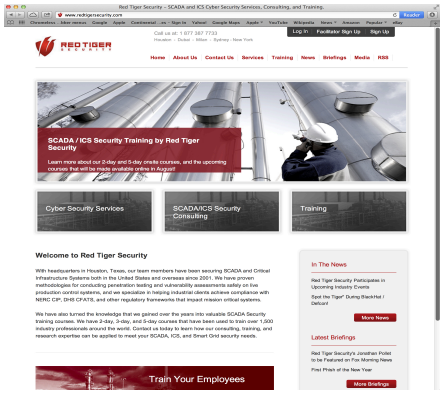


1

RED TIGER SECURITY

Red Tiger Security

- **Consulting**
  - Penetration Testing
  - Cyber Vulnerability Assessments on LIVE Industrial Control Systems
  - Network Architecture Analysis / Design Review
  - Cyber Security Advisory Services and Strategic Consulting
  - Risk Assessment, Compliance Gap Analysis, and ICS Security Program Development
- **Training**
  - 5-Day Intermediate Course for Securing Critical Infrastructures
  - 2-Day Advanced ICS Security Course (BlackHat)
- **Research**
  - Applicability and Usability of Cyber Security Solutions for SCADA / ICS
  - Product Evaluations
  - Various DHS Research Initiatives for ICS Security
  - Standards Development



© Copyright Red Tiger Security – Do not print or distribute without consent.

2

Jonathan Pollet – CISSP, PCIP, CAP

- 23 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 18 Years Focused on ICS Security
  - Published White Papers on SCADA Security early in 2001
  - Focused research and standards development for ICS Security since 2002 including one of the 4 founders of the ISA99/IEC62443 standard
  - Conducted over 300 security assessments on Critical Infrastructure systems
  - Conducted over 170 International conferences and workshops on ICS Security
  - Developed safe security assessment methodology for live SCADA Systems in 2005
  - Developed the SCADA Security Advanced 5-day training course
  - Trained over 3,000 Professionals Globally
  - Featured presenter on Fox News Live, CNN, CNBC, Vanity Fair, Popular Mechanics, CIO Magazine, and several security publications

© Copyright Red Tiger Security – Do not print or distribute without consent.

3

Automation systems and threats to these systems have changed in the past 15 – 20 years

< Defining the problem >

4

Evolution of ICS Systems

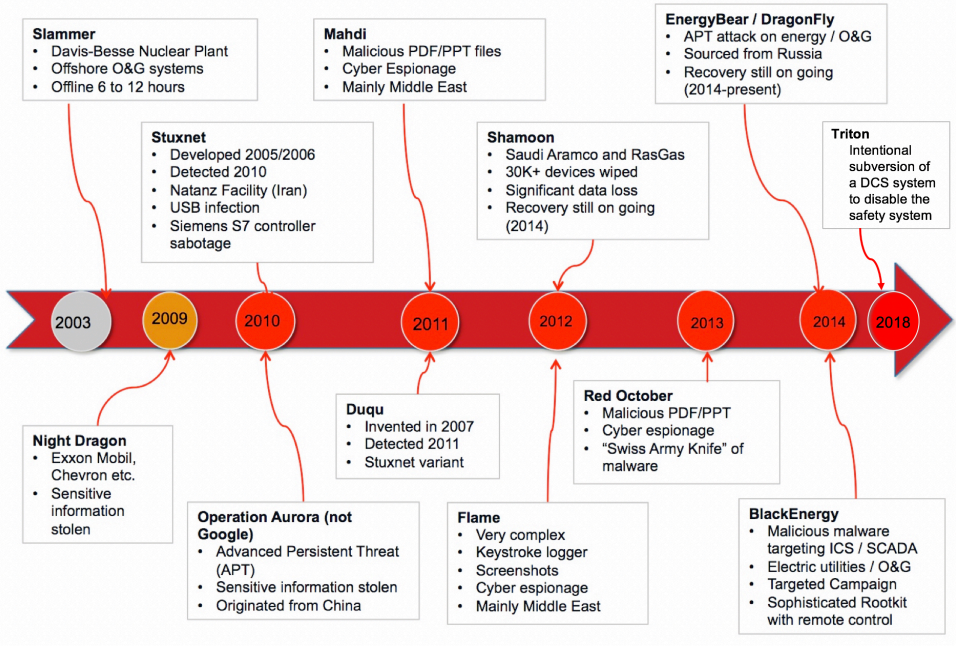
- 1960s/1970s/1980s
  - Controllers > proprietary interfaces, unique bus protocols, and no industry standards
  - HMI > proprietary operating systems (largely based on UNIX)
  - Network > no connection between ICS systems and corporate networks
- 1990s
  - Controllers > standardization on RJ45 ports, and proprietary protocols started to be wrapped in TCP/IP to port them to ethernet networks
  - HMI > Most operational interfaces ported to run on Microsoft Windows operating systems
  - Network > ICS devices and HMI workstations being deployed on TCP/IP networks with little or no separation from corporate networks

© Copyright Red Tiger Security – Do not print or distribute without consent.

Evolution of ICS Systems

- 2000s
  - Controllers > full adoption / standardization on RJ45 ports, and almost all ICS protocols wrapped in TCP/IP and deployed on ethernet networks
  - HMI > Almost all operator workstations and ICS software have been ported to Microsoft Windows operating systems
  - Network > ISA99/IEC62443 provided a layered network architecture model with firewall separation required between PCN (process control networks) and corporate IT networks. Many organizations start to separate their PCN networks
- 2010s
  - Controllers > full adoption / standardization on RJ45 ports, and all ICS protocols wrapped in TCP/IP and deployed on ethernet networks
  - HMI > All operator workstations and ICS software running on Microsoft Windows operating systems (only 3% still on non-windows platforms)
  - Network > International best practices/standards/regulations require at least one firewall between PCN and corporate networks

© Copyright Red Tiger Security – Do not print or distribute without consent.



© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Conditions Ripe for Perfect Storm

- ICS and operational systems are no longer proprietary, and no longer isolated
- ICS and operational systems now utilizing same technology as business IT systems, and becoming more connected and integrated
- Although ICS systems have the same technology and platforms as business systems, they lack the cyber security protections such as AV / End Point protection, authentication, encryption, logging, monitoring, incident response, and repeatable restoration processes
- Field Operations have grown dependent upon ICS systems to be available, and most systems can be remotely shut down by signals from the ICS systems

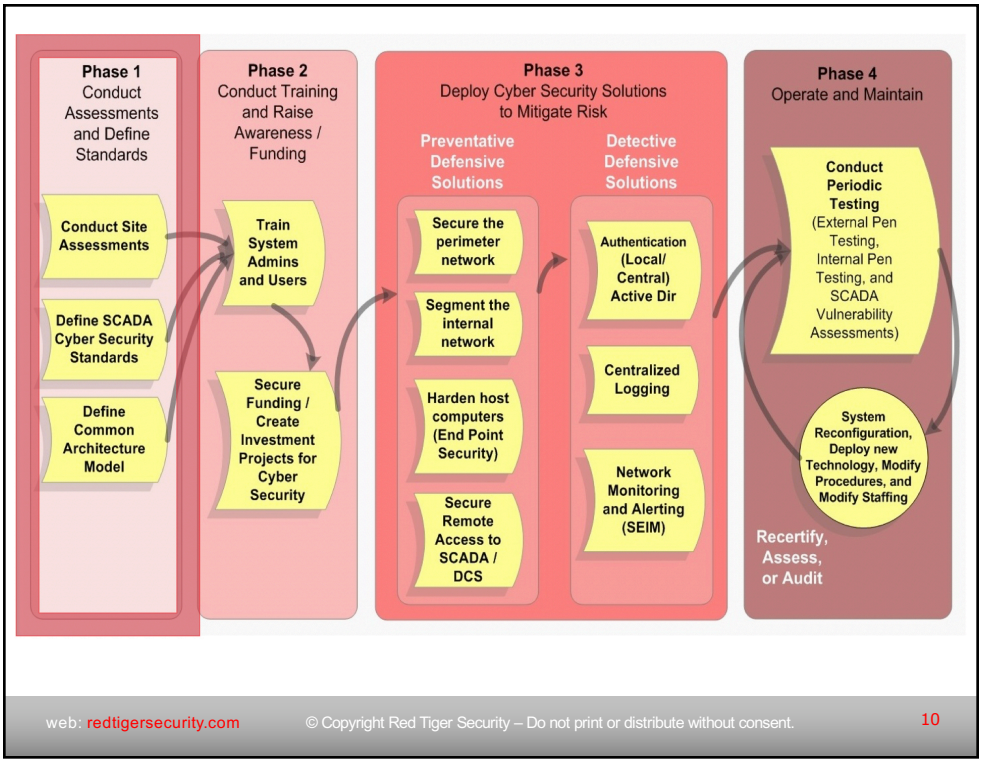
© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

How should we approach the problem?

