Intelligence & National Security Forum
May 11, 2018

This presentation is unclassified in its entirety

Control Systems Cyber Security – Why Bother?

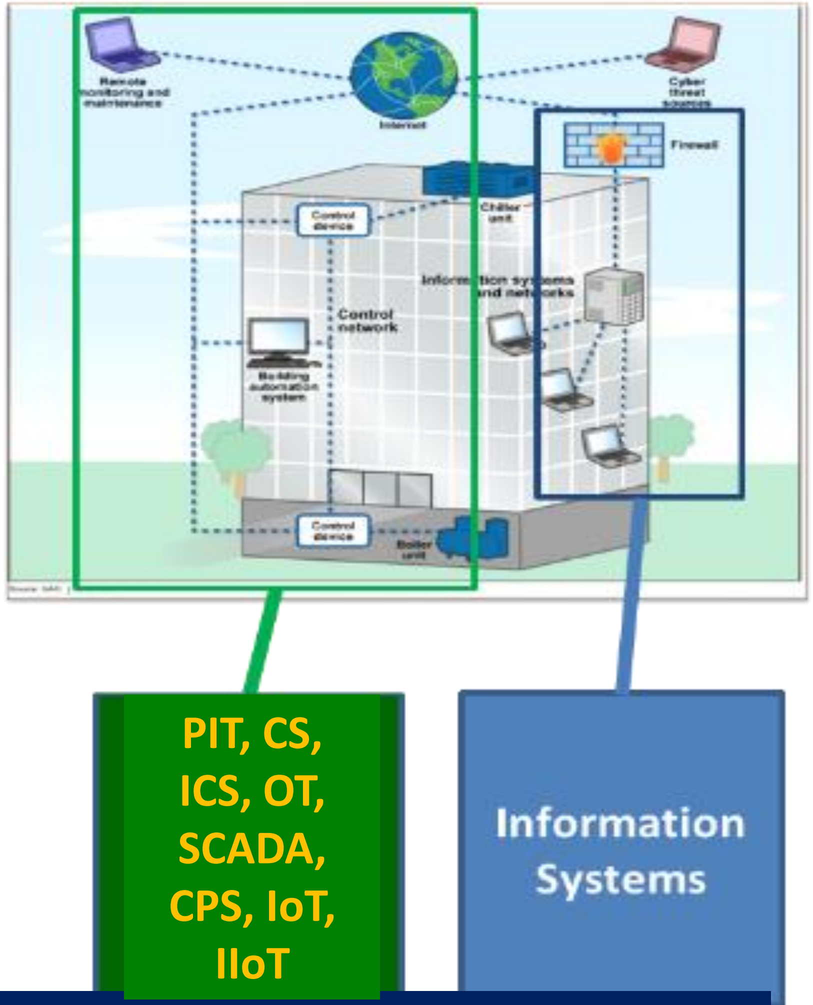
Daryl Haegley
11 May 2018

This presentation is unclassified in its entirety

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

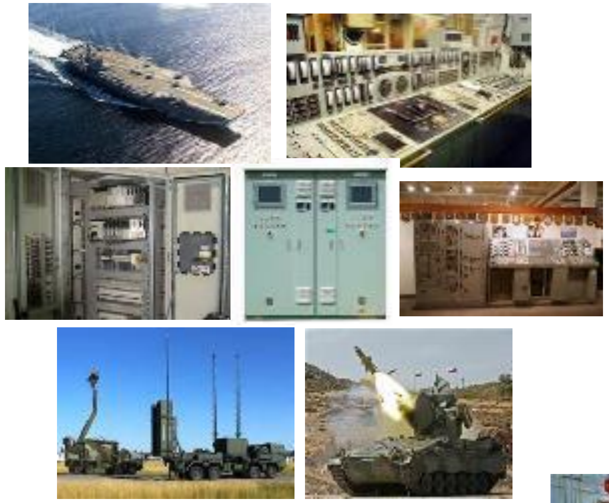
Information Systems

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

>500 Installations
>250K Buildings
>200K Structures

Buildings

Weapon Platforms



Operational Energy

Electrical and HVAC

Pumps and Motors

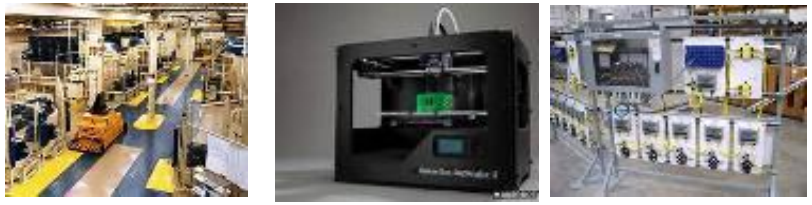
Nuclear

Typical Controller

Vehicles/Charging

Medical

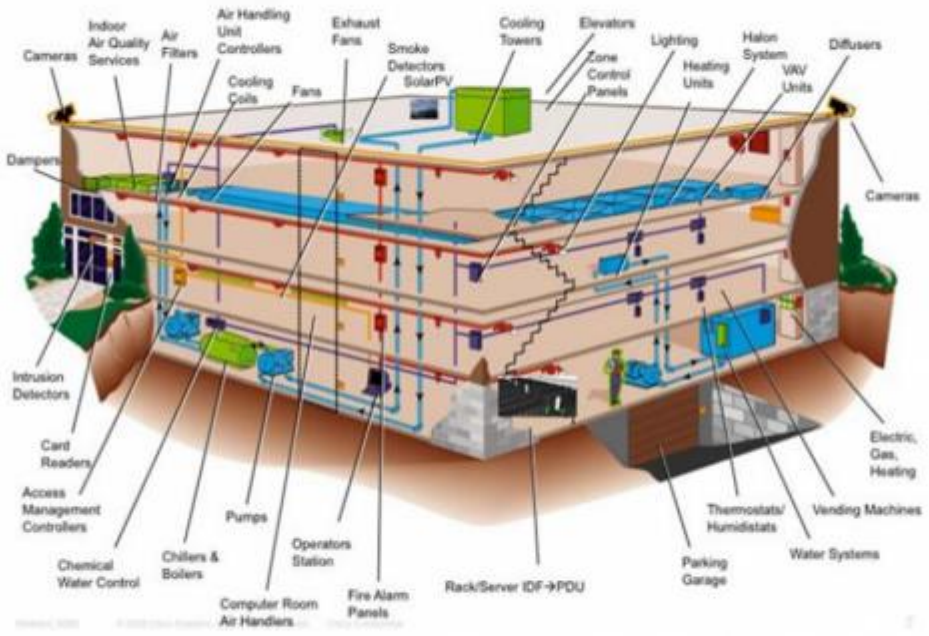
Manufacturing



UNCLASSIFIED

What's in Your 'Smart Building?'

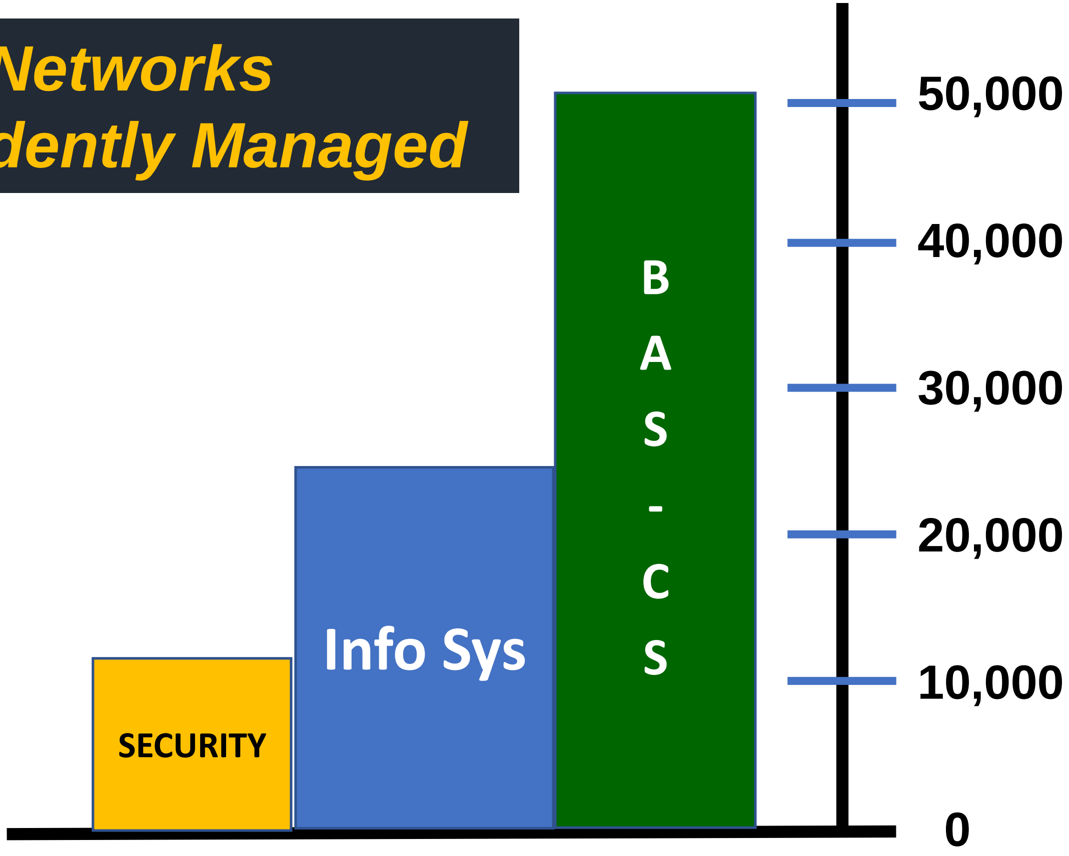
- "Smart" / High Performance Green Buildings
  - Since 2005 ~7,000+
  - Example: 5,000 desks, 20 floors, ~2M sqft



3 Networks Independently Managed

- 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



I'm at the station in Utrecht. My mobile phone has a fast Internet connection.

Existing Integration Systems

Acuity Brands Roam   Advantage Controls   ALC   Alerton AIE   Alerton BACtalk   Alerton BCM-WEB   American Auto-Matrix Auto Pilot   American Auto-Matrix   Andover Controls Continuum   Asi controls   Auto Matrix Sage   Automated Logic WebCTRL   Automated Logic   Barber Coleman Network 8000   Bristol Babcock   CAPRON   Carrier Carrier Comfort Network   Carrier   Com-Trol   Control Microsystems SCADAPack   Cylon Unitron UC32   Daikin   Data Aire   Dell Vostro   Delta Controls ORCA   Distech   Echelon i.Lon   Emerson-Liebert   EXHAUSTO   Flygt ITT Industries APP 700   General Electric WESDAC   General Electric   Honeywell Excel 5000   Honeywell WEBs-AX   HSQ Technology   Invensys I/A Series   Invensys Micronet   Invensys Network 8000   Johnson Controls Facility Explorer   Johnson Controls Metasys   Johnson Controls M-Series   KMC   LANDIS   Landis & Staefa Integral MS2000   Landis & Staefa   Liebert SiteGate   LOYTEC Electronics L-VIS   Lynxspring JENEsys   Merlin Gerin PowerLogic   Microwave Data Systems   Mitsubishi   Motorola SCADA Systems   Odessa Engineering   OmniaPRO   Orion Controls   Paragon EC7000 Series   Raco   Reliable Controls MACH-ProWebSys   Richards-Zeta   Robert Shaw DMS   RUGID   Schneider Electric I/A Series   Schneider Electric PowerLogic   Siebe Network 8000   Siemens ACCESS   Siemens Apogee   Siemens Desigo PX   Siemens Synco 700   Staefa   Staefa/Siemens   STULZ Air Technologies   TAC I/A Series   TAC Network 8000   TAC Xenta   TAC Vista   Telvent Smart Grid Solution   Trane Tracer   Trane Tracer Summit   Trane Varitrac   TREND   Trend Control Systems IQ2   Tridium Vykon

