SCADA Security Overview

National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

A JOINT INITIATIVE BY

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

सत्यमेव जयते
Ministry of Electronics & Information Technology
Government of India

National CoE Content Series Product Dissection
Doc ID: NCoE:0002

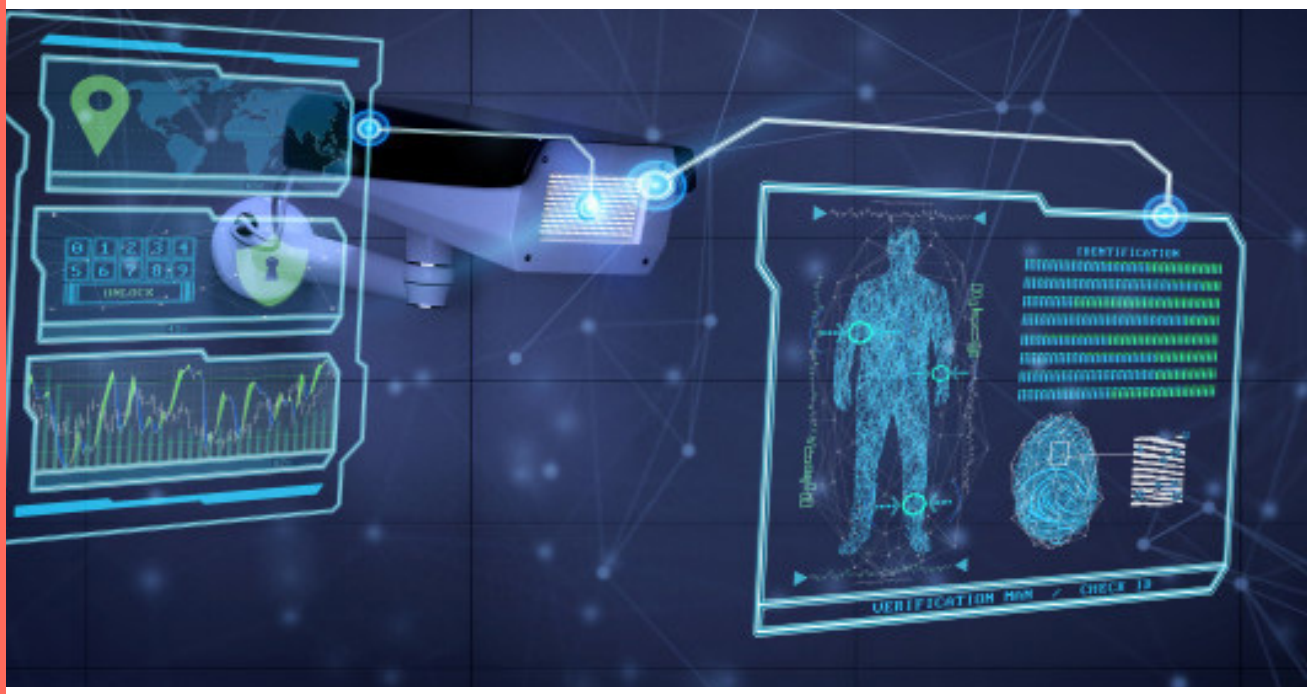
Doc ID: NCoE:0002

National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

INDEX

SCADA Security

Use Cases & Products



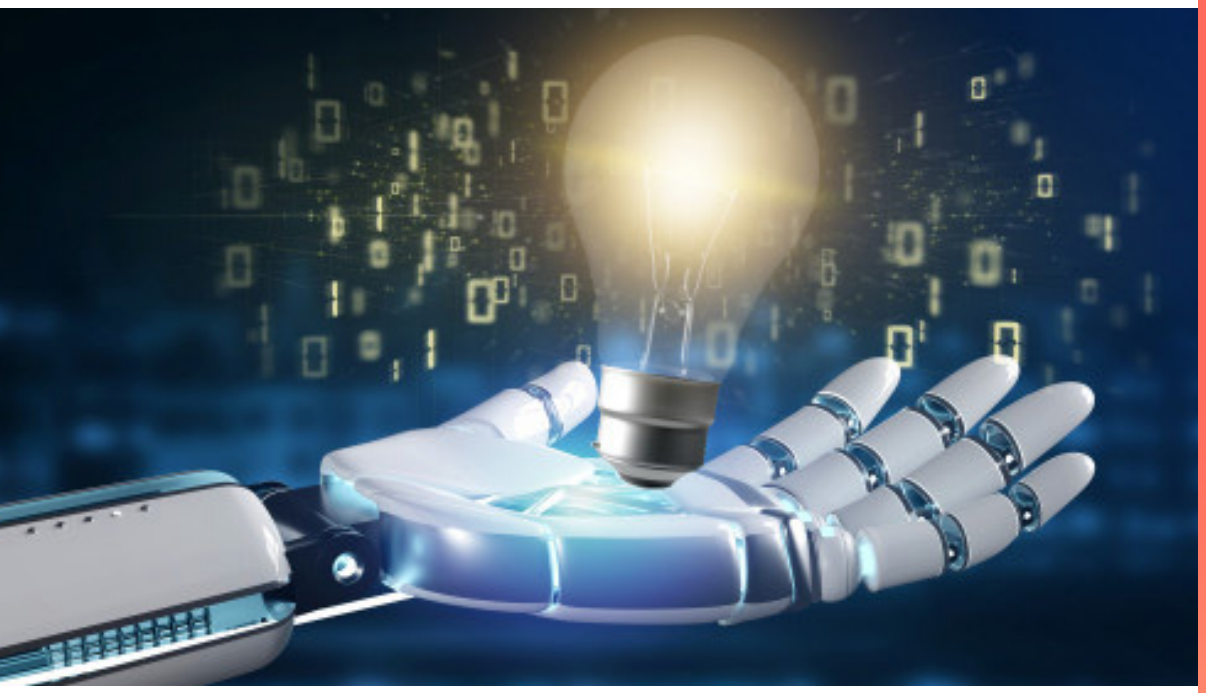
As the world gets better connected with the evolving technological changes, organizations continue to face an emerging threat landscape. With industries adopting newer technologies for improved efficiency and automation, the attack surface of the industriaal systems continues to