< Methodology for Assessing ICS systems >

9



© Copyright Red Tiger Security – Do not print or distribute without consent.

10

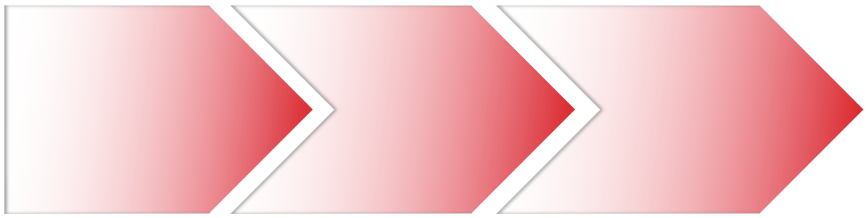
RED TIGER SECURITY

3-step process for understanding ICS/SCADA risk and building 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"



© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

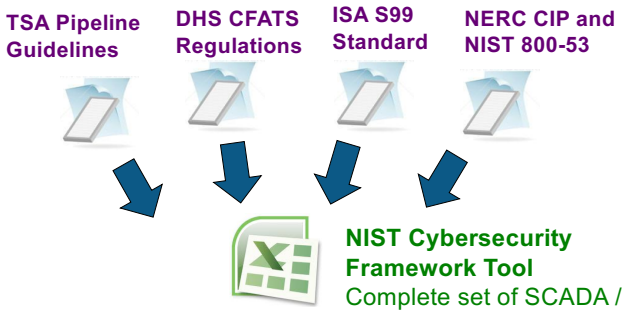
Site Assessments Should cover both **Technical** and **Policy/Procedures**

- Policy/Procedure Assessments should focus on the Controls Framework that are applicable to your industry:
  - 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

© Copyright Red Tiger Security – Do not print or distribute without consent.

NIST CSF for Critical Infrastructure

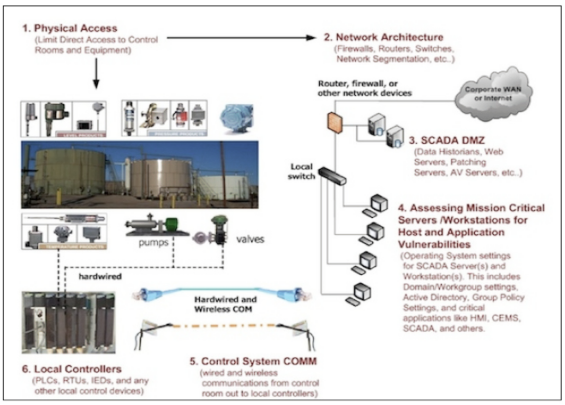
- The NIST Cyber Security Framework (CSF) harmonizes previously splintered cyber security standards that were written for various specific sectors, and creates one framework for measuring the current state of security controls
- NIST CSF is tailored for ICS/SCADA systems



© Copyright Red Tiger Security – Do not print or distribute without consent.

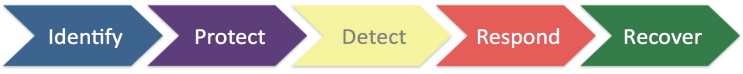
13

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



© Copyright Red Tiger Security – Do not print or distribute without consent.

14

RED TIGER SECURITY

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.

© Copyright Red Tiger Security –

15

RED TIGER SECURITY

Task 1 - Target State Definition

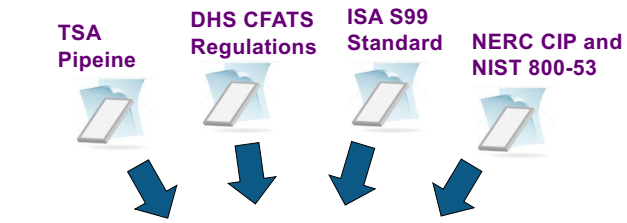
- **Positive Lessons Learned:**
  - The Target State Definition drives a stake into the ground to level-set the expectations for the ICS Security Program Development, and provides a common benchmark across the organization. The process creates a Target State for the organization that all departments 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, NER CIP, and ISA99/IEC62443 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.

© Copyright Red Tiger Security – Do not print or distribute without consent.

16

RED TIGER SECURITY

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



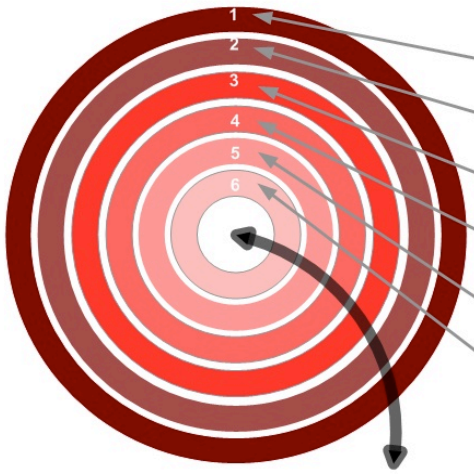
Policies, Procedures, and Controls Assessment

Technical Assessment of Sample Set of Field Sites

Conduct a Security Assessment of a Sample Set of sites and systems to determine the **Current State**

© Copyright Red Tiger Security – Do not print or distribute without consent.

17



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

18

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, NIST CSF, ISA99/IEC62443, CFATS, ISO, 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.

© Copyright Red Tiger Security – Do not print or distribute without consent.

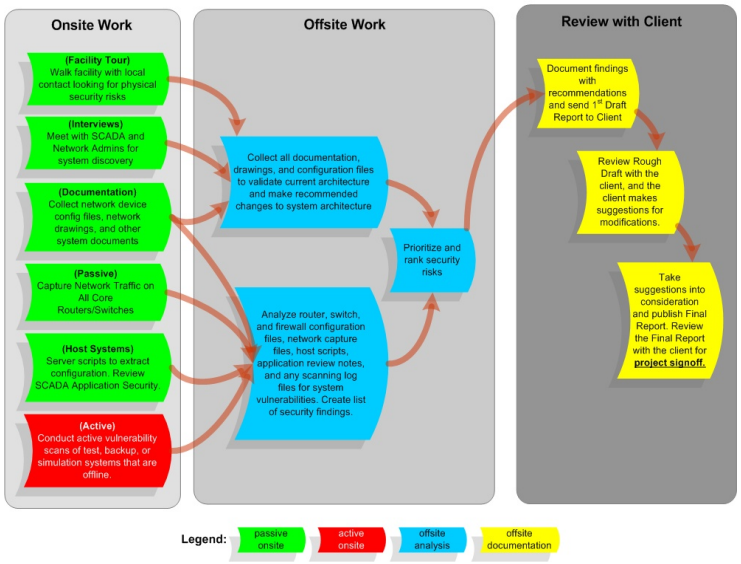
Objectives (continued)

- Follow a logical 6-layer approach that covers all system components in the following areas:
  1. Physical Security
  2. Network Infrastructure
  3. SCADA DMZ
  4. Control Room Assets (Servers/Hosts)
  5. SCADA Communications and Protocols
  6. Field Devices
- Pass on tips and tricks from 18 years of experience

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Vulnerability Assessment Methodology for SCADA / Process Control Systems