Existing CS Operating Software

Axon CAT SARL Desigo Insight KNX STANDARD ABB Symphony Plus OptimaxRev 4 ABB Symphony Plus 800xA SV 5.1 ABB Symphony Plus Composer 6.0 ABB Symphony Plus S+ Operations 1.1 Alerton BACTalk Envision 2.0 Alerton BACTalk Envision 2.6 Alerton VisualLogic Allen-Bradley RSLogix 500 Allen-Bradley RSLogix 500, RSView32 Automated Logic ExecB 6.0 Automated Logic SuperVision WebCTRL 5.5 Automated Logic WebCTRL WebCTRL 3 Automated Logic WebCTRL WebCTRL 3.0 Automated Logic WebCTRL WebCTRL 5 Automated Logic WebCTRL WebCTRL 5.2 Automated Logic WebCTRL WebCTRL 4.1 SP1 Automated Logic WebCTRL WebCTRL Automated Logic ExecB 4.1 SP1 Automated Logic ExecB drv_lge_4-02-175 Automated Logic ExecB drv_melgr_vanilla_4-02-175 Automated Logic ExecB Automated Logic Supervision 2.6b Automated Logic WebCTRL 4 SP1B Automated Logic WebCTRL 4.1 SP1 Automated Logic WebCTRL 4.1 SP1b Automated Logic WebCTRL SVR 5.5 Calsense Command Center 4.15.11.20 Carrier Comfort Network Comfort Network 3.0 Control Microsystems ClearSCADA 2009 Ed. R2.2 Data flow Systems HyperTAC 2 Data flow Systems HyperTAC HT3 Delta Controls ORCA ORCAview 3.30 Delta Controls ORCA ORCAview 3.40 Delta Controls Orcaview 3.22 Delta Controls Orcaview 3.30 Delta Controls OrcaView 3.3 Delta Controls Orcaview 3.33 Delta Controls Orcaview Delta Controls, TAC ORCA, I/NET ORCAview, Seven Rel 2.15 EFACAC Prism ERI Siemens Insight 3.6 GE, Intellution Proficy, iFIX, FIX Desktop _, _,4.0, _ General Electric Cimplicity Plant Edition 6.1 General Electric Multilin Config Pro 5.03 General Electric Proficy Cimplicity 7.0 General Electric Proficy iFIX 4.0 Honeywell Symmetre Station 3.5 Symmetre 3.5 Honeywell Webstation-AX Niagara Niagara 3.5.40.1 HSQ Miser 6.06 HSQ Miser HSQ, Sun Microsystems Miser, Xview 6.06 Iconics Genesis32 Genesis32 8.3 Iconics Genesis32 Genesis32 9.13 Iconics HMI SCADA Solutions Genesis 32 3.12.005 InduSoft Web Studio Intellution 7 Intellution FIX32 3.5 Intellution FIX32 Intellution iFIX 3.5 Intellution IFIX Intellution iFIX Reporter ITT Flygt AquaView AquaView 1.50 Johnson Controls Metasys 6.0.0.9000 Johnson Controls Metasys GX9100 7.05A Johnson Controls Metasys Metasys 5 Johnson Controls Metasys Metasys 5.1 Johnson Controls Metasys Project Builder 5:1 Johnson Controls Metasys Project Builder 3 Johnson Controls Metasys 5 Johnson Controls Metasys 12.04 Johnson Controls Metasys 2.0.0.70.0 Johnson Controls Metasys 5.2.0.5400 Johnson Controls Metasys Johnson Controls M-Graphics 5.3 Microsoft Explorer N/A N/A N/A N/A Pneu-Logic Pneu-Logic RACO RACO 3.14 Rainbird MAXICOM2 Central Control 4.3 ReLab Software ClearView-SCADA 7.2.8 Reliable Controls MACH ProWebSys RC-Studio 2.0 Robert Shaw Digital Management System Operator Interface 11.0 Rockwell FactoryTalk Service Platform 2.30 Rockwell FactoryTalk View, Rsview Site Editiion, Supervisory 6.0, 6.0 Rockwell Factory Talk 6.0 Rockwell Automation FactoryTalk View Machine Edition 5.1 Rockwell Automation FactoryTalk View Site Edition 4.0 Rockwell Automation FactoryTalk View Site Edition 5.1 Rockwell Automation FactoryTalk View Site Edition Rockwell Automation RSView Supervisory Edition 4.0 Rockwell Automation RSView Supervisory Edition Rockwell Automation RSView32 7.600.00 ScadaTEC SCADASIS 5.8.14.213 Schneider Electric PowerLogic ION Enterprise 5.6 Schneider Electric PowerLogic ION Enterprise Siebe Network 8000 Signal 4.4.1 Siemens S7 300 STEP 7 Siemens Apogee Insight Siemens Desigo Insight Siemens Insight Desigo Insight 2.31 Siemens Insight Desigo Insight 2.35.021 Siemens WinPM.Net 3.2 SP3 SUBNET Solutions SubSTATION Explorer 1.3.0 SUBNET Solutions SubSTATION Explorer 1.5.7 Sun Microsystems Xview 3.2 Symantec Backup Exec 2011? TAC 1/A Series WorkPlace Tech 5.7 TAC I/A Series Workbench TAC I/A Series WorkPlace Tech 5.7.2 TAC 4.1 TAC Signal, XPSI & ZPSIPC Teletrol eBuilding Telvent OaSys DNA 7.4.* Trane Tracer SC Tracer 3.5 Trane Tracer Summit Tracer 11 Trane Tracer Summit Tracer 16 Trane Tracer Summit Tracer 17 Trane Tracer Summit V14 Tracer 14 Trane Tracer Summit V16 Tracer 16 Trane Tracer Summit V17 Tracer 17 Tridium Vykon Niagara 2.301.428 Tridium Vykon Niagara 2.301.430.v1 Tridium Vykon Niagara 2.301.431.v1 Tridium Vykon Niagara 2.301.514 Tridium Vykon Niagara 2.301.514.v1 Tridium Vykon Niagara 2.301.522 Tridium Vykon Niagara 2.301.522.v1 Tridium Vykon Niagara 2.301.522.v2 Tridium Vykon Niagara 2.301.522V1 Tridium Vykon Niagara 2.301.527.v1 Tridium Vykon Niagara 2.301.529 Tridium Vykon Niagara 2.301.532 Tridium Vykon Niagara 2.301.532.v1 Tridium Vykon Niagara 3.3.31 Tridium Vykon Niagara 3.5.34 Tridium Vykon Niagara Workbench 3.6.31 Tridium Vykon Niagara Tridium Vykon Niagara AX 3.3.22.0 Tridium Vykon Niagara AX 3.5.25.0 "Tridium Vykon Niagara AX 3.5.25.0 3.3.22.0" "Tridium Vykon Niagara AX 3.5.25.0 3.4.51.0" Tridium Vykon Niagara AX 3.5.25.1 Tridium Vykon Niagara AX 3.5.34.0 Tridium Vykon Niagara AX 3.5.34.2 Tridium Vykon Niagara AX 3.5.39.0 Tridium Vykon Niagara AX 3.5.40.7 Tridium Vykon Niagara AX 3.5.7.0 Tridium Vykon Niagara AX 3.6.31.0 Tridium Vykon Niagara AX 3.6.31.4 Tridium Vykon Niagara AX 3.6.47 Tridium Vykon Niagara AX 3.6.47.0 Tridium Vykon Niagara AX Tridium Vykon Niagara R2 2.301.522 Tridium Vykon Niagara R2 2.301.522.v1 Tridium Vykon Niagara R2 2.301.529.v1 Tridium Vykon Niagara R2 2.301.532.v1 Tridium Vykon Niagara R2 R2.301.529 Tridium Vykon Niagara R2 Tridium Vykon Niagra 3.5.34.7 Tridium Vykon Workplace Pro 2.301.428 Tridium Vykon Workplace Pro 2.301.514 Tridium Vykon WorkPlace Pro 2.301.522 v2 Tridium Vykon Workplace Pro 2.301.532 Wonderware Intouch WindowViewer 10.1.200 Yokogawa Exaquantum EXAOPC R3.21 Yokogawa Exaquantum Exaquantum Server R2.60 Yokogawa DAQOPC for DARWIN R3.01 2 6.0 ACS Alerton 3.5.34 Alerton

