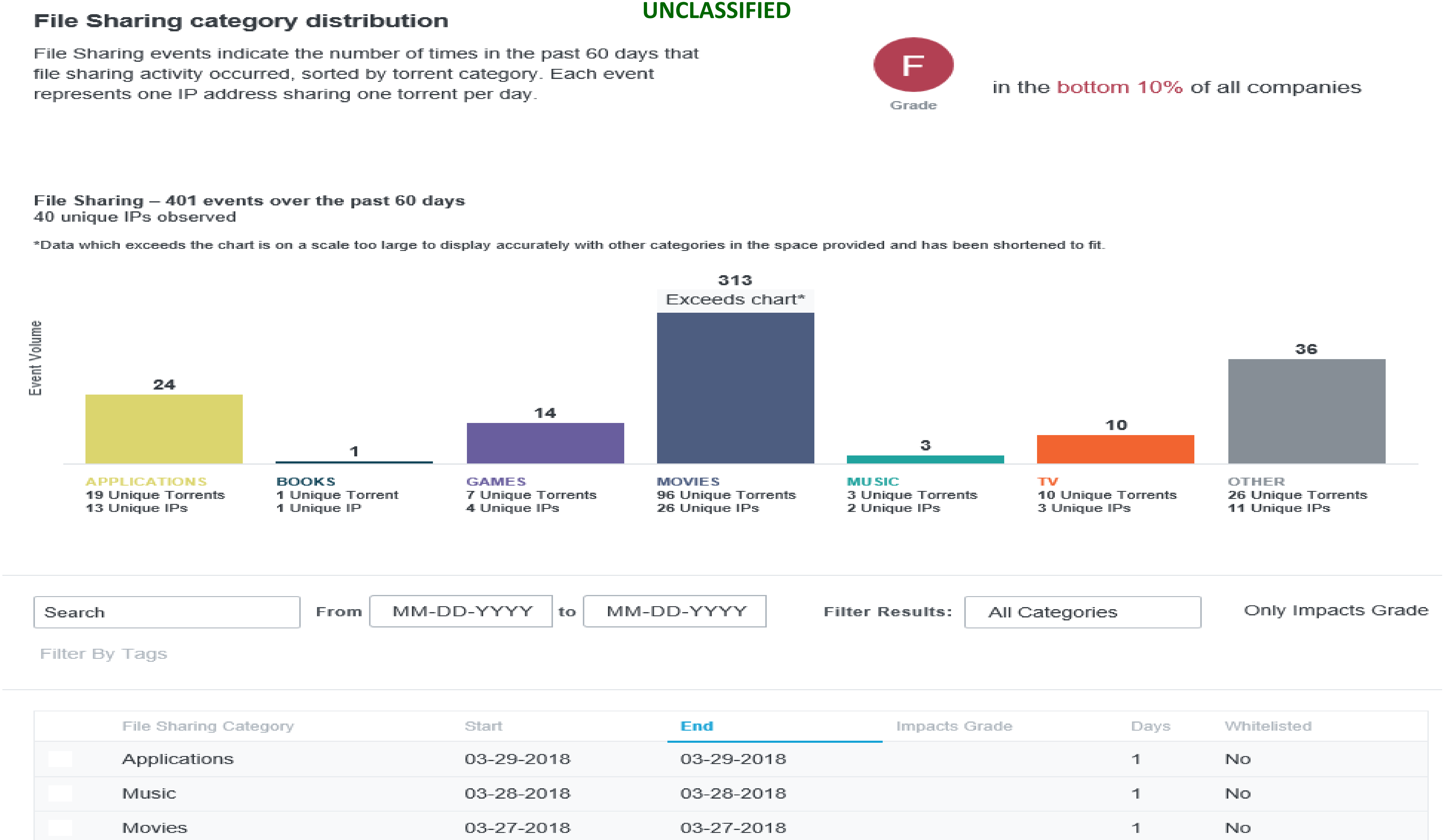
All	Botnet Infections	Spam Propagation	Malware Servers	Potentially Exploited	Unsolicited Communications
	1,079 events	41 events	1 event	974 events	1 event