evolve. With this paper we present a select few solutions that reveal the SCADA security use cases and possible ways to solve the issues.

Challenges in Securing SCADA Systems

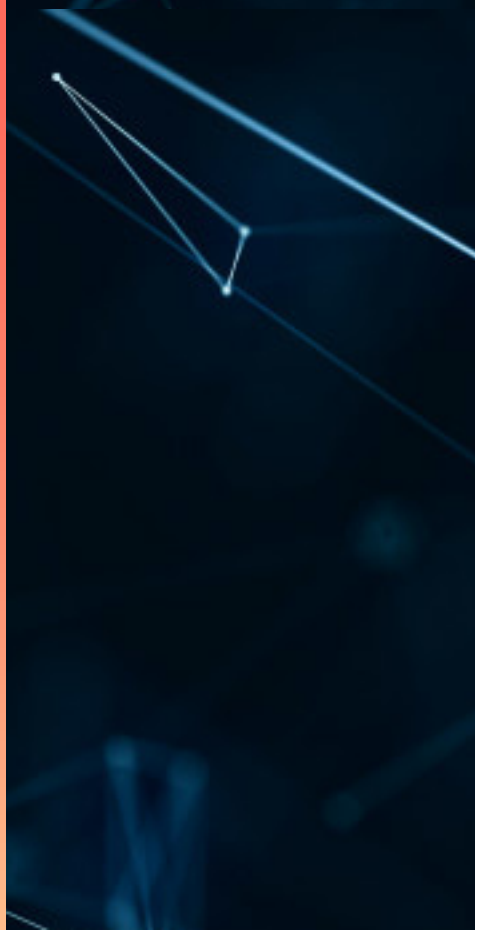
1. Lack of visibility to information assets and therefore to the threat's through the assets
2. Lack of visibility to access rights
3. Outdated system version
4. Lack of monitoring

Organizations are providing solutions in the following categories

- Vulnerability identification: Threat Detection and Threat Response (Configuration, CVE's,
- Backup Solution
- Policy Enforcement Solution by creating rules in Zones
- Penetration Testing solutions
- Visibility Solutions for Assets: Servers / Network / Databases
- Dashboarding solutions
- Sensor Efficacy
- Risk Assessment and Risk Quantification