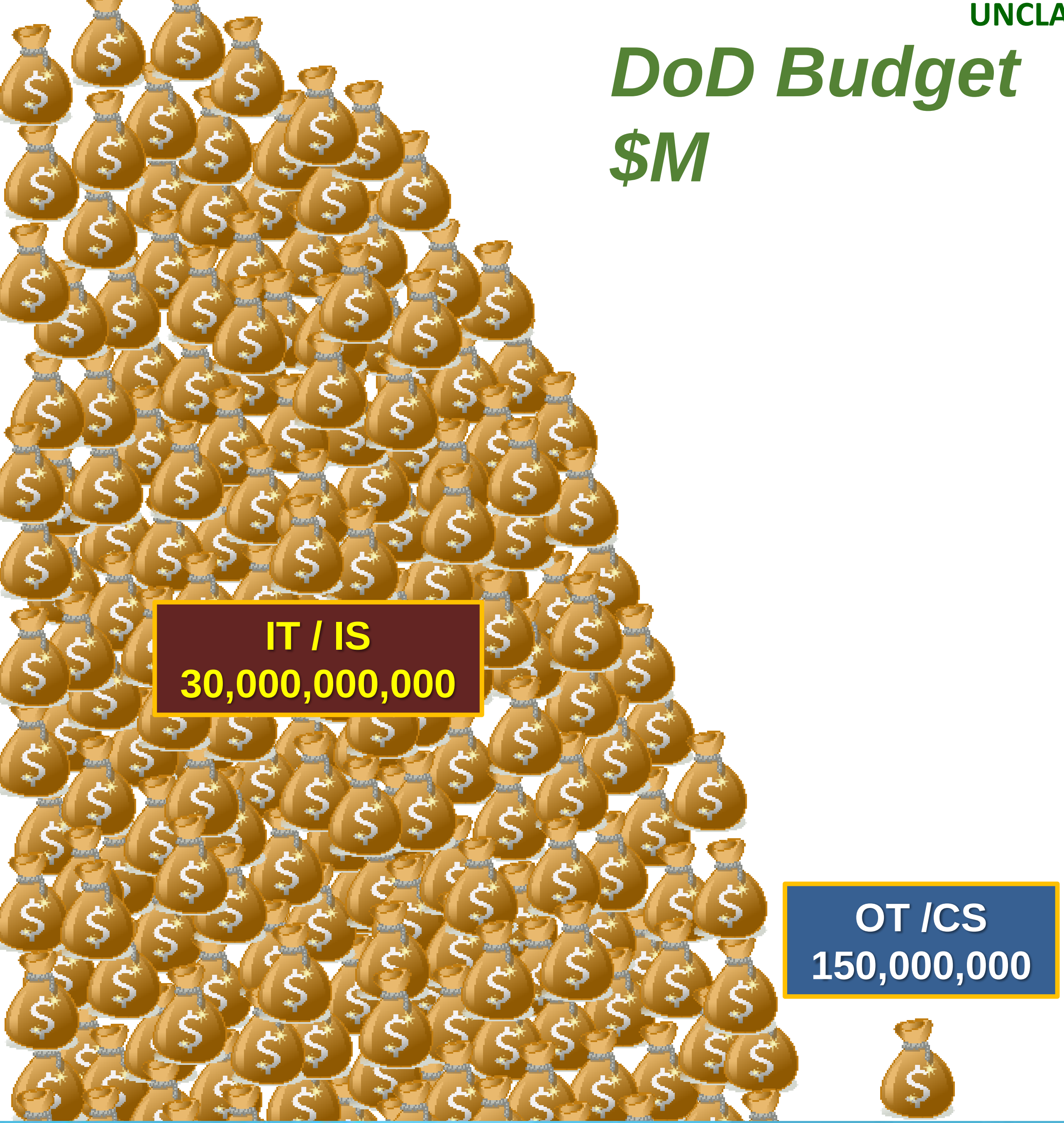
UNCLASSIFIED

Existing Device Level Controllers

- AAEON Electronics AAON SS1016 ABB ACH550-UH-045A-4 ABB ACH550-UH-04A1-4 ABB ACH550-UH-246A-4 Acuity Brands Roam Gateway ADDER ADDERLink INFINITY ALIF 1000R-US ADDER ADDERLink INFINITY ALIF 1000T-US Advantech Touch Panel Computer TCP-1770H-C2BE Advantech Touch Panel Computer TPC-1780H Advantech Touch Panel Computer TPC-650H AEG BLR-CX 04R AEG Schneider Automation Modicon Micro 612 Alerton VLC-1188 Alerton VLC-444 Alerton VLC-550 Alerton VLC-853 Alerton BACtalk BCM-PWS Alerton BACtalk VAV-SD Alerton BACtalk VLC-1180 Alerton BACtalk VLC-1188 Alerton BACtalk VLC-444 Alerton BACtalk VLC-550 Alerton BACtalk VLC-651R Alerton BACtalk VLC-660R Alerton BACtalk VLC-853 Allen-Bradley Allen-Bradley CompactLogix L23E Allen-Bradley CompactLogix L32E Allen-Bradley ControlLogix 1756-A10 Allen-Bradley ControlLogix 1756-L61 Allen-Bradley ControlLogix OEM Allen-Bradley FlexLogix 1794-L34 Allen-Bradley FlexLogix 5433 Allen-Bradley FlexLogix FLEX I/O Allen-Bradley Integrated Display Computers 6181P Allen-Bradley MicroLogix 1000 1761 Allen-Bradley MicroLogix 1000 1761-L16BWB Allen-Bradley MicroLogix 1100 1763 Allen-Bradley MicroLogix 1100 1763-L16AWA Allen-Bradley MicroLogix 1100 1763-L16BWA Allen-Bradley MicroLogix 1400 Allen-Bradley Micrologix 1400 1766-L32AWAA 8/10.00 Allen-Bradley MicroLogix 1500 1764-24AWA Allen-Bradley MicroLogix 1761-NET-ENI Allen-Bradley PanelView Plus 1000 Allen-Bradley PanelView Plus 2711P-KM420D Allen-Bradley PanelView Plus 600 Allen-Bradley PanelView Plus 700 Allen-Bradley PowerMonitor 3000 Allen-Bradley PowerMonitor 3000 1404-DM A Allen-Bradley PowerMonitor 3000 1404-M405A-ENT B Allen-Bradley SLC 500 DH-485 Allen-Bradley SLC 500 SLC 5/00 Allen-Bradley SLC 500 SLC 5/02 Allen-Bradley SLC 500 SLC 5/03 Allen-Bradley SLC 500 SLC 5/04 Allen-Bradley SLC 500 SLC 5/05 Allen-Bradley VersaView 1500P Andover Controls Continuum Infinet II i2810 Andover Controls Infinity SCX 920 APC AP7960 APC PNET 1 APC Back-UPS BE350R APC Back-UPS BE750G APC Back-UPS BX900R APC Back-UPS ES550 APC Back-UPS Pro 1000 APC Back-UPS RS800 APC Back-UPS XS1500 APC Smart-UPS 1000XL APC Smart-UPS 2200 APC Smart-UPS 2200XL APC Smart-UPS 750 APC Smart-UPS AP5719 APC Smart-UPS SMT3000RM2U APC Smart-UPS SU2200NET APC Smart-UPS SU220RMXL APC Smart-UPS SU3000RMXL APC Smart-UPS SU3000XLM APC Smart-UPS SUA1000RM1U APC Smart-UPS SUA1500 APC Symettra APC Symmetra AP9617 / Symmetra 40K Arena EX III Arista ARP-2217AP Armstrong SteamEye Gateway 3000M Autoflame DTI MK6DTI Automated Logic LGR1000 Automated Logic LGR25 Automated Logic M line M0100 Automated Logic M line M220nx Automated Logic M line M4106 Automated Logic M line M8102 Automated Logic M line M8102nx Automated Logic M line Mcpu Automated Logic ME812u line ME812u Automated Logic S line S6104 Automated Logic U line UNI/32 AutomationDirect DL06 AutomationDirect DL205 AutomationDirect EA7-T10C AutomationDirect EA-T10C AutomationDirect C-More EA7-T6CL AVG EZ-T10C-F AVG EZ-T15C-FSU Axiomtek DIN-rail Embedded System rBOX201-4COM-FL Axis 214 PTZ Axis 2400PTZ Axis 241Q Axis P5512 B&B Electronics MES1B Badger Meter Disc Series 120 Badger Meter Disc Series 170 Badger Meter Disc Series 35 Badger Meter Disc Series 70 Badger Meter M Series 4000 Badger Meter Turbo Series 2000 Badger Meter Turbo Series 450 Barber Coleman Network 8000 MZ2A Basler Electric BE1-25 Basler Electric BE1-700V Basler Electric BE1-CDS220 Basler Electric BE1-GPS100 E3N2R0U Bay Controls BayNet Belkin F6C1100-AVR Belkin F6C750-AVR Bitronics PowerPlex MTWIN3 Black Box ME838A-R2 Black Box ME838A-R3 BOCA Bristol Babcock DPC 3335 Brother HL-2270DW Brother HL-4040CDN Brother HLYOC Buffalo TS-H0.0TGL\RG Buffalo TeraStation Pro TS-H03TGL-R5 CalAmp VIPER SC Campbell Scientific CR1000 Carel pCO3 Carrier 30RRB06052_00__3 Carrier 30XAB50062-03X93 Carrier Comfort Network Comfort Controller 6400 Cohen OEM Computrol 32X Control Microsystems 5000 Series 5302 Control Microsystems SCADAPack 100 Control Microsystems SCADAPack 334 Cooper Power Systems CL-6A Cooper Power Systems CL-6A WA366B67G6AR Cooper Power Systems CL-6A WE383F44K6XR CyberPower 1500ADR CyberPower CPS1500AVR Cylon Unitron UC32 Daikin McQuay MicroTech II WMC Danfoss OEM Danfoss BACLink VLT DEC LA400-A2 Dell 3000CN Dell 71PXP Dell UPS1000W Dell Color Laser Printer 1320C Dell Laser Printer 1110 Dell Laser Printer 2330dn Dell Laser Printer 3100CN Dell PowerValut MD3000i Dell PowerValut TL2000 Delta Controls ORCA DSC-1212E Delta Controls ORCA DSC-1616E Delta Controls ORCA DSC-633E Deltak OEM Digi AccelePort C/X (1P) 50000598-01 Digital Loggers Web Power Switch III Dolch ORCA-19 Dolch ORCA-19PM DROBO 902-00001-001 Eason Technology 950 Eaton RO LIC-100 HMI Eaton Power Xpert PX4000 Eaton Powerware 3105 Eaton Powerware 5125 Eaton Powerware 9125 Eaton Powerware FE2.1KVA Eaton Powerware PW9130L1500T-XL Electro Industries Nexus 1262 Electro Industries Nexus 1270-S-SWB2-20-60-4IPO-SE Electro Industries Nexus 1272 Electro Industries Shark 100S elo Touch Solutions Touch systems Elo Touch Solutions Touchmonitor ET1739L Elo TouchSystems Elster American Meter 3.5M Elster American Meter AL-425 Elster American Meter AL-800 Elster American Meter GT-3 Elster American Meter RPM Series 1.5M Elster American Meter RPM Series 2M Elster American Meter RPM Series 3.5M EMC CLARiiON CX4-120 Emerson M-Series MD Plus Encorp KWS GDU Encorp KWS2222501 Encorp UPC GDU Endress+Hausser Promass 80 Endress+Hausser Prowirl 72W EPSON FX 2190 Fireye Nexus NX6100 Flygt ITT Industries APP 700 APP700F Fuji HDC 500 Fuji Micrex-F F120S F120S Fuji Micrex-SX SPH3000MM Gamewell 1033502501VD General Electric 16SB1BB339SSS2V General Electric 16SB1CB201SDM2Y General Electric 510-0183-01A General Electric 526-2006 General Electric IC695ETM001 General Electric Fanuc 90-30 IC693CPU311 General Electric Fanuc 90-30 IC693CPU311-AD General Electric Fanuc 90-30 IC693CPU311-AE General Electric Fanuc 90-30 IC693CPU311-BE General Electric Fanuc 90-30 IC693CPU311N General Electric Fanuc 90-30 IC693CPU311T General Electric Fanuc 90-30 IC693CPU311W General Electric Fanuc 90-30 IC693CPU311-XX General Electric Fanuc 90-30 IC693CPU311Y General Electric Fanuc 90-30 IC693CPU350 General Electric Fanuc 90-30 IC693CPU352 General Electric Fanuc 90-30 IC693CPU360 General Electric Fanuc 90-30 IC693CPU363 General Electric Multilin 469 General Electric Multilin 750P5G5S5HIA20R General Electric Multilin SR489-P5-HI-A20 General Electric Multilin SR74555HI485 General Electric PACSystems RX3i General Electric PQMII PQMII General Electric RRTD RRTD General Electric Rx3i PacSystem IC694MDL240 General Electric Rx3i PacSystem IC694MDL940 General Electric Rx3i PacSystem IC695ALG112 General Electric Smart Meter kV2c General Electric SR 745 General Electric SR 750 General Electric Versamax IC200CPUE05 Genicom 3850 Hach SC100 Hadax Series 6000 Heliodyne Delta-T Pro Honeywell HC900 Honeywell XL50-MMI Honeywell Excel 5000 Q7055A BNA- Honeywell Excel 5000 Q7750A-2003 Honeywell Excel 5000 XC5010 Honeywell Excel 5000 XCL5010 Honeywell Excel 5000 XL100 Honeywell Excel 5000 XL100C Honeywell Excel 5000 XL20 Honeywell Excel 5000 XL50 Honeywell Excel 5000 XL5010 Honeywell Excel 5000 XL5010C Honeywell Excel 5000 XL50-MMI Honeywell Excel 5000 XL80 Honeywell Excel 5000 XLC50 Honeywell Excel 5000 XLC5010 Honeywell Excel 5000 XLC50-MMI Honeywell Excel 5000 XLC8010 Honeywell Excel 5000 XLC8010A HP HP 700/43 HP 8100 ELITE HP Color LaserJet 4500 HP Color LaserJet CP2025 HP Deskjet 6122 HP InkJet BC354A HP Jetdirect 170x J3258B HP LaserJet HP LaserJet 02461A HP LaserJet 4 HP LaserJet 4600n HP LaserJet 4MV HP LaserJet 5 C3916A HP LaserJet 5200tn HP LaserJet C3980A HP LaserJet CB94A HP LaserJet CP2025 HP LaserJet CP2025DN HP LaserJet CP5225DN HP LaserJet P1102W HP LaserJet P2015 HP LaserJet P4014dn HP OfficeJet 7000 E809a HP Officejet CM755A/8500A HP StorageWorks Tape Array 5300 HSQ Technology HSQ Technology 22501 HSQ Technology 86004862 HSQ Technology 8600-4862 HSQ Technology 8600-6135L HSQ Technology 8602 HSQ Technology 8602-080 HSQ Technology 8602-080A Rev E HSQ Technology 8602-RTU-080-A Rev E HSQ Technology HSQ9588T HSQ Technology V86VR-R030 iEi Technology AFOLUX LX AFL-12A Infinias Intelli-M eIDC Invensys Invensys I/A Series FCM 10E Invensys I/A Series UNC-520-2 ITRON IX100X Johnson Controls Johnson Controls Facility Explorer FX-PCG2611 Johnson Controls M Series MS-N30 Supervisory Controller Kiltech Embedded Field Controllers SX-CPU/RS-485 190715 Koyo DL205 Koyo DL206 Koyo DL207 Koyo DL250 CPU Landis & Staefa Integral MS2000 NRK16-NICO Landis & Staefa Integral RSA NRK16/A Lantronix Lantronix Universal Device Server UDS100 Lexmark Optra E312L LG V-NET PQNFB17B0 Liebert StieLink 12 Liebert StieLink 4 LOYTEC Electronics LINX LINX-101 LOYTEC Electronics L-VIS LVIS-3E100 LOYTEC Electronics L-VIS ME215 Maple Systems OIT3175 Maple Systems OIT3250-B00 Maple Systems PC217B Mcquay H62PY McQuay Maverick I OM 1077 MCS MCS-R010 MechoShade Systems SunDialer I-Con Meidensha ADC5000 Meidensha T01E-E01A Meidensha T01E-E01A-A Meidensha Uniseque RC500 MGE UPS SYS UPS 1500 MGE UPS SYS UPS 800 Mitsubishi Mitsubishi AG-150A Mitsubishi MP-22-AF Mitsubishi MP-22-AR Mitsubishi MP-22-CB Mitsubishi CITY MULTI BAC-HD150 Mitsubishi CITY MULTI GB-50ADA Mitsubishi MELSEC Q63P Mitsubishi Q Series FX2N Modicon Micro Modicon Momentum 170ADM39030 Modicon Quantum Automation Series 140CPU113 MODICON TSX Quantum Modicon TSX Series TSX3705028 Modicon TSX TSX3705028 Motion Control Engineering Motion Control Engineering 24-10-0012 Motorola MOSCAD-L Motorola SCADA Systems ACE3600 Moxa MGate IMC-101-M-SC Nalco Switch 2226 3D Trasar NETGEAR ReadyNAS 3200 NETGEAR ReadyNAS Pro NOVAR NL INC B541200039 NovaTech Orion5r Obvius Holdings AcquiSuite A8812 Odessa Engineering DiaLog Plug Okidata MicroLine 321 Turbo Okidata MICROLINE ML420 OMNTEC OEL8000II OEL8000IIP Opto 22 Opto Brian Panasonic BB-HCM531 Panasonic GN 15 Panasonic i-Pro WV-NP244 Panasonic i-Pro WV-NS202A Panasonic i-Pro WV-NW964 Patton Copper Link 2156 Perle IOLAN SCS PML ION7350 PML PowerLogic ION7300 PML PowerLogic ION7330 PML PowerLogic ION7350 PML PowerLogic ION7500 PML PowerLogic ION7550 PML PowerLogic ION7600 PML PowerLogic ION7650 PML PowerLogic ION7700 PML PowerLogic ION8600 Pneu-Logic 10A22646 Pneu-Logic PL4000 DCM Powerlynx OEM Preferred Instruments PCC-III Preferred Instruments PCC-III-0000 Preferred Instruments PCC-III-F000 Preferred Instruments PCC-III-FZ00 Pro-Face GP577R-TC11-OY ProSoft MVI46-MNET Qualitrol ITM 509 ITM RACO VERBATIM DFP RACO VERBATIM SFP Raritan CompuSwitch CS4R Raritan Dominion KX II 216 Raritan Dominion KX II DKX2-216 Raritan Dominion KX II DKX2-432 Red Lion G308 Red Lion G310C Ricoh Aficio MP C2050 RUGID RUG6D RUGID RUG7D RUGID RUG9 RUGID RUG9B RUGID RUG9D Sanyo Denki SANUPS A11H Schneider Electric 170INT11000 Schneider Electric 171CCS76000 Schneider Electric HMIPSCIDE03 Schneider Electric Modicon M340 Schneider Electric I/A Series MNB-1000 Schneider Electric Magelis XBT GT 2330 Schneider Electric Momentum Processor 171CCC96020 Schneider Electric Momentum Processor 171CCS78000 Schneider Electric Powerlogic CM2000 Schneider Electric Powerlogic CM3000 Schneider Electric Powerlogic CM4000 Schneider Electric Powerlogic ECC Schneider Electric Powerlogic EGX 100 Schneider Electric Powerlogic EGX 200 Schneider Electric Powerlogic EGX 400 Schneider Electric Powerlogic enercept Meter Schneider Electric Powerlogic Energy Meter Schneider Electric PowerLogic ION7330 Schneider Electric PowerLogic ION7350 Schneider Electric PowerLogic ION7500 Schneider Electric PowerLogic ION7600 Schneider Electric PowerLogic ION7650 Schneider Electric PowerLogic ION8300 Schneider Electric PowerLogic PM710 Schneider Electric PowerLogic PM850 Schneider Electric Powerlogic Power Meter Schneider Electric TSX Momentum Schneider Electri chweitzer Engineering Laboratories SEL-2032 Schweitzer Engineer boratories SEL-351S-7 Schweitzer Engineering Laboratories SEL chweitzer Engineering Laboratories

Difference Between DoD & Commercial Products = None!

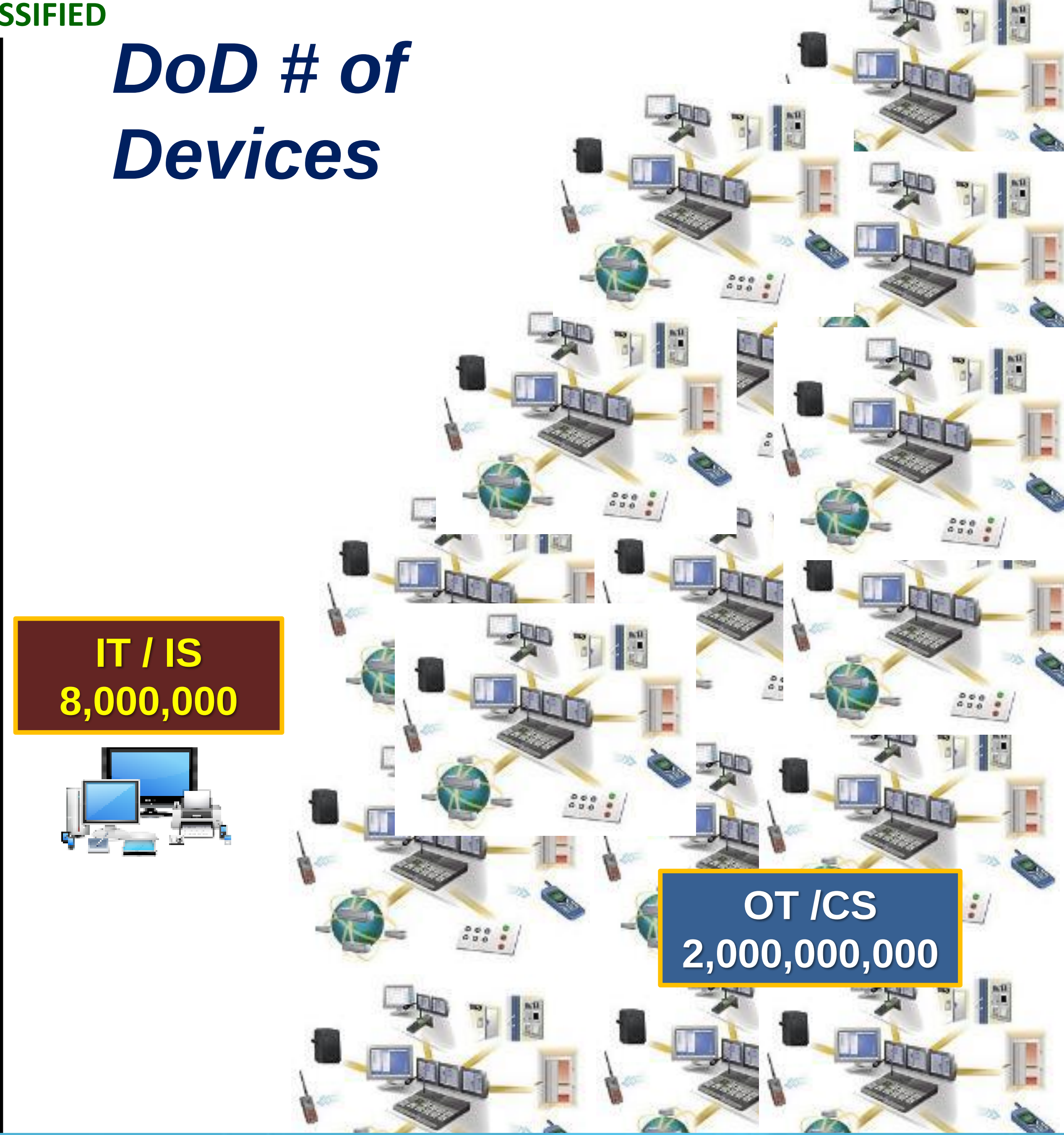
DoD Budget $M



IT / IS
30,000,000,000

OT /CS
150,000,000

DoD # of Devices



IT / IS
8,000,000

OT /CS
2,000,000,000

Recent Headlines…

- ***Marines are testing their Light Armored Vehicles*** looking for vulnerabilities that could put Marines' C4I systems at risk (*meritalk.com*)
- ***'Operation GhostSecret':*** North Korea Is Suspected in Intensifying Global Cyberattack to steal sensitive data from a wide range of industries including critical infrastructure, entertainment, finance, healthcare, and telecommunications (WSJ)
- ***U.K. Sentenced Teenager Who Admitted to Targeting U.S. Officials & Information Using a Social Engineering & Hacking Spree***
  - Secretary of the Department of Homeland Security Jeh Johnson, whose home television was hacked to read "I own you"
  - Tricked call centers run by Comcast, Verizon & U.S. Govt to gain access to individuals' personal accounts / confidential personal information as well as sensitive military / intelligence operations in Afghanistan and Iraq (*govinfosecurity.com*)
- ***Russia seeking to hack into residential routers***
  - FBI and GCHQ confirmed they are "confident" Russia is seeking to hack into residential routers, allowing them to access and monitor all personal internet data including browsing history, passwords and correspondences (*express.co.uk*)

No Longer If You'll Need to Operate in Cyber Contested Environment

What's It Going to Take…?