Filter By Tags

Click infection names for remediation instructions

	Type	Location	Start	End	Days	Details	collapse all expand all
	Botnet Infections	RU	03-29-2018	03-29-2018	1	**Infection:** Ghokswa	Details
	Potentially Exploited	US	03-28-2018	03-28-2018	1	**Infection:** Grayware	Details
	Botnet Infections	RU	03-28-2018	03-28-2018	1	**Infection:** Pykspa	Details
	Botnet Infections	RU	03-28-2018	03-28-2018	1	**Infection:** Ghokswa	Details
	Botnet Infections	ES	03-28-2018	03-28-2018	1	**Infection:** Necurs	Details
	Botnet Infections	RU	03-27-2018	03-27-2018	1	**Infection:** Ramnit	Details
	Potentially Exploited	RU	03-27-2018	03-27-2018	1	**Infection:** Dealply	Details

UNCLASSIFIED



File Sharing category distribution

File Sharing events indicate the number of times in the past 60 days that file sharing activity occurred, sorted by torrent category. Each event represents one IP address sharing one torrent per day.

F

Grade

in the bottom 10% of all companies

File Sharing – 401 events over the past 60 days
40 unique IPs observed

*Data which exceeds the chart is on a scale too large to display accurately with other categories in the space provided and has been shortened to fit.

Search From MM-DD-YYYY to MM-DD-YYYY Filter Results: All Categories Only Impacts Grade

Filter By Tags

	File Sharing Category	Start	End	Impacts Grade	Days	Whitelisted
□	Applications	03-29-2018	03-29-2018		1	No
□	Music	03-28-2018	03-28-2018		1	No
□	Movies	03-27-2018	03-27-2018		1	No

Best Practices to Cyber Secure Control Systems

Mission Assurance Senior Steering Group Control Systems Working Group

- Develop Password Policies
- Security Awareness and Training
- Patch Management
- Maintenance Activities
- Modem Connection
- Network Design
- Securing Host Systems

Advanced Cyber Industrial Control System Tactics, Techniques, Procedures

Detection

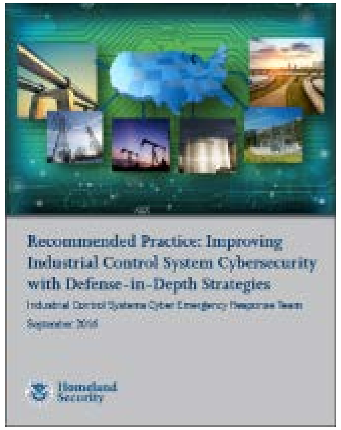
- Routine Monitoring, Inspection, Identification of adversarial presence, Documentation, Notifications

Mitigation

- Protect the information network, Acquire and protect data for analysis, Maintain operations during an active attack

Recovery

- Identify mission priorities, Acquire and protect data for analysis, Systematically Recover each affected device, Systematically reintegrate devices, processes, and network segments, Test and verify system to ensure devices are not re-infected