Overall Visibility Solution of the Enterprise Attack Surface / Enterprise Risk



SOLUTION

Automatic Asset Inventory

METHODOLOGY

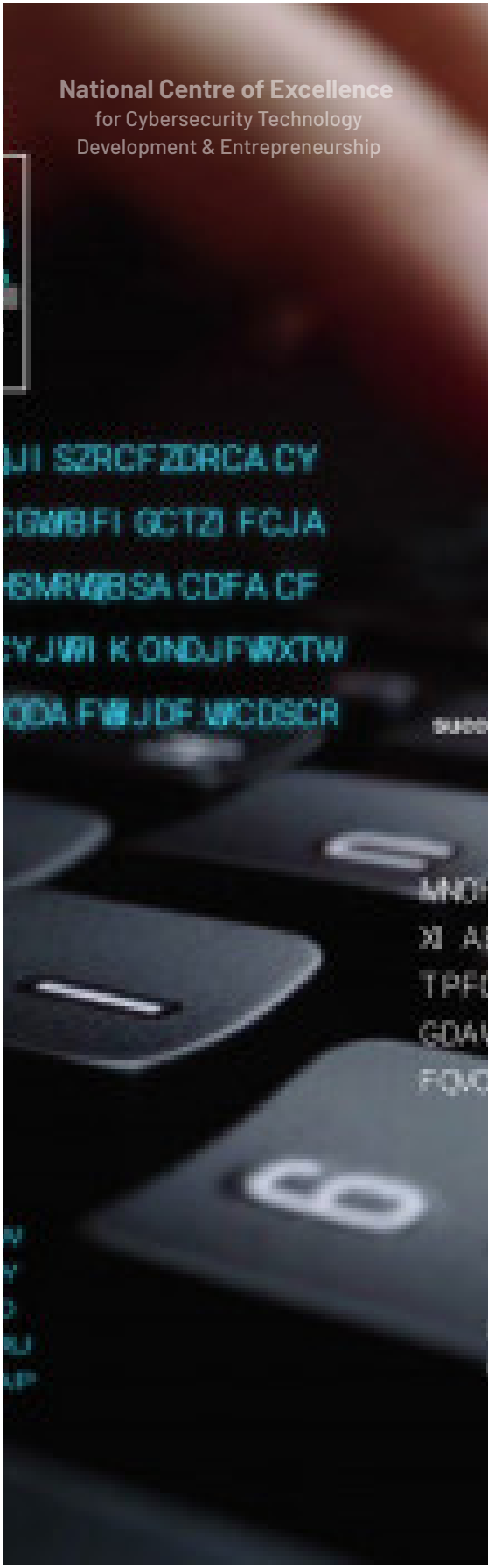
Sensors are integrated throughout the entire ecosystem and maintains an up to date inventory of organization's devices, apps and services; managed and unmanaged infrastructure; on premise and cloud; fixed and mobile; IoT, ICS etc. Assets are automatically classified into specific asset types and as per criticality (basis analysis of usage and network traffic).

SOLUTION

Risk Based Vulnerability Management

METHODOLOGY

Risk based approach used for arriving at the overall cybersecurity posture visibility. Prioritization done based on 5 factors: Vulnerability Severity, Threat Level, Business Criticality, Exposure & risk negating effect of compensating controls. One can also define risk areas specific to organization (e.g. Intellectual property, for higher risk rating). Ticketing system is integrated for driving closure.



SOLUTION

Cyber Risk Reporting for Board of Directors

METHODOLOGY

Arrives at internal benchmarking and risk heatmap: Can be drilled down from business level risk score into a clickable risk heatmap which shows groups of assets that are driving the risk matrix. Also shows evolution of threat landscape over a period.

SOLUTION

Gamification of Cybersecurity Posture Transformation

METHODOLOGY

Uses natural language search to define groups and assign them to specific owners. As risk owners' complete tasks in a timely fashion, points are awarded. Helps in improving overall ownership of colleagues. Leaderboards can be published periodically.

DEPLOYMENT

Sensors are integrated in the environment and automatically create an enterprise wide risk heat map

Risk Quantification and Asset Identification Tool

SOLUTION

Risk Quantification Tool – Risk and Vulnerability Management Tool

METHODOLOGY

- The tool is an automated ICS threat modelling solution and enumerated information about the most likely attack vector paths an attacker would take to compromise the most critical asset.
- Prioritizes risk based on risk quantification and includes mitigation steps.
- Risk quantification based on categorization of high risk / high impact attack vectors.
- Enumerates device level vulnerabilities such as: missing patches, weak passwords, unused open ports, remote access ports.
- Enumerates network level vulnerabilities such as: Unauthorized internet connections, weak firewall rules, rogue subnet connections between IT and IoT and ICS, Unauthorized Wireless Access Points (WAPs), Rogue Devices.
- Detects:

  a. Behavioral anomalies by spotting baseline deviations by modelling ICS networks as deterministic sequences of states and transitions.

  b. Protocol violtions indicating the use of packet structures and field values that violate ICS protocol specifications as defined by IoT and ICS vendors.

  c. Industrial malware by looking at behaviors indicating presence of malware such as WannaCry, NotPetya, TRITON, Industroyer.

d. Unusual M2M Communication identified via ICS-aware heuristics. Eg. PLCs should not be communicating with other PLCs.

e. Operational issues indicating early signs of equipment failure.

