Are You Ready for Stuxnet 2.0?

:: jonathan pollet – red tiger security

jonathan pollet – CISSP, PCIP, CAP

- **22 Years of Electrical Engineering, SCADA, Industrial Controls, and IT Experience**
  - PLC Programming and SCADA System Design and Commissioning
  - Wireless RF and Telecommunications Design and Startup
  - Front-end Web Development for SCADA data
  - Backend Database design for SCADA data
  - Acting CIO for Major Oil Company for 2 years – Enterprise IT Management

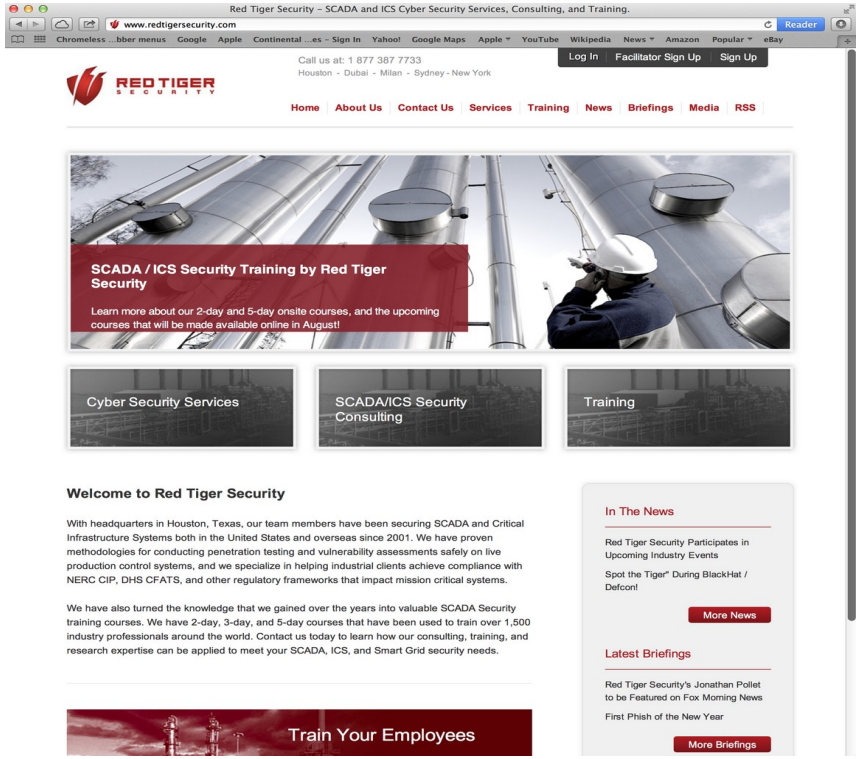
- **Last 17 Years Focused on SCADA and IT Security**
  - Published White Papers on SCADA Security early in 2001
  - One of the 5 people that chartered the ISA99/IEC62443 standard in 2002, and helped review and provide guidance for several cyber security standards for ISA, NERC, NIST, AGA, AWWA, and DOE that have become industry standards
  - Conducted over 300 security assessments on Critical Infrastructure systems
  - Conducted over 125 International conferences and workshops on ICS/SCADA
  - Developed safe security assessment methodology for live ICS/SCADA Systems
  - Trained over 4,000 professionals globally with various ICS/SCADA Training Courses
  - Featured presenter on Fox News Live, Vanity Fair, Popular Mechanics, CIO Magazine, and several security publications

Red Tiger Security

- **Consulting**
  - Penetration Testing
  - Cyber Vulnerability Assessments
  - Network Architecture Analysis / Design
  - Compliance / Security Controls Consulting
  - Cyber Security Advisory Services and Strategic Consulting
  - Development of ISA/SCADA Test Beds (US National Test Bed, Malaysia, Qatar, University of Tulsa, University of Houston, and several private industry clients)

- **Training**
  - 5-Day Advanced Security Course for Critical Infrastructures
  - 2-Day SCADA Security Course (BlackHat)

- **Research**
  - Applicability and Usability of Cyber Security Solutions for SCADA / ICS
  - Product Evaluations
  - Various DHS Research Initiatives for ICS
  - Standards Development



outline

- **Quick Terms and Definitions**
- **Why Cyber Security Matters so much today**
  - ICS/SCADA systems have changed – they are digital and connected
  - the world has changed – its digital and connected
  - threats have changed – they are digital and connected
- **Signs that the spotlight has shifted from traditional IT systems to ICS, SCADA, IoT systems**
  - the number of SCADA Vulnerability Disclosures and Exploits have exploded in the past years
  - 100 SCADA bugs in 100 days
  - ICS-CERT facts and statistics
  - 0-day Market
  - Foreign Governments Using Surveillance, Interception, and Tracking systems on their own people
  - They want access to Critical Infrastructure as well – i.e. Night Dragon example
- **How can bad stuff get in? – SCADA HACKING VIDEO**
- **Proven Process for Developing a Strategic Plan to Secure ICS / SCADA**

terms and definitions

Classification of Various Types of ICS Systems

- Automation: Allowing a process to run efficiently without constant human intervention.
- SCADA: Supervisory Control and Data Acquisition
- DCS: Distributed Control Systems
- SIS: Safety Instrumented Systems
- Power Industry
  - DCS: Distributed Control System
  - EMS: Energy Management Systems
  - DMS: Distributed Management Systems
  - AMR / AMI: Automated Meter Reading / Infrastructure (New technology being implemented as the based for the Smart Grid)
  - Smart Grid
- MES: Manufacturing Execution Systems (used mostly in batch systems)
- BAS: Building Automation Systems
- **ICS: Industrial Control Systems** (most common term used to describe SCADA, DCS, EMS, MES, and all control system family of technologies)

ICS / SCADA systems have changed …



all we had to worry about before was physical access



now ICS / SCADA systems are digital and connected...



modern SCADA systems are running on the same OS as corporate desktops



they send data in the clear, without any requirement for encryption or authentication



ICS/SCADA systems have evolved from proprietary components to the same components used by Corporate IT systems

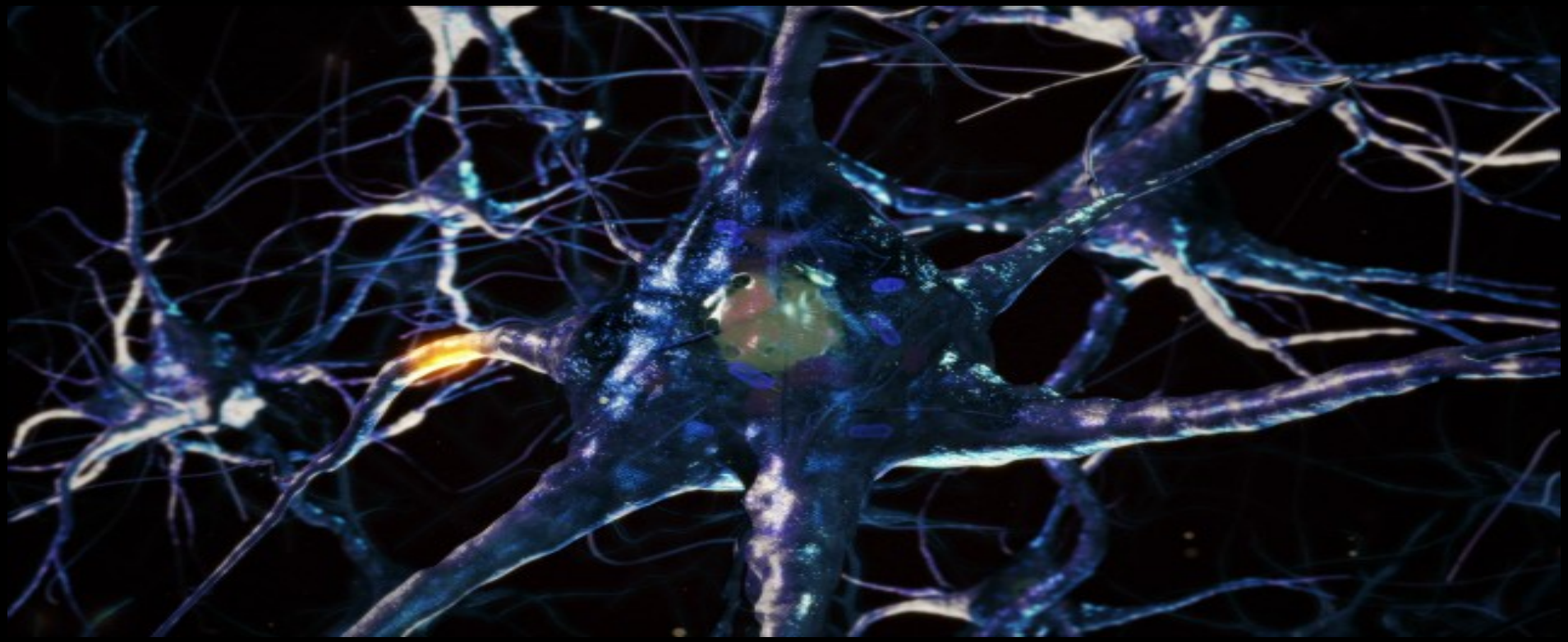


- Cisco ASA firewalls or equivalent
- Cisco switch fabric
- Servers and workstations running on Windows platforms (some still on XP/Server 2000)
- Active Directory
- File/Print servers
- **However…. They often lack the protection that typical Corporate IT systems have**

major world ISP and telecom trunks



malware can spread at the rate of 125 machines per second…



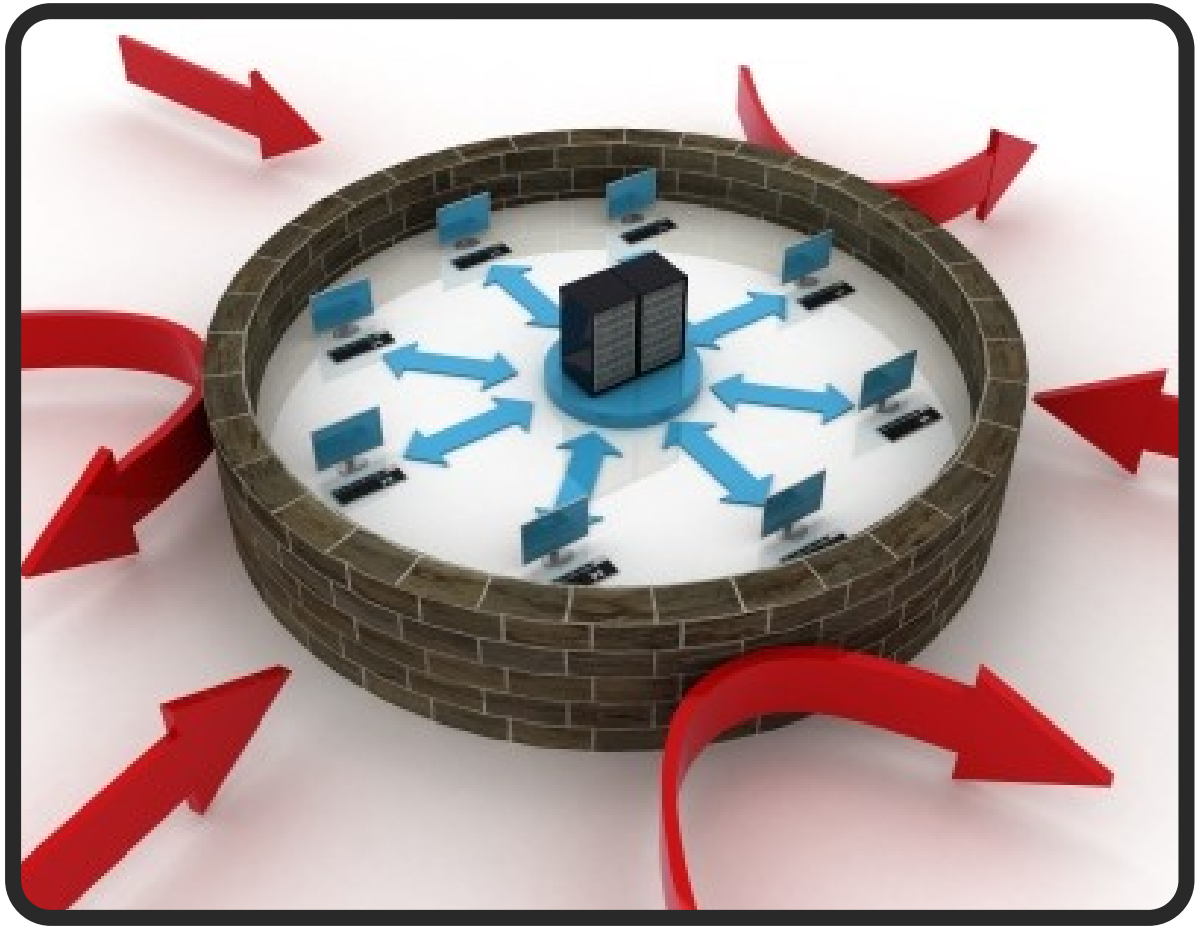
…within ten minutes of the start of the SQL Slammer worm, 75,000 machines were already infected. This included many critical infrastructure systems…

so how does bad stuff get in?

