CHECK POINT ICS SECURITY

Cyber attacks on Industrial Control Systems (ICS) and in particular critical and manufacturing infrastructures are now a reality. Power grid, water supply systems and factories, as well as Building Management Systems (BMS) have become targets of attackers and have been hit recently with an array of network breach, ransomware and denial of service activity. Service uptime, data integrity, compliance and even public safety require that organizations implement steps to deal with these security concerns. It is time to take action.

SECURE BOTH OT AND IT ENVIRONMENTS

Many of the recent attacks on OT and ICS networks were found to be based on IT attack vectors, such as spear phishing, Endpoint and Ransomware. Using Check Point Threat Prevention solutions, such as SandBlast, Endpoint, IPS and others will prevent and eliminate those attacks prior to breaching the ICS equipment.

SEGMENTATION

The ICS-CERT of the US states that the most prevalent weakness on ICS networks is the weak or missing boundaries between ICS and enterprise networks. Using Check Point GW's will provide Boundary protection between the networks and even micro segmentation among product lines and departments on the shop floor.

EXTREME VISIBILITY FOR INDUSTRIAL CONTROL SYSTEMS

- Protocols and Commands/Functions
  — Log each command in the management
- Assets Discovery provide assets Information and Inventory
- Assets Connectivity and Network topology
- Behavior patterns and analysis
  — Set traffic baseline

ENFORCEMENT WITH ZERO IMPACT TO EXISTING SYSTEMS AND PROCESSES

Policies:

- Set baseline based on allowed traffic such as protocol's commands, queries and responses within the protocol, based on allow/block rules
- Set specific rules based on time of day or restrict specific type of commands or specific sources or destination

Anomaly Detection:

- Alert on deviation from the behavioral communication baseline
- Alert on new assets
- Identifies security gaps – including known vulnerabilities and network hygiene issues
- Detects security posture changes
- Continuously monitors for known and unknown threats
- Secures, monitors, and records remote connections to ICS assets

Continuous Vulnerability Monitoring:

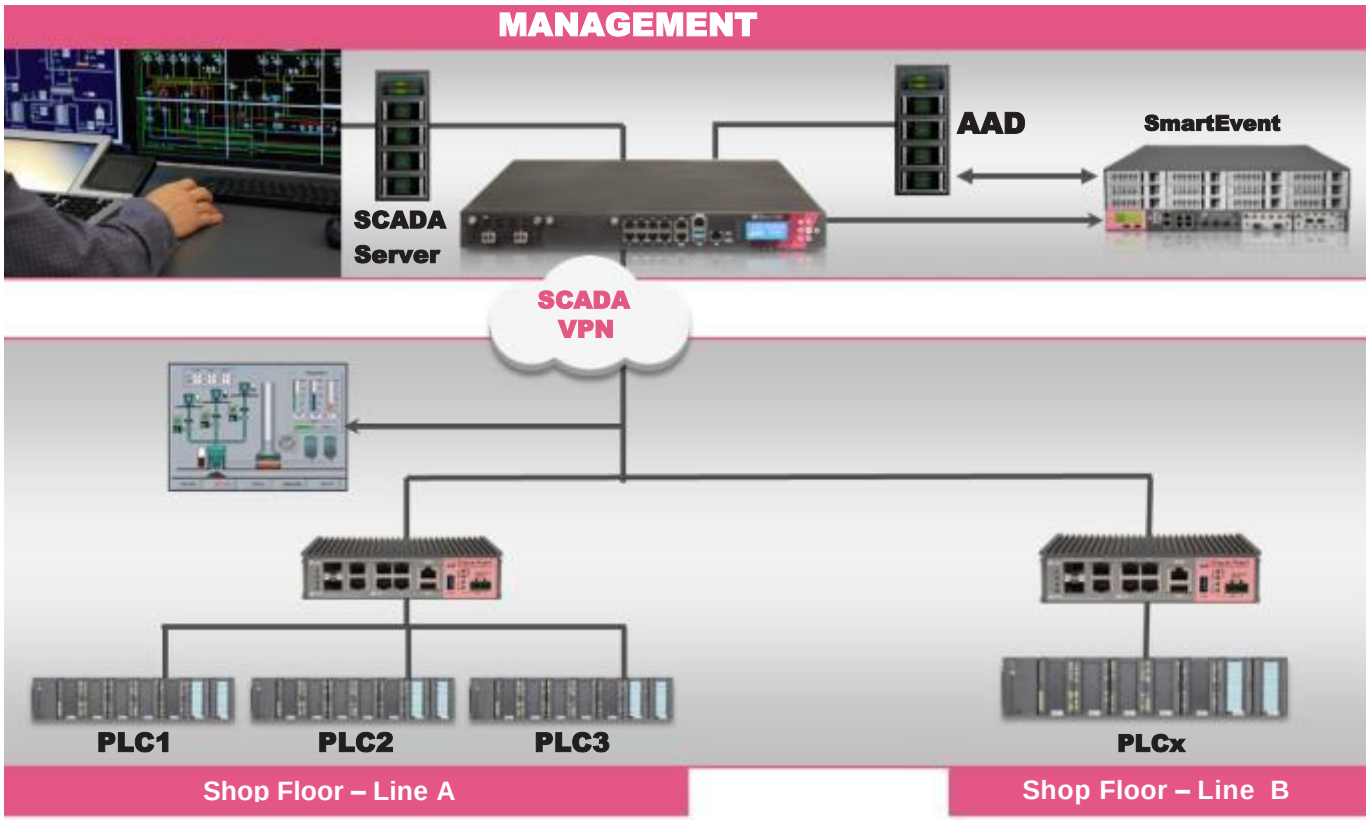
- Provide precise CVE matching – down to firmware versions for industrial devices.

Check Point
SOFTWARE TECHNOLOGIES LTD

CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

ICS SECURITY BLUEPRINT



ICS PRODUCTS

- **Application Control Blade**

  Part of any NGFW, NGTP and NGTX bundle, available in any Check Point GW or VM license, provides Protocols and commands Visibility and Policies rules and enforcement – passive or active.

  Updated list of applications (Protocols and Commands): appwiki.checkpoint.com

- **IPS**

  Signature based blade, available in any NGFW, NGTP and NGTX bundle, provides Virtual patching for known vulnerability of Windows based workstations and servers, we well as SCADA equipment.

- **AAD – Asset and Anomaly Detection**

  Virtual Machine software provides the Asset discovery and management and the Anomaly detection.

- **Security GW**

  Using any Check Point GW model with NGTF, NGTP, NGTX license.

- **For Harsh Environments – 1200R**

  Ruggedized Security GW, compliant to rigid environmental standards and use in harsh environments.

- **Management – SmartEvent**

  R80 management provides unified IT and OT management