SOLUTION

IoT and ICS Asset Identification Tool

METHODOLOGY

Uses natural language search to define groups and assign them to specific owners. As risk owners' complete tasks in a timely fashion, points are awarded. Helps in improving overall ownership of colleagues. Leaderboards can be published periodically.

DEPLOYMENT

1. Vendor Agnostic.

2. Agentless / Passive monitoring solution: connects to a SPAN port or network TAP and immediately begins collecting ICS network traffic.

3. Integrates with SIEM, Firewall., Sec Orchestration and Ticketing system, PAM solutions.

Nozomi Networks

Overall solution for OT and IoT Security and Visibility

SOLUTION

Gaurdian: Combines Asset Discovery, Vulnerability Assessment, Threat Detection & Anomaly Detection in a single unified solution

METHODOLOGY

- Data collected from remote locations and sent to Gaurdian for further Analysis.
- Central Management Console monitors and manages cybersecurity across distributed industrial sites, which helps manage and consolidate OT risk across the enterprise.
- Add on Module: Smart Polling:
  - **a.** Extends asset discovery functionality with active capabilities by gathering info of assets: OS, Firmware, Patch Level etc.
  - **b.** Identifies non-communicating and rogue devices.
  - **c.** Provides exact vulnerability assessment and advanced ICS security monitoring.
- Add on Module: OT Threat Feeds:
  - **a.** Delivers up-to-date threat intelligence.
  - **b.** Makes it easier to detect threats and identify vulnerabilities and provides insights into potential risk in the network.
  - **c.** Solution correlates multiple, advanced detection techniques.

- Real Time Analytics Engine:
  - **a.** Analyzes process control variables for indication of nefarious activities and critical issues that could impact reliability.
  - **b.** Identifies early stages of cyberattacks, failing equipment,causes of lost resources or raw materials and mores.
- Automated asset inventory using passive network monitoring.
- Improves cyber resiliency of the organization with up-to-date vulnerability assessment and identification of which vendor devices are vulnerable.
- Threat and Anomaly Detection done based on comprehensive anomaly and signature-based threat detection.
- Deep Packet Inspection and Protocol Analysis:
  - **a.** Evaluates communication of 100's of ICS and IT protocols.
  - **b.** Examines packets at all 7 layers of OSI model.
  - **c.** Provides packet capture for deeper analysis.
- Customized dashboards and reports for improved security and productivity.

DEPLOYMENT

1. Centrally monitors 100's of facilities and integrates with IT/OT systems.

2. Integrates to IT/SOC environments via many built-in integrations plus an OpenAPI.

3. Includes Protocol SDK and on-demand engineering services for additional protocols

PAS Security

Compliance Management Solution

SOLUTION

Inventory Management

METHODOLOGY

Automates collection and contextualization of both proprietary and traditional IT system configuration data including I/O cards, firmware, software installed and control strategies.

SOLUTION

Vulnerability Management

METHODOLOGY

Automates VA by using NCD database and mapping to assets. Conducts automated patch management and provides dashboards.

SOLUTION

Project Integrity

METHODOLOGY

Captures configuration data from automation or decision support systems and identifies discrepancies between each manufacturer's control system databases. Ensures auditability with full reporting of status, modifications and resolutions.

SOLUTION

Configuration Management

METHODOLOGY

Establishes a configuration baseline and monitors for unauthorized changes. Detects changes in PCN.

SOLUTION

Backup and Recovery

METHODOLOGY

Automates onsite and offsite backup for all major control systems.

SOLUTION

Automation Integrity

METHODOLOGY

Captures and archives configuration data from all major automation and decision support systems. Visually maps complex configurations and interdependencies.