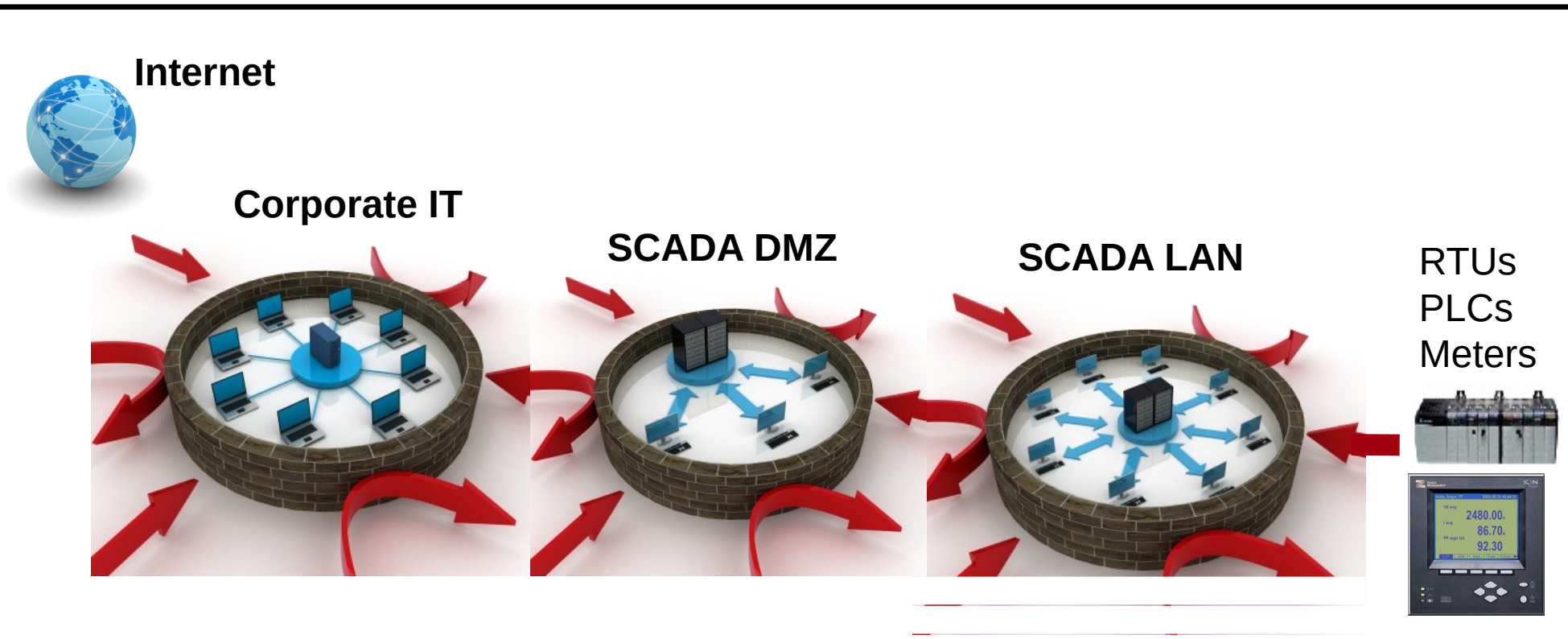
- **perfect security**



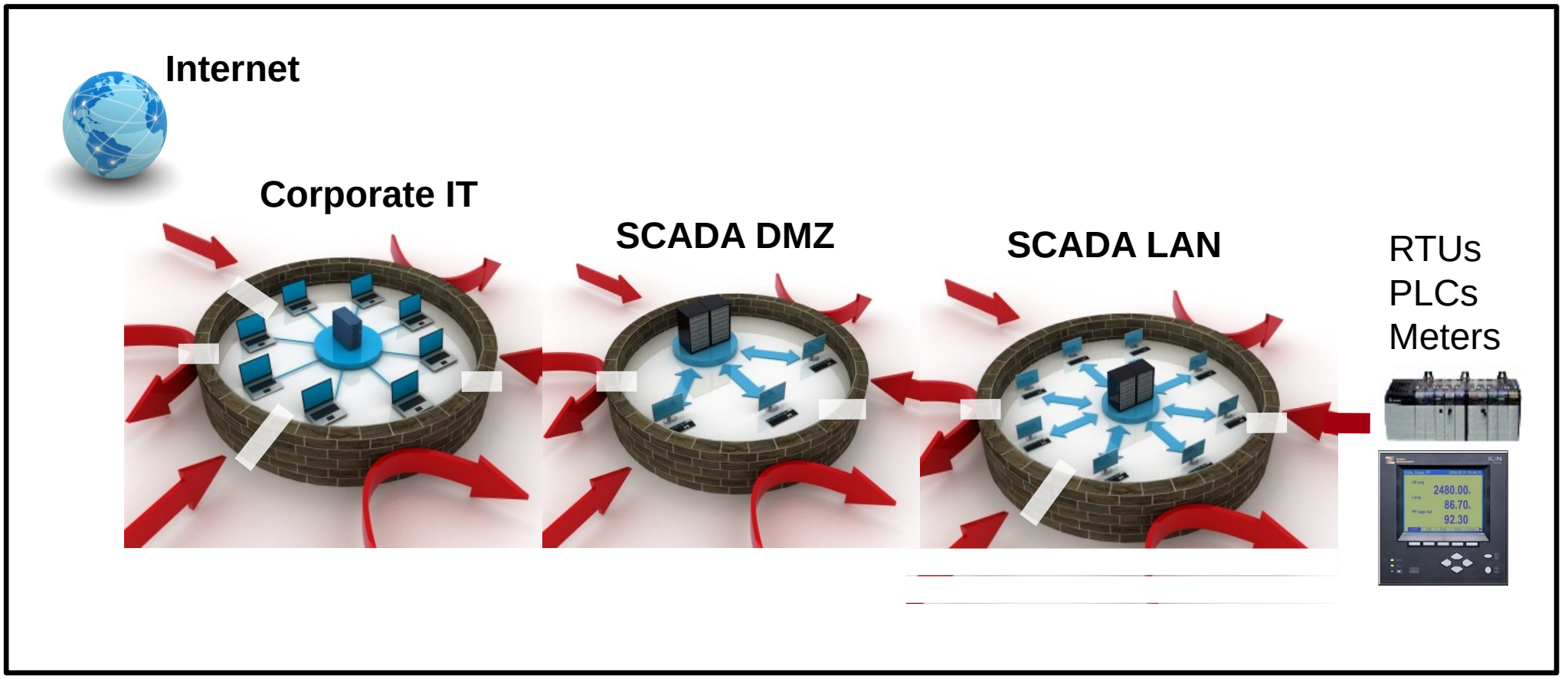
originally, these ICS/SCADA systems were isolated, air-gapped, and running on proprietary systems



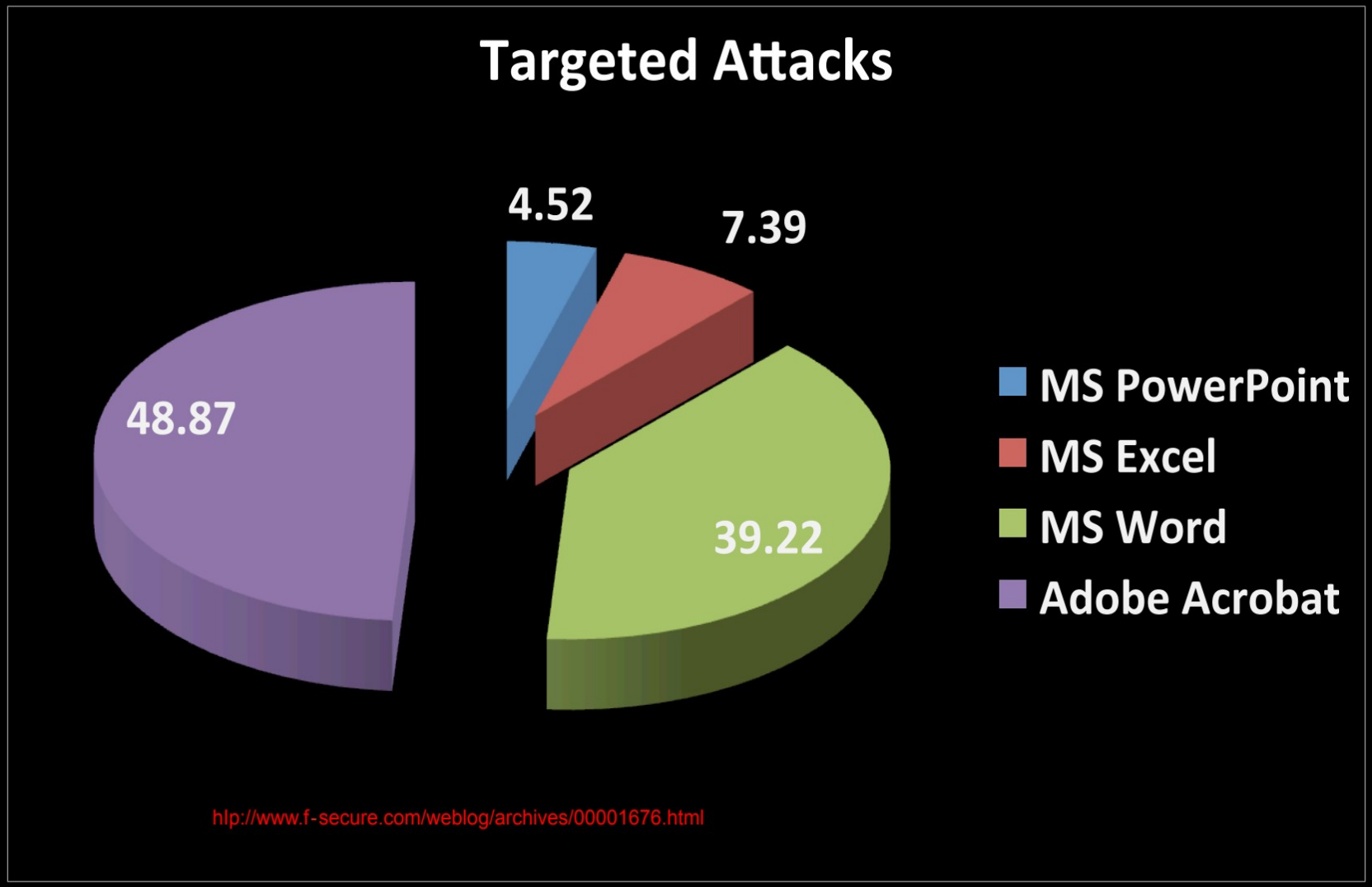
…we have a growing need to share information, and provide remote monitoring/support, so we create islands of operations and then DMZs between security zones



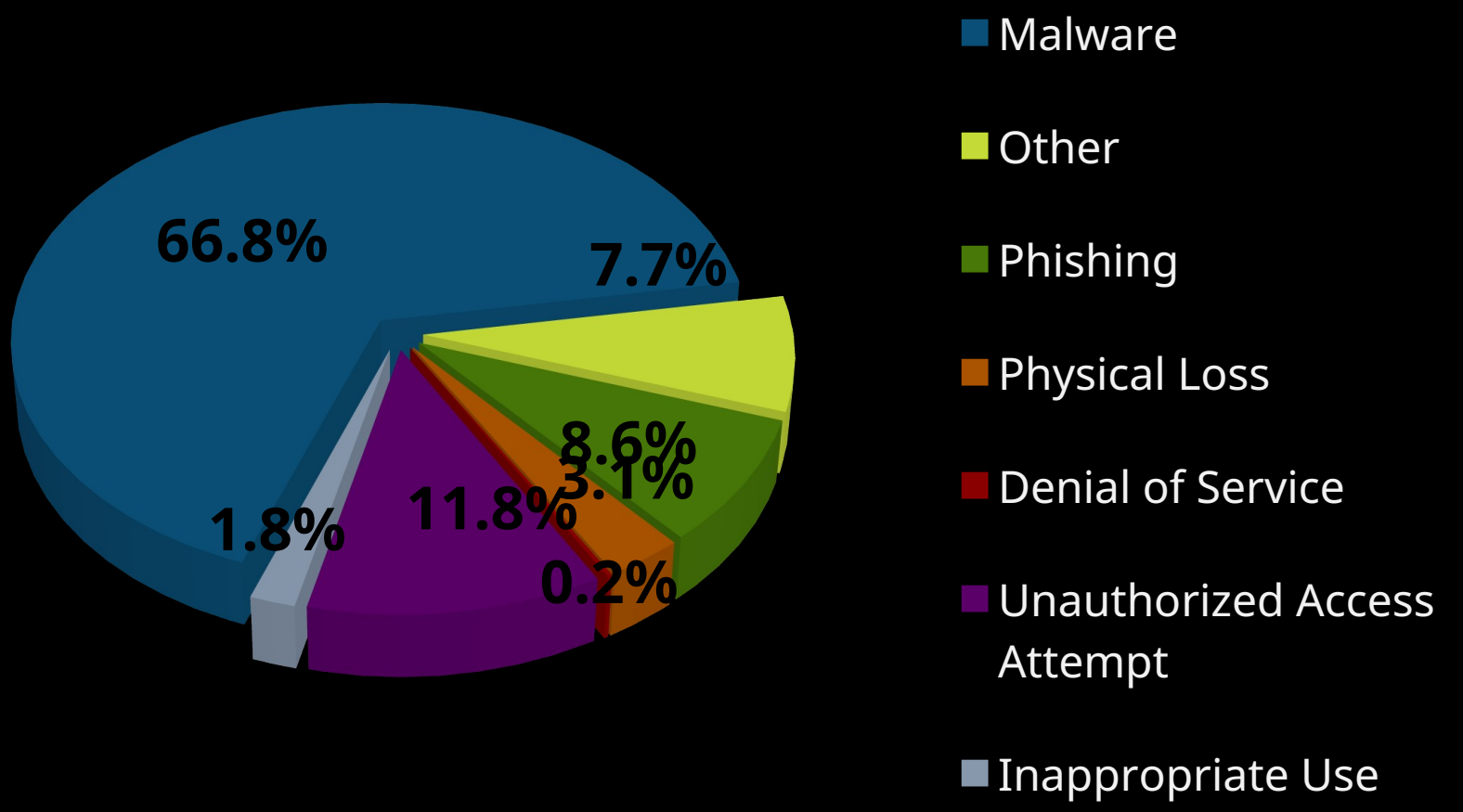
unfortunately, we become under pressure to open holes for communications between what used to be trusted security zones