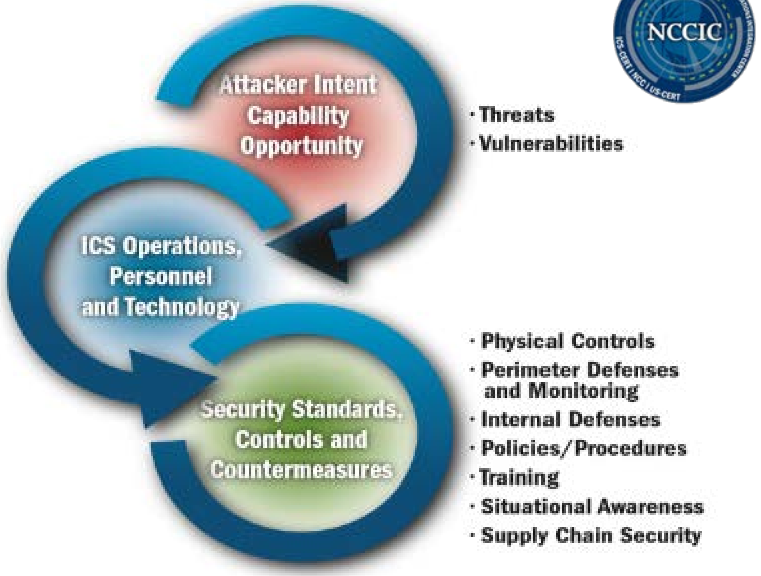


Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response Team

September 2016

Homeland Security



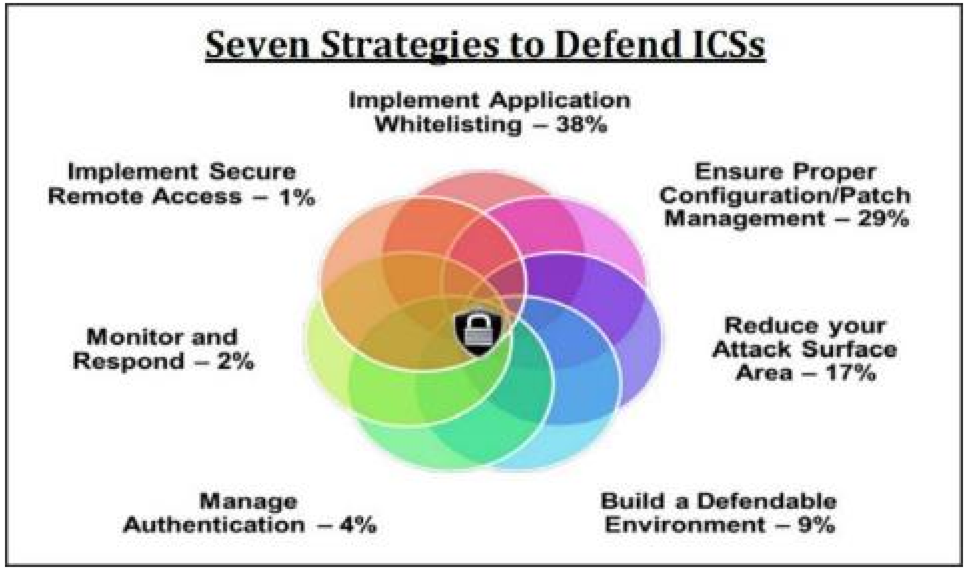
Attacker Intent
Capability
Opportunity

- Threats
- Vulnerabilities

ICS Operations, Personnel and Technology

Security Standards, Controls and Countermeasures

- Physical Controls
- Perimeter Defenses and Monitoring
- Internal Defenses
- Policies/Procedures
- Training
- Situational Awareness
- Supply Chain Security



Seven Strategies to Defend ICSs

- Implement Application Whitelisting – 38%
- Ensure Proper Configuration/Patch Management – 29%
- Reduce your Attack Surface Area – 17%
- Build a Defendable Environment – 9%
- Manage Authentication – 4%
- Monitor and Respond – 2%
- Implement Secure Remote Access – 1%

Discussion

KAL 2009
The Economist
Q
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY
CYBER ATTACKS AHEAD

DoD & Commercial Resources

DoD CIO Knowledge Service (requires CAC) https://rmfks.osd.mil/login.htm

Department of Defense Advanced Control System Tactics, Techniques, and Procedures (TTPs) 2018:
https://www.cybercom.mil/ICSTTP/Forms/AllItems.aspx

UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS Sept 2016
https://wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) [info & funding solicitations]
https://serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Cybersecurity-Guidelines

DoD OASD(EI&E) and Federal Facilities Council (FFC), under the National Research Council (NRC) sponsored a 3-day Building Control System Cyber Resilience Forum in Nov '15.
http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792

DoDI 5000.02 Cybersecurity in the Defense Acquisition System Jan 2017
http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf

Whole Building Design Guide website cyber references
http://www.wbdg.org/resources/cybersecurity

Tools
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

Workshops / Building Control Systems Cyber Security Training
http://hpac.com/training/workshop-what-do-when-building-control-systems-get-hacked-set

Industrial Control Systems Joint Working Group (ICSJWG_
https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG