Proven Strategies for Securing ICS/SCADA Systems :: jonathan pollet – red tiger security

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

Outline

- Quick Intro to Red Tiger Security and project lead Jonathan Pollet
- What has changed in the world over the past 10 to 15 years that has made Cyber Security critical for both Corporate Business IT and Operational Industrial Control Systems
- Quick review on a proven methodology for assessing risk in ICS systems, and lessons learned from a sample of over 300 ICS security projects conducted over the past 15 years (TECHNICAL)
- Comparison of several ICS security compliance requirements ranging from NIST CSF in North America, NESA in the UAE, and the Critical Infrastructure requirements in Oman, Qatar, and other GCC countries (POLICY)
- Interesting trends, statistics, and tips learned along the way
- Question and Answers with Speaker (ICS Security Expert)

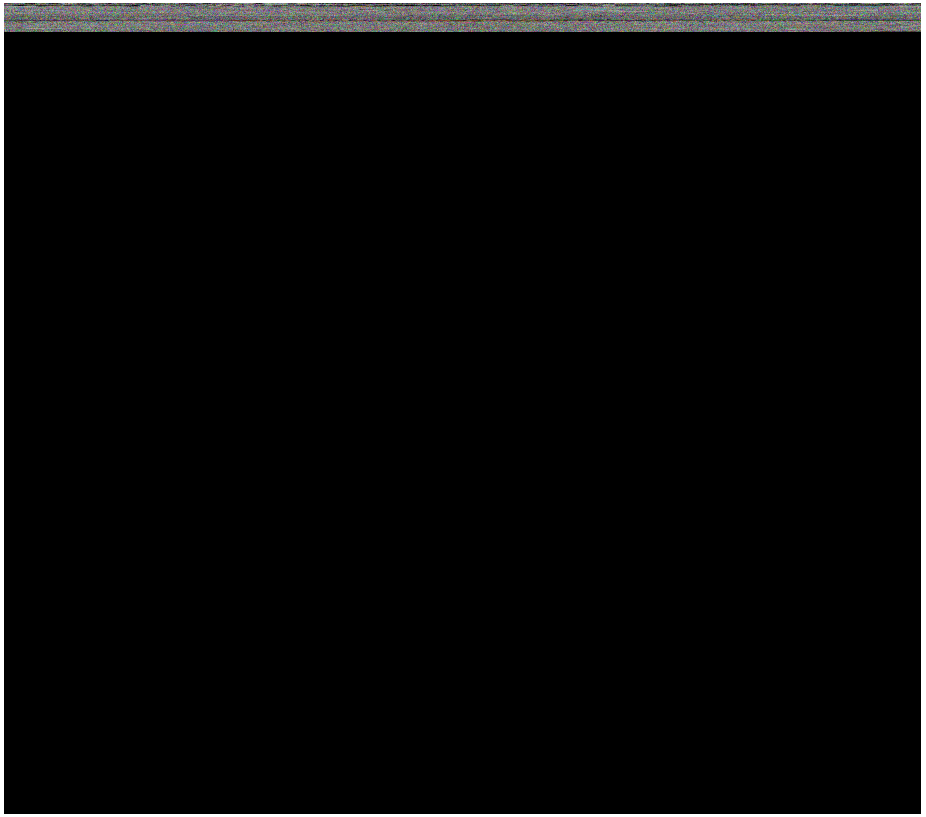
© Copyright Red Tiger Security – Do not print or distribute without consent.

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.

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 ICS Security
  - Published White Papers on SCADA Security early in 2001
  - Focused research and standards development for ICS Security since 2002
  - Conducted over 300 security assessments on Critical Infrastructure systems
  - Conducted over 150 International conferences and workshops on CIP
  - Developed safe security assessment methodology for live SCADA Systems
  - Co-developed the SCADA Security Advanced 5-day training course
  - Trained over 2500 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.

Clients in the GCC Area (2008 to present)

- Qatar
  - ictQatar
  - Dolphin Energy
  - Maersk Oil
  - Qatar Steel
- Oman
  - PAEW
- UAE
  - (DEWA) Dubai Electric and Water Authority
  - (EMAL) Emirate Aluminum
  - (ADNOC) GASCO
  - ADMA
- Saudi Arabia
  - Aramco

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

RED TIGER SECURITY

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

< Defining the problem >

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.

SCADA and Industrial Control Systems technology has changed over the past 20 years



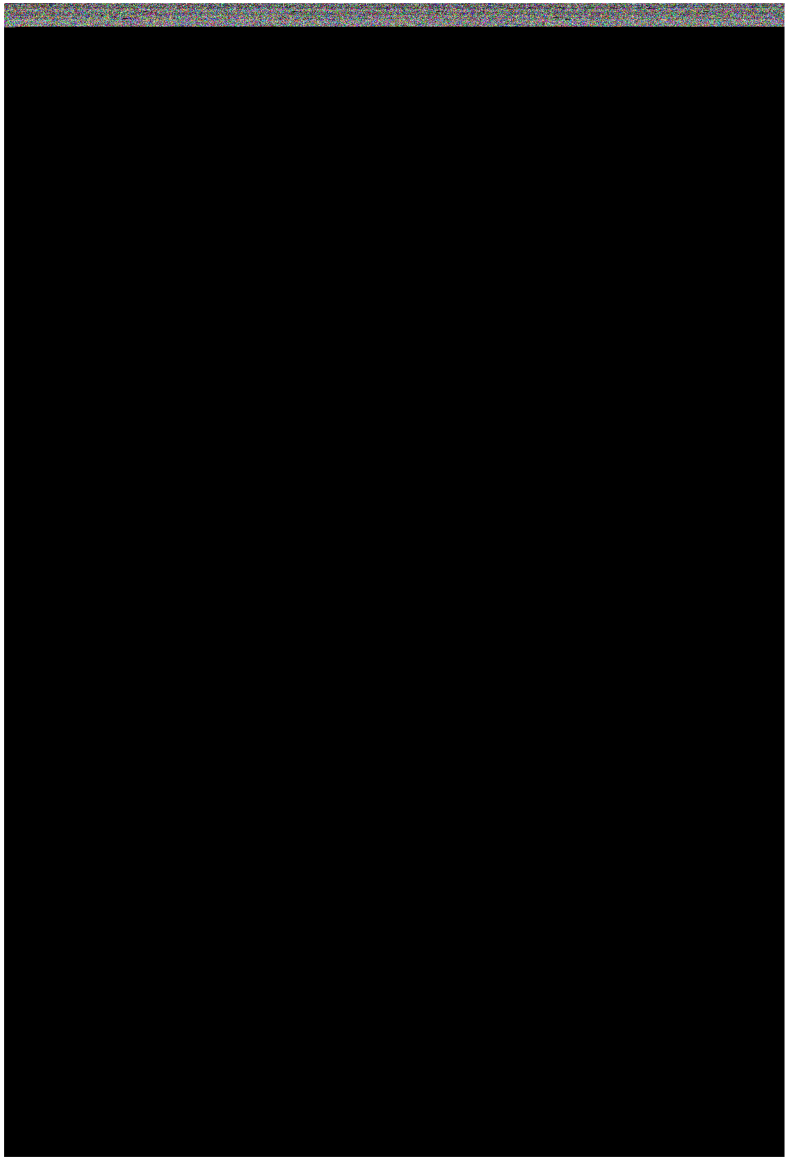
© Copyright Red Tiger Security – Do not print or distribute without consent.

All we had to worry about before was physical access



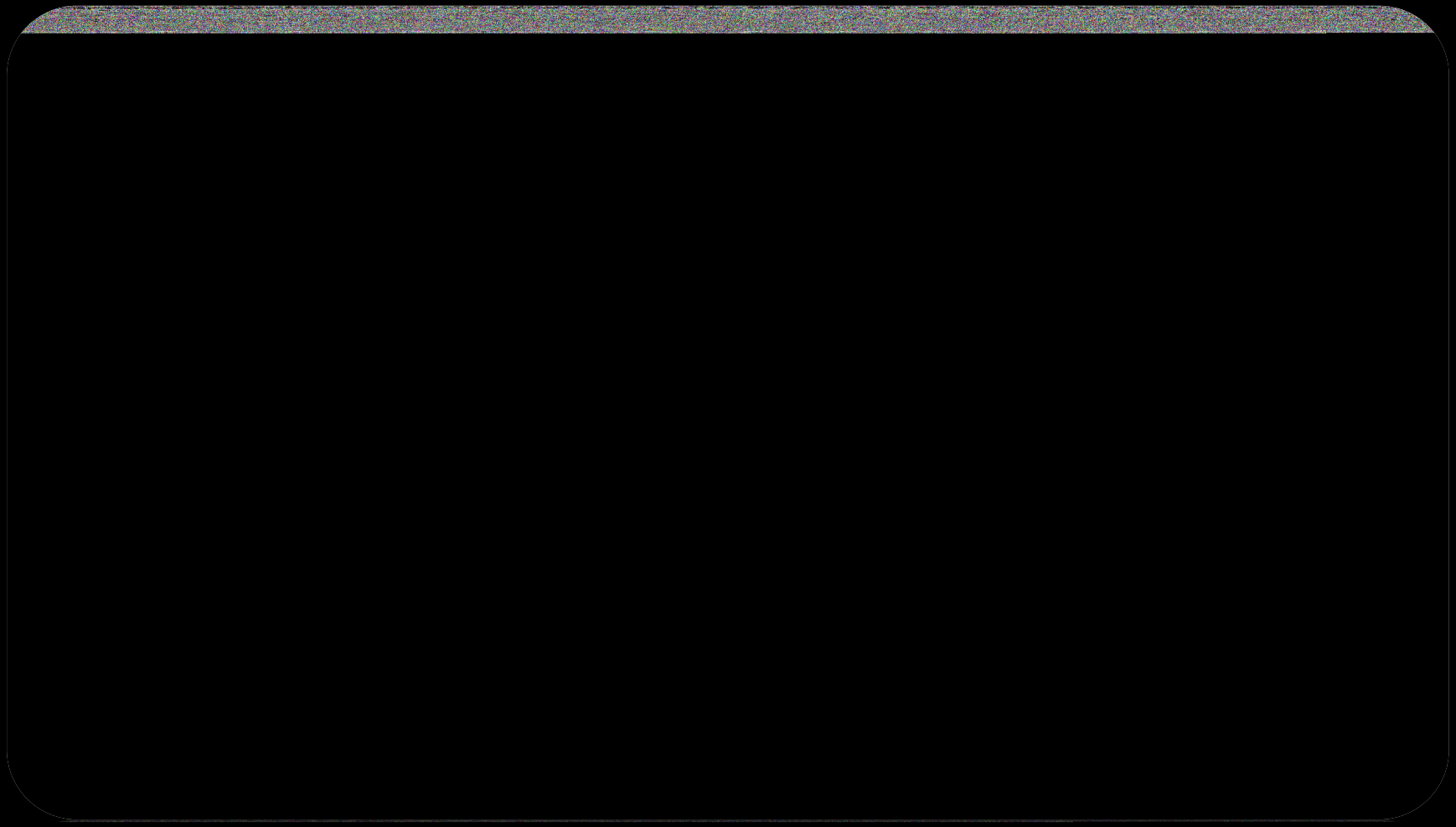
© Copyright Red Tiger Security – Do not print or distribute without consent.