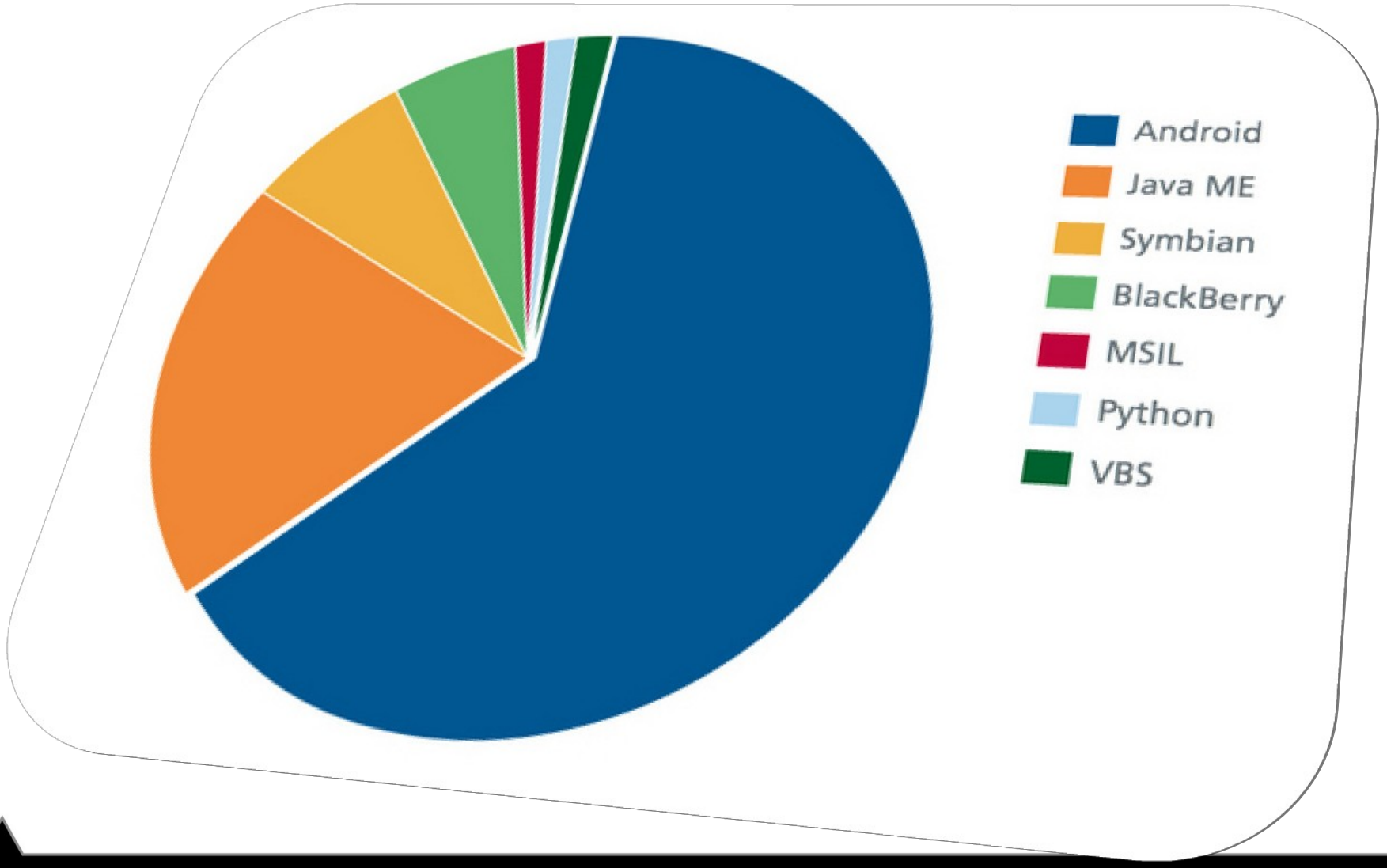
initial attack vector is almost always malware / rootkits, and adobe is still leading the pact



malware still the most utilized attack vector



smartphones = rootkit in your pocket that knows your location, and has access to your email, data, bank accounts, and the Internet



we have to worry about our phones

- **Google pulled more than 50 apps in March from the Android Marketplace after security researcher found a Trojan that used applications to spread.** The Trojan, called DroidDream, infected more than a quarter million Android phones. One sign of a DroidDream infection was resource consumption due to the way the malware exploits the phone.

- ***SOURCE: DroidDream used a fake bowling game to infect devices. Image courtesy of Lookout Mobile Security***



ICS / Systems are Low Hanging Fruit for Security Researchers – why?

- SCADA and ICS Hardware/Software do not go through the same rigorous security lifecycle process as Information Technology systems
- On average, Microsoft will put their software through 100,000 various fuzzing loops and debugging processes to test for crashes and bugs….and yet we still find plenty of vulnerabilities still being discovered and reported for Microsoft software
- Control System vendors, if they actually test their systems for bugs at all, will typically only run their applications through basic regression tests, and this process is maybe 5% of what Microsoft does to test their code.
- The SCADA / ICS world lags the IT world typically by 5 to 10 years, so we are only recently seeing the larger Control System vendors building plans to test their products for security flaws.
- All of those thousands of legacy products out there were NEVER tested for simple cyber security flaws like buffer overflows.

100 SCADA bugs in 100 days - McCorkle & Rios

- **Terry McCorkle (Boing Red Team by day, security researcher by night)**
- **Billy Rios (Google Security Lead by day, security researcher by night)**
- **Teamed up as friends and ran the project independent from their employers resources**
- **All data and SCADA/ICS software used in their research was found FREE on the web (over 3600 SCADA and ICS executable files found using:**

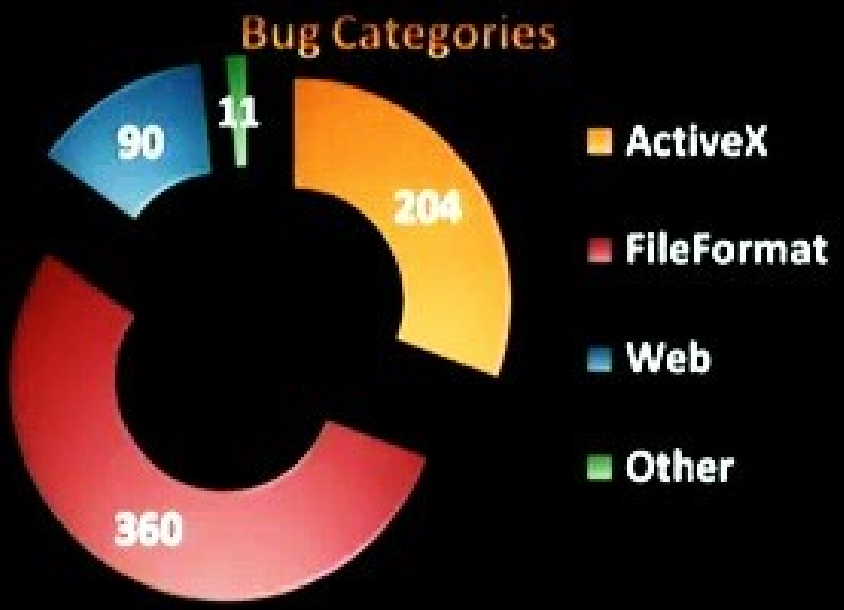
  +HMI +Download + filetype :(exe,zip,msi)

  +HMI +<Vendor Name> +Download

- **Used simple fuzzers:**
  - Comraider (ActiveX)
  - FileFuzz (bitflipper)
  - Sully and Peach (allows custom fuzzings)
  - Blasty.py (Service Fuzzer)

100 SCADA bugs in 100 days - McCorkle & Rios

- Downloaded over 380 HMI and Control Workbench software packages, but only tested 76 of them
- Found 665 bugs – all unique crashes
- Found 75 exploitable bugs out of 665 bugs.
- Reported all to ICS-CERT, who worked with the vendors for remediation next steps and sent out advisories to the community



- Most bugs and crashes were code problems that were straight out of the 90s – Simple Buffer Overflows
- They would setup the automated fuzzing software at night, go to sleep, and find bugs and crashes in the morning… or set the fuzzers in the morning, and come back home from work and find more waiting for them at night.

exploit frameworks now contain ICS/SCADA specific modules, scripts, and auxiliaries

- **Metasploit 115 Exploit Modules (and growing after the Basecamp PLC project)**
- **Core Impact 72 Exploit Modules**
- **Canvas 83 Exploit Modules**
  - Gleg Agora SCADA+ Exploit pack for Immunity CANVAS
  - they are aggressively acquiring SCADA vulns and creating exploits
  - 2 ICS vendors have purchased the CANVAS modules
  - Canvas is $8,930
    - Gleg pack is $5,000 and the canvas package is 3,930.

After 10 years of virtually no action from vendors… Researchers try to “shame” them into action

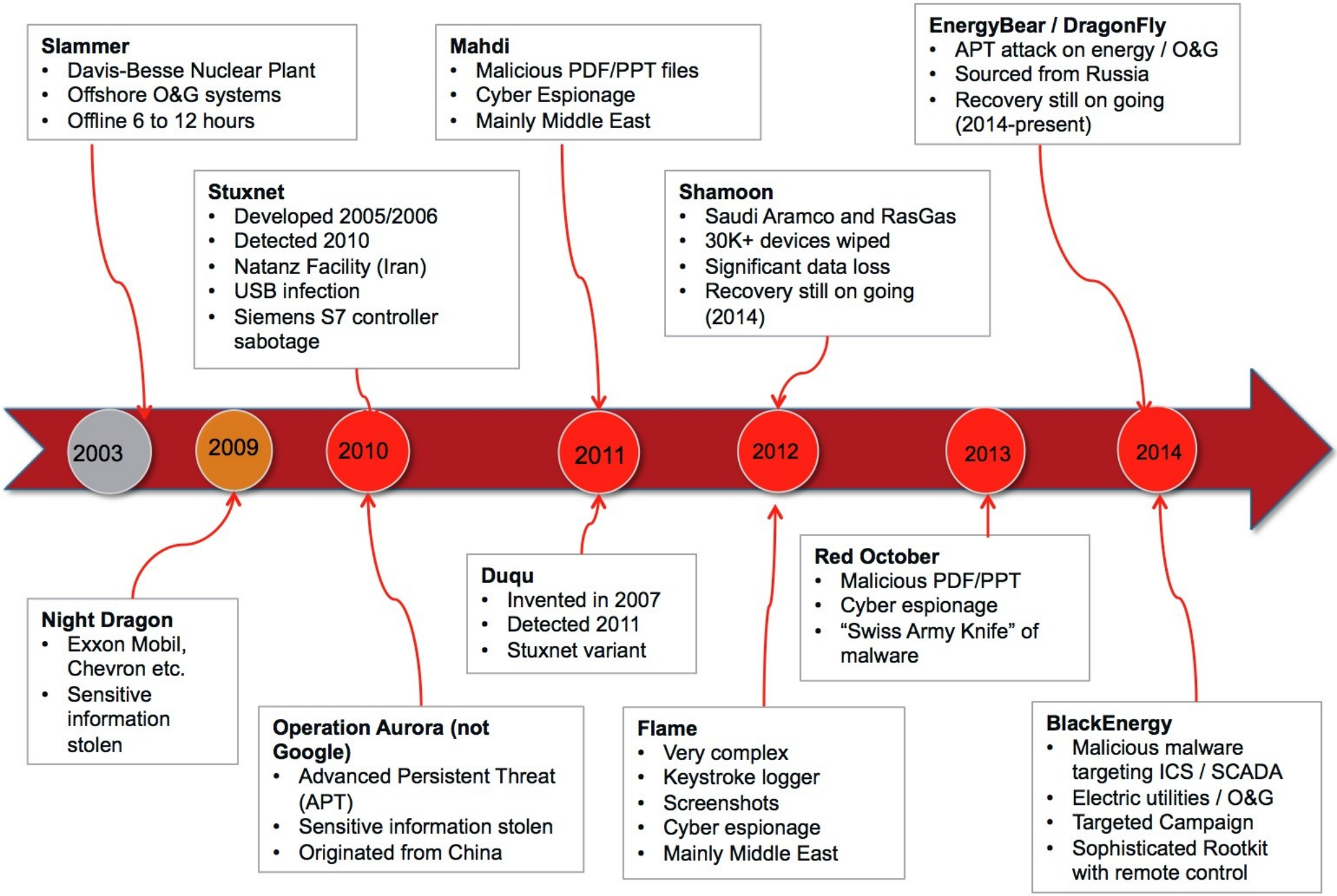
RT @jwunder: A bunch of PLC exploits are about to drop in Metasploit, meaning soon hacking SCADA systems can be push of a button easy