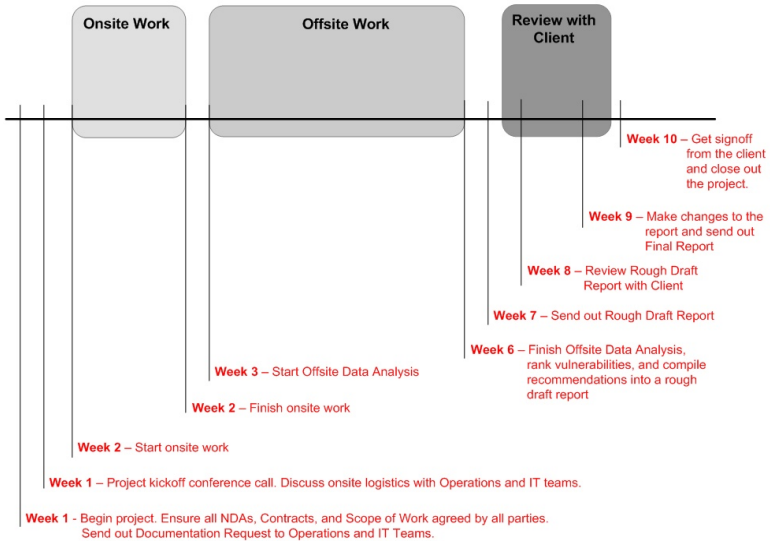


© Copyright Red Tiger Security – Do not print or distribute without consent.

21

RED TIGER SECURITY

Sample SCADA / Process Control Systems Vulnerability Assessment Timeline



© Copyright Red Tiger Security – Do not print or distribute without consent.

22

VA Team Resources

- Onsite Data Collection
  - Project Manager with Interview Skills
  - Network Engineer with Traffic Capture Capabilities
  - SCADA Engineer with Host/Application experience
- Offsite Data Analysis
  - Vulnerability Researchers who can parse PCAP files and compare Host/Application findings with CERT data
- Developing the Report Deliverable
  - Technical Writer to pull all pertinent data together and frame the recommendations

© Copyright Red Tiger Security – Do not print or distribute without consent.

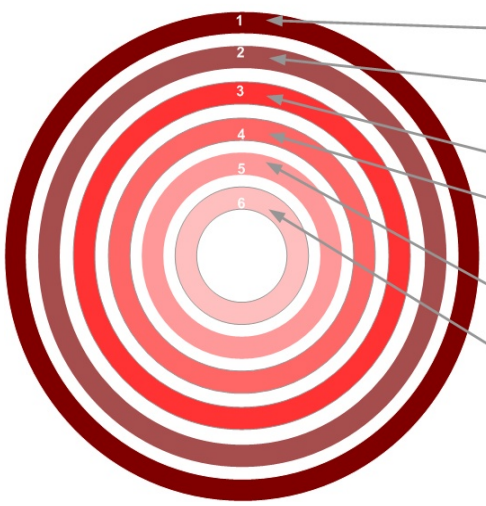
Planning for the Site Visit

- Conference call with local operations team ahead of time
  - coordinate best time for the trip onsite
  - ensure the right local resources will be present and available for interviews and assistance with collecting the network and control room data
  - discuss any operational risks during that time *(such as power plants during the heat of the summer)*
  - discuss any safety issues and proper personal protective equipment (PPE) that should be worn while onsite
  - provide an overview of what to expect from the team
  - send documentation request ahead of the trip so local resources can begin pulling together data and documents for the team
  - communication encryption for emailed documents and data collected onsite

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Six Layer SCADA Vulnerability Assessment Approach



1. **Physical Security**
   (Fencing, Surveillance, Guards, Gates, Locks)
2. **Network Infrastructure**
   (Switches, Routers, Firewalls, 3rd Party Connections, and Modems)
3. **Testing the SCADA DMZ**
   (Data Historians, Data Logging, Web Servers)
4. **Assessing the Mission Critical Servers / Workstations for Host and Application Vulnerabilities**
   (Operating System Security, Application Security)
5. **Communications to Field Devices**
   (Clear text transfers, traffic injection, hijacks)
6. **Field Devices**
   (PLCs, RTUs, IEDs, Plant Equip.)

© Copyright Red Tiger Security – Do not print or distribute without consent.

25

RED TIGER SECURITY

Control System Component Layers Involved in Security Audit

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

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



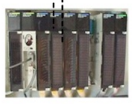




pumps

valves

hardwired



Hardwired and Wireless COM



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

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

Router, firewall, or other network devices

Corporate WAN or Internet

Local switch

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.

© Copyright Red Tiger Security – Do not print or distribute without consent.

26

Typical Folder Structure

- **/Site Name**
  - **/Onsite Data Collection**
    - **/Physical**
      - /Digital Pics
      - /Interview Notes
    - **/Network Infrastructure**
      - /Network Diagrams
      - /Device Configs
      - /Packet Captures
      - /Network Scans
    - **/SCADA DMZ**
      - /Host Scripts
      - /Packet Captures
      - /Network Scans
    - **/Control Room Assets**
      - /Host Scripts
      - /Packet captures
      - /Network Scans
      - /Application Security
    - **/SCADA Protocols**
      - /Packet Captures
    - **/Field Devices**
      - /Device Testing
  - **/Offsite Data Analysis**
    /Report Deliverable

© Copyright Red Tiger Security – Do not print or distribute without consent.

Data Encryption and Communication Tools

- TrueCrypt
  - Free (price is right Bob)
  - Available for Windows, Mac OSX, and Linux
  - Allows all team members to use same encrypted file vault
  - Password should be kept to only team members and sent through non-standard channels. For example, if data sent over email, then password spoken over the phone or sent through a text
  - Should use a 2GB or less file vault size, so entire file vault can be sent over the Internet or easily mailed on an inexpensive USB stick or DVD
- YouSendIT
  - Allows transmission of up to 2 Gig file sizes through email by sending a link to the file. File self-destructs in 7 days. Never send unencrypted data.

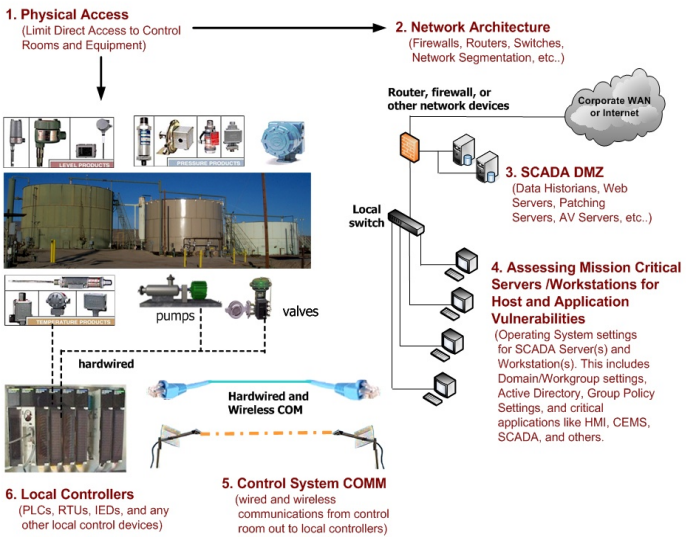
© Copyright Red Tiger Security – Do not print or distribute without consent.

Client and VA Team must decide on encryption level / tools up front

- PGP
  - Overly priced, complicated, and not supported easily on all operating system platforms
  - Thumbs Down ☹
- WinZip
  - Relatively cheap solution, supported by multiple platforms, most know how to use it, but encryption methods are weak
  - Thumbs Down ☹
- **TrueCrypt**
  - Free, supported on all major operating systems, easy enough to talk someone through over the phone to use, and supports many encryption standards including AES
  - Thumbs Up ☺

© Copyright Red Tiger Security – Do not print or distribute without consent.

Control System Component Layers Involved in Security Audit



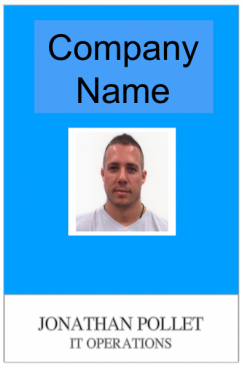
© Copyright Red Tiger Security – Do not print or distribute without consent.