Old Federal Reserve Bank Vault Underground in Houston, Texas



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

Now ICS systems are digital and connected…



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

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



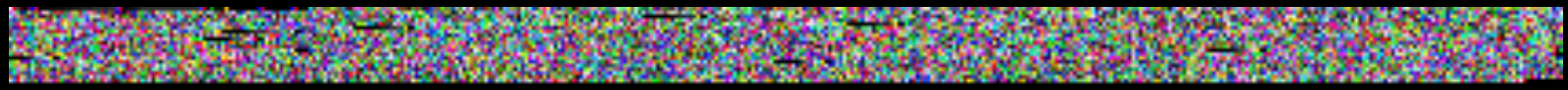
© Copyright Red Tiger Security – Do not print or distribute without consent.

Data is sent in the clear, without any requirement for encryption or authentication



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

ICS control rooms and are morphing into IT data rooms



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

From a cyber perspective, ICS systems look similar to business systems

- Cisco ASA firewalls or equivalent
- Cisco 3750 / 6509 switch fabric
- Servers and workstations running on Windows platforms (WinXP/2003/Vista/7/2008)
- Active Directory
- File/Print servers
- However…. They often lack the protection that typical Corporate IT systems have

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

ICS Systems Are Now Targets

- Security vulnerability disclosures for insecure ICS system components and software applications increased %763 from 2008 to 2018
- All penetration testing platforms (including the freely available Metasploit) have SCADA-specific exploits
- Cyber incidents that impact SCADA and Industrial Control Systems increased from 2003 through 2018
- Since Stuxnet was released in 2010 there has been numerous cyber attacks developed specifically to take control over SCADA and ICS systems for destructive purposes

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

Publicly Disclosed Vulnerabilities Affecting ICS on the rise



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



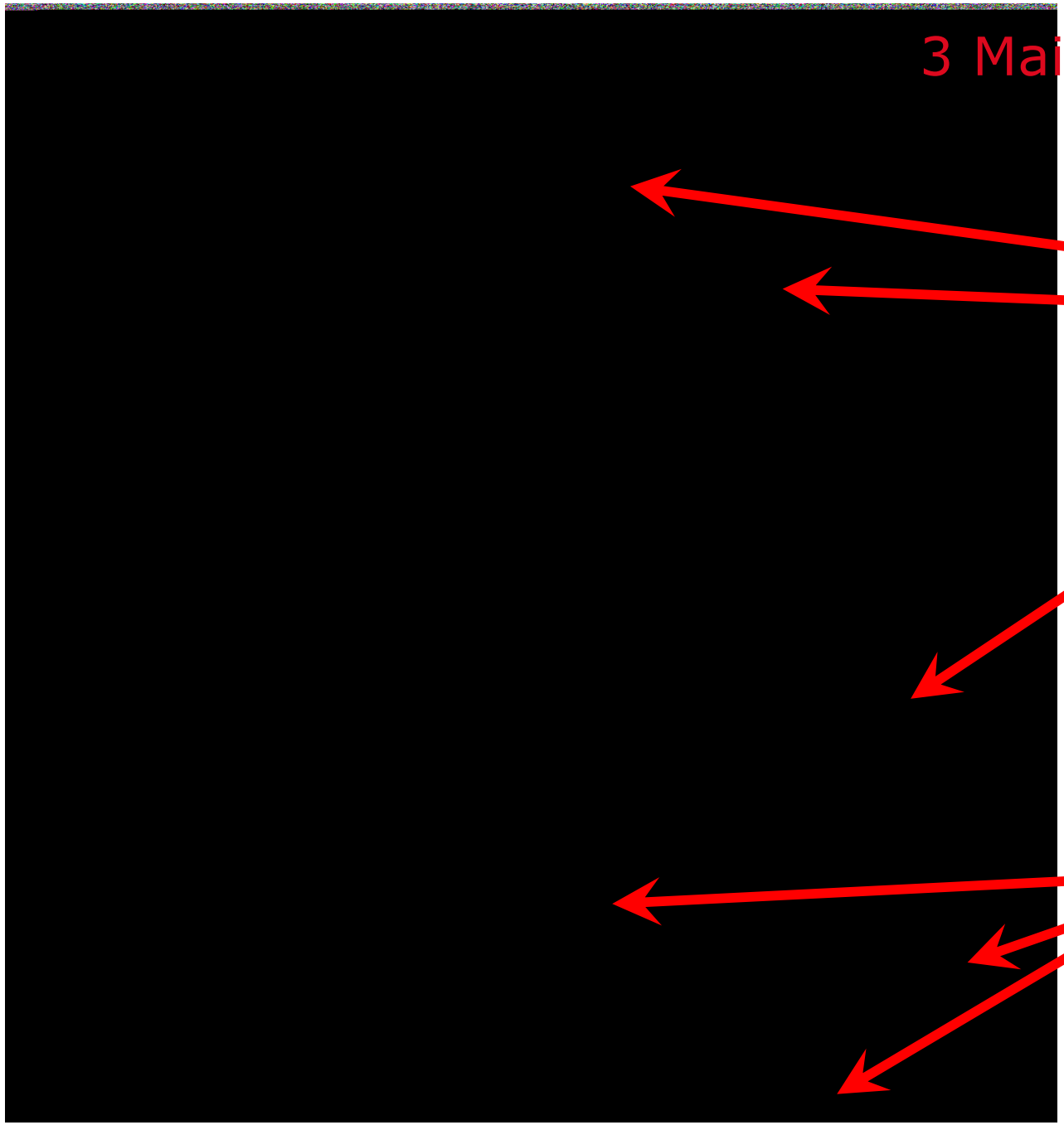
© Copyright Red Tiger Security – Do not print or distribute without consent.

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.