1 hour ago via TweetDeck

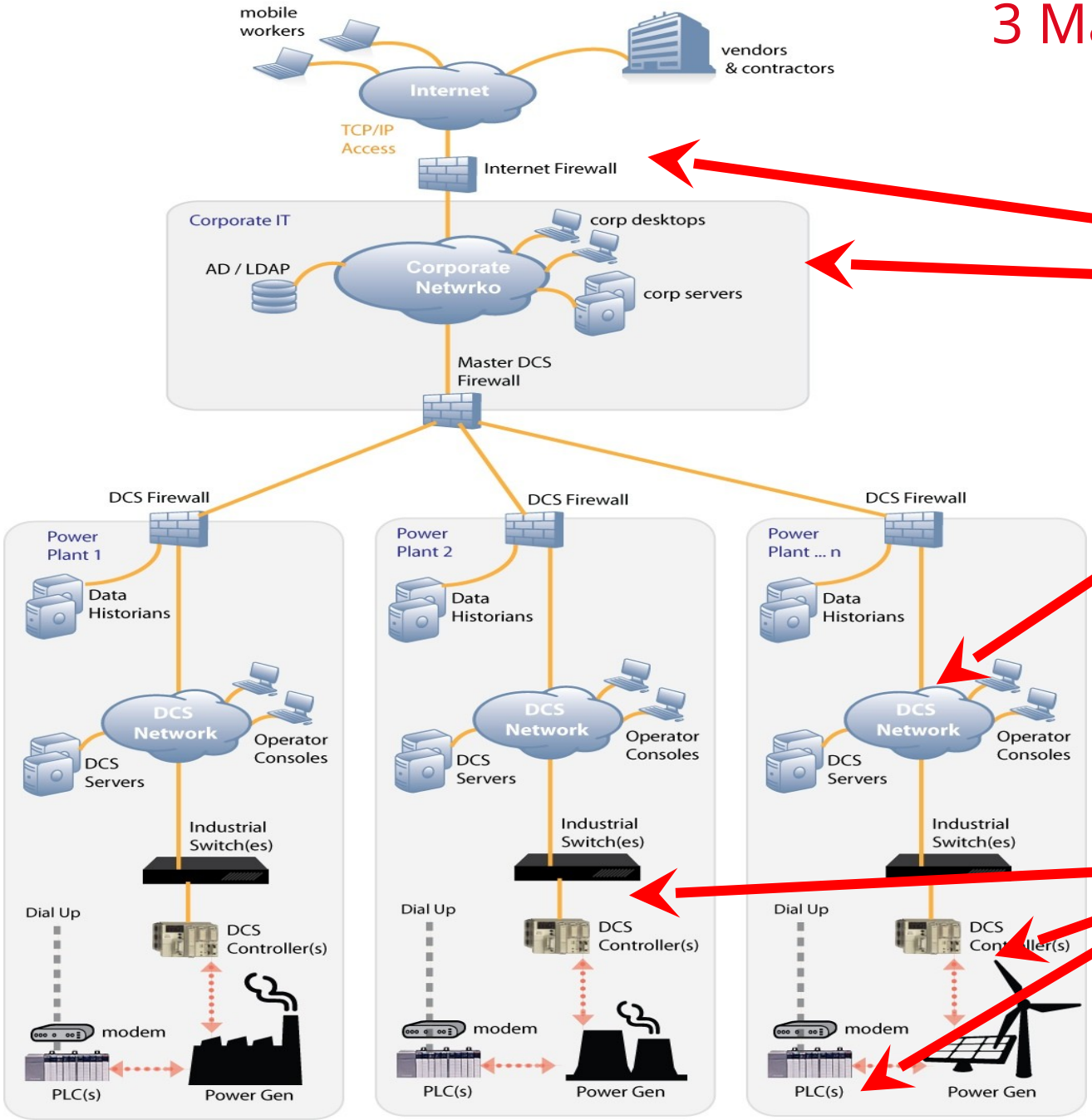


"Project Basecamp had six great researchers looking for vulnerabilities in six different PLC's / field devices, and the PLC's took a beating," Digital Bond reported. "There were backdoors, weak credential storage, ability to change ladder logic and firmware, command line interface, overflows galore, TFTP [Trivial File Transfer Protocol] for important files and so much more." The image to your left was posted on Digital Bond.

Dale Peterson, founder of Digital Bond, said, "We felt it was important to provide tools that showed critical infrastructure owners how easy it is for an attacker to take control of their system with potentially catastrophic results. These attacks have existed in theory for a while, but were difficult to demonstrate to a Plant Manager. By creating exploit modules for the most widely used exploit framework - Metasploit - we hope that security professionals in critical infrastructure companies, consultants, and penetration testers will prod vendors to add basic security measures to PLCs after decades of neglect."


Slammer
• Davis-Besse Nuclear Plant
• Offshore O&G systems
• Offline 6 to 12 hours
Mahdi
• Malicious PDF/PPT files
• Cyber Espionage
• Mainly Middle East
EnergyBear / DragonFly
• APT attack on energy / O&G
• Sourced from Russia
• Recovery still on going (2014-present)
Stuxnet
• Developed 2005/2006
• Detected 2010
• Natanz Facility (Iran)
• USB infection
• Siemens S7 controller sabotage
Shamoon
• Saudi Aramco and RasGas
• 30K+ devices wiped
• Significant data loss
• Recovery still on going (2014)
2003
2009
2010
2011
2012
2013
2014
Night Dragon
• Exxon Mobil, Chevron etc.
• Sensitive information stolen
Operation Aurora (not Google)
• Advanced Persistent Threat (APT)
• Sensitive information stolen
• Originated from China
Duqu
• Invented in 2007
• Detected 2011
• Stuxnet variant
Flame
• Very complex
• Keystroke logger
• Screenshots
• Cyber espionage
• Mainly Middle East
Red October
• Malicious PDF/PPT
• Cyber espionage
• "Swiss Army Knife" of malware
BlackEnergy
• Malicious malware targeting ICS / SCADA
• Electric utilities / O&G
• Targeted Campaign
• Sophisticated Rootkit with remote control

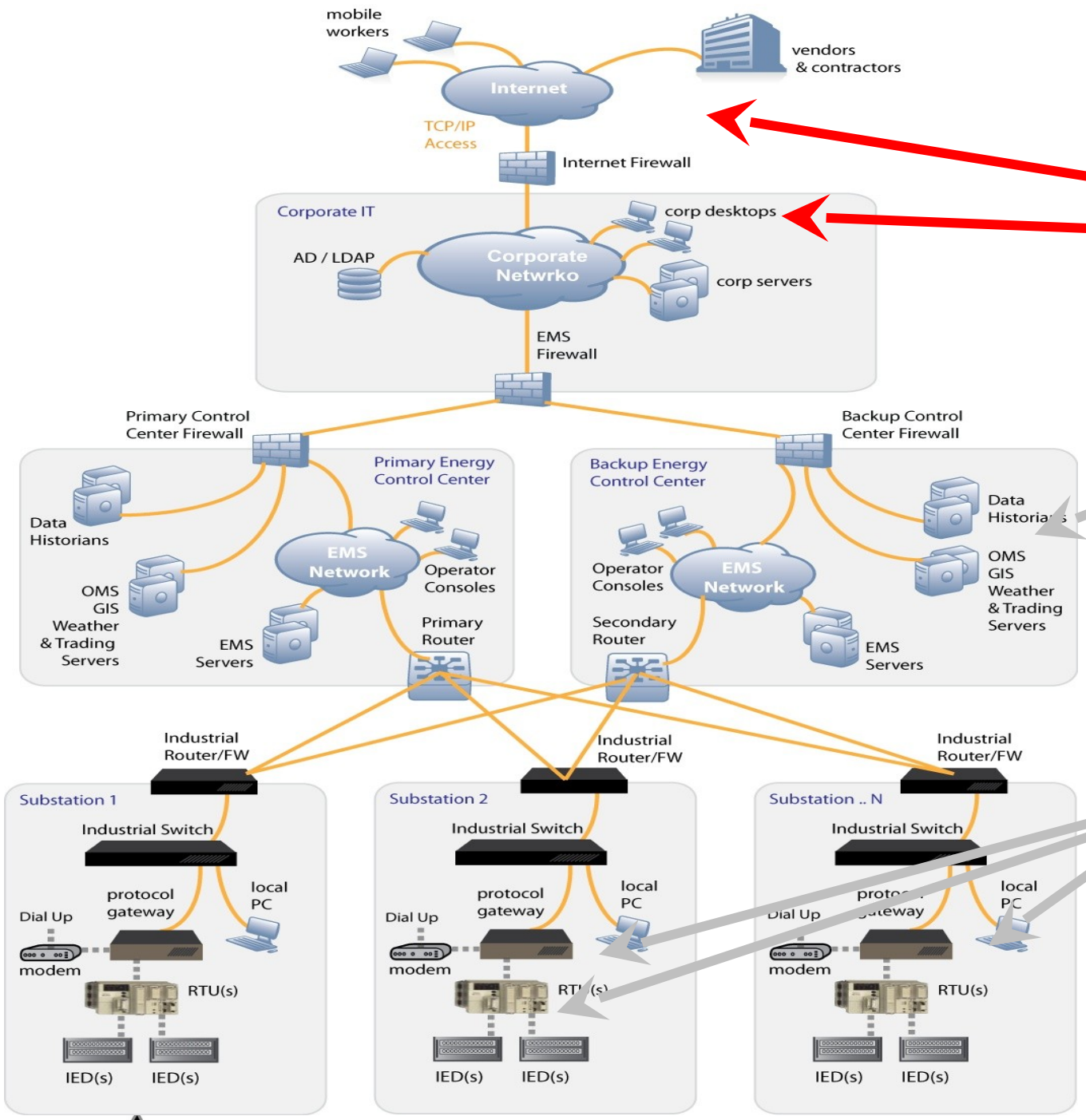
3 Main Areas of Concern



Internet & Corporate IT Networks

Servers, Workstations, & Applications

Embedded Devices



APT Style Attacks
- Night Dragon

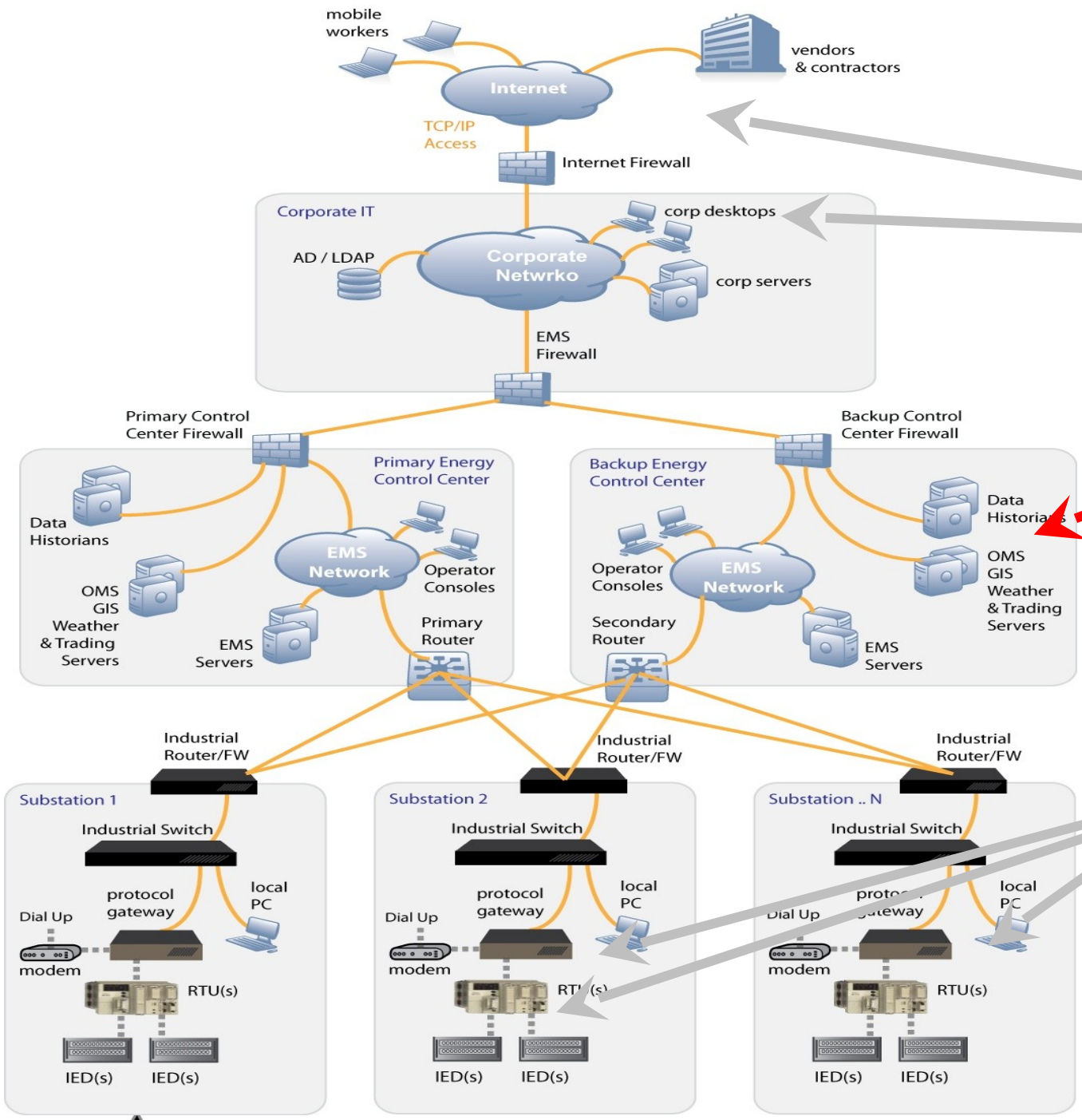
Phishing

Botnets

Self-propagating malware

Servers and Workstations
- Rootkits / Malware
- Metasploit
- Core Impact
- (Easy to pop boxes)

Growing number Of Vulnerabilities
- Clear Text Protocols
- No Authentication
- Little to no encryption
- Known weaknesses
- Stuxnet / TRITON