- ***70% of Energy Firms Worry about Physical Damage from Cyberattacks*** (Dark Reading)

Operational outages and physical injury to employees due to cyberattacks are among the main worries of more than 95% energy and oil & gas firms, according to a recent study of 151 IT and technology (OT) security professionals at energy and oil and gas companies. Of those surveyed, 65% say their organizations properly invest in ICS security, while 56% of those without sufficient security budgets say it would take a major cyberattack to pressure their firm to properly invest in security.

- ***A Lack Of Cybersecurity Funding And Expertise Threatens U.S. Infrastructure*** *(Forbes)*

As our physical infrastructure becomes increasingly digitalized, it also becomes increasingly vulnerable to cyber attack. Most leaders in infrastructure-related industries take cyber risk seriously, but their public sector counterparts need to start addressing vulnerabilities with more urgency. Many experts are already pressuring lawmakers and regulators to take more decisive action across all of our physical systems. Despite this pressure, there are a number of obstacles that need to be addressed alongside the implementation of new policies.

- ***When it comes to zero-day threats, we're all just sitting ducks. Or are we?*** *(Belden)*

If a hacker discovers exploitable software code and there is no patch or workaround yet available, the hacker can wreak havoc while the good guys frantically catch up. The responsibility to stop attacks lies not with the individual device manufacturers, but with the individual OT network operators. After all, it is their organization that is going to suffer the primary financial, legal and reputational fallout. Industrial cyber security should be viewed as an "aftermarket" issue, with operators using internal and third-party resources to secure their networks.

On the Lookout for Malware That Can Kill

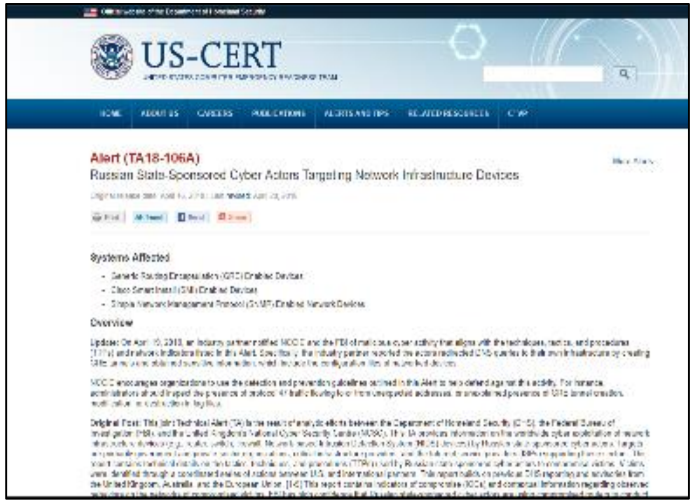
- Dragos & FireEye identified Trisis, a malware that targets a "safety instrumented system," or a machine whose sole function is to prevent fatal accidents.
- I.E: Petrochemical plant - machines operate at very high pressures, and if a valve blows, pressure or the leak of hazardous materials could kill a human being
- One known deployment of the Trisis malware — FireEye called it Triton — at a petrochemical plant in Saudi Arabia Aug’17. But a coding error prevented the malware from working as intended and a potential catastrophe was averted.
- "It's reasonable to assume that [what happened last year] is not a one-time event."

Justin Cavinee in a training room with simulators at Dragos.
BILL O'LEARY/THE WASHINGTON POST

- Dragos recently has identified five nation-state groups outside the United States that are actively targeting industrial systems
- Ability to sabotage industrial equipment — as opposed to stealing information — remains a specialized mission available only to the most highly skilled, best-funded hacking groups

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

Systems Affected

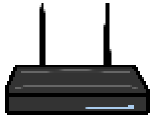
- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

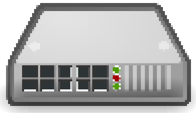
Overview

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 [illegible]

NCCIC encourages organizations to use the detection and prevention guidelines outlined in this Alert to help defend against this activity. [illegible]

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). [illegible]



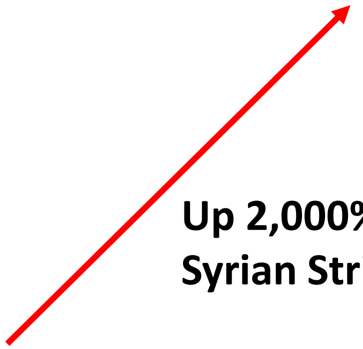


Exploiting:

- Routers
- Switches
- Firewalls
- Network-based Intrusion Detection Systems

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.

Russian "Trolling" Activity



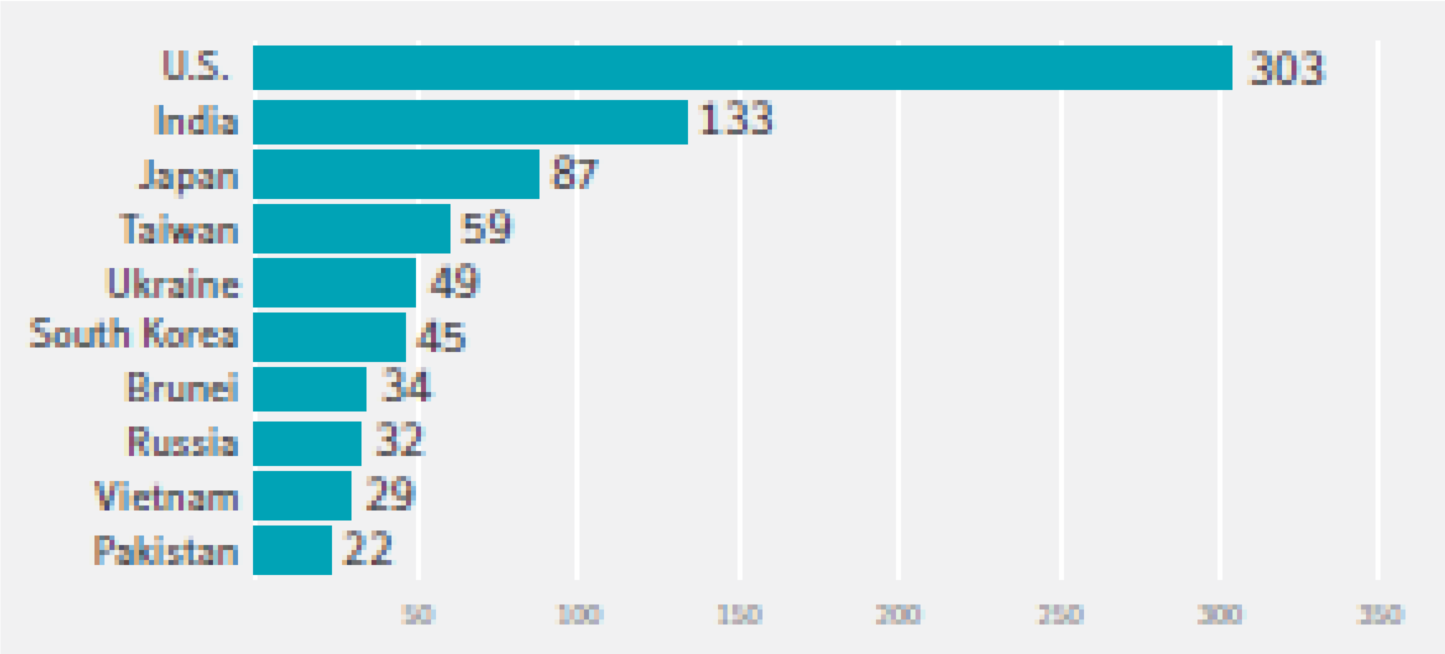
Up 2,000% After Syrian Strike

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

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)

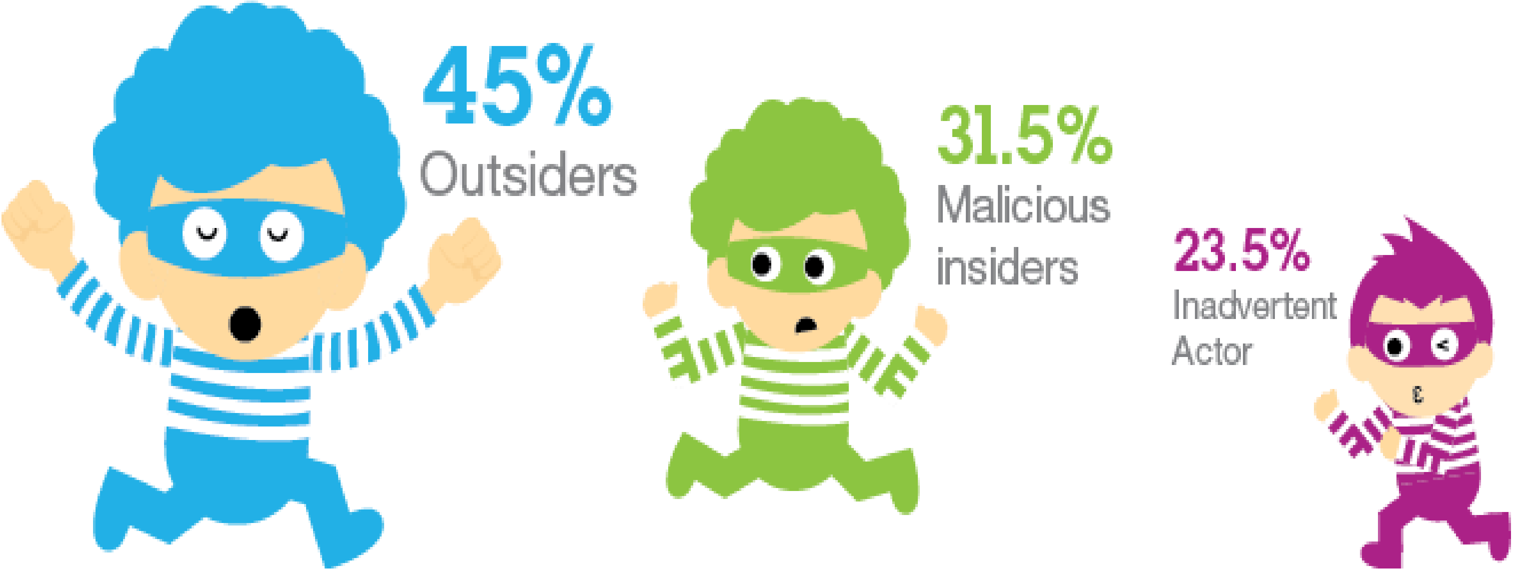


Colorado Dept. of Transportation Hacked

- Ransomware attack – Feb 2018- disrupted agency operations for a week
- State officials had to shut down 2,000 computers
- Affected payroll systems and vendor contracts

Estimated cost of attack= 1.5 MILLION!

- UK's GCHQ now estimates ***34 separate nations have serious, well-funded cyber-espionage teams*** **-** Mark Ward Technology correspondent, BBC News



- 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.

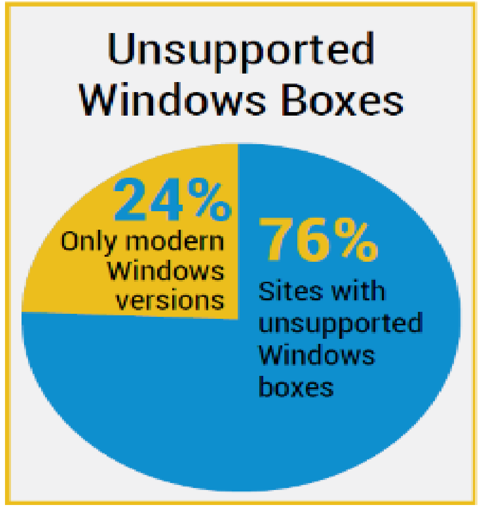
Global ICS & IIoT Risk Report

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

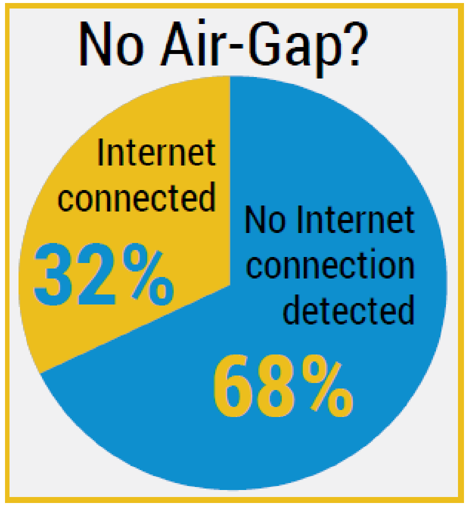
October 2017

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

www.cyberx-labs.com

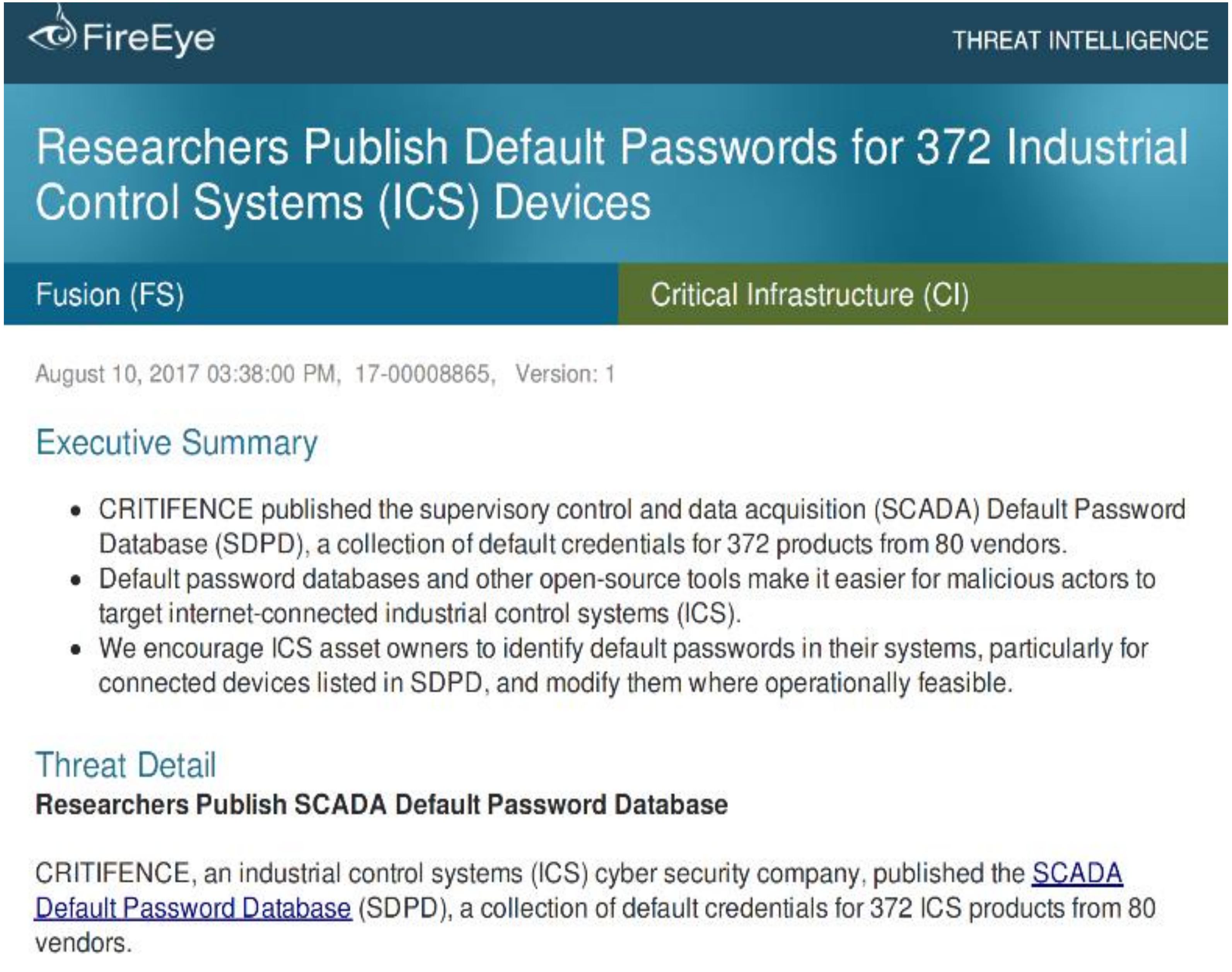


Unsupported Windows Boxes



No Air-Gap?