3 Main Areas of Concern

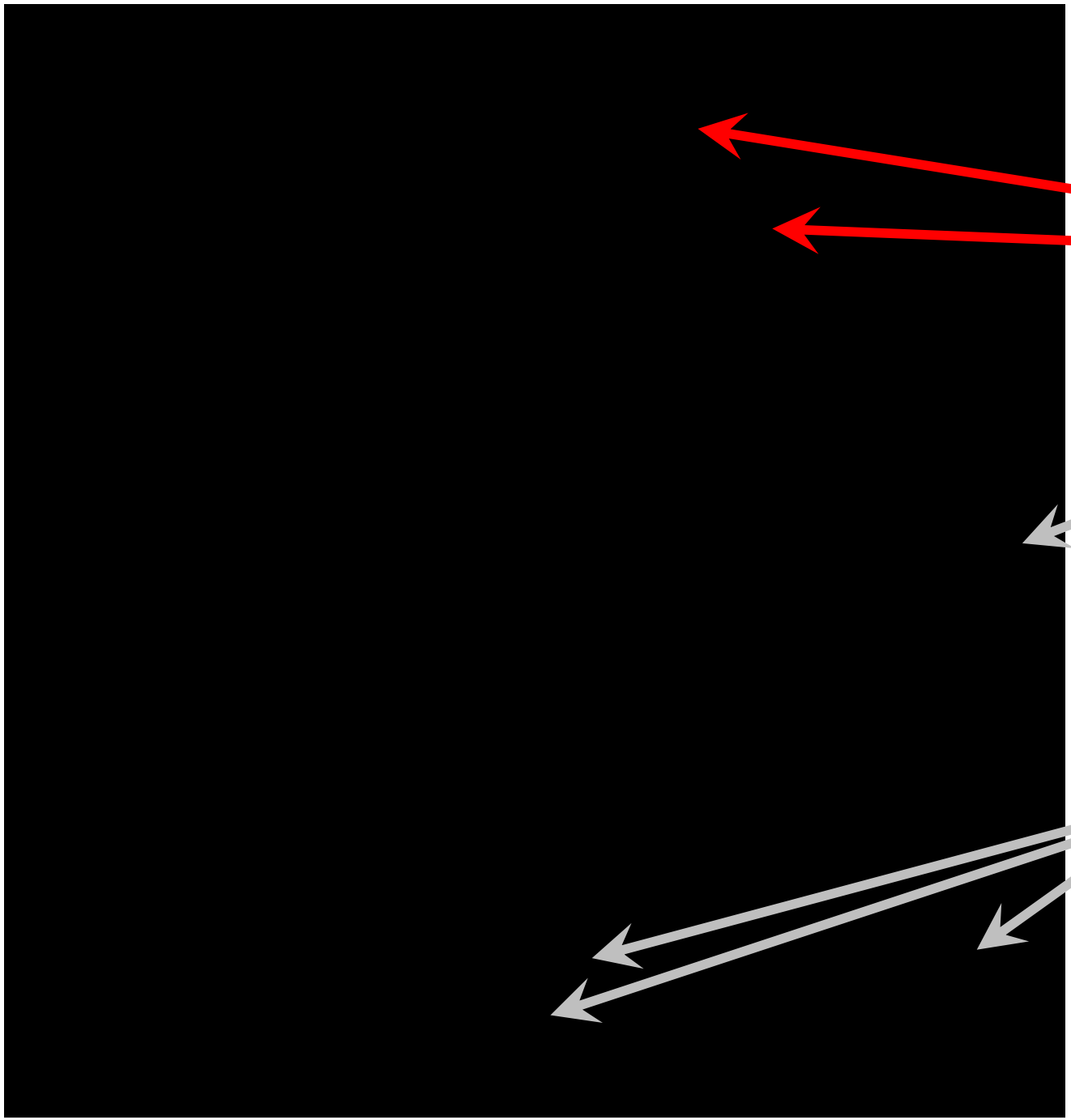


Internet & Corporate IT Networks

Servers, Workstations, & Applications

Embedded Devices

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



APT Style Attacks
- Night Dragon

Phishing

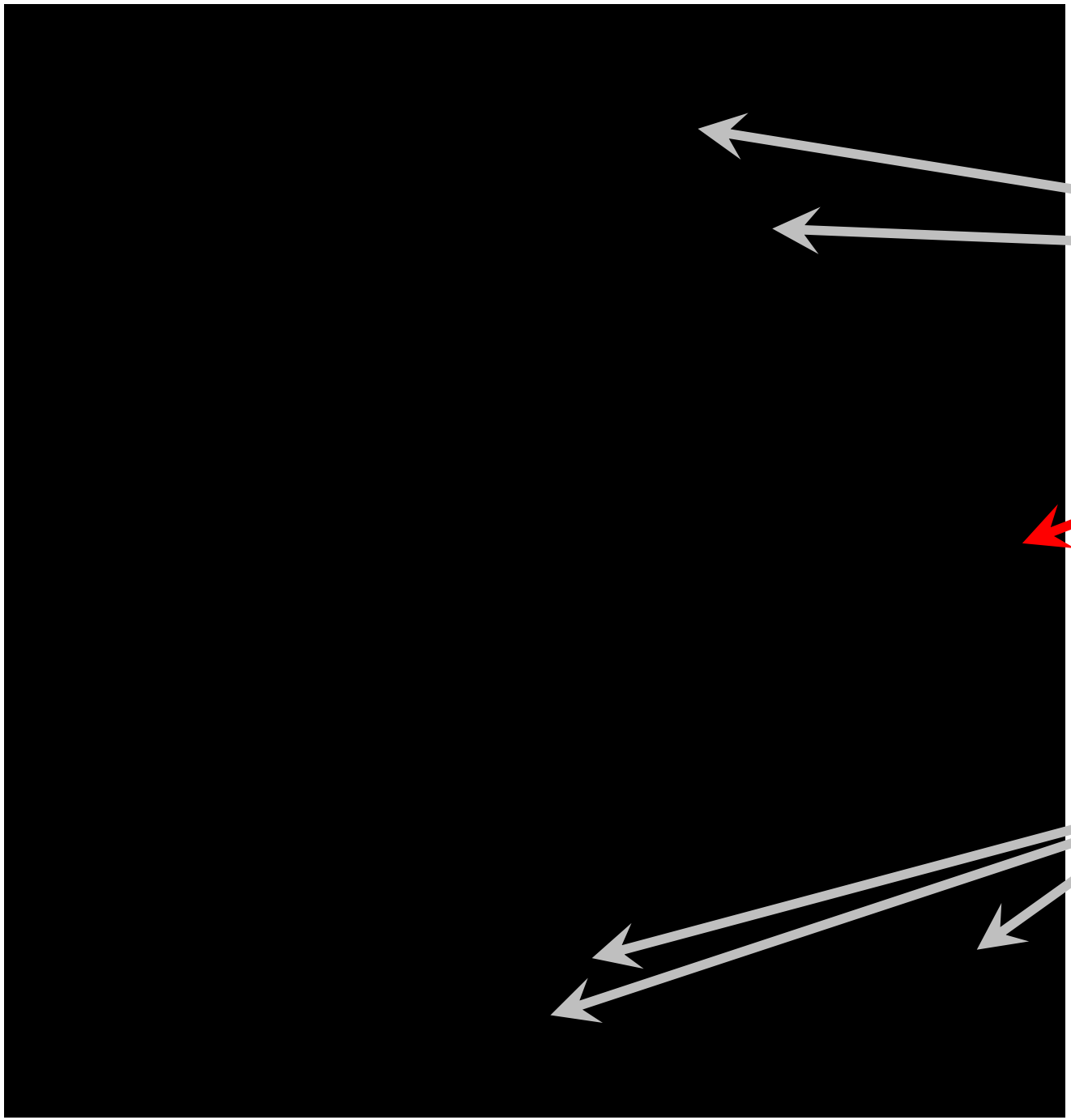
Botnets

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

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





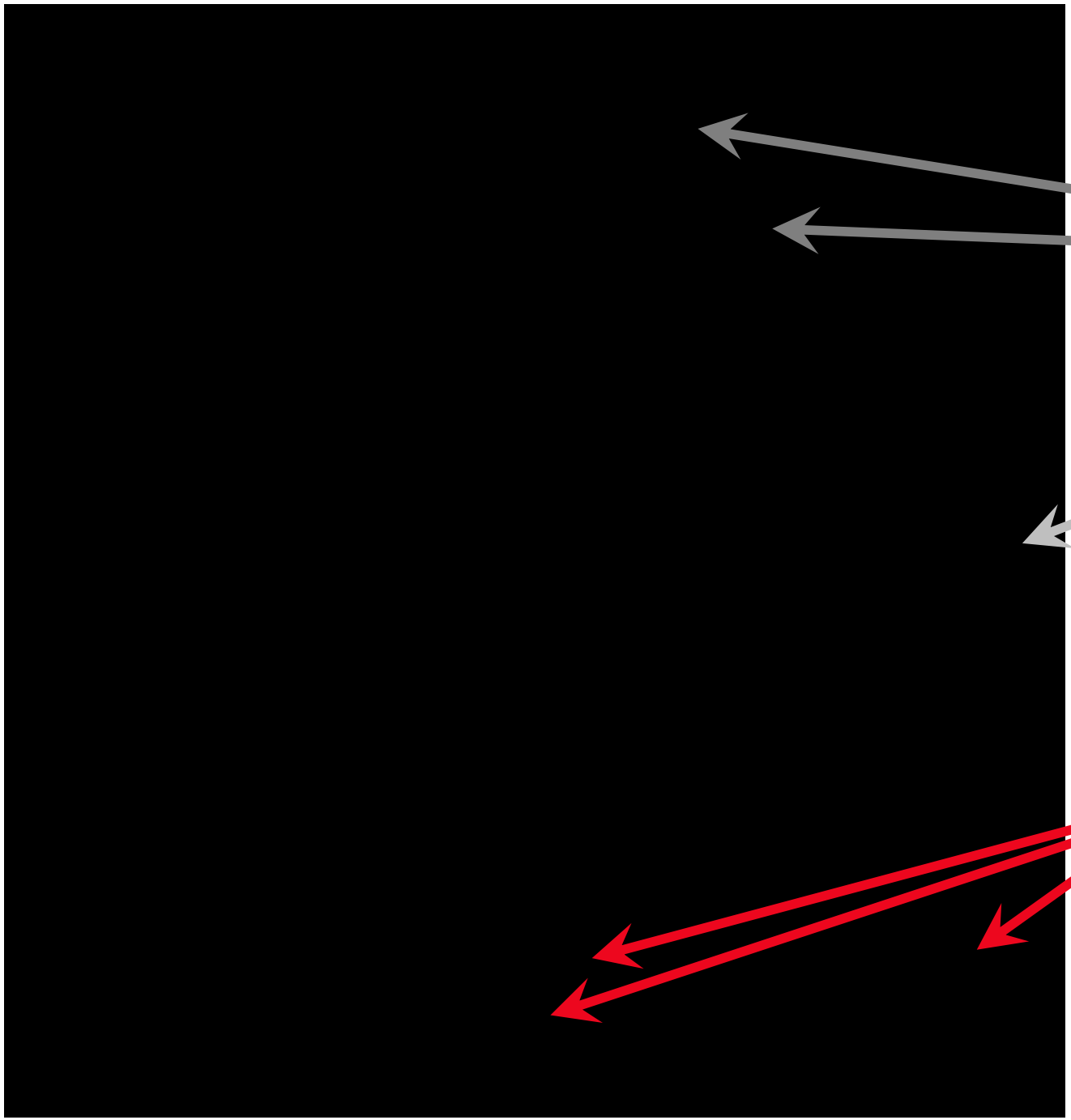
APT Style Attacks
- Night Dragon

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

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





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

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

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.