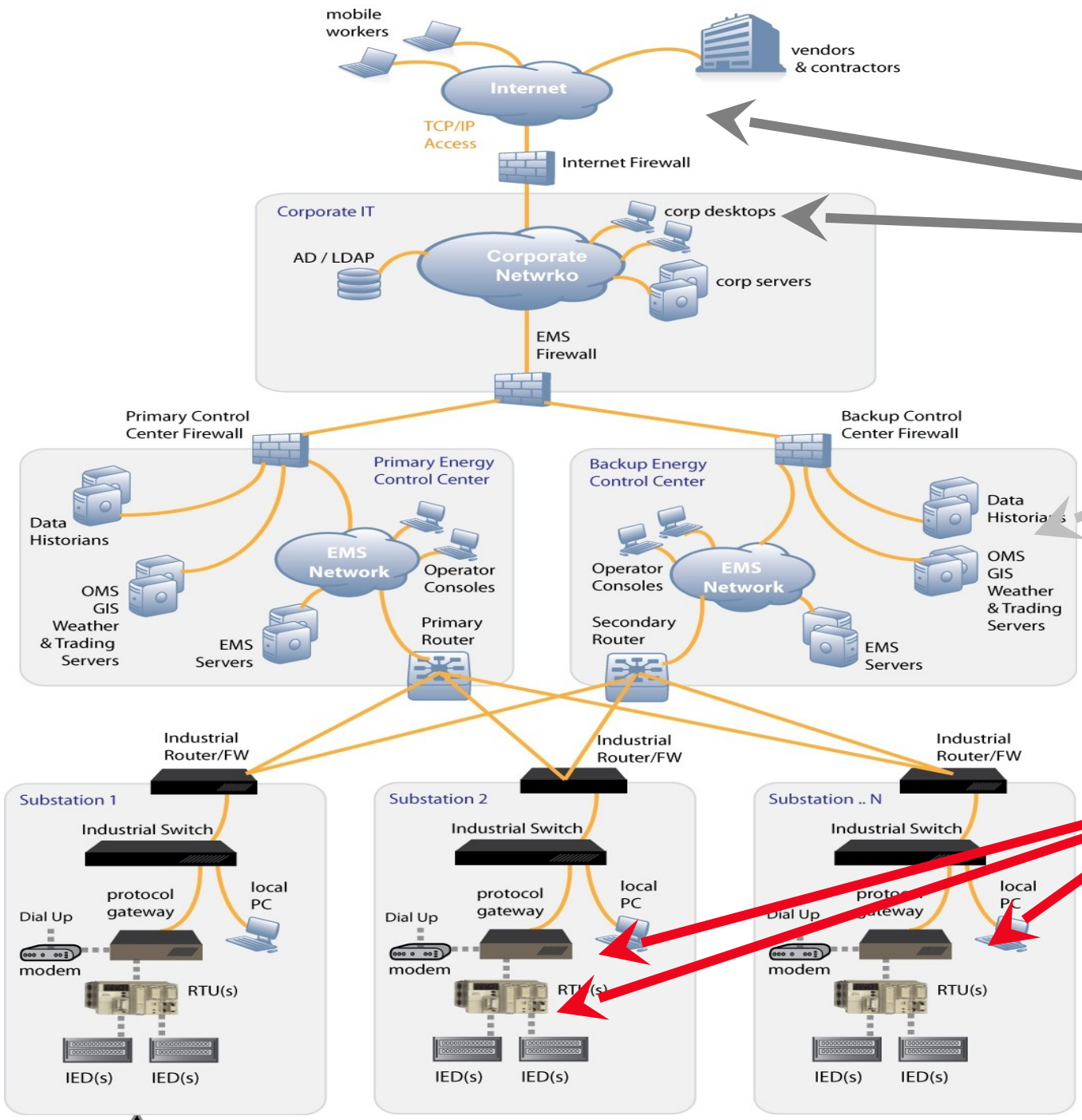


APT Style Attacks
- Night Dragon

Phishing
Botnets
Self-propagating malware

Servers and Workstations
- Rootkits / Malware
- Metasploit
- Core Impact
- (Easy to pop boxes) LATERAL MOVEMENT

Growing number Of Vulnerabilities
- Clear Text Protocols
- No Authentication
- Little to no encryption
- Known weaknesses
- Stuxnet / TRITON



APT Style Attacks
- Night Dragon

Phishing
Botnets
Self-propagating malware

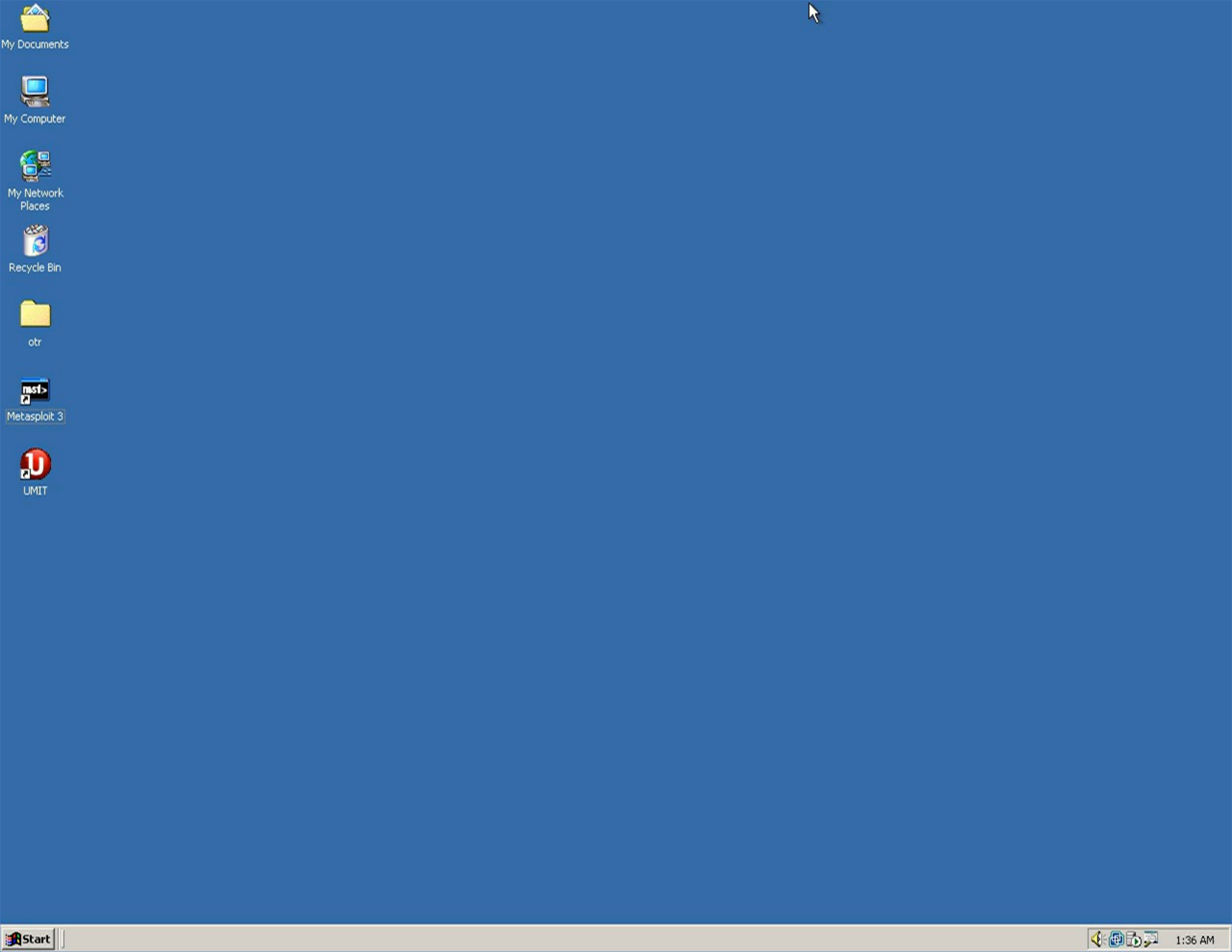
ICS Servers run same OS as Corporate
- Metasploit
- Core Impact
- (Easy to pop boxes)

Growing number Of Vulnerabilities
- Clear Text Protocols
- No Authentication
- Little to no encryption
- Known weaknesses
- Stuxnet / TRITON

dcs hacking demo video: locating and compromising an Operator Console in under 3 minutes

- From open source intelligence gathering, Google searches, or social engineering, an attacker determines the asset is running a DeltaV DCS system*
- The attacker has no accounts on the system, no passwords, and is an unauthorized entity that has gained access to the network
- What is possible?

* Disclaimer: This example only used DeltaV because we had access to this system. All DCS vendors have the same security issues, and this is not an attempt to single out any one vendor.


My Documents
My Computer
My Network Places
Recycle Bin
otr
Metasploit 3
UMIT
Start
1:36 AM

the sky is not falling (yet)

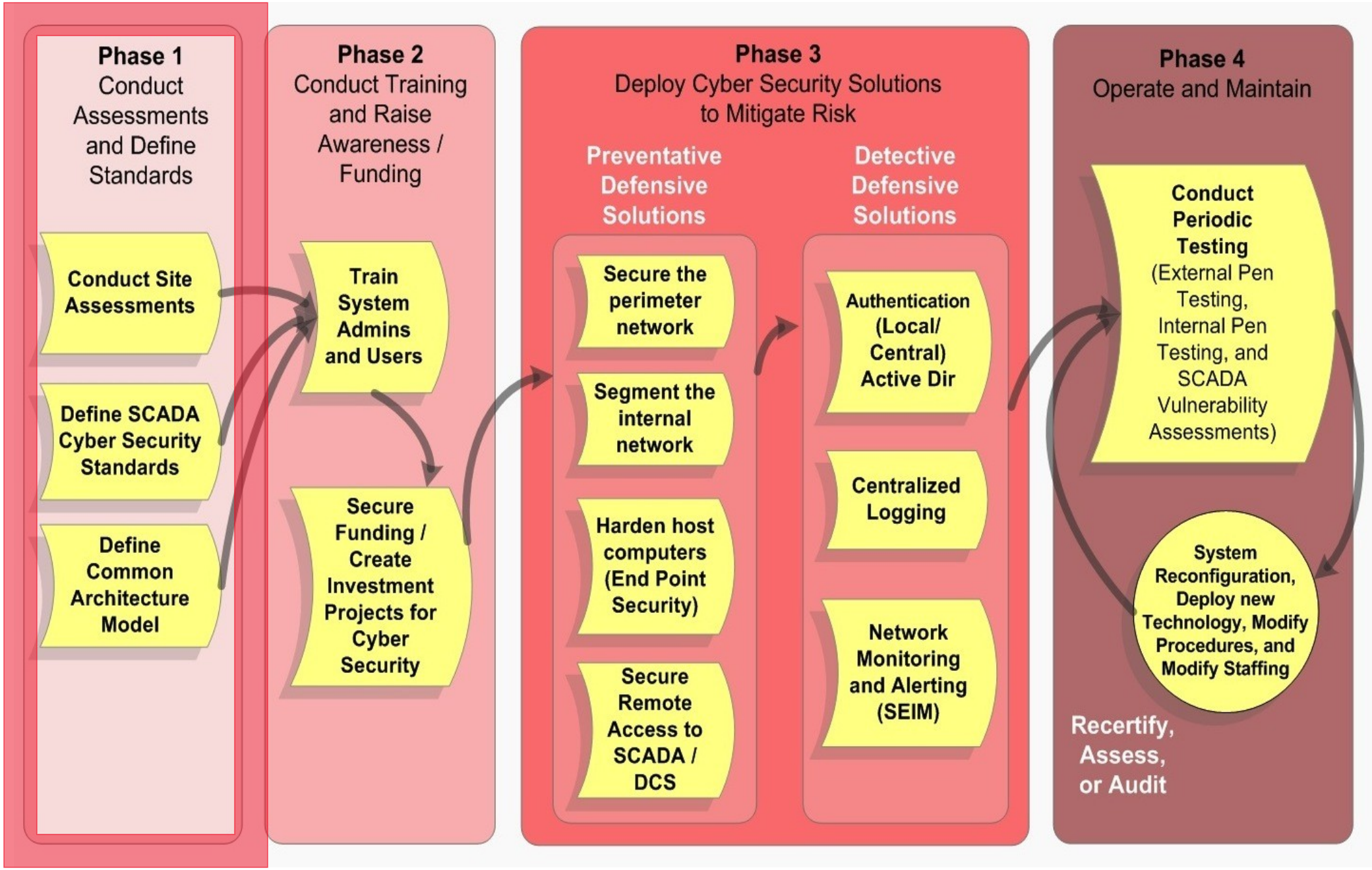
Cyber Security for ICS / SCADA can seem overwhelming…

1. Understand Your Current ICS / SCADA Security Maturity (Current State Assessment)

2. Determine Your Desired Target State (Is it Compliance Driven?)

3. Create a Strategic Plan to Drive your security program from it's Current State to the Desired State over a period of time (3-to-5 years)

- Most Security Frameworks (i.e. NERC CIP, ISA S99, ISO 270001, DHS CFATS, and NIST CSF) include both **Technical** and **Procedural** required controls