> **“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.

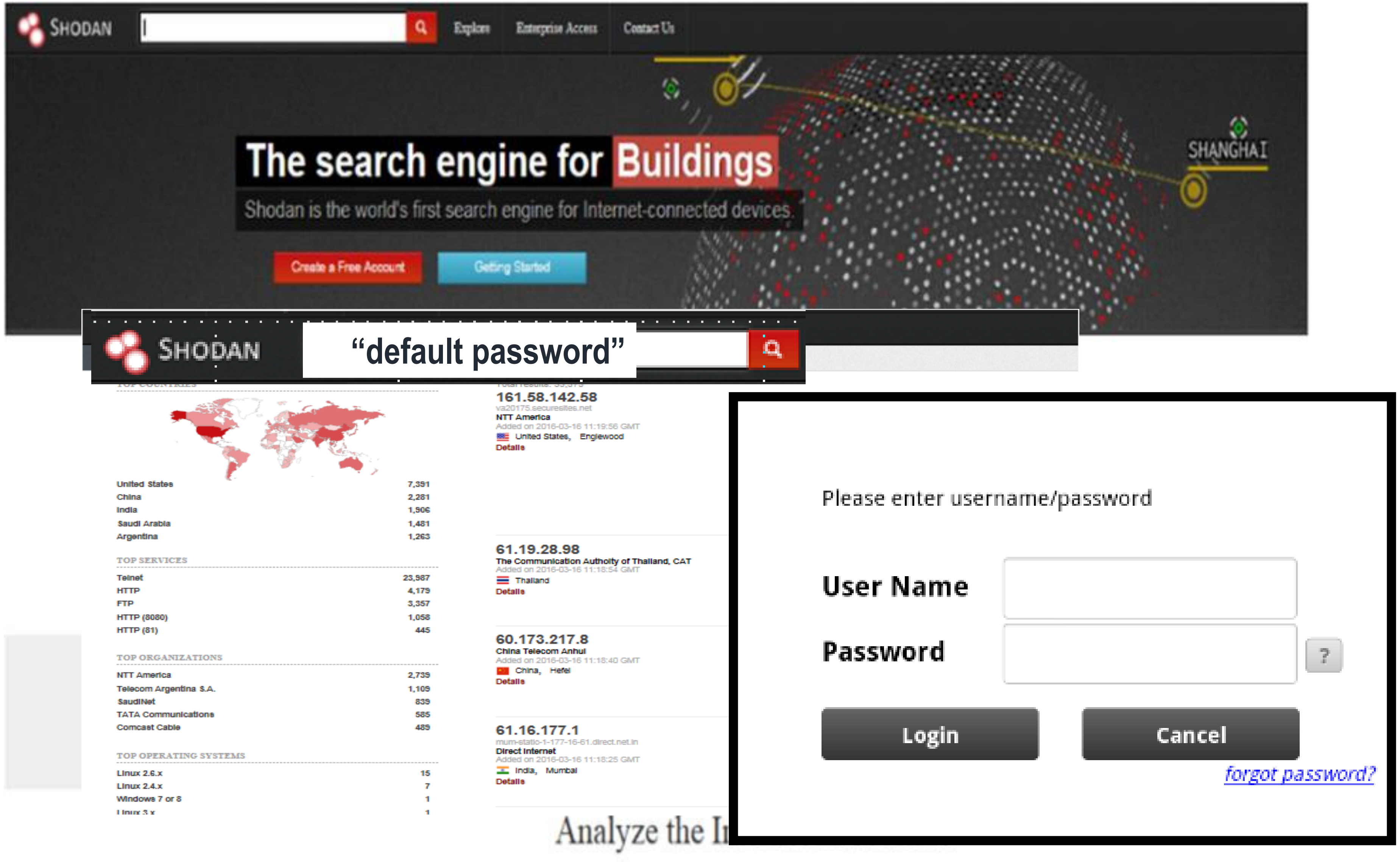
Threat Detail

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

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

61.19.28.98
The Communication Autholty of Thailand, CAT
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

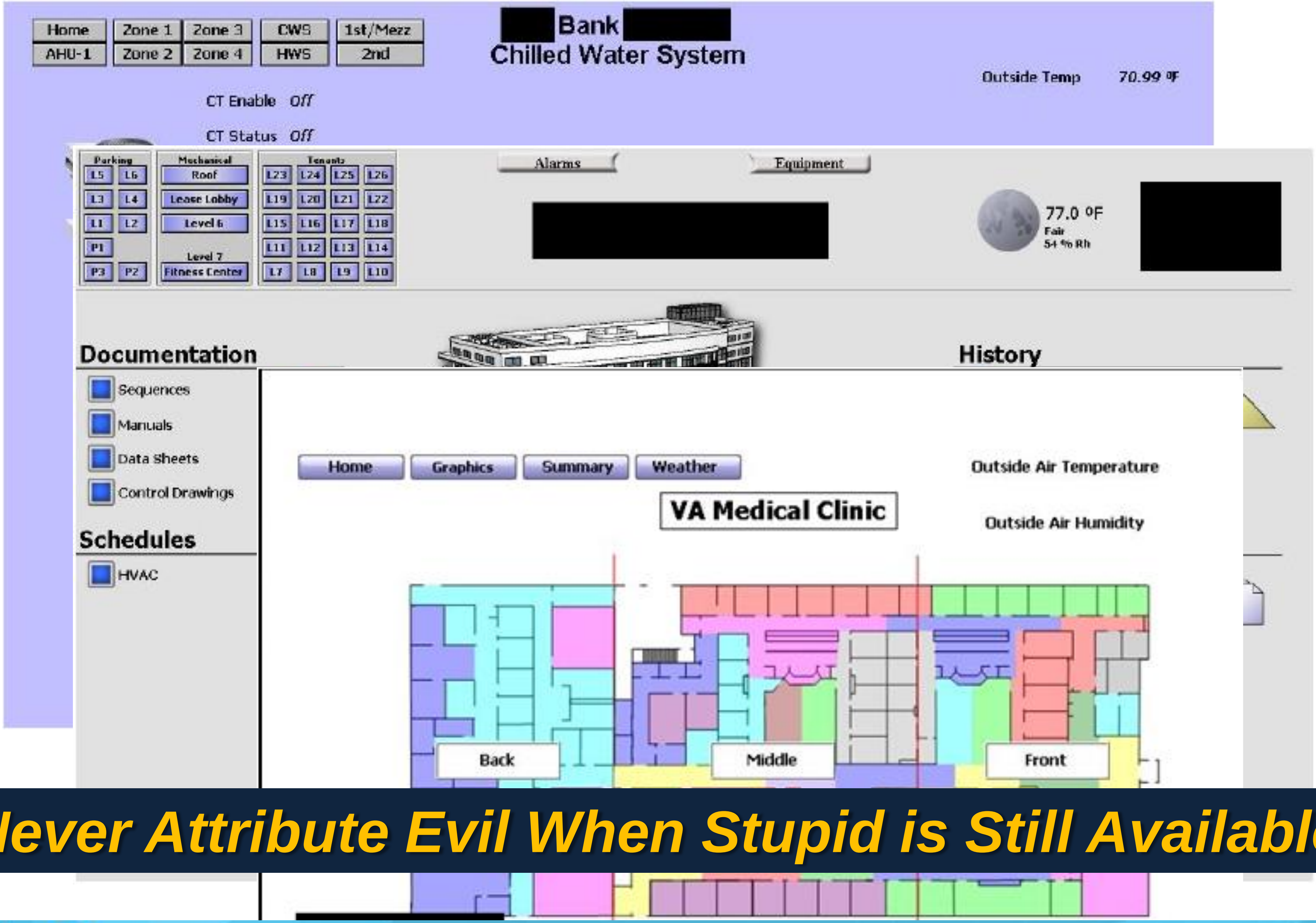
61.16.177.1
mum-static-1-177-16-61.direct.net.in
Direct Internet
Added on 2016-03-16 11:18:25 GMT
India, Mumbai