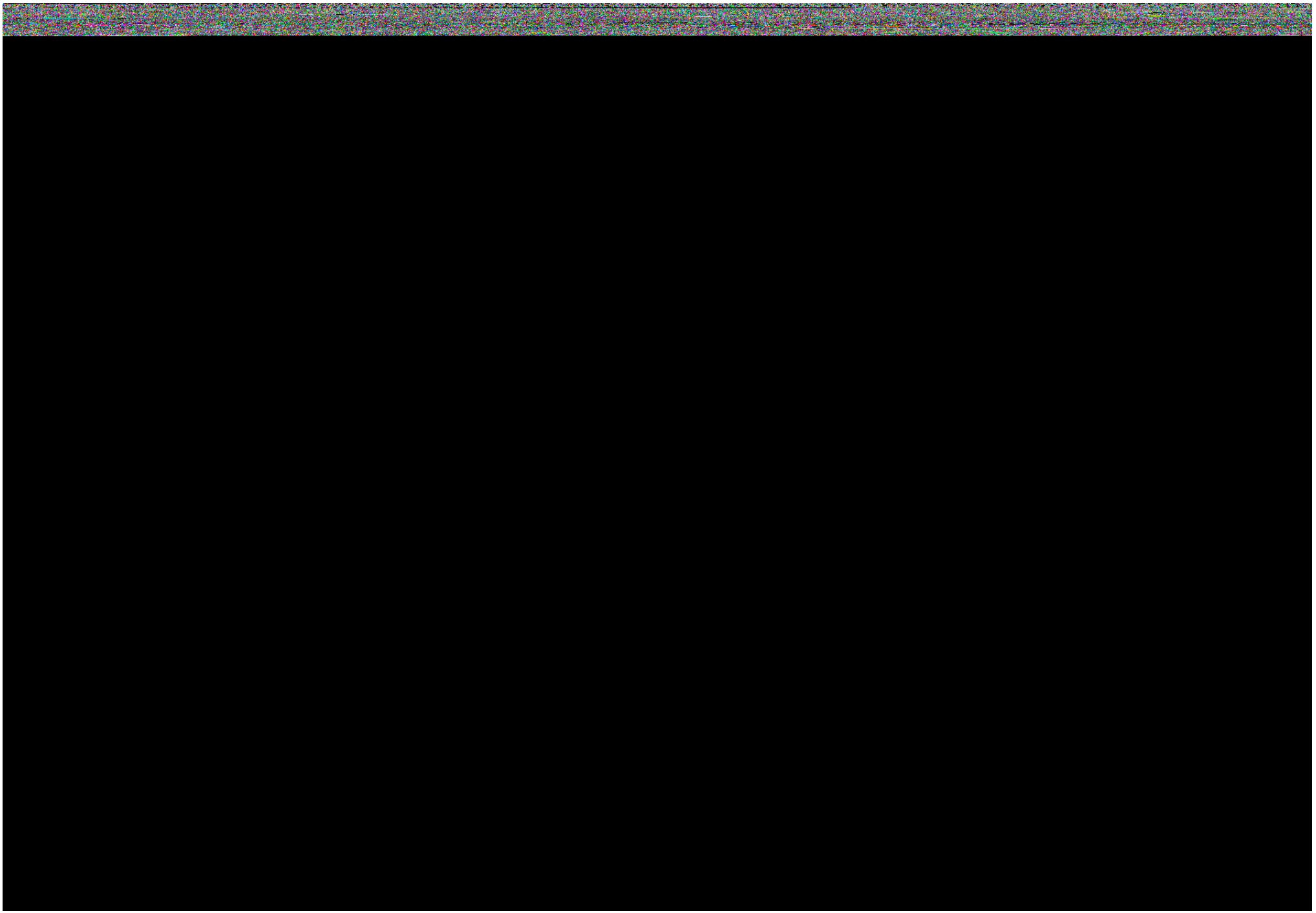
© Copyright Red Tiger Security – Do not print or distribute without consent.



RED TIGER SECURITY

How should we approach the problem?

< Methodology for securing ICS systems >



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

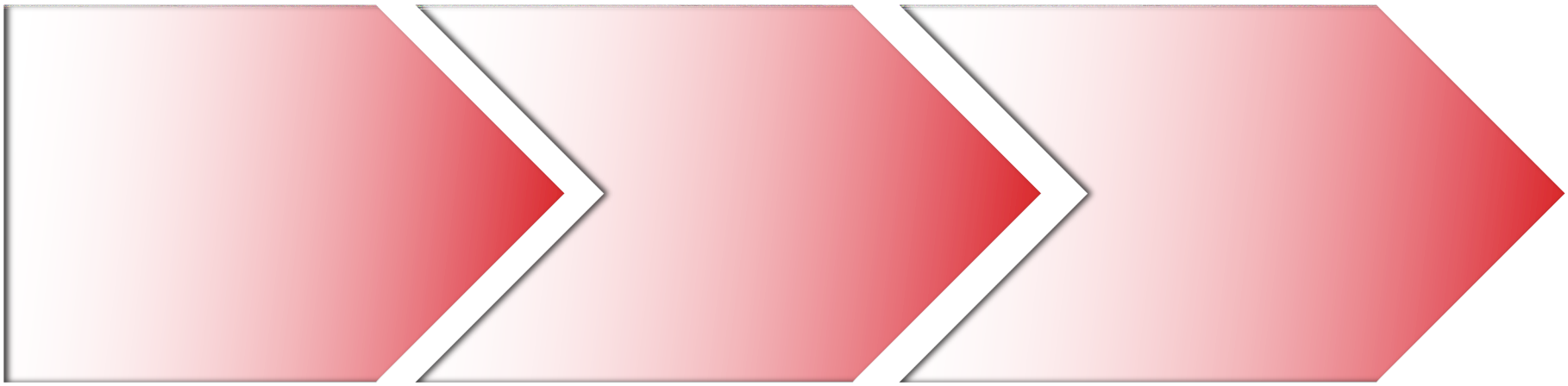
RED TIGER SECURITY

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"



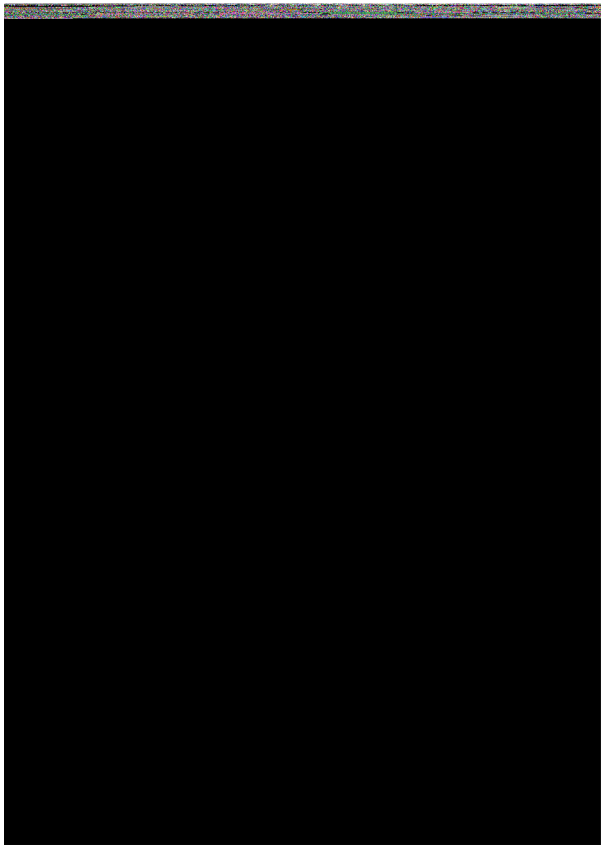
© Copyright Red Tiger Security – Do not print or distribute without consent.

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

- Technical Assessments cover these areas:
  - Red Team Exercises (physical breach)
  - External Penetration Testing
  - Internal Penetration Testing
  - War Dialing
  - Wireless Audits
  - Social Engineering/Phishing
  - Cyber Vulnerability Assessments (CVA)

© 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.

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.