Phase 1
Conduct Assessments and Define Standards
Conduct Site Assessments
Define SCADA Cyber Security Standards
Define Common Architecture Model
Phase 2
Conduct Training and Raise Awareness / Funding
Train System Admins and Users
Secure Funding / Create Investment Projects for Cyber Security
Phase 3
Deploy Cyber Security Solutions to Mitigate Risk
Preventative Defensive Solutions
Secure the perimeter network
Segment the internal network
Harden host computers (End Point Security)
Secure Remote Access to SCADA / DCS
Detective Defensive Solutions
Authentication (Local/ Central) Active Dir
Centralized Logging
Network Monitoring and Alerting (SEIM)
Phase 4
Operate and Maintain
Conduct Periodic Testing (External Pen Testing, Internal Pen Testing, and SCADA Vulnerability Assessments)
System Reconfiguration, Deploy new Technology, Modify Procedures, and Modify Staffing
Recertify, Assess, or Audit

3-step process for understanding ICS/SCADA risk and build a strategic roadmap to drive the CURRENT state to the TARGET state

1. Define "Target State"

2. Determine "Current State"

3. Risks and Gaps drive "Strategic Roadmap"



alphabet soup of standards

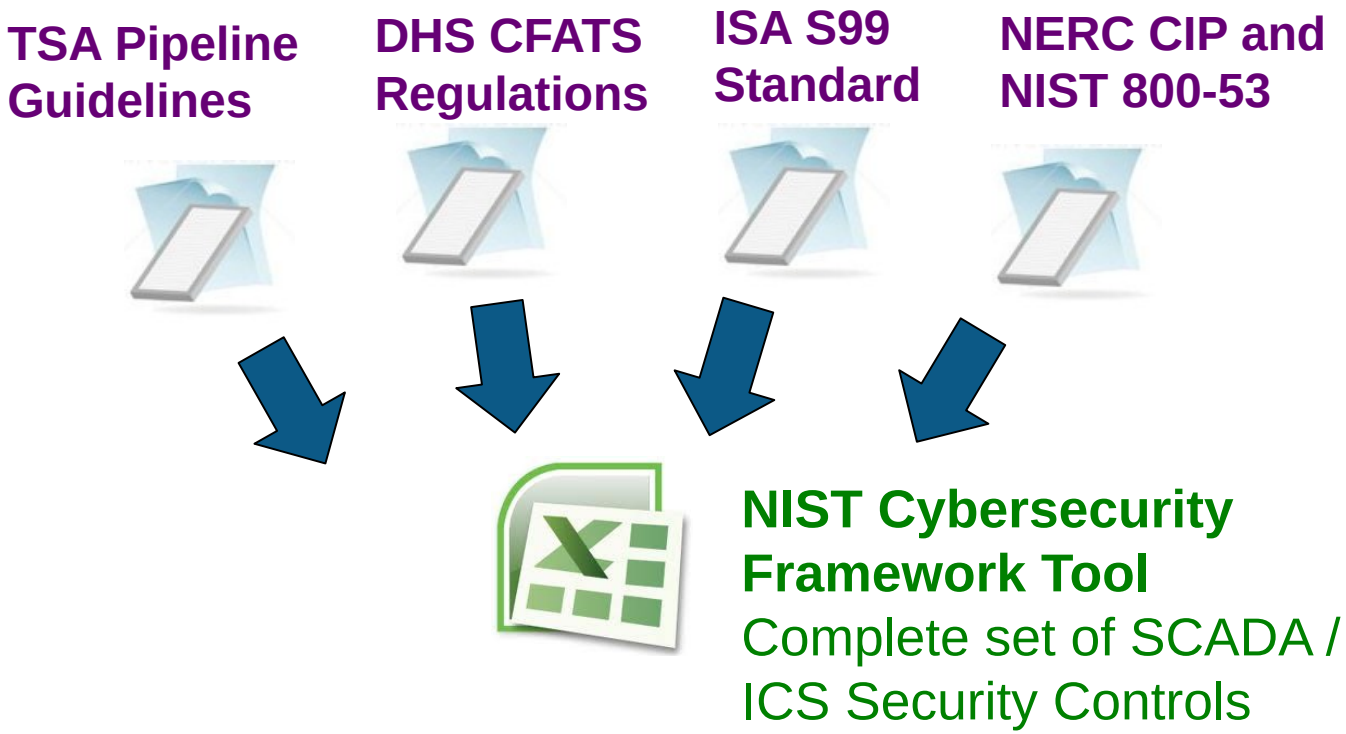
NERC CIP, CFATS, API, TSA, AWWA, FTA,ISO, NIST etc…

- NERC CIP: Electric Power
- CFATS: Chemicals
- API 1164 / AGA 12: Oil and Gas
- TSA Pipeline: Pipelines
- HIPPA: Health Privacy Concerns
- PCII: Credit Card Privacy
- FISMA/FIPS: US Federal / Military Systems
- ISO 270001: ISO Framework
- SANS Top 20: Top 20 Controls Mapped to NIST 800-53
- **NIST CSF for Critical Infrastructure** >> NEW COMMON FRAMEWORK

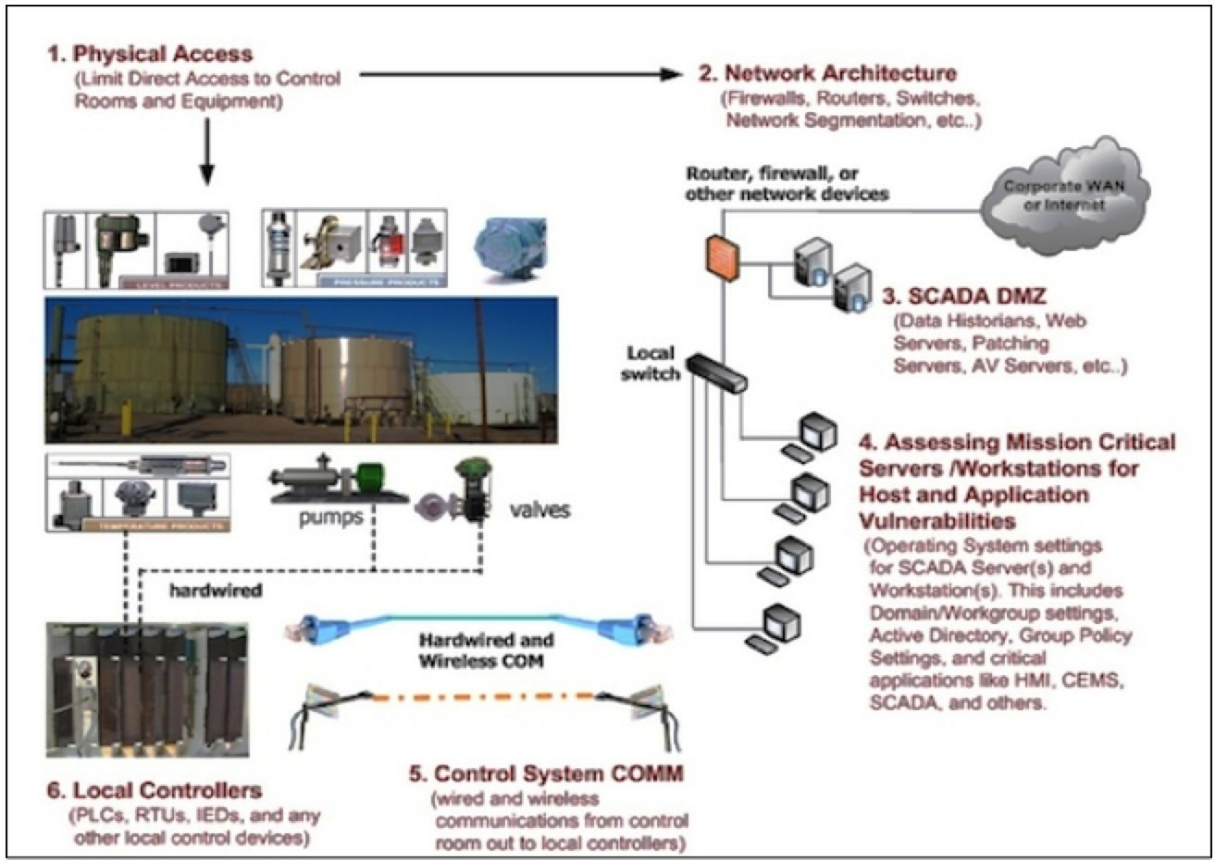
NIST CSF for Critical Infrastructure

- The NIST Cyber Security Framework (CSF) harmonizes previously splintered cyber security standards that were written for various specific sectors, and creates one framework for measuring the current state of security controls

- NIST CSF is tailored for ICS/SCADA systems



ICS Subsystems mapped to NIST Framework Capabilities



1. Physical Security (preventing physical access to ICS / SCADA components)
2. Network Infrastructure (firewalls, and network segmentation)
3. ICS / SCADA DMZ host systems (Historians, Web-enabled HMIs, and Informational Systems
4. Control Room Host Systems (HMI Workstations, I/O Servers, and Applications)
5. Telemetry Communications (IACS Protocols)
6. Field Devices (PLCs, RTUs, and embedded devices)

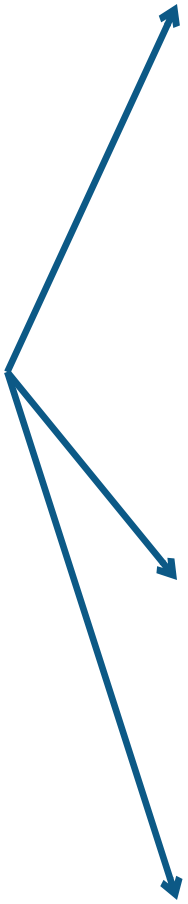
Cyber Security Framework Capabilities



NIST CSF helps define a "Target State" for ICS / SCADA Systems Maturity

- The Target State definition process uses interviews with IT, Security, and all applicable Operations groups to create and adopt a common set of ICS Security Controls tailor fit to the organization's operational structure and constraints.

- The control definitions language typically uses high level descriptions of the required controls to leave flexibility for implementing solutions custom to each unique environments.