Analyze the I

Please enter username/password

User Name

Password



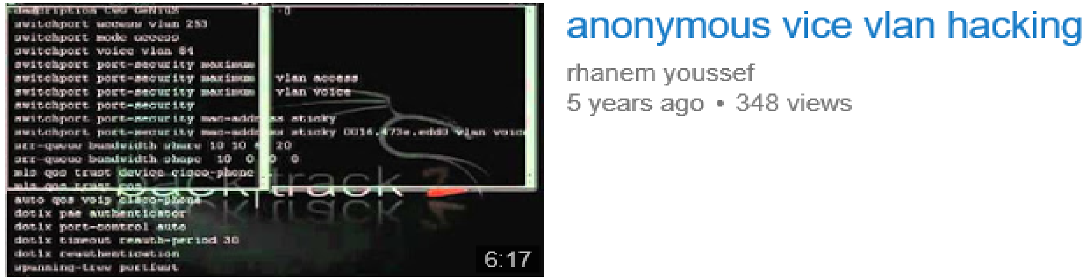
Outside Temp 70.99 °F

CT Enable Off

CT Status Off

77.0 °F
Fair
54 % Rh

Never Attribute Evil When Stupid is Still Available

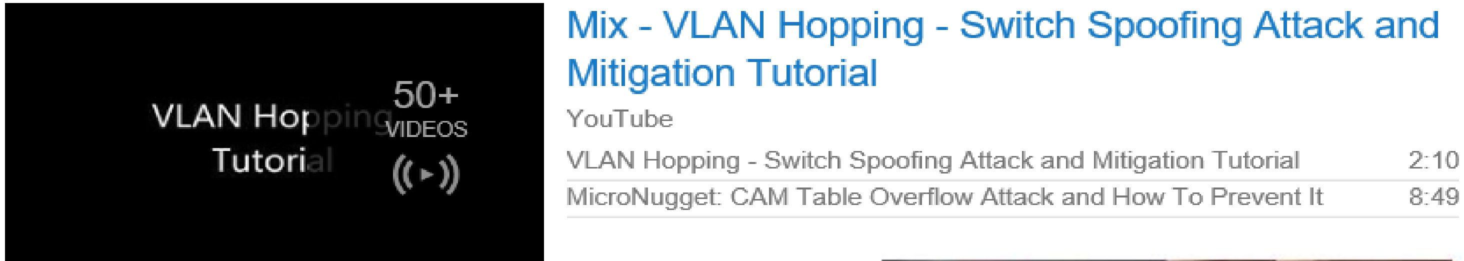


```
description two Genius
switchport access vlan 253
switchport mode access
switchport voice vlan 84
switchport port-security maximum
switchport port-security maximum  vlan access
switchport port-security maximum  vlan voice
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0016.473e.edd0 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



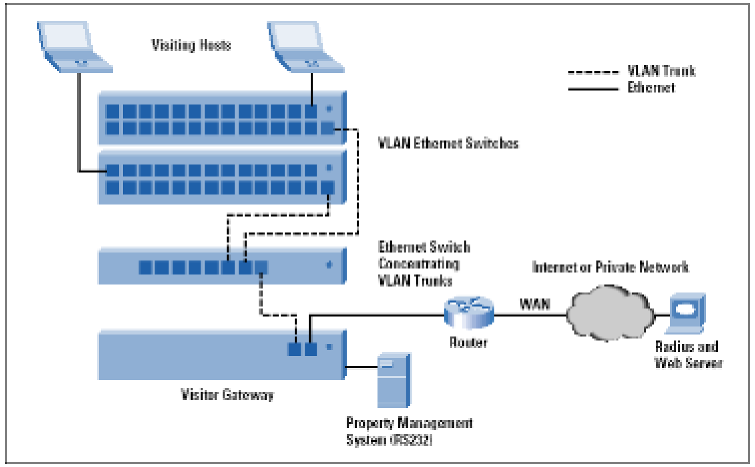
Mix - VLAN Hopping - Switch Spoofing Attack and Mitigation Tutorial

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



Visiting Hosts
VLAN Trunk
Ethernet
VLAN Ethernet Switches
Ethernet Switch Concentrating VLAN Trunks
Internet or Private Network
WAN
Router
Radius and Web Server
Visitor Gateway
Property Management System (RS232)

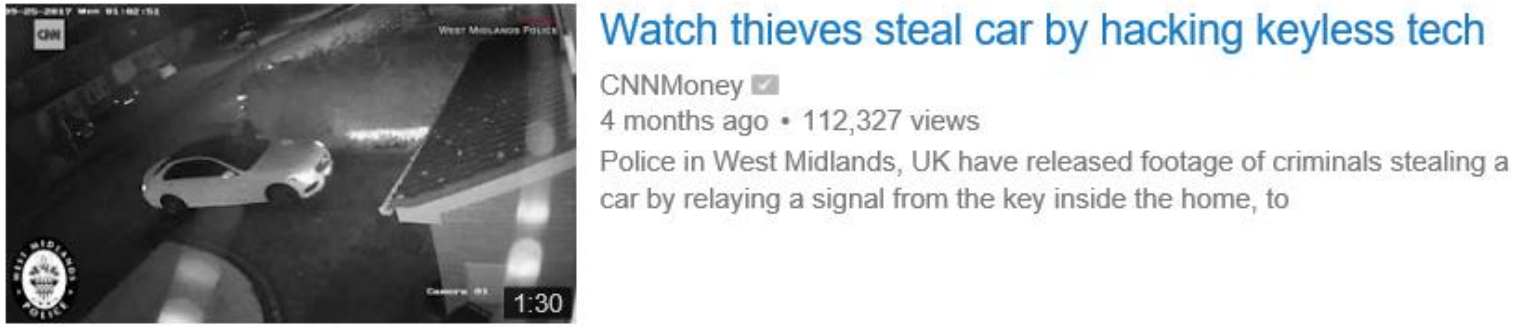
High-tech car theft: How to hack a car (CBC Marketplace)

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

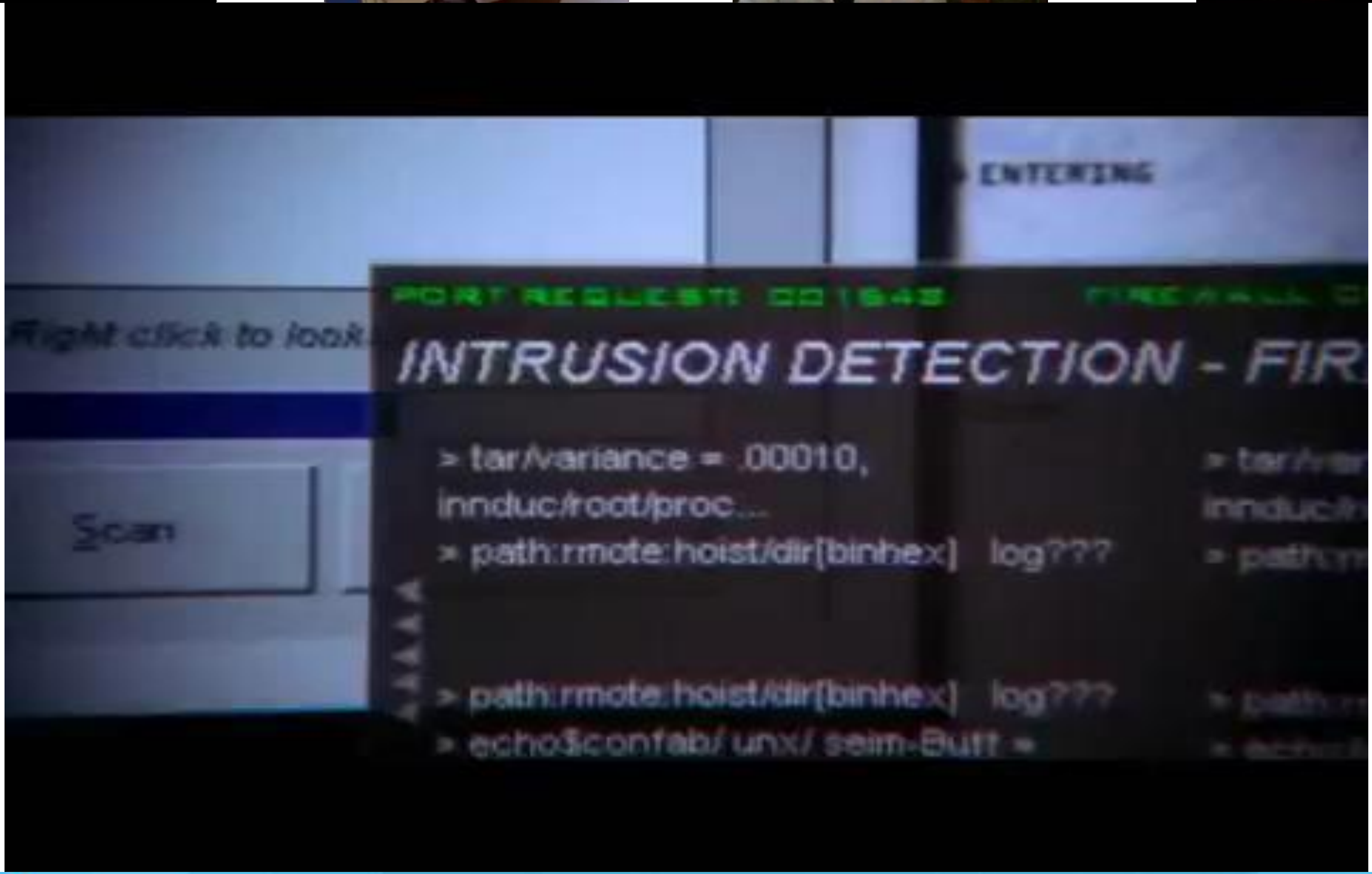


Watch thieves steal car by hacking keyless tech

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

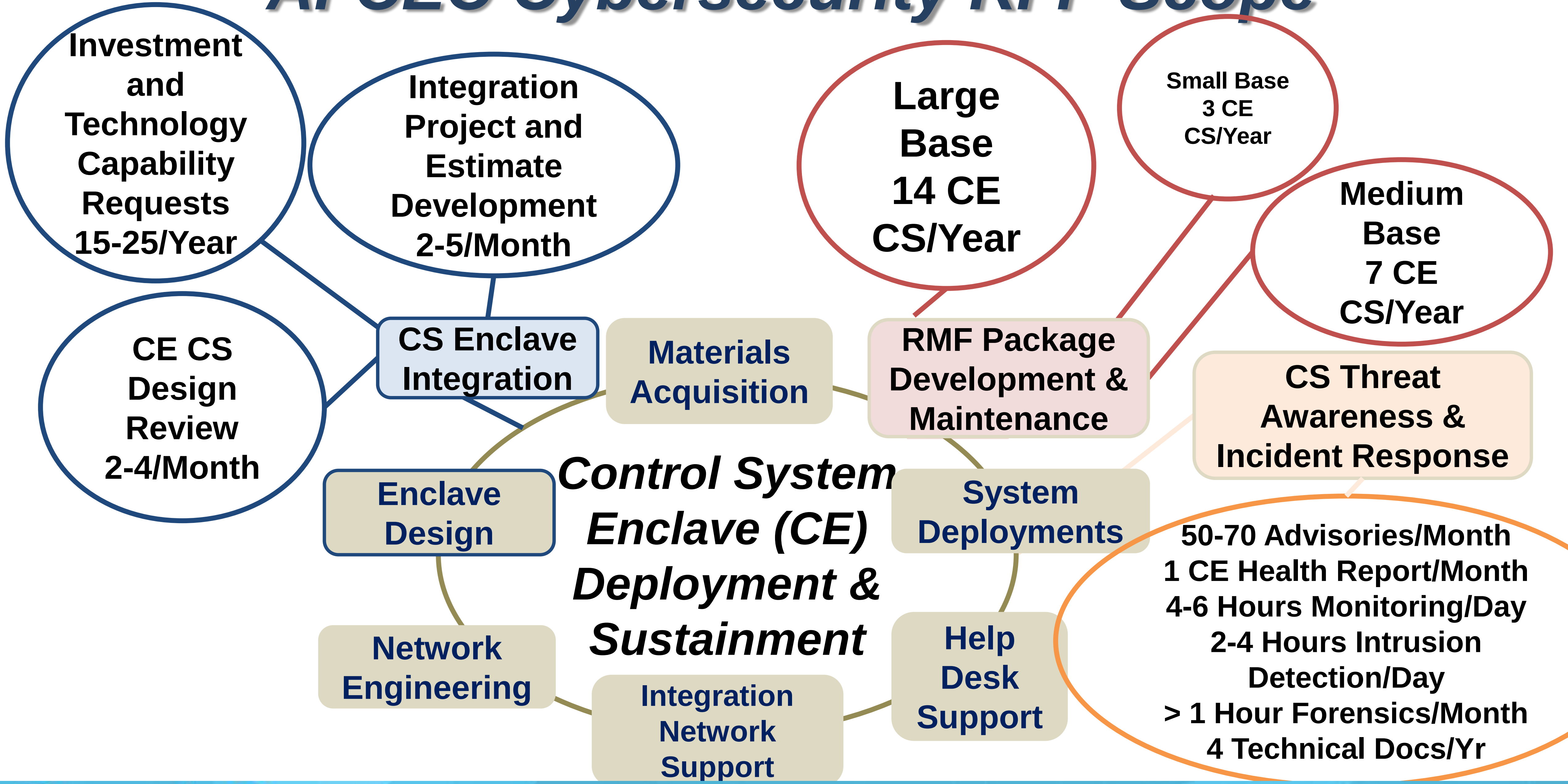


```
PORT REQUEST: 001643          FIREWALL C
INTRUSION DETECTION - FIR

> tar/variance = .00010,                      > tar/var
innduc/root/proc...                           innduc/r
> path:rmote:hoist/dir[binhex]   log???       > path:r