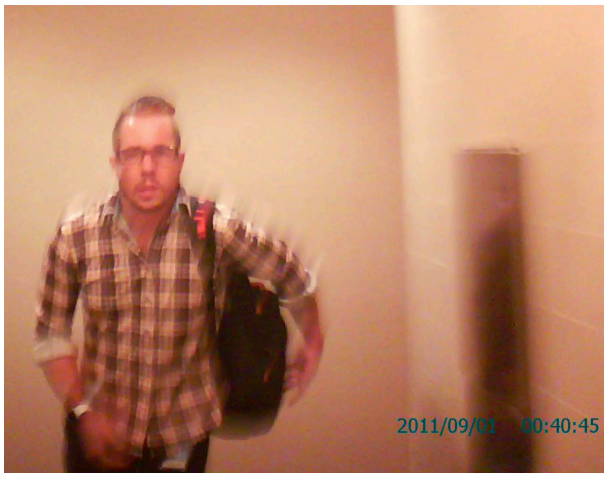
Layer 1. Physical Security

- Entire team takes facility tour and all look for potential physical security gaps in areas of access control and monitoring
- What steps do we take in order to go from the outside of the facility to the control room?
- Refer to any required specific compliance requirements (CFATS, NERC CIP, and others all have physical security requirements)

© Copyright Red Tiger Security – Do not print or distribute without consent.

Physical Security Must Compliment Cyber Security





© Copyright Red Tiger Security – Do not print or distribute without consent.

Layers 2 Through 6

- Divide and conquer along skill lines for remainder of the week onsite
  - Layer 2 and 5 - Network Engineer meets with network administrative contact on site
  - Layers 3 /4 and 6 - SCADA Engineer meets with the SCADA administrator onsite
  - Project Manager helps coordinate meetings, and captures notes from all interviews
- **Never** initiate any network scans without full knowledge and authorization from Control Room Operations

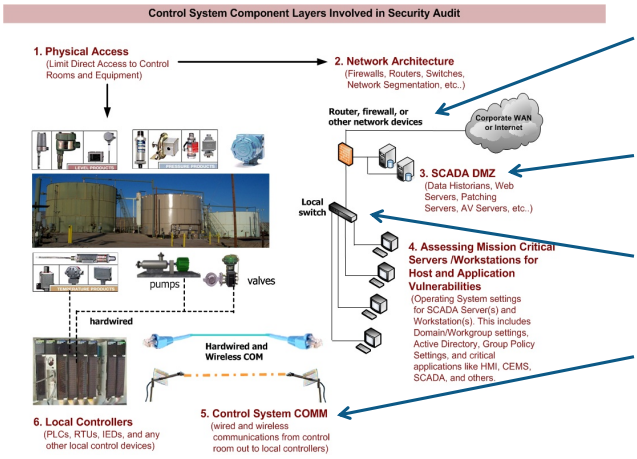
© Copyright Red Tiger Security – Do not print or distribute without consent.

Layer 2. Collecting Network Data

- PASSIVE - Capture network traffic at all core SCADA switches, and routers both on the inside and outside of the firewall (using TCPDUMP)
- Meet with local network and SCADA administrators to draw out local network (be thinking about the ISA 99 security levels, since report should include network re-design recommendations)
- Collect running configurations from all network devices
- ACTIVE - Scan all network segments outside of the SCADA LAN that are low-risk to Operations (with NMAP, NESSUS, or similar scanners)
- ACTIVE - Scan secondary SCADA networks, including development or testing systems, as long as the scan can not interrupt primary real-time networks (with NMAP, NESSUS, or similar scanners)

© Copyright Red Tiger Security – Do not print or distribute without consent.

Where to Capture Traffic?



- Outbound traffic to 3rd Parties and Corporate IT
- SCADA DMZ network
- Control Room HMI switch
- Field side communications

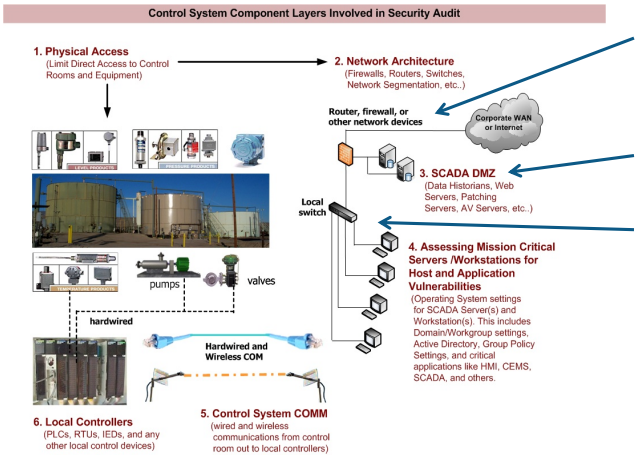
© Copyright Red Tiger Security – Do not print or distribute without consent.

Capturing Network Traffic

- Linux/Mac works best, but TCPDUMP can be compiled for Windows
- Wireshark has been known to drop packets on larger networks. *Command line has better kung foo :]*
- Set NIC interface without an IP address so all data packets exposed to the NIC interface will be captured
- **tcpdump -i eth0 -nn -vvv -tttt -XX -C 20 -s 0 -w filename**
- Above syntax chops up PCAP files into 20MB files, which are easier to parse > try this out now using your own laptops

© Copyright Red Tiger Security – Do not print or distribute without consent.

Where to Perform Vulnerability Scans?



- IT networks outside of SCADA firewall
- SCADA DMZ network
- Secondary, Development, or Testing SCADA systems
- NEVER SCAN LIVE PRIMARY SCADA NETWORKS

© Copyright Red Tiger Security – Do not print or distribute without consent.

ARP Scanner, Port Scanners, and Vulnerability Scanners

- ARP (Address Resolution Scanners) are software calls to the ARP tables on the network to request the MAC address, IP address, and host names for each device the network knows about. CAIN is an example.
- Port Scanners, like NMAP, can perform ARP scans and PING scans, but in addition to retrieving the IP address and host names of the device, they can also probe for the presence of particular TCP and UDP ports and retrieve their status (open, closed, filtered, etc..). Port scanners can not determine if a device is vulnerable, but they can provide what ports and services are running on the device.
- Vulnerability Scanners, like NESSUS, can dive deeper into the target device(s) on the network to not only bring back the IP address and open ports, but also determine the version of the services running on the device, then quickly compare the version of the services present on the device with its own known database of known vulnerable services.

© Copyright Red Tiger Security – Do not print or distribute without consent.

Use Active Tools with CAUTION

- SCADA VA Rule: **Know Thy Tools**
- Know what your scanning tools actually do, watch them in Wireshark
- Don't just point-click-shoot… *other scanners include:*
  - OpenVAS
  - Bindview RMS (Control Compliance Suite – Symantec)
  - GFI LANguard N.S.S
  - NetIQ Vulnerability Manager
  - Retina
  - SNSI

© Copyright Red Tiger Security – Do not print or distribute without consent.

Net Flow Interviews

- Network Engineer on the VA Team should be able to understand the current SCADA and Process Control networks, and how they connect to Corporate IT and other networks
- Should be able to draw the current state and recommended changes to the architecture to bring into compliance with applicable standards
- Next two slides show sample diagrams for current and recommended changes

© Copyright Red Tiger Security – Do not print or distribute without consent.

Testing SCADA DMZ and Control Room Host/Application Assessment

- Obtain permission to capture current state of:
  - operating system
  - patches
  - installed applications
  - users/groups/permissions
  - local security policy
  - network configuration (all NICs)
  - network connections
  - services/active ports
- NOTE: Consider automation of this with scripts tuned for the operating system

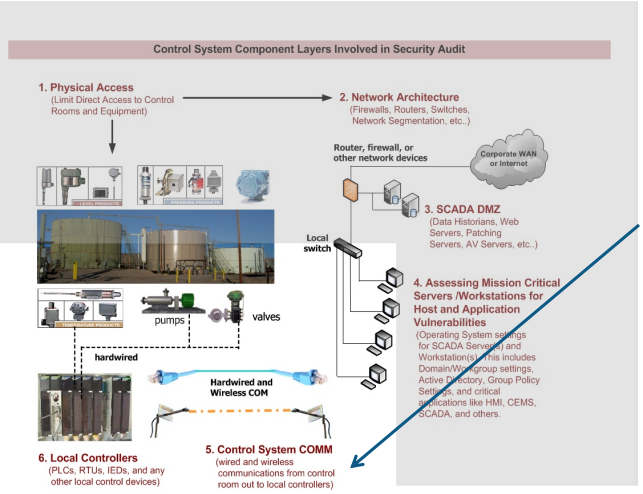
© Copyright Red Tiger Security – Do not print or distribute without consent.