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

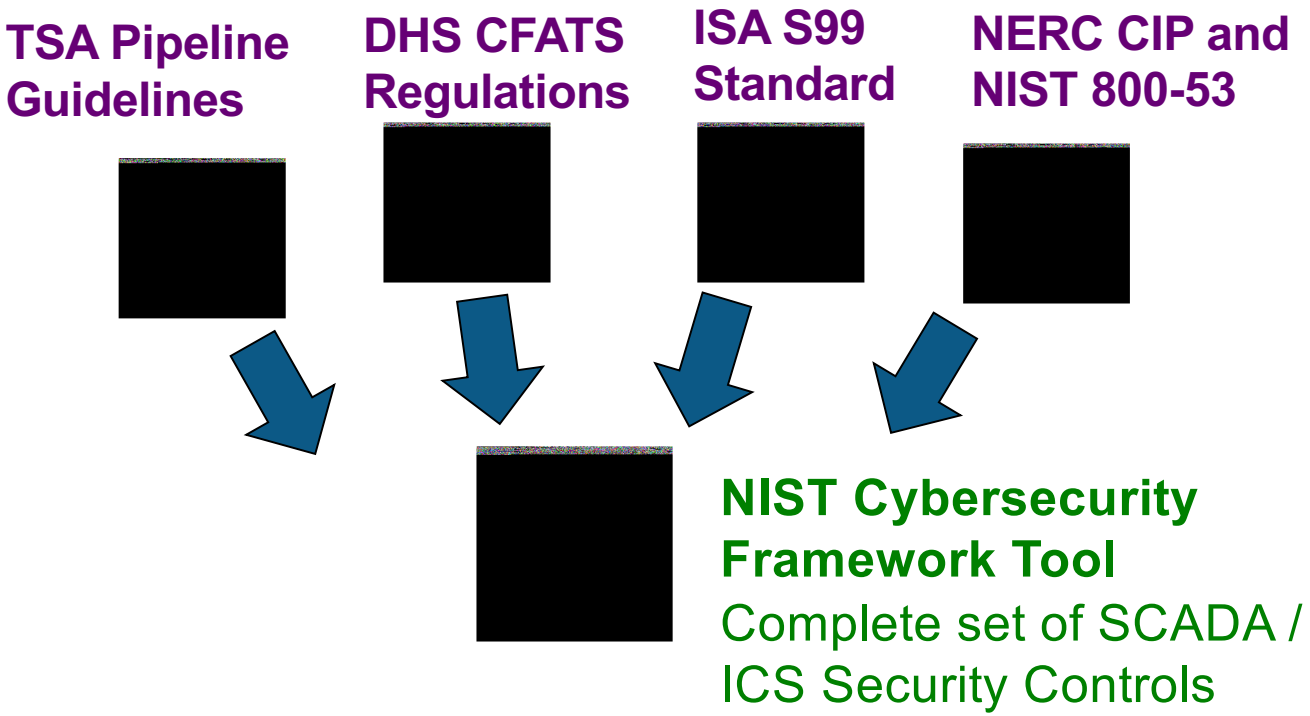
- Other Countries (Including GCC Countries) are using the same approach to build their ICS Security Policies:
  - Qatar National ICS Security Standard
  - UAE NESA Critical Infrastructure Standard
  - Oman SCADA AND DCS CYBER SECURITY STANDARD

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

NIST CSF for Critical Infrastructure

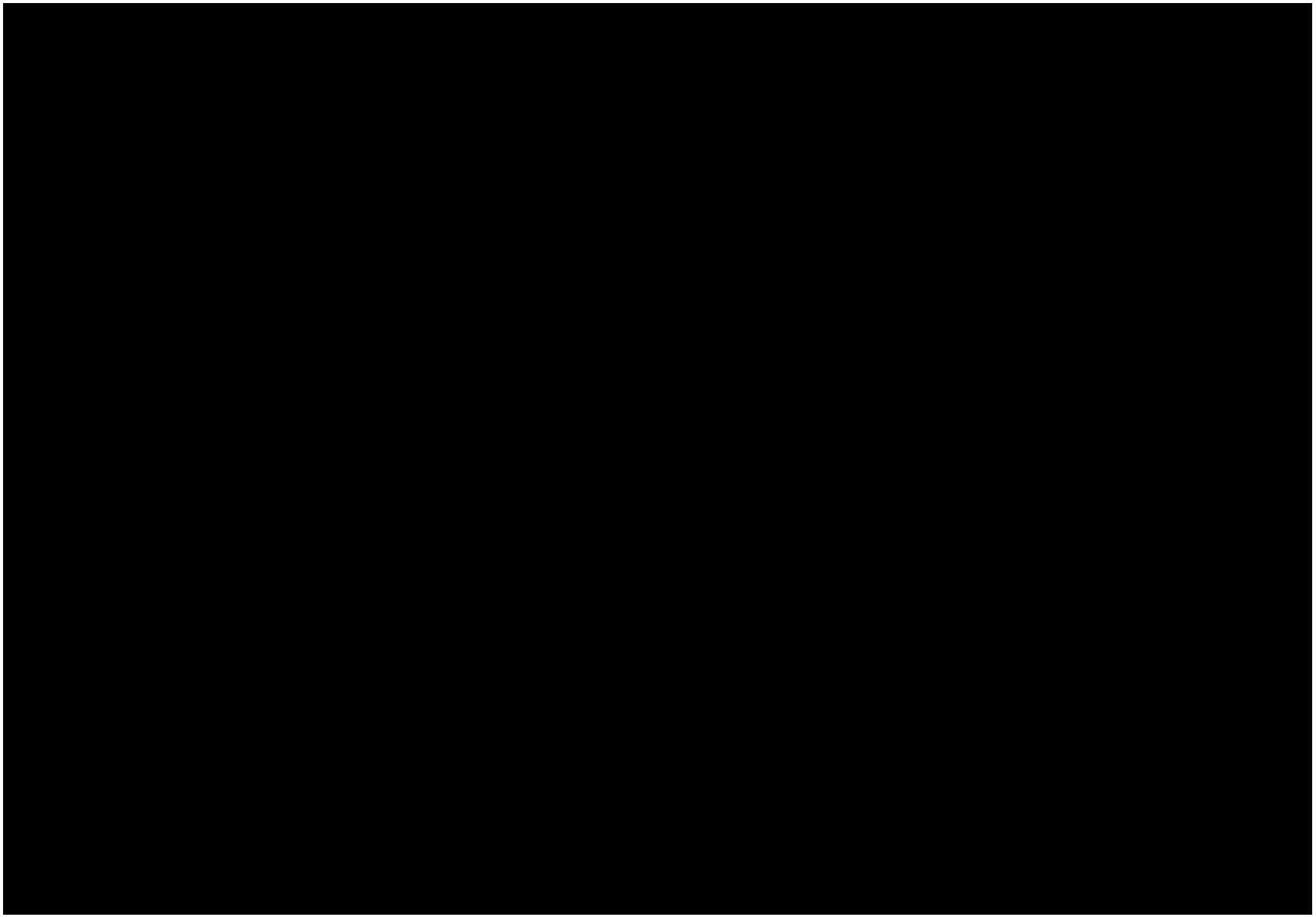
- The NIST Cyber Security Framework (CSF) harmonizes previously splintered cyber security standards that were written for various specific sectors, and creates one framework for measuring the current state of security controls

- NIST CSF is tailored for ICS/SCADA systems



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

ICS Subsystems mapped to NIST Framework Capabilities



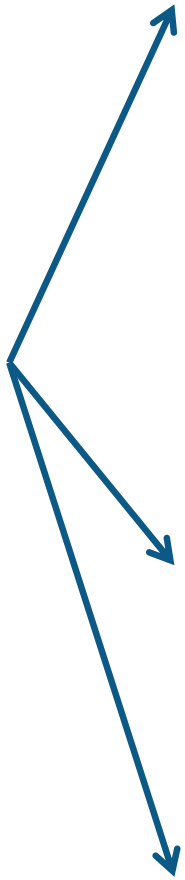
© Copyright Red Tiger Security – Do not print or distribute without consent.