> path:rmote:hoist/dir[binhex]   log???       > path:r
> echo$confab/ unx/ seim-Buff =               > echo
```

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

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

System Deployments

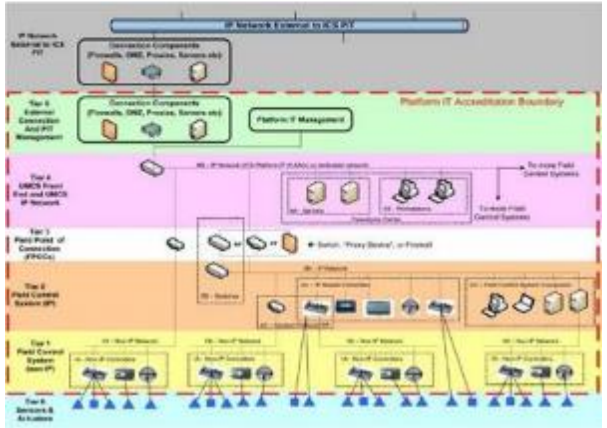
Help Desk Support

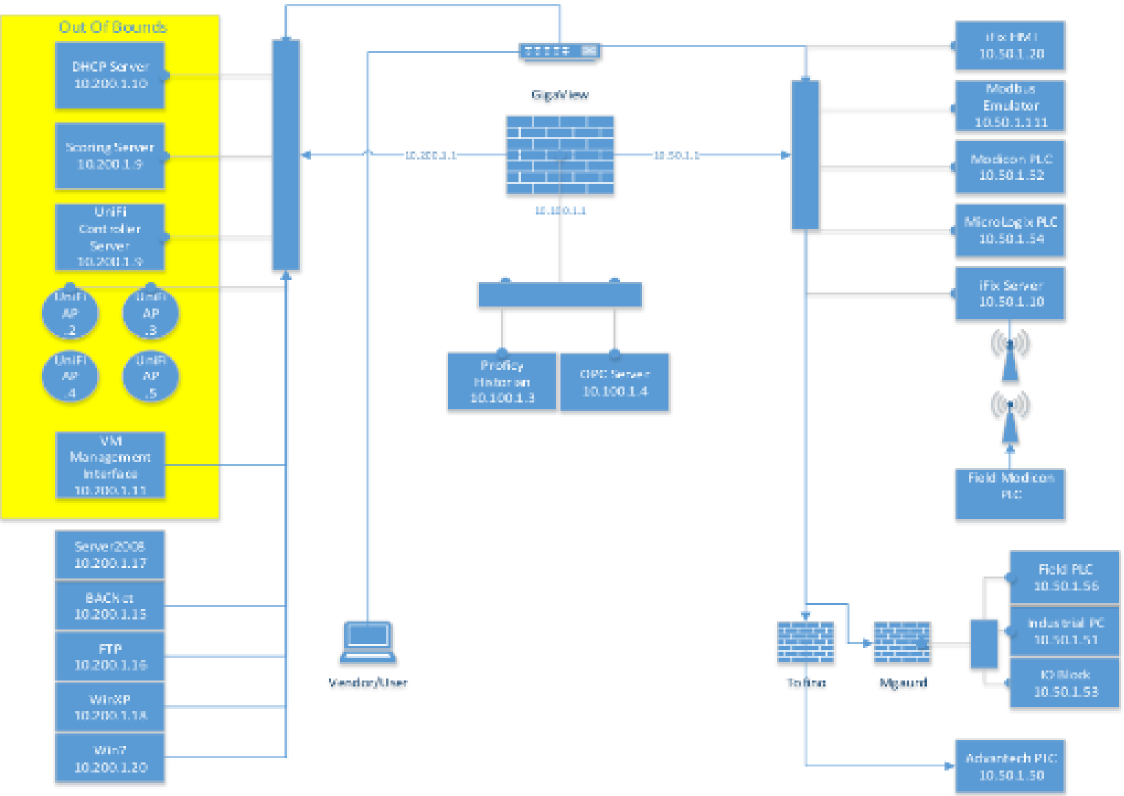
Integration Network Support

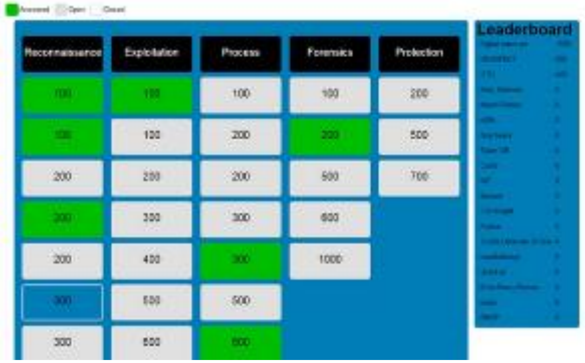
Network Engineering

Enclave Design

SCADA Security Scientific Symposium (S4) Target Network


IP Network External to ICS PIT
Platform IT Accreditation Boundary
Platform IT Management




🟩 Answered □ 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

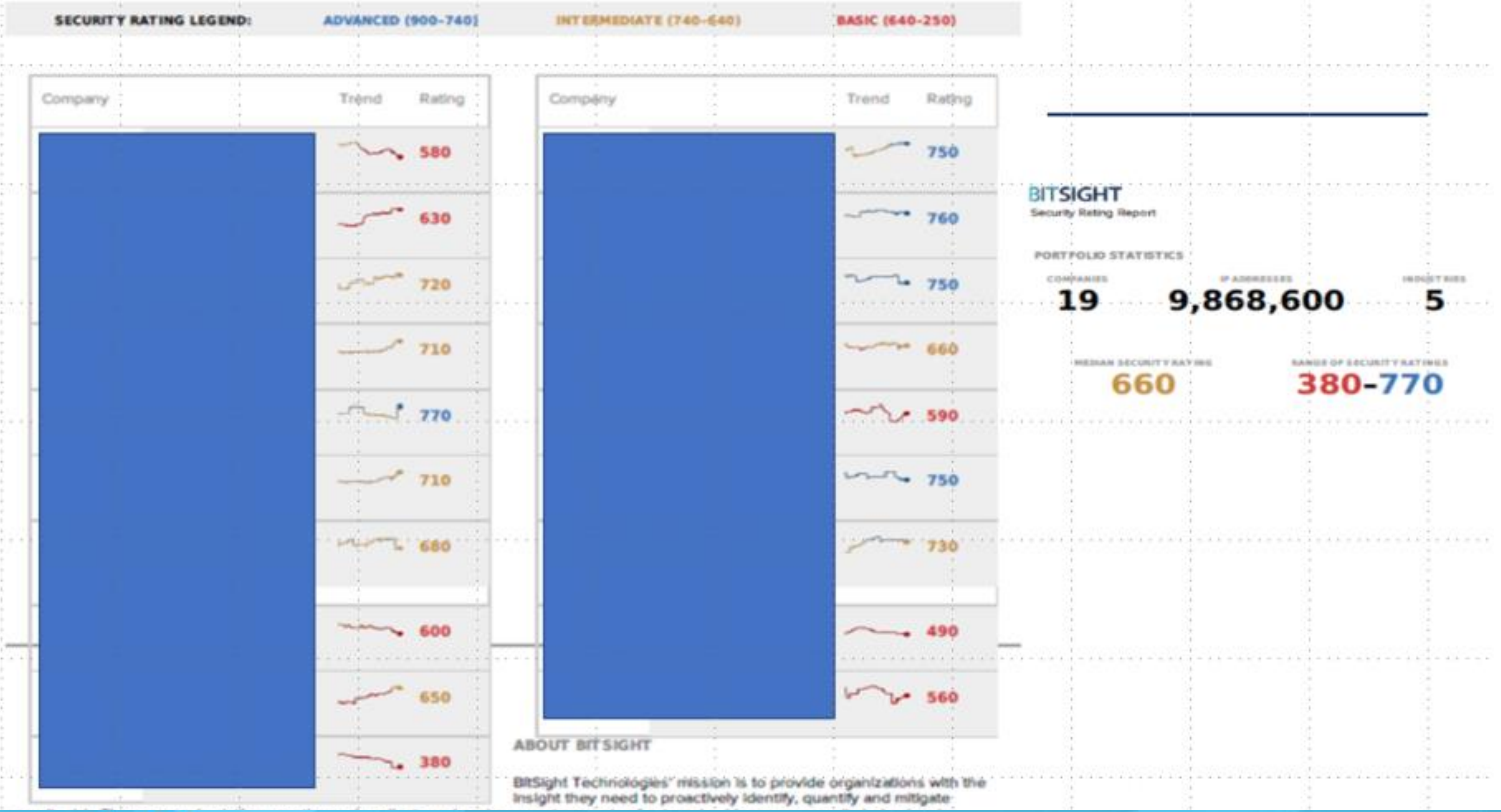
- Corporate Zone
- Domain Controller
- FTP Server
- Windows 7 Workstation
- Windows XP Workstation
- BACnet Controller
- DMZ
- Advantech OPC Server
- Proficy Historian
- Control Zone
- iFix Server
- iFix HMI
- Schnider Electric Modicon PLCs
- Allen Bradley MicroLogix PLC
- ADAM Advantech PLC

Team Name

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

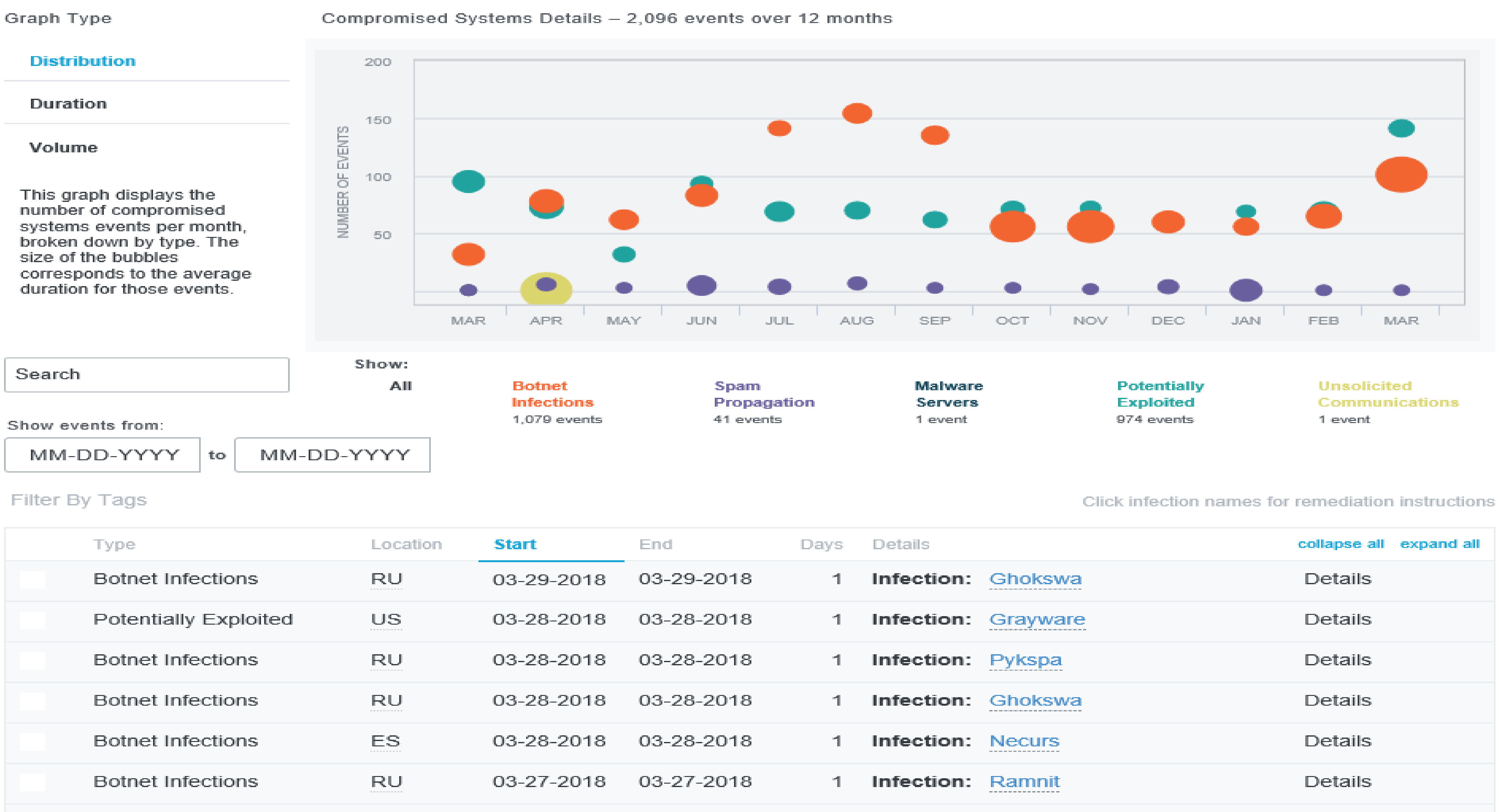
COMPANIES	IP ADDRESSES	INDUSTRIES
19	9,868,600	5

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

UNCLASSIFIED



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

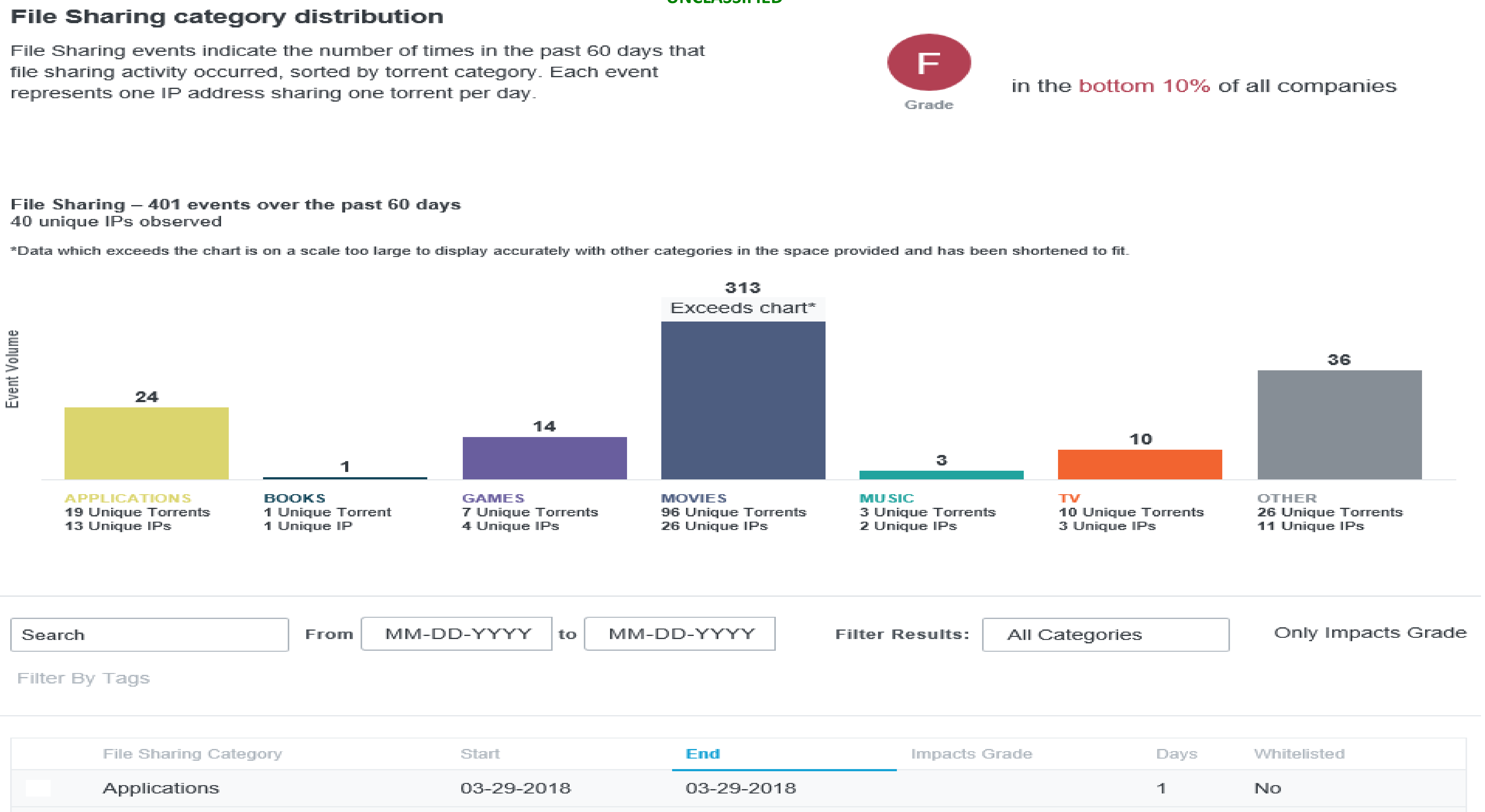
Show:

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



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.

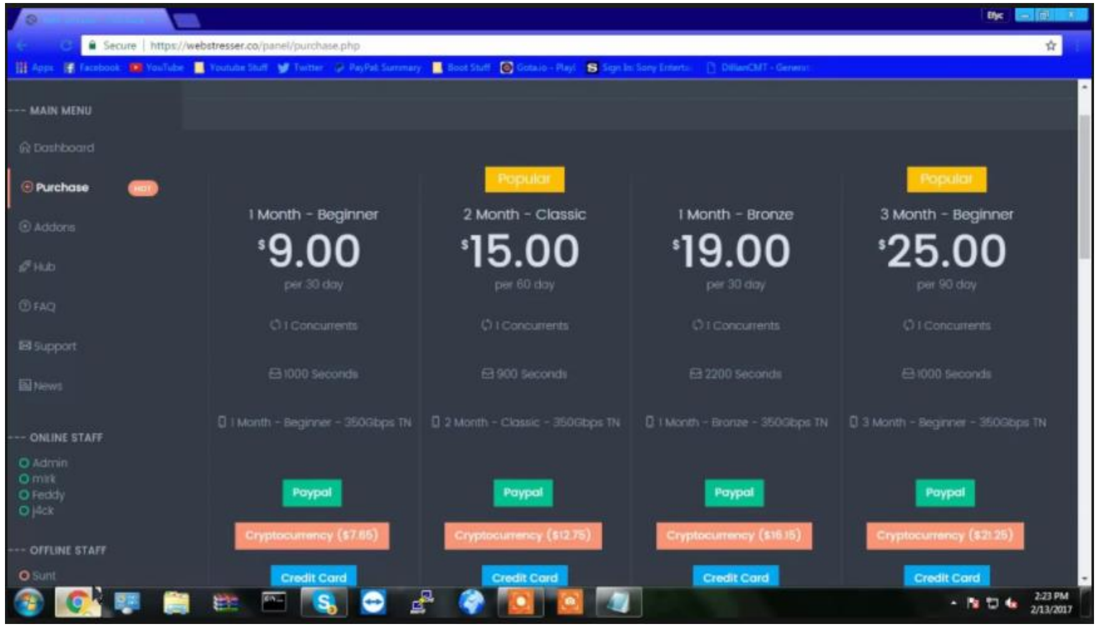
Search From MM-DD-YYYY to MM-DD-YYYY Filter Results: All Categories Only Impacts Grade

Filter By Tags

File Sharing Category	Start	End	Impacts Grade	Days	Whitelisted
Applications	03-29-2018	03-29-2018		1	No

World’s biggest provider of DDoS Attacks Taken Down

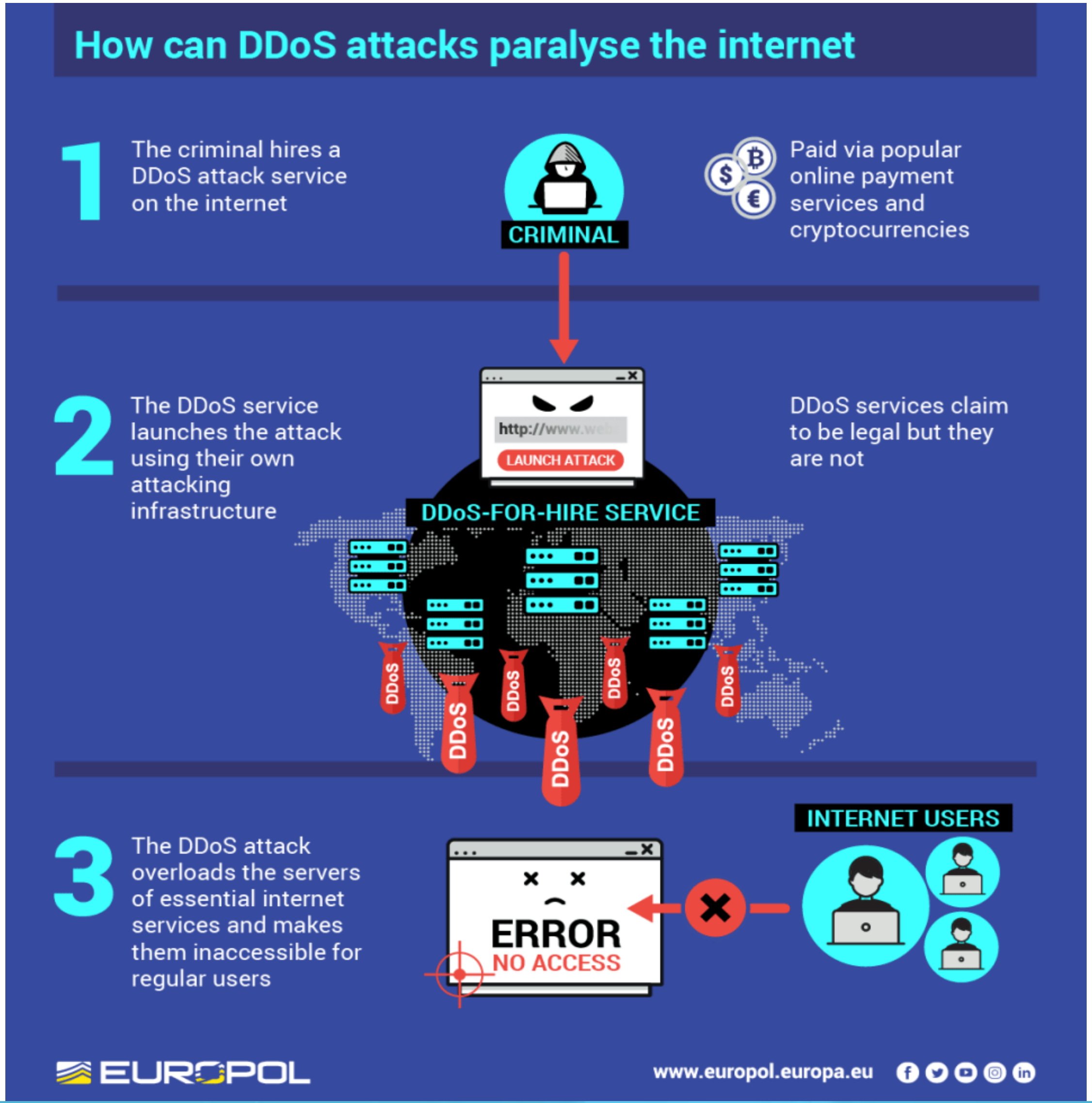
- Webstressor.org administrators taken down in Britian, Croatia, Canada and Serbia.
- Computers & other infrastructure seized in the Netherlands, the US and Germany.



https://webstresser.co/panel/purchase.php

	Popular		Popular
1 Month - Beginner	2 Month - Classic	1 Month - Bronze	3 Month - Beginner
$9.00	$15.00	$19.00	$25.00
per 30 day	per 60 day	per 30 day	per 90 day
1 Concurrents	1 Concurrents	1 Concurrents	1 Concurrents
1000 Seconds	900 Seconds	2200 Seconds	1000 Seconds
1 Month - Beginner - 350Gbps TN	2 Month - Classic - 350Gbps TN	1 Month - Bronze - 350Gbps TN	3 Month - Beginner - 350Gbps TN
Paypal	Paypal	Paypal	Paypal