Extracting Useful Information from ICS Servers and Workstations

- Either manually, or by leveraging a mobile app that does not require installation on the local host, obtain the following types of information from the SCADA workstation or server:
  - operating system
  - patches
  - installed applications
  - users/groups/permissions
  - local security policy
  - network configuration (all NICs)
  - network connections
  - services/active ports
- Data extraction demonstration using a USB tool created and customized by Red Tiger Security called REDCAT

© Copyright Red Tiger Security – Do not print or distribute without consent.

Layer 5. Testing SCADA Communications/Protocols



- We've looked at layers 1 through 4, now we have 5 and 6 left
- Passively Capture live SCADA traffic to analyze offline for clear text transfer
- NEVER ACTIVELY SCAN LIVE SCADA NETWORKS

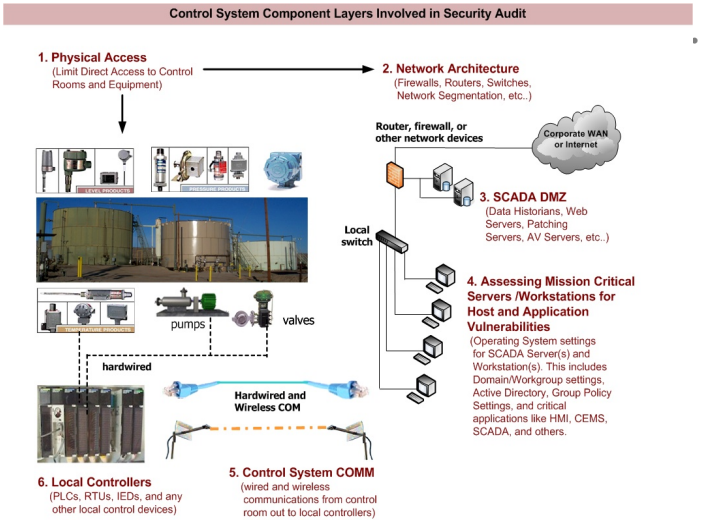
© Copyright Red Tiger Security – Do not print or distribute without consent.

Scanning Field Controllers (on a testbench or lab environment)

- Scan the controllers with NMAP (intense all TCP and UDP ports) to fully understand all ports and services exposed on the devices
  - Many have embedded web servers, ftp servers, email servers, and backdoor ports for support (telnet)
  - Knowing all ports and services available on each device is a required part of NERC CIP vulnerability assessments
- Scan the controllers with NESSUS to determine:
  - How the device behaves when under an active scan
  - If the device is running any vulnerable services

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY



Review Time…

- Match the layer to be tested with the VA Team resource best suited to collect the data onsite:

- Network Engineer
- SCADA Engineer
- Project Manager

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Project Manager should combine data collected by all team members.

One master copy of all data collected onsite should be kept by the Project Manager, and also given back to each team member.

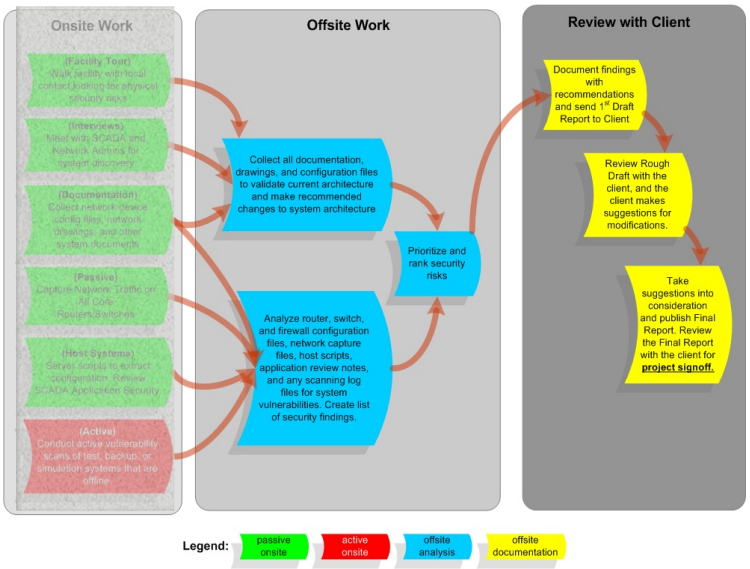
Data must be encrypted.

- **/Site Name**
  - **/Onsite Data Collection**
    - **/Physical**
      - /Digital Pics
      - /Interview Notes
    - **/Network Infrastructure**
      - /Network Diagrams
      - /Device Configs
      - /Packet Captures
      - /Network Scans
    - **/SCADA DMZ**
      - /Host Scripts
      - /Packet Captures
      - /Network Scans
    - **/Control Room Assets**
      - /Host Scripts
      - /Packet captures
      - /Network Scans
      - /Application Security
    - **/SCADA Protocols**
      - /Packet Captures
    - **/Field Devices**
      - /Device Testing
  - **/Offsite Data Analysis**
    /Report Deliverable

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Vulnerability Assessment Methodology for SCADA / Process Control Systems



© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Offsite Data Analysis – Workload Broken Down by Team Resource

- Network Engineer (layers 2 and 5)
  - Analyze network device configuration files
  - Analyze network traffic captures (PCAP Analysis)
  - Analyze and research vulnerabilities detected from active scans
- SCADA Engineer (layers 3,4, and 6)
  - Review output from all Host DUMP scripts for operating system vulnerabilities
  - Analyze the information captured from onsite SCADA Application Testing work
  - Report on the results from the Field Controller scans and attack tests
- Project Manager (layer 1 and help with others as needed)
  - Analyze and report on physical security findings
  - Summarize notes from all onsite interviews
  - Assist with Data Analysis as needed by the Network and SCADA engineers

© Copyright Red Tiger Security – Do not print or distribute without consent.

Network Engineer – Offsite Analysis > Device Configuration Analysis

- Noteworthy Network Device Configuration Checks
  - Review all running config files from switches, routers, and firewalls to ensure Rule of Least Privilege has been used in the configuration
  - Check to see if network devices are at the latest firewall release available
  - Check for the ability to configure these devices over the network, if SSH (secure shell) is required when configuring devices, and in critical cases, configuration should only be allowed over serial (console cable) connection
  - Check for proper SNMP configuration
  - Check for proper logging for forensic and compliance purposes
  - Check for consistent time source for all device
  - If physical access is not restricted to the ports on the switches, then consider recommending port security (sticky MAC addresses)
  - If man-in-the-middle threats exist, consider ARPwatch recommendation

© Copyright Red Tiger Security – Do not print or distribute without consent.

Network Engineer – Offsite Analysis > Traffic and Protocol Analysis

- Noteworthy PCAP Traffic Dump Checks
  - Run .CAP files through several network analysis tools
    - NetworkMiner
      HoneySNAP
    - Free Packet Analyzer
  - Should be using an eye for detecting:
    - Flow / network connections in and out of SCADA
    - Clear text protocols (TELNET, FTP, HTTP, most SCADA Protocols)
    - Passwords and SCADA Traffic sent in the clear
    - Known malicious protocols
    - Excessive broadcast storms indicative of mis-matched switchport settings
    - Excessive net flows to or from a particular source or destination address

© Copyright Red Tiger Security – Do not print or distribute without consent.