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 –

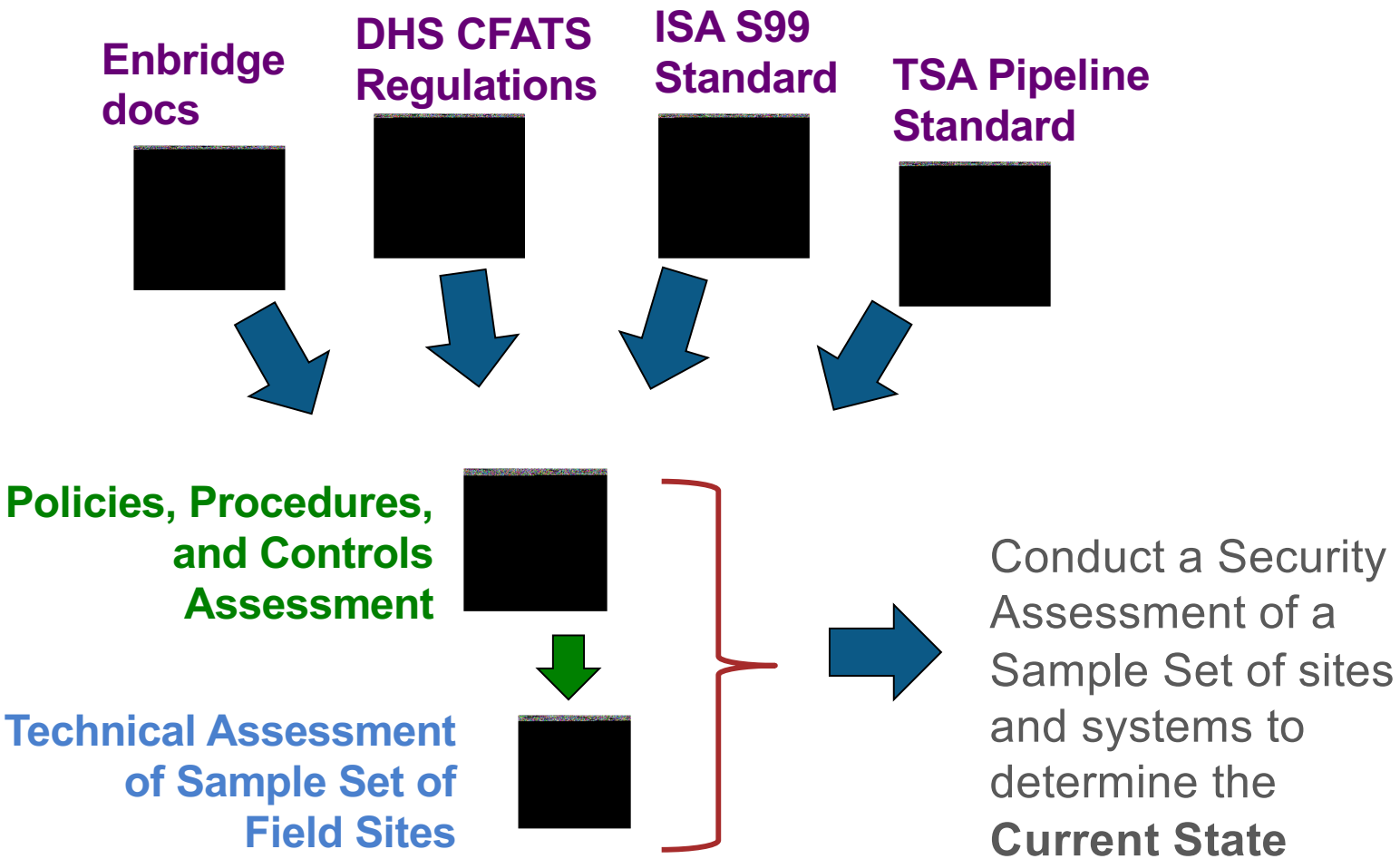
Task 1 - Target State Definition

- **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.

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

RED TIGER SECURITY

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



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

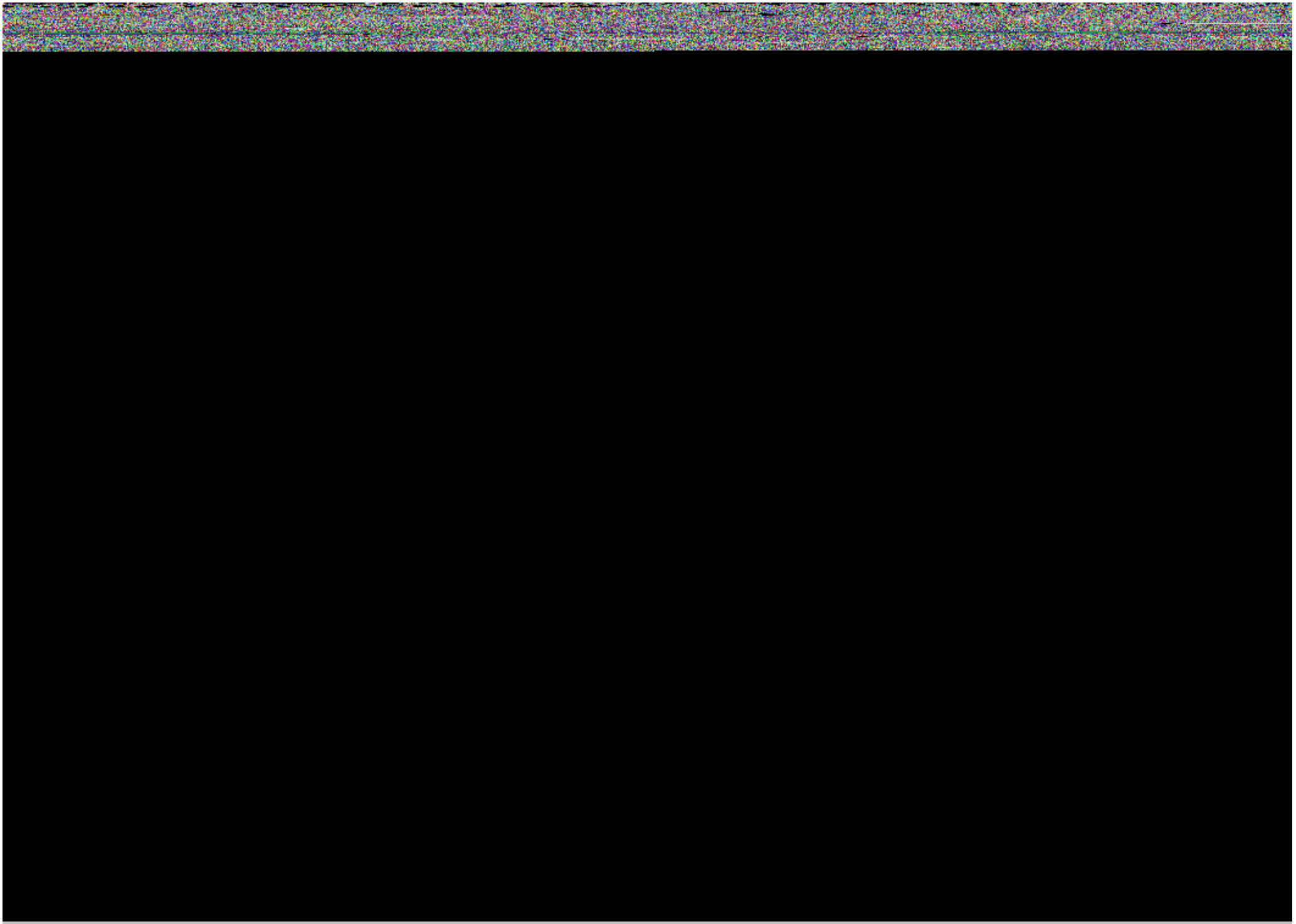
Current State Assessment = **Policy/Procedures + Technical**

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…)

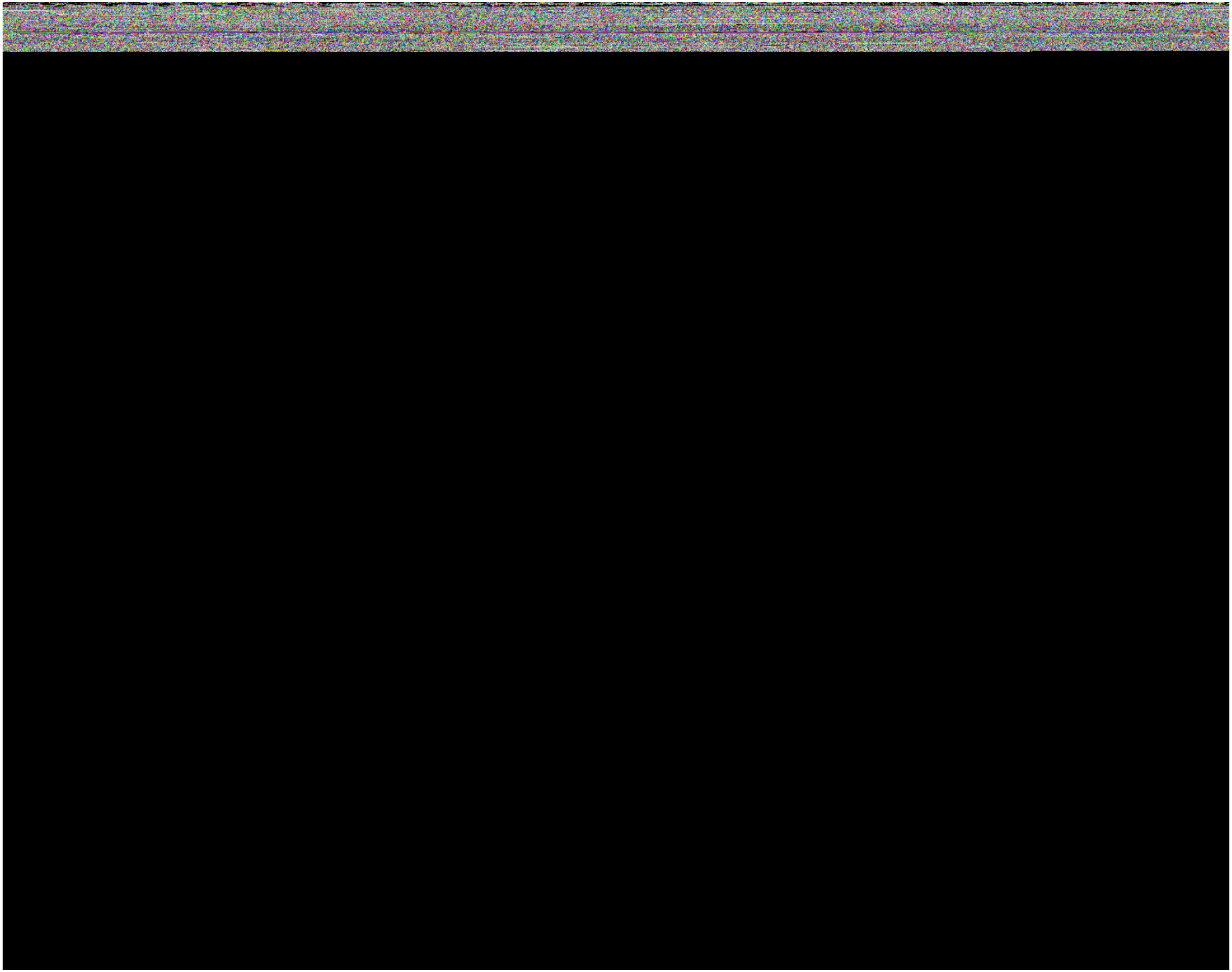
2. Current State Assessment = Policy/Procedures Gap Analysis + Technical Assessment

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.