SOLUTION

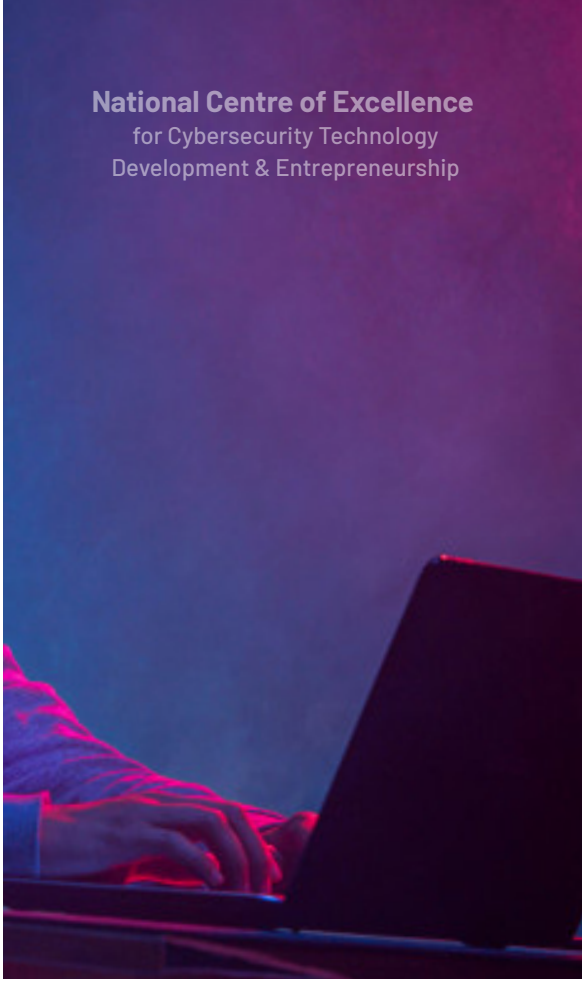
Risk Analytics

METHODOLOGY

Simplified visualization of asset risk based on vulnerabilities, patch status and baseline deviations.

Claroty

Integrated and Comprehensive IoT-OT Security



SOLUTION

Continuous Threat Detection

METHODOLOGY

- Proactively discover and eliminate vulnerabilities, misconfigurations and unsecure connections.
- Uses 5 DPI engines.
- Correlates past and predictive models of behavior with online patterns to eliminate distracting and costly false positives.
- Real time asset discovery across entire industrial network: IP assigned nested assets and assets that communicate across serial connections.
- Alerts raised per groups: Critical changes, malicious activities, failed login, new asset etc.
- Extracts fine grained details about each device on the industrial network, profiling all communications and protocols, using which CTD generates behavioral pattern that characterizes legitimate traffic, alerting about any network changes, vulnerabilities and threats.

SOLUTION

Security Posture Assessment

METHODOLOGY

Solution ingests a network capture (PCAP) file and generates a comprehensive report detailing the industrial network, its assets, and deep insights including CVEs, configuration and other weaknesses.

SOLUTION

Secure Remote Access

METHODOLOGY

- Provides a single manageable and clientless interface that all external users connect through, completely segregated from the internal network.
- Minimizes the risks remote users, including employees and third-party vendors introduce to OT networks.
- Implements network segmentation and manages remote access by enforcing granular access policies and recording sessions.
- Eliminates direct interactions between remote users and network assets and enforce a single access pathway.
- Consolidated tracking, approval and auditing of remote access requests from a centralized location.

SOLUTION

Enterprise Management Console

METHODOLOGY

A centralized management interface that aggregates data from all Claroty products across multiple sites and displays a unified view of assets, activities, alerts and access requests across complex SOX deployments.

DEPLOYMENT

1. Analysis is applied to a copy of real time traffic through SPAN ports (Ethernet) or hardware taps (serial); never impacts live plant traffic.

2. Claroty integrates with existing SOC infrastructures including SIEM, security analytics and others.

Some other organisations with SCADA security solutions

1. APERIO

2. Applied Risk

3. DRAGOS SAFEGUARDING CIVILIZATION

4. SCADAfence

5. sentryo CYBERSECURITY FOR THE INDUSTRIAL INTERNET

6. veracity

7. radiflow

About Us

About DSCI's National Centre of Excellence (National CoE)

DSCI's National Centre of Excellence (National CoE) is a Joint Venture between Data Security of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY) with the objective of providing impetus to the startup ecosystem in India. DSCI has set up a facility, which houses technology research lab, experience zone for demonstration of national cyber capability, experimental SOC, co-creation spaces, training facility for niche capability building, and an incubation center.

Disclaimer: This is a content series for National Centre of Excellence to dissect the emerging security technology products to reveal use-cases, technology stack and deployment strategies. This effort is to create awareness and understanding of technology and not to promote any particular product or company.

#scada_security #sensors #asset_discovery #iot #ics #risk_heatmap #gamification_of_risk #risk_quantification #behavioural_anomolies #baseline_deviation #protocol_violations #equipment_failure #centralised_monitoring #threat_intelligence #deep_packet_inspection #backup_solution #secure_remote_access

@nationalcoe **@CoeNational** **company/nationalcoe**

www.dsci.in/content/national-centre-excellence-cyber-security-technology-development

ncoe@dsci.in

National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

A JOINT INITIATIVE BY

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Ministry of Electronics & Information Technology
Government of India
सत्यमेव जयते