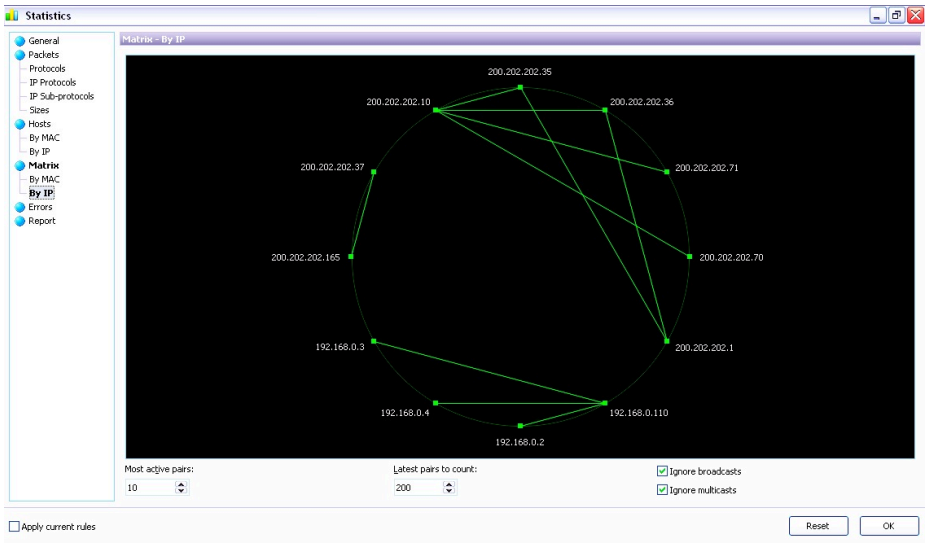
Network Engineer – Offsite Analysis > Traffic and Protocol Analysis

- Traffic Analysis report should indicate a protocol breakdown.
- Tcpdstat, ipsumdump, and Netdude can generate similar protocol breakdown analysis.

```
### Protocol Breakdown ###
< <<<
     protocol          packets                bytes          bytes/pkt
-------------------------------------------------------------------------
[0] total        134347439 (100.00%)     101530372750 (100.00%)    755.73
[1] ip           134347439 (100.00%)     101530372750 (100.00%)    755.73
[2]  tcp         118172509 ( 87.96%)      97361936181 ( 95.89%)    823.90
[3]   ftpdata        18640 (  0.01%)         16529412 (  0.02%)    886.77
[3]   ftp            72372 (  0.05%)          4697330 (  0.00%)     64.91
[3]   ssh        13849679 ( 10.31%)      11113777353 ( 10.95%)    802.46
[3]   telnet          9007 (  0.01%)          1526445 (  0.00%)    169.47
[3]   smtp         2133471 (  1.59%)       1447293494 (  1.43%)    678.38
[3]   name              23 (  0.00%)             1426 (  0.00%)     62.00
[3]   dns           35071 (  0.03%)          7071657 (  0.01%)    201.64
[3]   http(s)     25043480 ( 18.64%)      30677552254 ( 30.22%)   1224.97
[3]   http(c)     16165378 ( 12.03%)       2182851897 (  2.15%)    135.03
[3]   kerb5             370 (  0.00%)            30610 (  0.00%)     82.73
[3]   pop3            82382 (  0.06%)         26718043 (  0.03%)    324.32
```


© Copyright Red Tiger Security – Do not print or distribute without consent.

Review live network sessions



© Copyright Red Tiger Security – Do not print or distribute without consent.

Network Traffic Analysis

- Conducting the protocol analysis allows us to compare what traffic was on the wire at the time of the assessment, and we can compare the traffic collected with the applications and services that should be expected
- Vulnerable clear-text protocols such as TELNET, and FTP should be further researched
- Any known malware protocols such also be further researched
- Sorting by the hosts with the most bytes SENT or RECEIVED discloses the devices that are the most “chatty” on the network. Does those devices make sense, or have the device been compromised by a rootkit?
- Drawing out the communications matrix “by IP address” allows us to see what devices where communicating with other devices at the time of the assessment

© Copyright Red Tiger Security – Do not print or distribute without consent.

Network Engineer – Offsite Analysis > Vulnerability Scan Analysis

- Review the results from all active Vulnerability Scans, and group similar vulnerabilities
- Compare vulnerability findings at the host level with those detected by the SCADA engineer in the host DUMP scripts
- Remove any false positives from the list of vulnerabilities at both the network and host/application layer

© Copyright Red Tiger Security – Do not print or distribute without consent.

Network Engineer – Offsite Analysis > Summarizing the security findings

- Create an overall list of security findings based on the analysis of:
  - Network device configurations
  - Traffic dumps (PCAP analysis)
  - Vulnerability Scans
- If the same vulnerability is found on multiple devices or hosts, then group this under one vulnerability, bust site the “Systems Impacted”
- For each security finding, research and document a recommended remediation strategy
- Rank the findings, and generate individual security finding tables for each vulnerability to feed into the Draft Report

© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Finding Table

(sample)

Find #: 2

Vulnerability	Severity Level
2. TELNET Protocol Enabled	

Description	Business Impact
The identified service is running and has been identified to have several high level vulnerabilities that can be exploited on mission critical systems. Additionally the possibility of the interception of both user name and password combinations remains present. The review and analysis of the use of the protocol should be identified within the automation network.	Know vulnerabilities exist for this application and the protocol that supports the appliance. The business reason for this application to be in use should be examined and preferably denied in favor of a more secure protocol (SFTP) as well as a vigilant patching cycle.

Systems Affected:	Unit 3, Unit 2, Coal Handling, Unit 2/3 Scrubber
Recommendations	Review the use of this application and service within the automation environment
Level of Effort:	L

Response / Actions

© Copyright Red Tiger Security – Do not print or distribute without consent.

Network Engineer – Offsite Analysis > Summarizing the security findings

- The Network Engineer should also provide the Project Manager with two network diagrams developed through interviews with the client while onsite
  - Current State Network Diagram
  - New Proposed Network Redesign Diagram
- These two diagrams should be in the Rough Draft report, and any recommended changes to the network design should be backed up with content as to why the new design will mitigate existing and future security vulnerabilities
- This should include how remote users access the SCADA and Process Control systems, along with how data flows from the SCADA system out to the Corporate IT network and 3rd parties that require real-time or historical data.

© Copyright Red Tiger Security – Do not print or distribute without consent.

SCADA Engineer – Offsite Analysis > Host DUMP script Analysis

- Noteworthy things to look for in operating system DUMP logs:
  - Missing operating system security patches
  - Missing application patches that impact security
  - Excessive installed applications, or existence of applications that may not be job essential (*iTunes, Peer-to-Peer file sharing, IM, weird video Codecs, games, etc…)*
  - Users/groups/permissions – especially excessive use of Administrator accounts
  - Stale or vendor default accounts
  - Insufficient or weak password change policy
  - Weak or insecure AD / Windows Domain configuration
  - Weak Local / Group Security Policy
  - Network configuration (all NICs)
  - Excessive network connections or connections to unknown devices
  - Excessive or non-essential available services/active ports
  - Connectivity to other systems

© Copyright Red Tiger Security – Do not print or distribute without consent.

SCADA Engineer – Offsite Analysis > SCADA Application Testing Analysis

- Noteworthy things to notice from SCADA Application Testing:
  - Application-to-Operating System Security
    - Does the application limit user access to either the desktop, OS, or start menu
    - Does the application restrict implementing CTRL-ALT-DEL on windows-based systems, because this can be used to launch new applications or open windows explorer. Alternatively, on *nix systems, can the user evoke a new shell.
    - What underlining OS user accounts the application has been configured to run in, and note if the application is running in the “Administrator” or “Root” accounts, or if the user account has those privileges
  - Application-to-User Security
    - Analyze the user security profile for the application. Is it role based? It is connected with the Host security? If so, are the accounts local accounts or domain accounts? If domain accounts, is there a separate domain for SCADA?
  - Application-to-Application Security
    - Analyze traffic captured while onsite while application was in use. Is data sent in the clear between applications? Are usernames and passwords sent in the clear. Traffic should have been captured while a user was remotely logging into an application over the network.

© Copyright Red Tiger Security – Do not print or distribute without consent.