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

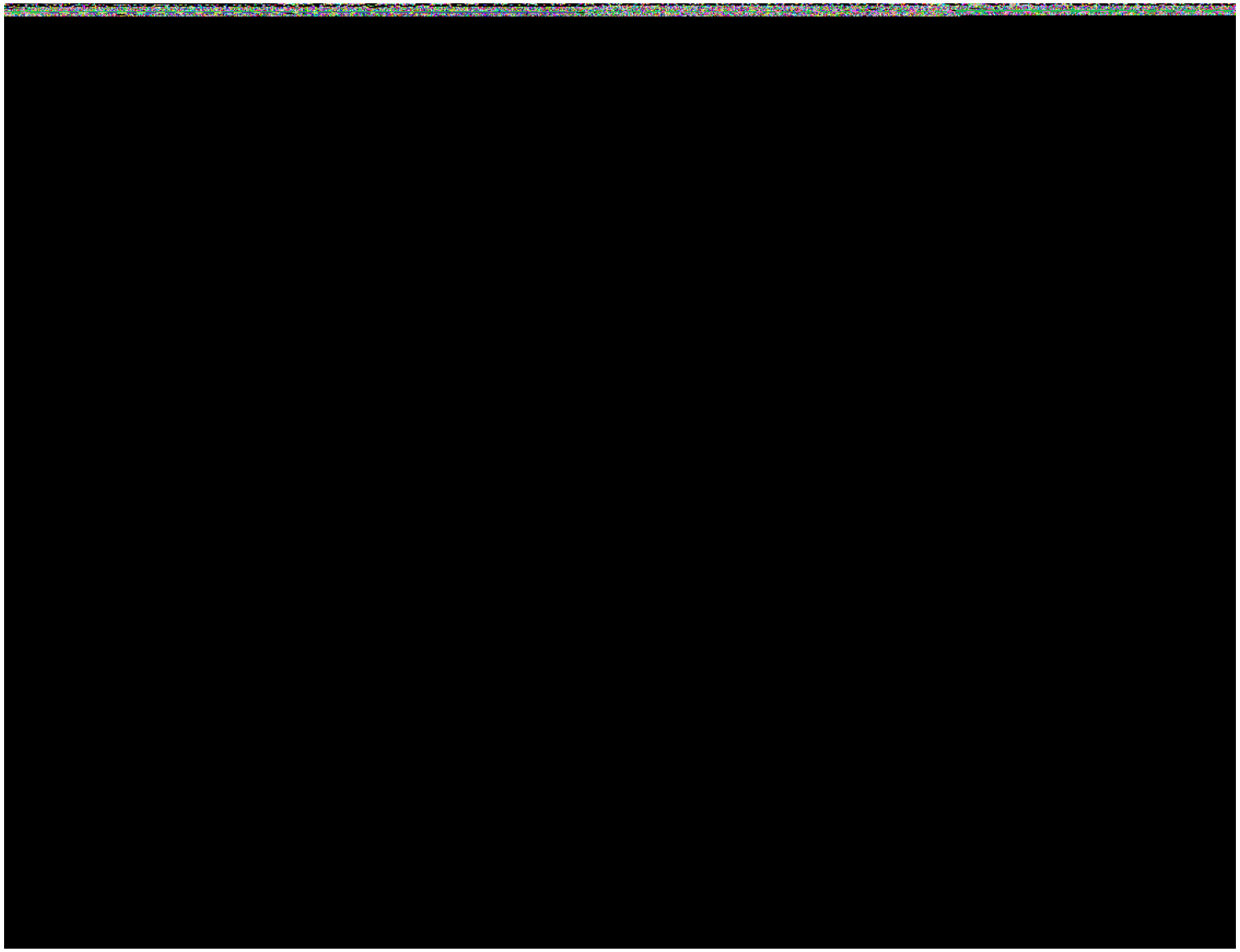


© Copyright Red Tiger Security – Do not print or distribute without consent.



© 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

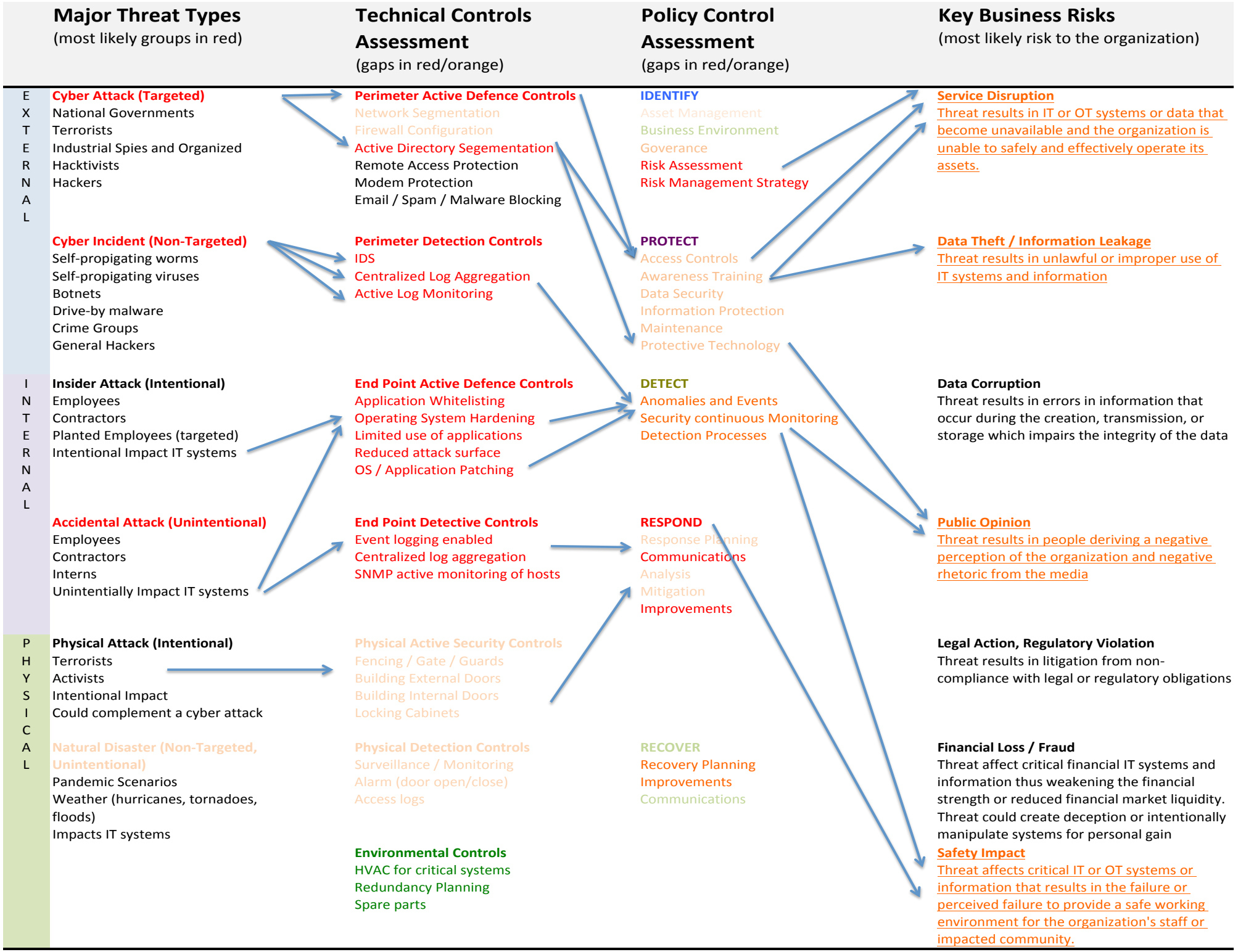
- The controls assessment exposes High, Medium, and Low risk from a Policy/Procedures/Controls perspective. In this sample case, High risk areas included:
  - Defining Cybersecurity Roles and Responsibilities for the Entire Workforce
  - Establishing an Organizational Information Security Policy
  -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