Cryptocurrency ($7.65)	Cryptocurrency ($12.75)	Cryptocurrency ($16.15)	Cryptocurrency ($21.25)
Credit Card	Credit Card	Credit Card	Credit Card

Webstressor.org had ***more than 136,000 registered users*** and racked up ***more than 4m attacks*** on banks, governments, police forces, and the gaming industry.



How can DDoS attacks paralyse the internet

1 The criminal hires a DDoS attack service on the internet

Paid via popular online payment services and cryptocurrencies

2 The DDoS service launches the attack using their own attacking infrastructure

DDoS services claim to be legal but they are not

3 The DDoS attack overloads the servers of essential internet services and makes them inaccessible for regular users

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

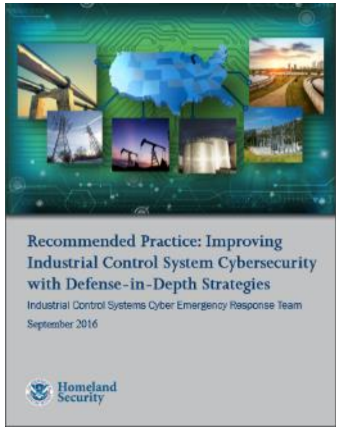
- Routine Monitoring, Inspection, Identification of adversarial presence, Documentation, Notifications

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

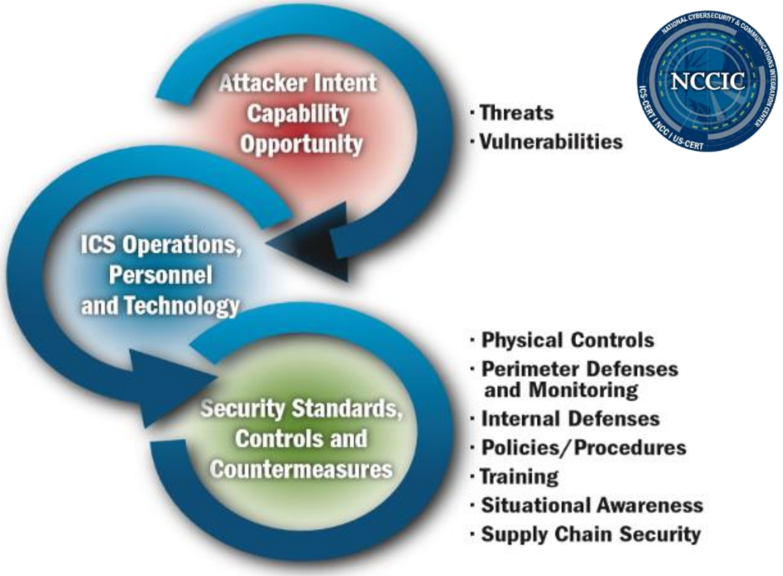


Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response Team

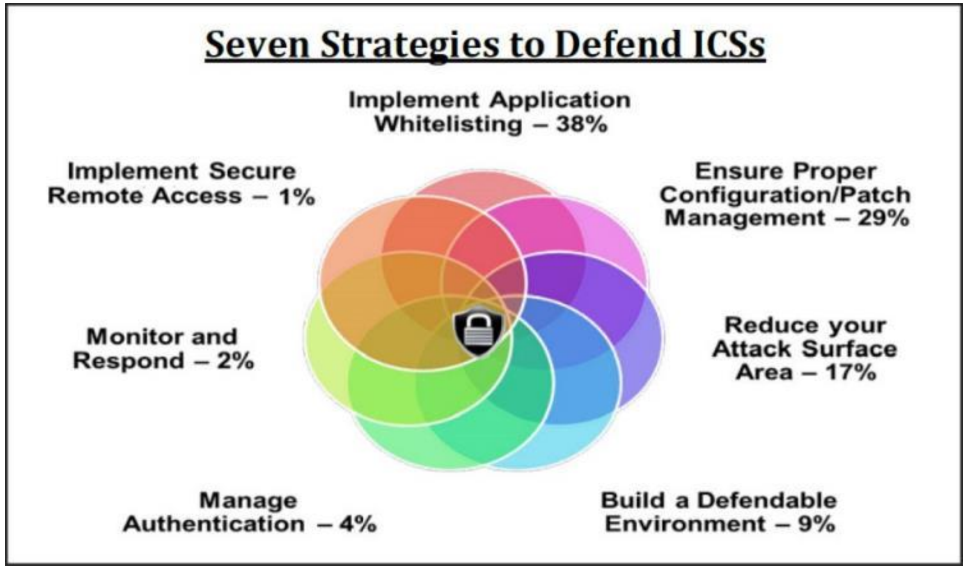
September 2016

Homeland Security


Attacker Intent
Capability
Opportunity
ICS Operations, Personnel and Technology
Security Standards, Controls and Countermeasures

- Threats
- Vulnerabilities

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

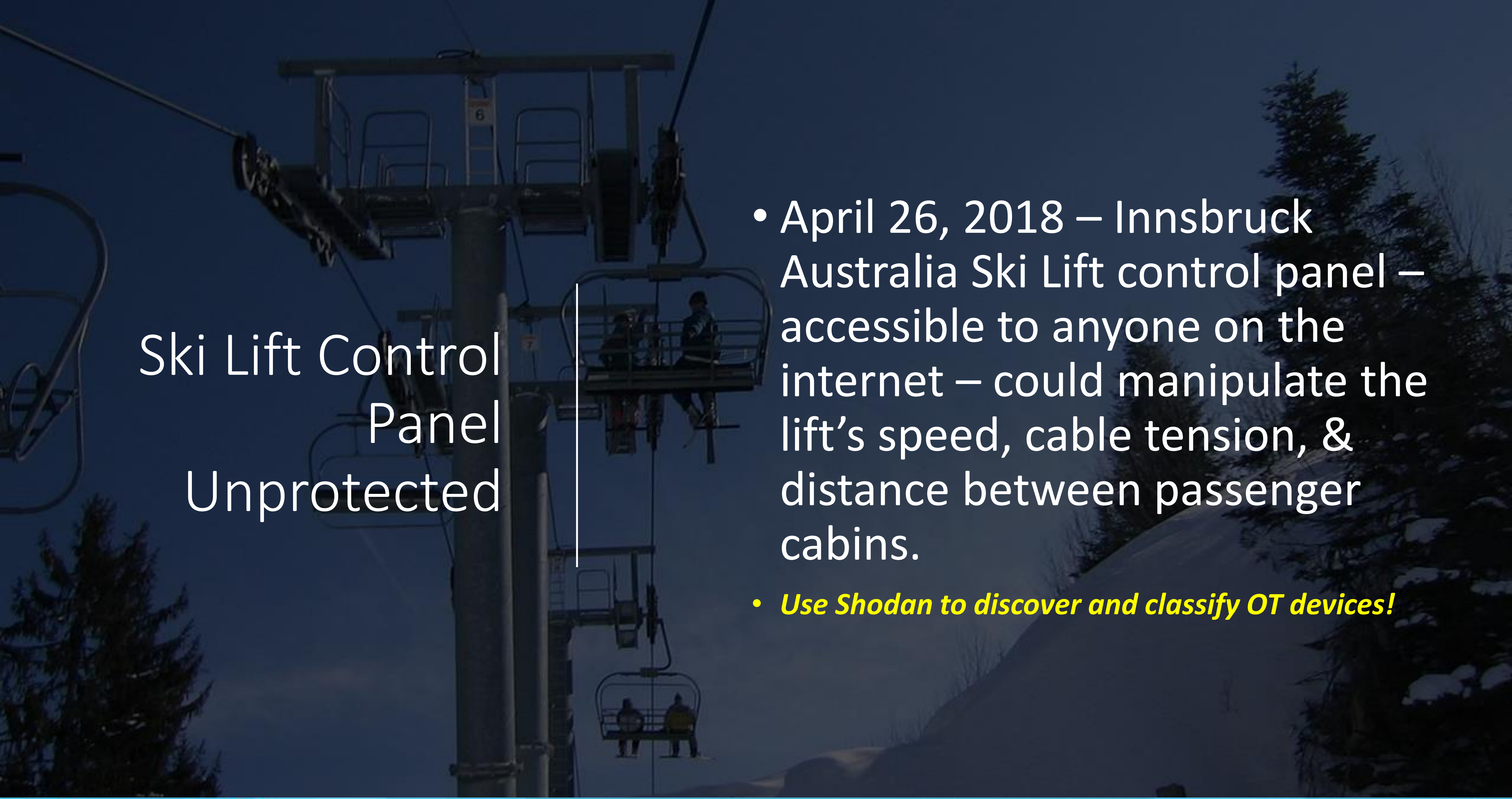


Seven Strategies to Defend ICSs

- 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%

Casino Hacked Via Thermometer

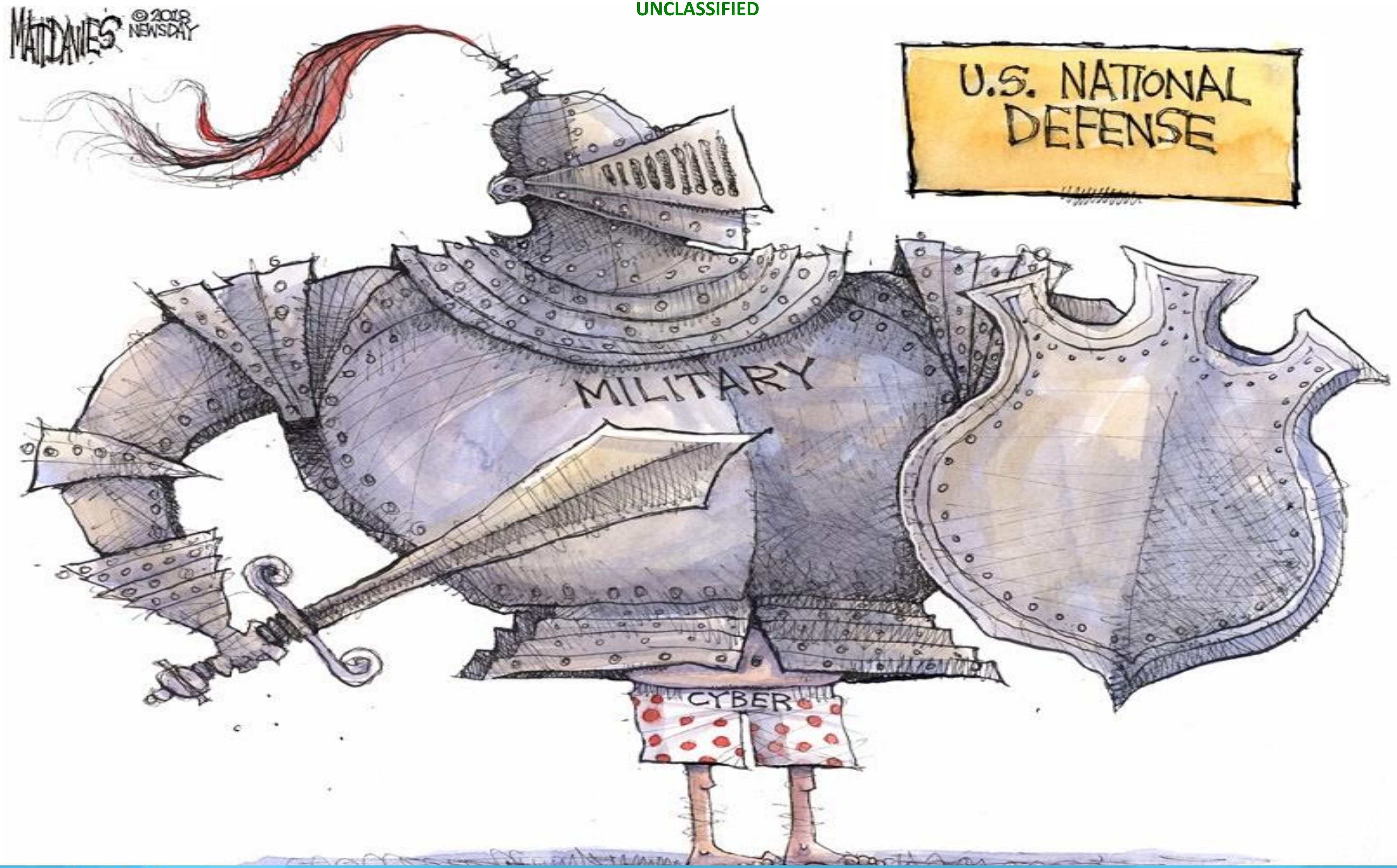
Thermometer in lobby aquarium hacked to pull high roller database to the cloud



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!***

MATT DAVIES © 2018 NEWSDAY
U.S. NATIONAL DEFENSE
MILITARY


MATT DAVIES © 2018 NEWSDAY
U.S. NATIONAL DEFENSE
MILITARY
CYBER

Discussion

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

CYBER ATTACKS AHEAD

Questions

Please wait for the **microphone** before asking your questions

State your **name & organization**

Please don't forget to…

Complete the Post Event Survey

Contact Information

Daryl Haegley GICSP, OCP

Control System Cybersecurity

Daryl.r.haegley.civ@mail.mil

Thank You

OSIsoft®

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

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

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