SCADA Engineer – Offsite Analysis > Field Controller Testing Analysis

- Noteworthy things from Field Controller Testing:
  - NMAP or Vulnerability Scans results
    - Note the active services and available ports on the controller
    - Note any security vulnerabilities exposed by the scanner
    - Note if simply scanning the controller impairs the operation of the controller
  - DoS Attacks
    - Note how the field controller stands up to DoS (Denial of Service) attacks as they increase from a small byte size to larger byte size
    - Document how the controller recovers when the attack is over
  - Malformed Attacks
    - Note how the field controller stands up to malformed packet attacks as various payloads are altered
    - Document how the controller recovers when the attack is over
  - Summarize vulnerabilities discovered

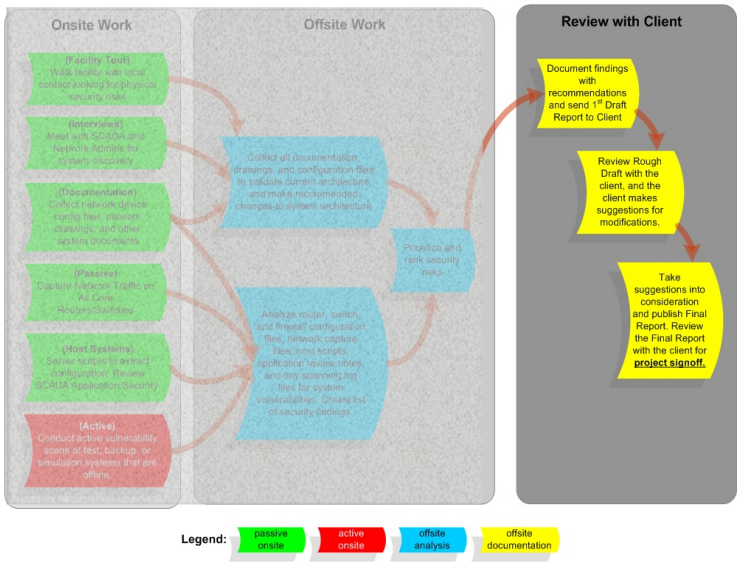
© Copyright Red Tiger Security – Do not print or distribute without consent.

Project Manager – Offsite Analysis > Building Draft Report

- Analyze physical security findings, rank them, and create security finding tables for each area that needs improvement
- Obtain finding tables from the Network and SCADA engineering team members, and sort all security findings from all system layers from highest security severity to lowest
- Compile all findings, interview results, diagrams, and security finding tables into a Rough Draft report
- Write the Executive Summary for the Rough Draft and send it to the Operational and IT teams for the facility being assessed

© Copyright Red Tiger Security – Do not print or distribute without consent.

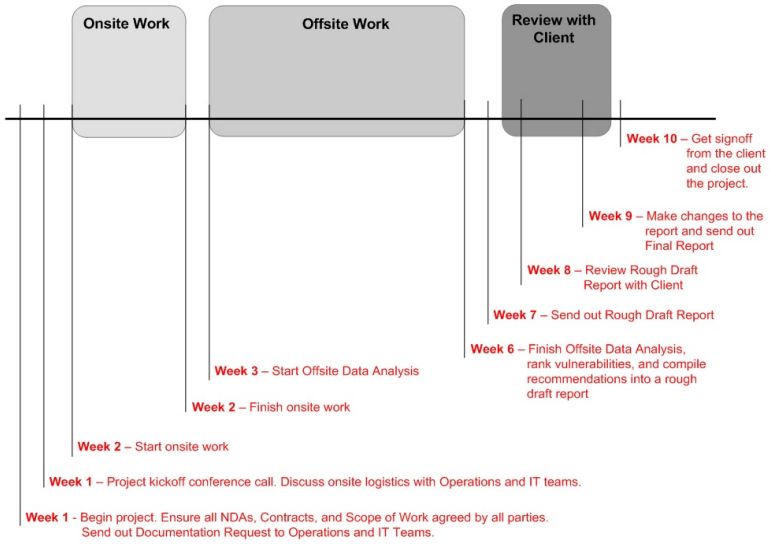
Vulnerability Assessment Methodology for SCADA / Process Control Systems



© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Sample SCADA / Process Control Systems Vulnerability Assessment Timeline



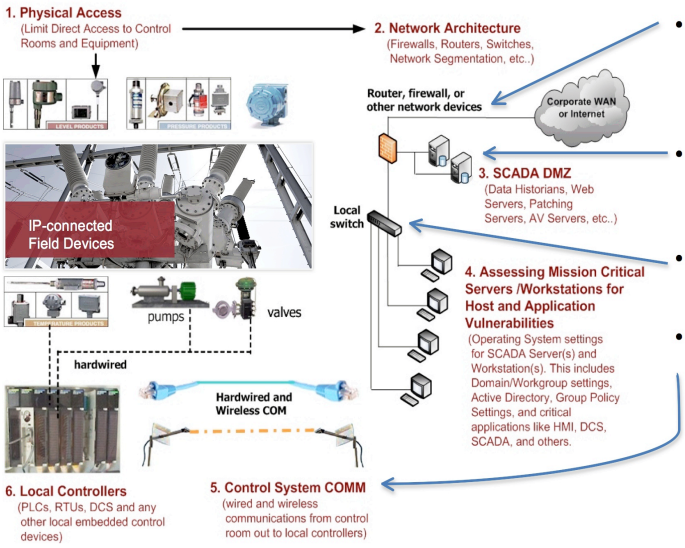
© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Summary

- This session was developed to pass along a time-proven methodology for safely conducting Vulnerability Assessments on SCADA and Process Control Systems. These type of projects are easier to manage when tasks are divided into three stages:
  1. Onsite Data Collection
  2. Offsite Data Analysis
  3. Developing the Report Deliverable
- This session also specifically covered how to safely collect the data onsite from the (6) layers of a typical system:
  - 1. Physical, 2. Network Infrastructure, 3. SCADA DMZ, 4. Control Room Hosts and Applications, 5. SCADA Protocols and Communications, and 6. Field Controllers.
- This session provided typical project timelines, VA Team Resources, Team member roles, tasks to be performed at each stage in the project, tips and techniques for onsite and offsite work, and a sample report deliverable

© Copyright Red Tiger Security – Do not print or distribute without consent.



- Outbound traffic to either the Corporate IT network or other foreign networks
- Traffic flowing through the SCADA DMZ interfaces
- Control Room HMI Traffic
- Field device protocols if they are being polled over a TCP/IP connection

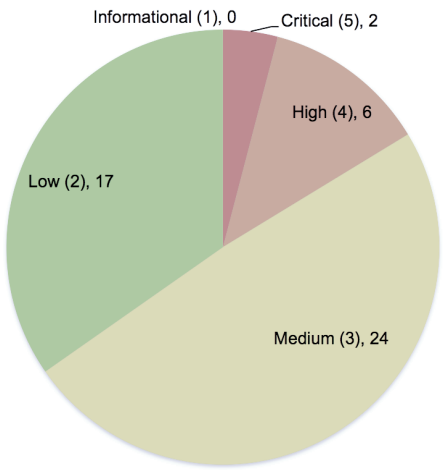
© Copyright Red Tiger Security – Do not print or distribute without consent.

Sample Vulnerability Finding Table

Finding Number (unique identifier)	Find No. 4
Severity Rating (from 1 through 5)	Vulnerability - Severity: 4
Vulnerability Title	Rules Allow Access to Administrative Services
Vulnerability Description	Description: Administrative network services are essential to enable network administrators to remotely configure, update, modify and monitor the systems. Typically these services fall in to two groups: - remote command, graphical or web-based environments that enable administrators to quickly configure and manage devices; - informational services which either provide alerts, notifications and may also enable the modification of settings using specialist software.
Impact of the vulnerability	Business Impact: The administrative services by their nature enable the remote configuration of a device and access to a wealth of sensitive configuration information. These services are likely to be a prime target for an attacker who may attempt to gain access by exploiting a vulnerability or attacking the authentication systems.
Systems Affected by the Vulnerability	Systems Affected: XXX.XXX.XXX.XXX
Recommended Remediation Action Plan	Recommendations: Red Tiger Security recommends that network filter rules should only be configured to allow access to administrative network services from those who are authorized. Red Tiger Security recommends that: - filter rules should only allow access to specific destination addresses; - filter rules should only allow access to specific destination network ports; - filter rules should only allow access from specific source addresses; - filter rules should specify a specific network protocol; - ICMP filter rules should specify a specific message type; - filter rules should always drop network packets and not reject them; - filter rules should perform a specific action and not rely on a default action.
	Response/Actions

© Copyright Red Tiger Security – Do not print or distribute without consent.