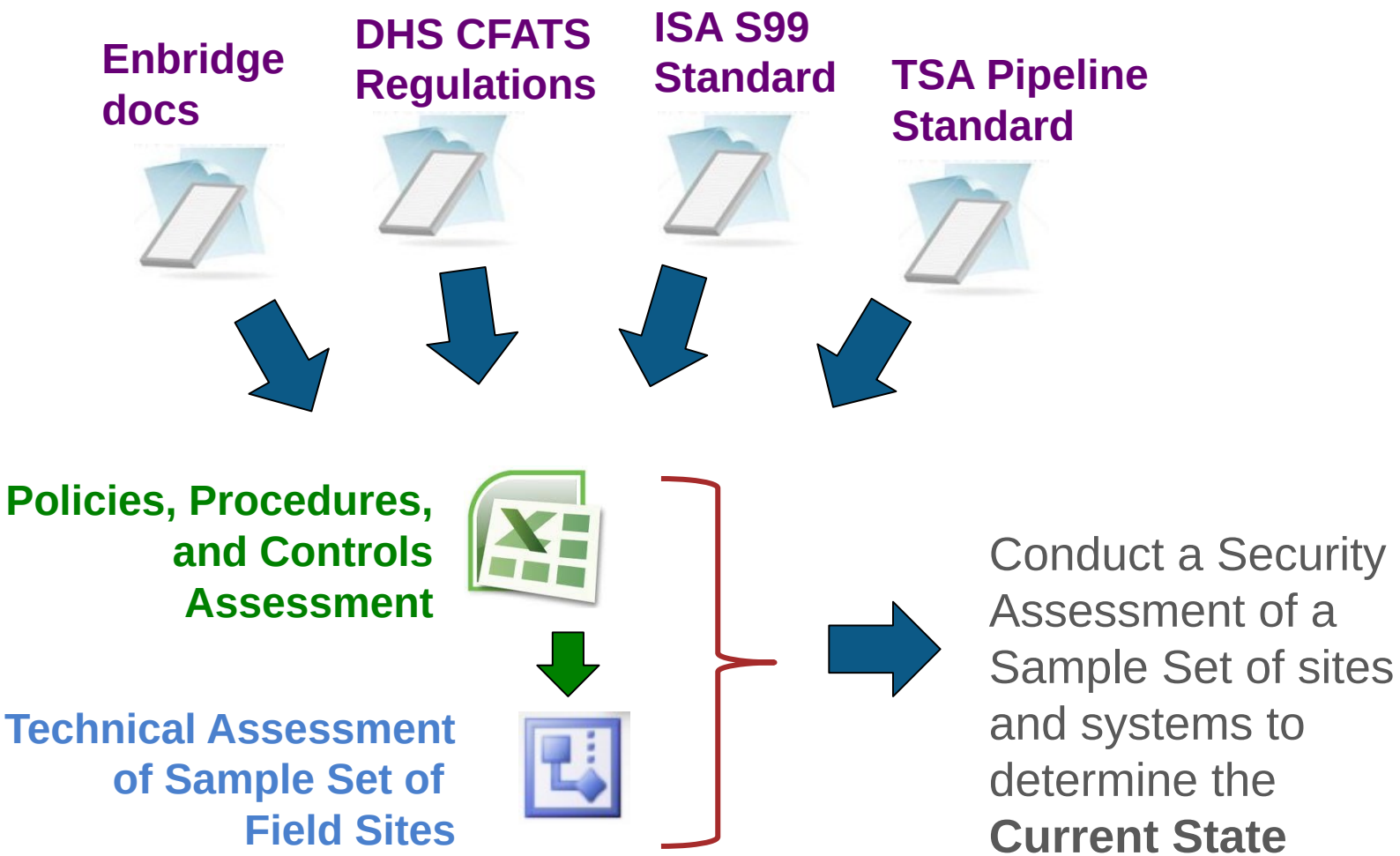


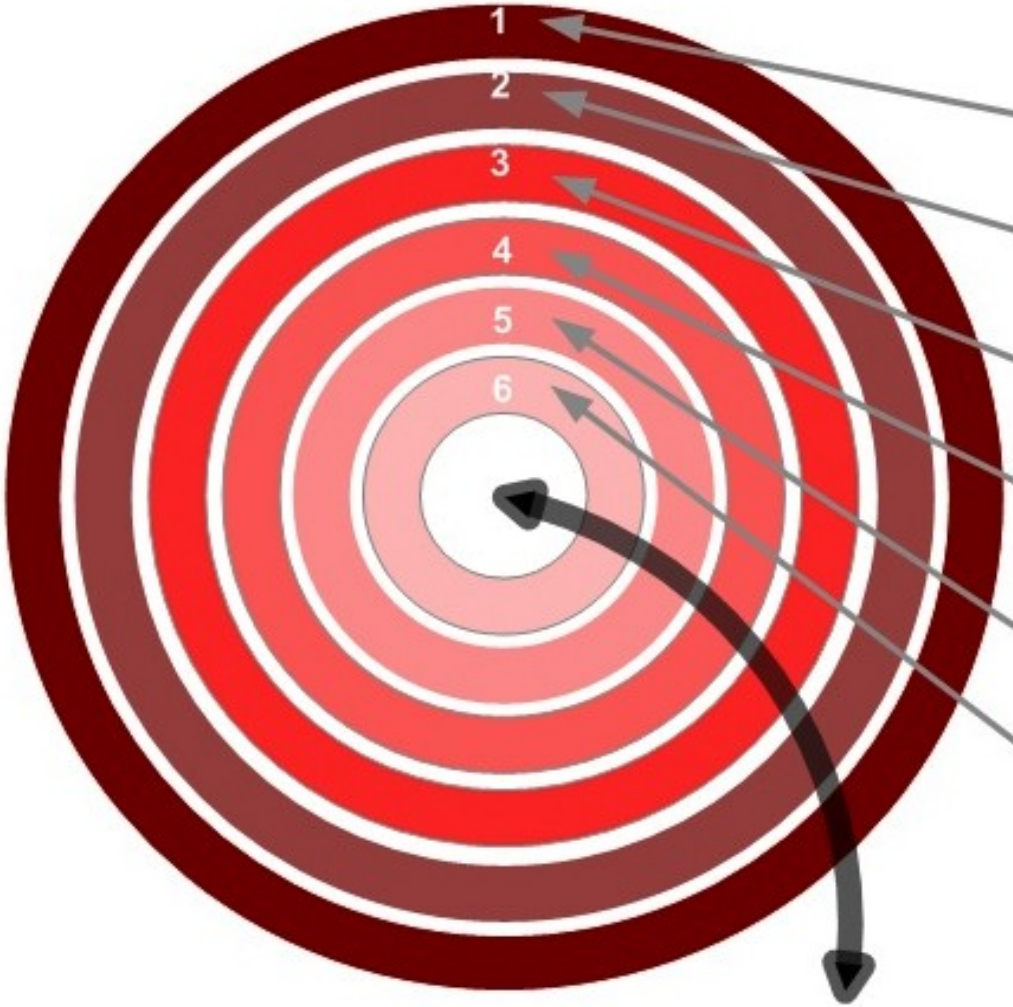
Function	Category
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

task 1 - Target State Definition

- **Positive Lessons Learned:**
  - The Target State Definition drives a stake into the ground to level-set the expectations for the ICS Security Program Development, and provides a common benchmark across the organization. The process creates a Target State for the organization that all departments can get behind and support since it is developed from a Best-in-Breed set of controls based on Industry Best Practices and Standards.
  - Using the NIST Cybersecurity Framework for Securing Critical Infrastructure brings IT, OT, Physical Security, and HR together to the table and **agree on a common set of security controls**
  - Once the “Target State” is defined and agreed upon, the rest of the process falls into line smoothly, since the gaps and risk drives the resources prioritization during the Strategic Roadmap development.

task 2 – After the **Target State** is defined, then the **Current State** can be evaluated to determine gaps and risk





Technical Controls

1. **Physical Security**
   (Fencing, Surveillance, Guards, Gates, Locks)
2. **Network Infrastructure**
   (Switches, Routers, Firewalls, 3rd Party Connections, and Modems)
3. **Manufacturing IT DMZ**
   (Data Historians, Data Logging, Web Servers)
4. **Mission Critical DCS Servers, Workstations, and Operator Consoles**
   (Operating System Security, Application Security)
5. **Communications to Field Devices**
   (Profibus, Modbus, OPC, and other protocols...)
6. **Field Devices**
   (PLCs, RTUs, IEDs, Plant Equip.)

Procedural Controls

Across all **Six Layers** spans the need for procedural controls that include:

- Governance, Security Policies, Plans, Procedures, and System Ownership
- Asset Inventory, System Documentation, Management of Change, and Test / Development Systems
- Risk Management, Patch Management, Lifecycle Planning, and Routine Assessments
- Crisis Management, Emergency Planning, Safety, and Safe Shutdown Procedures, Backup and Recovery

Current State Assessment = **Policy/Procedures + Technical**

1. First, define the Target State, or the Ideal Security Posture for your system based on the Controls Framework you are driving for compliance
   (i.e. NERC CIP, CFATS, ISO, NIST, etc…)

2. Current State Assessment = Policy/Procedures Gap Analysis + Technical Assessment

3. Lastly, develop a Strategic Roadmap that will put into place key specific investments over a 3 to 5 year period to move from the CURRENT state to the TARGET state.

1. Physical Access
(Limit Direct Access to Control Rooms and Equipment)

2. Network Architecture
(Firewalls, Routers, Switches, Network Segmentation, etc..)





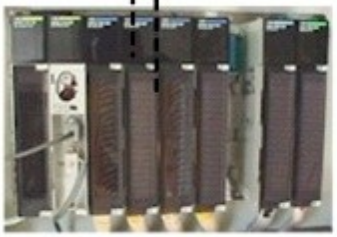








hardwired

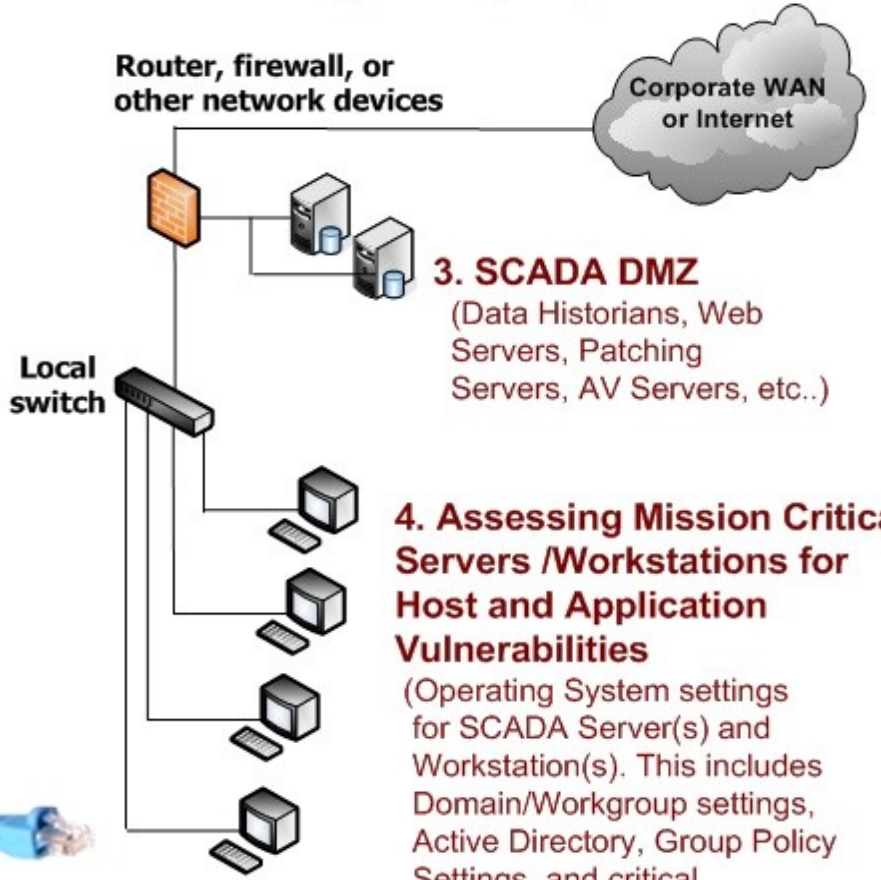






5. Control System COMM
(wired and wireless communications from control room out to local controllers)

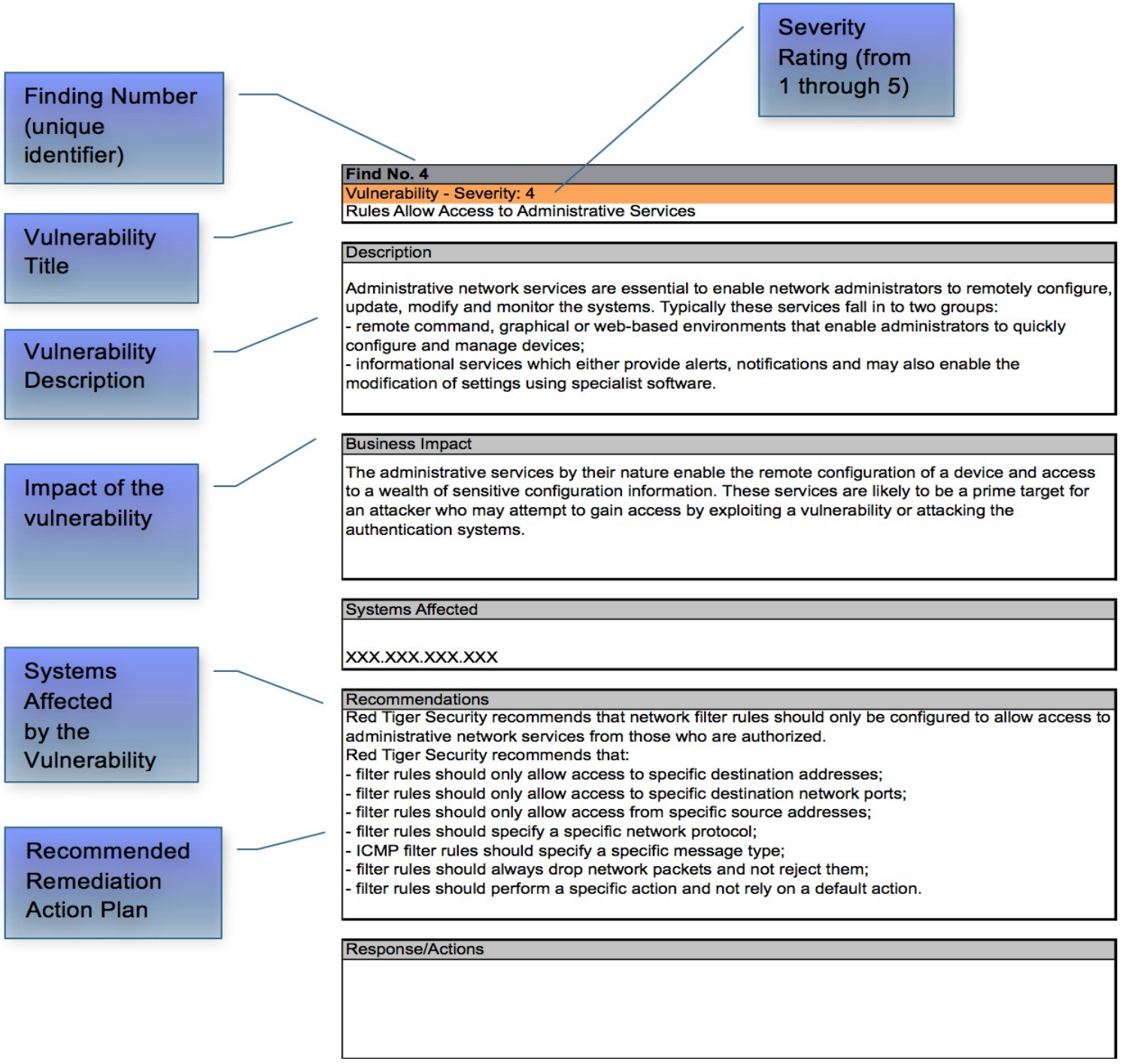
6. Local Controllers
(PLCs, RTUs, IEDs, and any other local control devices)



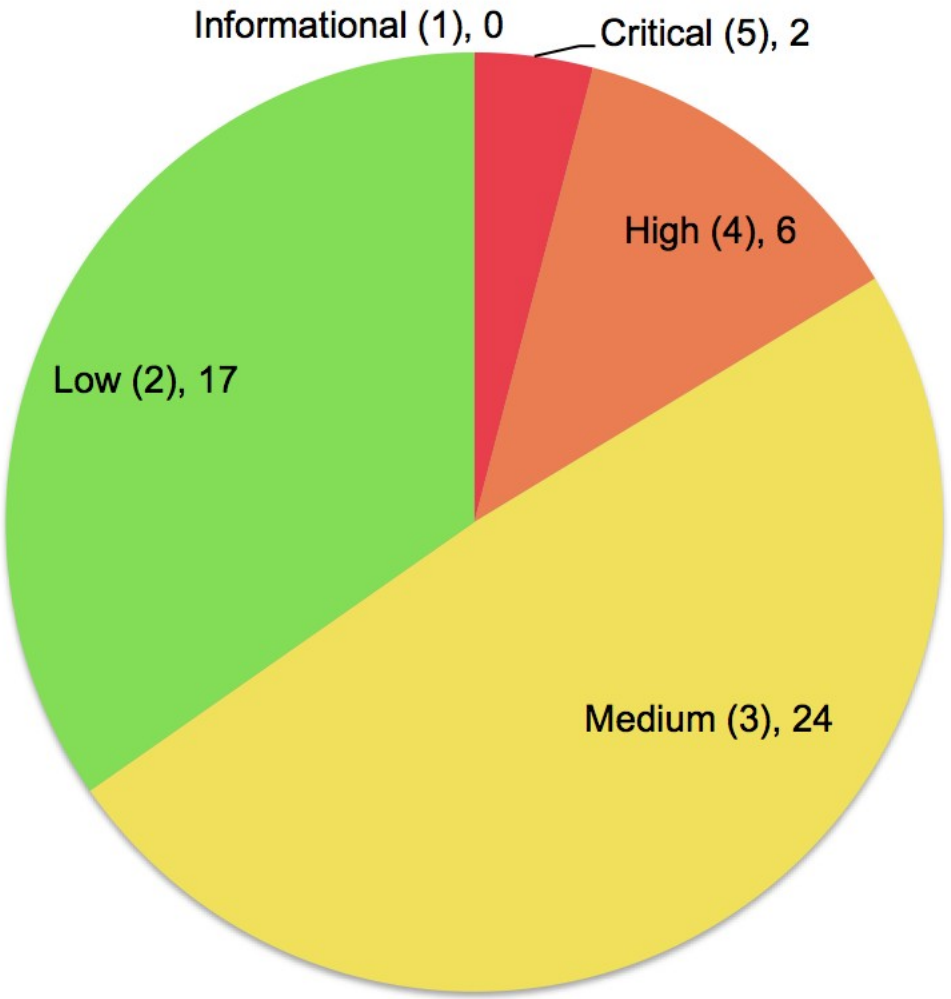
3. SCADA DMZ
(Data Historians, Web Servers, Patching Servers, AV Servers, etc..)