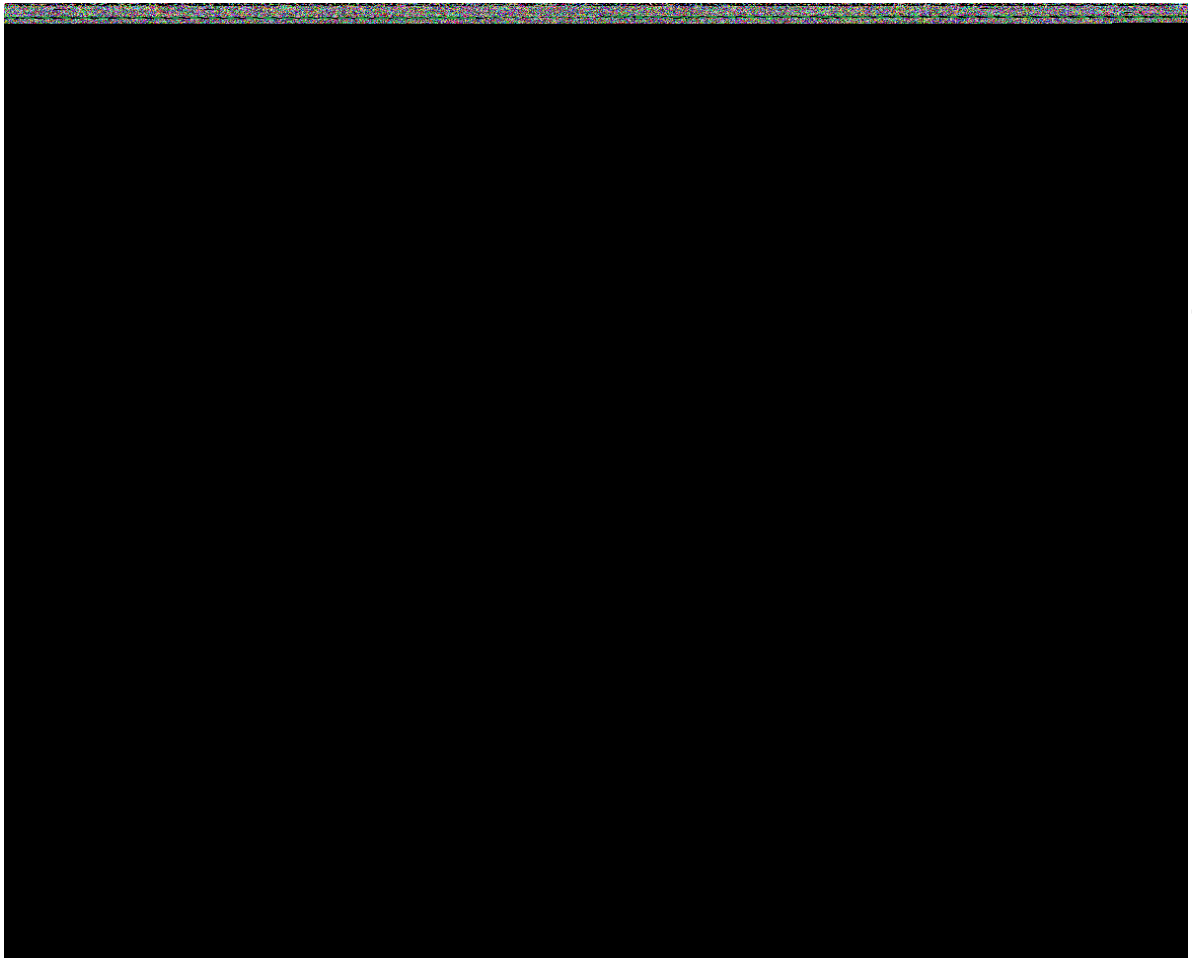
Start with the End in Mind

- 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.


Major Threat Types
(most likely groups in red)
Technical Controls Assessment
(gaps in red/orange)
Policy Control Assessment
(gaps in red/orange)
Key Business Risks
(most likely risk to the organization)
EXTERNAL
Cyber Attack (Targeted)
National Governments
Terrorists
Industrial Spies and Organized
Hacktivists
Hackers
Cyber Incident (Non-Targeted)
Self-propigating worms
Self-propigating viruses
Botnets
Drive-by malware
Crime Groups
General Hackers
INTERNAL
Insider Attack (Intentional)
Employees
Contractors
Planted Employees (targeted)
Intentional Impact IT systems
Accidental Attack (Unintentional)
Employees
Contractors
Interns
Unintentially Impact IT systems
PHYSICAL
Physical Attack (Intentional)
Terrorists
Activists
Intentional Impact
Could complement a cyber attack
Natural Disaster (Non-Targeted, Unintentional)
Pandemic Scenarios
Weather (hurricanes, tornadoes, floods)
Impacts IT systems
Perimeter Active Defence Controls
Network Segmentation
Firewall Configuration
Active Directory Segementation
Remote Access Protection
Modem Protection
Email / Spam / Malware Blocking
Perimeter Detection Controls
IDS
Centralized Log Aggregation
Active Log Monitoring
End Point Active Defence Controls
Application Whitelisting
Operating System Hardening
Limited use of applications
Reduced attack surface
OS / Application Patching
End Point Detective Controls
Event logging enabled
Centralized log aggregation
SNMP active monitoring of hosts
Physical Active Security Controls
Fencing / Gate / Guards
Building External Doors
Building Internal Doors
Locking Cabinets
Physical Detection Controls
Surveillance / Monitoring
Alarm (door open/close)
Access logs
Environmental Controls
HVAC for critical systems
Redundancy Planning
Spare parts
IDENTIFY
Asset Management
Business Environment
Goverance
Risk Assessment
Risk Management Strategy
PROTECT
Access Controls
Awareness Training
Data Security
Information Protection
Maintenance
Protective Technology
DETECT
Anomalies and Events
Security continuous Monitoring
Detection Processes
RESPOND
Response Planning
Communications
Analysis
Mitigation
Improvements
RECOVER
Recovery Planning
Improvements
Communications
Service Disruption
Threat results in IT or OT systems or data that become unavailable and the organization is unable to safely and effectively operate its assets.
Data Theft / Information Leakage
Threat results in unlawful or improper use of IT systems and information
Data Corruption
Threat results in errors in information that occur during the creation, transmission, or storage which impairs the integrity of the data
Public Opinion
Threat results in people deriving a negative perception of the organization and negative rhetoric from the media
Legal Action, Regulatory Violation
Threat results in litigation from non-compliance with legal or regulatory obligations
Financial Loss / Fraud
Threat affect critical financial IT systems and information thus weakening the financial strength or reduced financial market liquidity. Threat could create deception or intentionally manipulate systems for personal gain
Safety Impact
Threat affects critical IT or OT systems or information that results in the failure or perceived failure to provide a safe working environment for the organization's staff or impacted community.

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

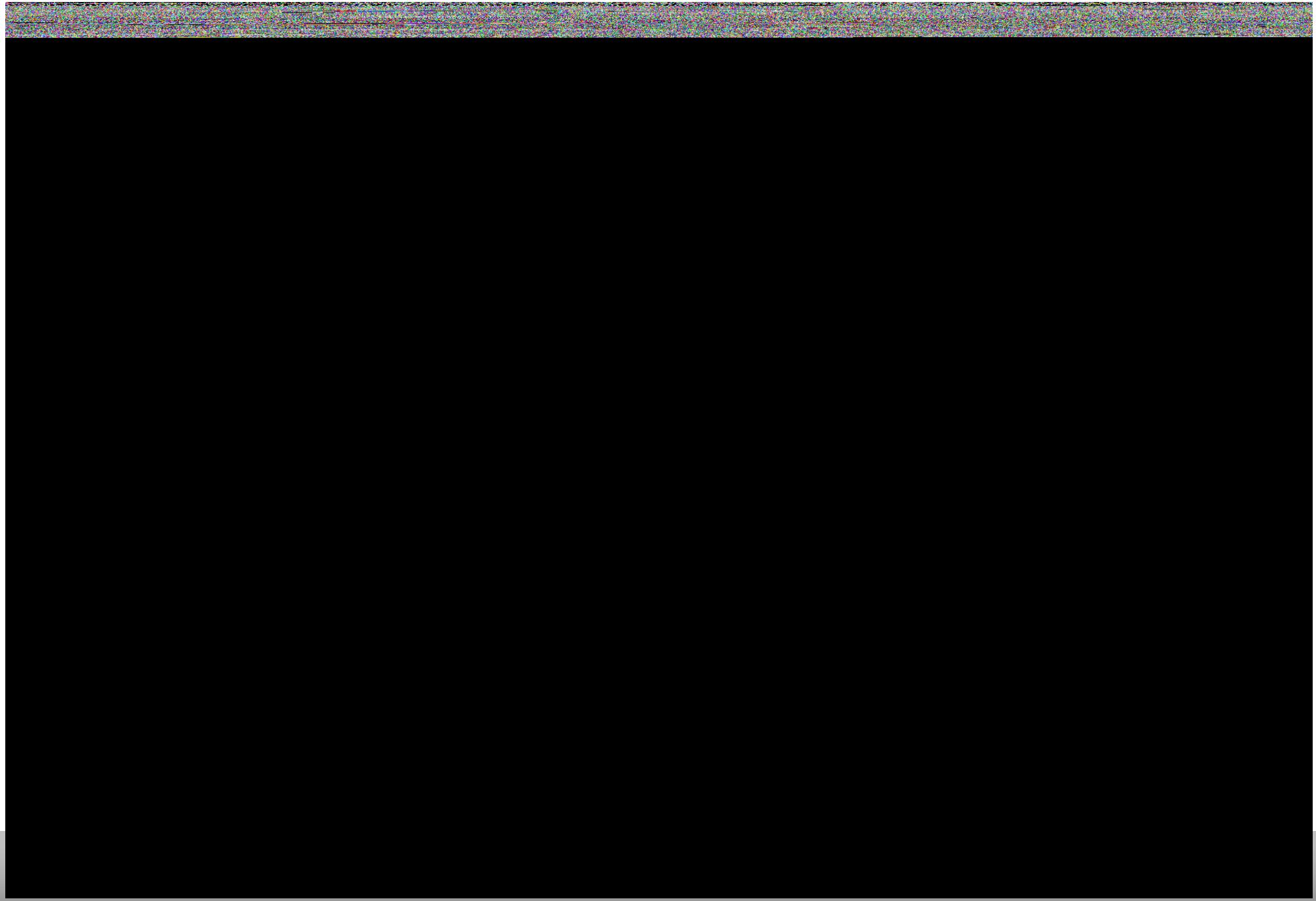
- The process of prioritizing these areas for improvement included taking into consideration the threats and risk to ICS / SCADA systems, comparing the current level of compliance to the controls identified in the Target State, and then prioritizing the control areas into three priority areas based on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



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.

RED TIGER SECURITY

5 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.

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