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



© Copyright Red Tiger Security – Do not print or distribute without consent.

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

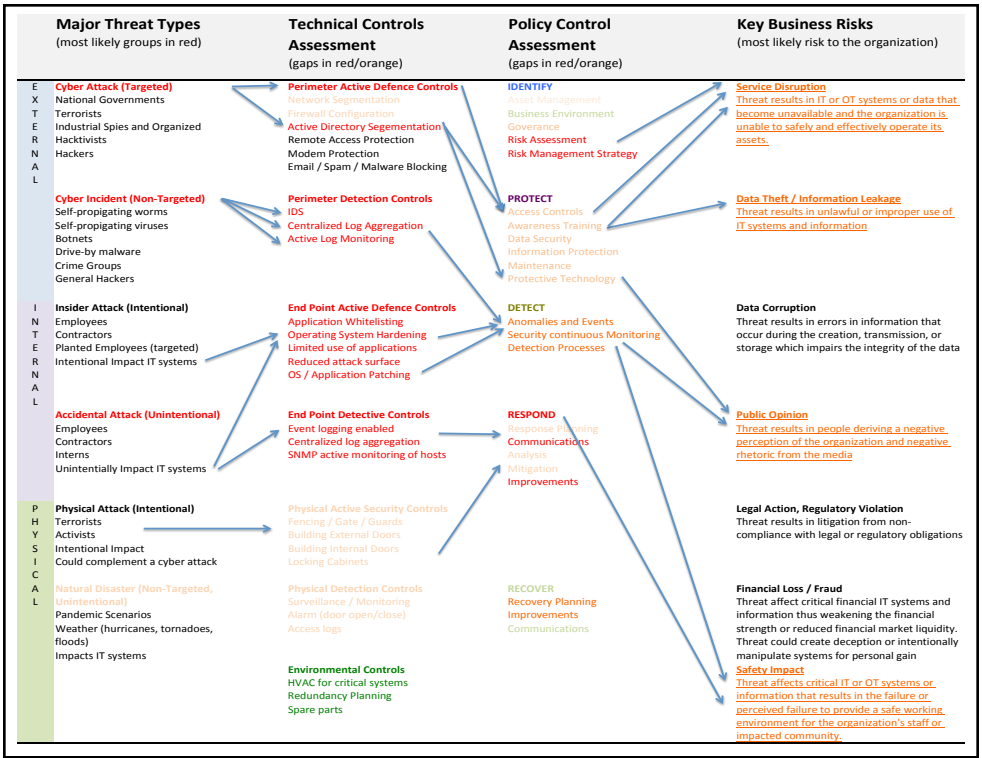
- The controls assessment exposes High, Medium, and Low risk from a Policy/Procedures/Controls perspective. In this sample case, High risk areas included:
  - Defining Cybersecurity Roles and Responsibilities for the Entire Workforce
  - Establishing an Organizational Information Security Policy
  - 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

© Copyright Red Tiger Security – Do not print or distribute without consent.

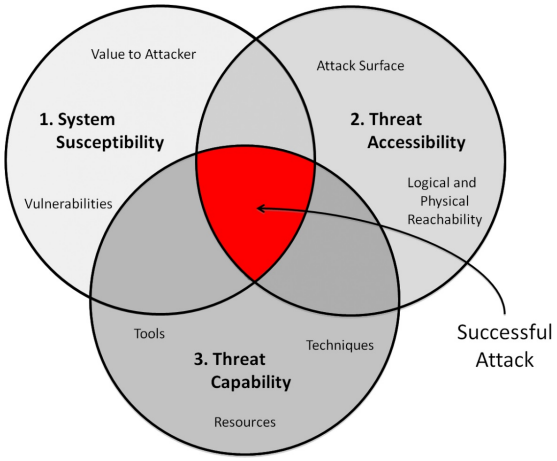
Start with the End in Mind

- The outcome should be a clear focused and actionable plan that reduces the GREATEST about of risk (both technical and procedural) in the SHORTEST amount of time
- Avoid spinning your wheels chasing technical solutions or implementing policies that do not actually reduce risk
- It can be difficult, but the only way to get traction in your organization is to convert technical problems into the language that executives can understand and get behind

© Copyright Red Tiger Security – Do not print or distribute without consent.



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 true Cyber Risk

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

© Copyright Red Tiger Security – Do not print or distribute without consent.

Biggest Myths Concerning Operational Risk

- Rick is not determined by threat motivation
  - "Why would someone want to target us" is the wrong place to start
  - In over 90% of cyber incidents, the victim of the attack was not the intended target
- Risk is determined by a combination of System Susceptibility *(unhardened and unmanaged assets)* and Threat Accessibility *(vulnerable architecture, weak configurations, or lack of technical controls)*
- If the system assets are vulnerable to exploitation, and the threat can access these assets with relative ease, then the system is in a **High Risk** state
- Most of our ICS Security Assessments have proven that ICS systems **are operating in a High Risk state**.

© Copyright Red Tiger Security – Do not print or distribute without consent.

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

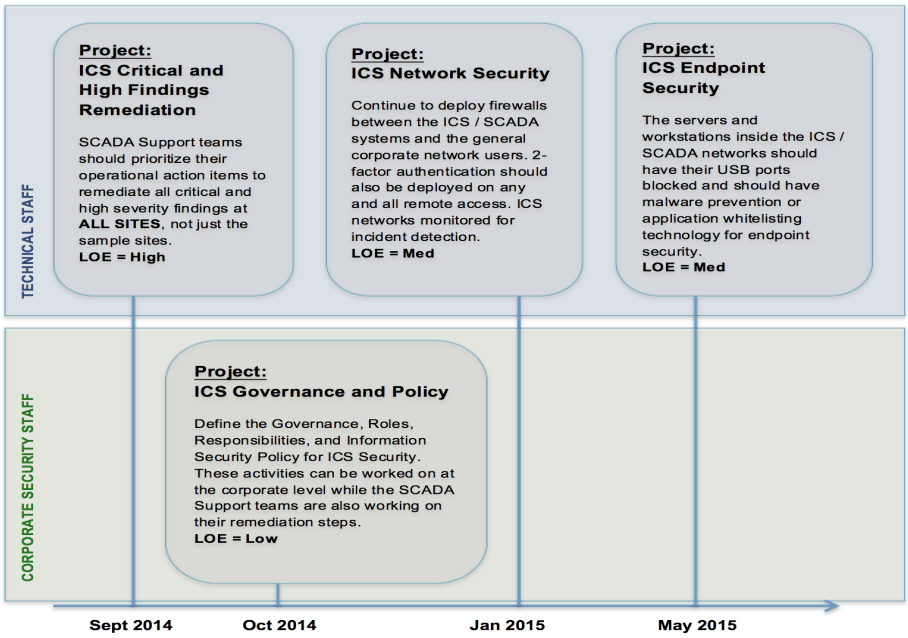
© Copyright Red Tiger Security – Do not print or distribute without consent.

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.

© Copyright Red Tiger Security – Do not print or distribute without consent.

Strategic Roadmap – Highest Priority



75

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.

© Copyright Red Tiger Security – Do not print or distribute without consent.

76

RED TIGER SECURITY

6 years experience using this same 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

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Summary

ICS and operational systems are no longer proprietary, and no longer isolated

ICS systems are more vulnerable than ever in history

Your system will most likely be impacted by a cyber treat that was not intentionally targeting your organization

Use a proven approach designed to access the gaps and reduce both technical and procedural risk by using the three steps:

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

© Copyright Red Tiger Security – Do not print or distribute without consent.



Jonathan Pollet, CAP, CISSP, PCIP
Founder, Executive Director
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