4. Assessing Mission Critical Servers /Workstations for Host and Application Vulnerabilities
(Operating System settings for SCADA Server(s) and Workstation(s). This includes Domain/Workgroup settings, Active Directory, Group Policy Settings, and critical applications like HMI, CEMS, SCADA, and others.

Sample Vulnerability Finding Table



technical vulnerabilities ranked by criticality (info, low, med, high, and critical high)

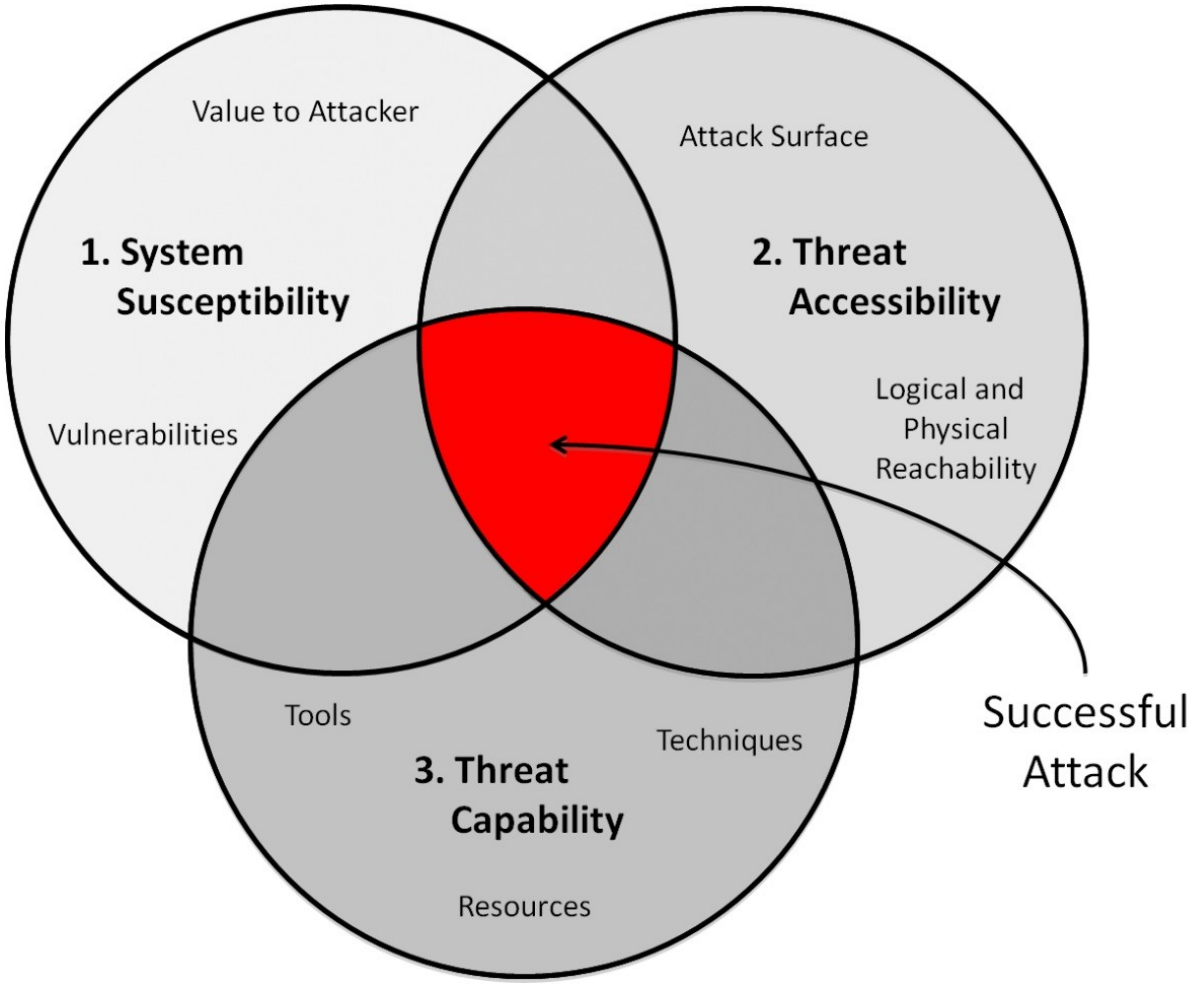


Function	Category
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

(Sample) High Risk Gaps from a Controls Framework Assessment

- **The controls assessment exposes High, Medium, and Low risk from a Policy/Procedures/Controls perspective. In this sample case, High risk areas included:**
  - Defining Cybersecurity Roles and Responsibilities for the Entire Workforce
  - Establishing an Organizational Information Security Policy
  - Establishing and Maintaining a Cybersecurity Risk Management Process
  - Protecting ICS Systems with Cyber Access Controls and Secure Remote Access
  - Establishing an Enforcing the Restriction of Removable Media in ICS networks

threats that can exploit missing or soft controls elevates those impacted controls or missing solutions to a higher risk



Controls Framework Assessment

+ Technical Field Assessments
+ Threat Assessment

= True Valuation of real ICS / SCADA Risk

Source: http://timreview.ca/article/712

task 2 - Current State Key Findings

- **Positive Lessons Learned:**
  - To obtain a complete Current State Assessment, this requires performing both a technical assessment of the state of the security of the ICS system, and an assessment of the policies, procedures, and controls
  - This Current State Assessment approach uncovers security findings, vulnerabilities, and missing controls (gaps from the target state). **We are able to group these into High, Medium, and Low priority in terms of risk reduction remediation steps**
  - The next task in the project grouped these remediation steps into logical solution projects in a Strategic Roadmap

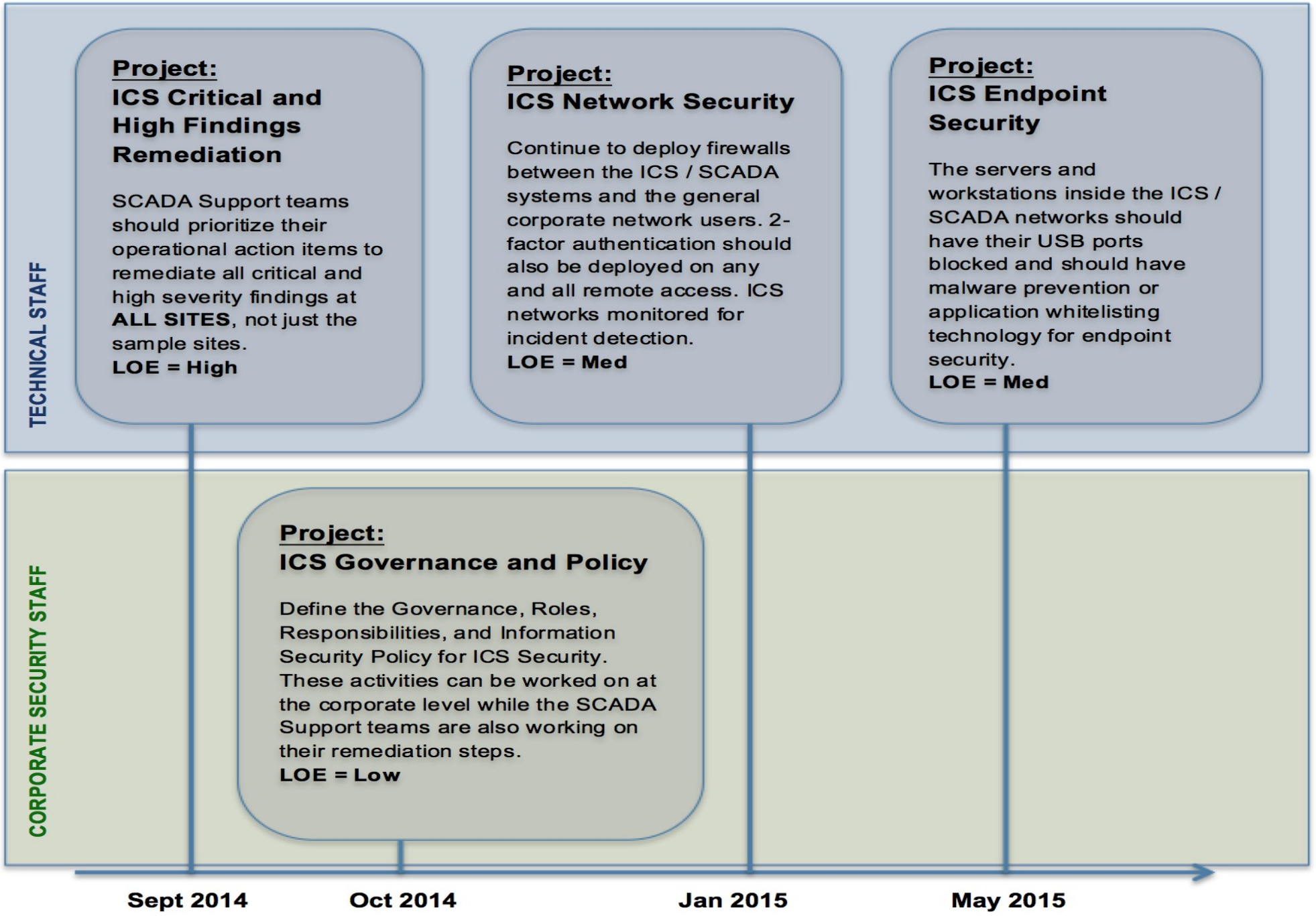
prioritizing Gaps into Short, Medium, and Long Term Strategy

- The process of prioritizing these areas for improvement included taking into consideration the threats and risk to ICS / SCADA systems, comparing the current level of compliance to the controls identified in the Target State, and then prioritizing the control areas into three priority areas based on risk: High, Medium, and Low.

- Not knowing how fast our clients would like to move through these solution areas, we grouped the gaps into the following categories:
  - **Highest Priority** (Short Term Strategy: 0 to 12 months)
  - **Medium Priority** (Next Wave of Projects within the next 12 to 24 months)
  - **Low Priority** (Long Term Strategy: Longer than 24 months)

- Our clients may ultimately decide to accelerate the pace of these categories or re-prioritize individual control remediation steps.

Strategic Roadmap – Highest Priority



task 3 – Strategic Roadmap Key Findings

- The timelines contained in the Strategic Roadmap groups remediation efforts into projects and then prioritizes those projects in terms of high, medium, and low priority.
- The strategic roadmap also allows the work to occur in parallel streams, since the technical projects can be driven by the ICS / SCADA support staff, while the corporate security staff can focus on governance and policy projects.
- The highest priority projects were also prioritized because they will reduce the likelihood of incidents identified in the Threat Assessment performed in the current state assessment report.

4 years experience using this proven approach

Marathon Pipeline

Revenue US$75.369 billion

Walt Disney

Revenue US$55.137 billion

Enbridge

Revenue C$32.9 billion

Huntsman Corporation

Revenue US$8.36 billion

Duke Energy

Revenue US$5.2 billion

Newfield Exploration

Revenue US$1.77 billion

American Styrenics

Revenue US$458 million

Santee Cooper

South Carolina's state-owned electric and water utility

conclusion

This proven process has been applied to over a dozen ICS / SCADA clients to:

1. Define the Target State for the SCADA / ICS Security Program

2. Compare the Current State of the systems to the Target State to uncover technical risk and any missing controls

3. Prioritize the remediation and correction of these security findings to bring the system up to the desired Target State

contact info / q & a

Jonathan Pollet, CAP, CISSP, PCIP

Founder, Principal Consultant

Red Tiger Security, USA

office: +1.877.387.7733

Mobile: +1.281.748.6401

fax: +1.800.864.6249

jpollet@redtigersecurity.com

www.redtigersecurity.com

Credits

:: Ty Bodell for assistance with the demos

:: Thievery Corporation and Pendulum for the soundtracks