WHITE PAPER

EVALUATION CRITERIA FOR CHOOSING AN ICS CYBERSECURITY MONITORING SYSTEM

CLAROTY

CONTENTS

CHANGING RISK AND A NEW CYBER FOCUS FOR INDUSTRIAL SYSTEMS

A rapidly changing threat landscape, combined with convergence between traditional IT and industrial control networks is having a dramatic impact on the risk to industrial systems. Industrial control systems (ICS) include national "critical infrastructure" ranging from energy production and distribution to transportation, manufacturing and building control systems that are all important underpinnings to global business and everyday life. Risks to these systems range from disruption to destruction of critical assets with the potential for collateral impact to the safety of employees and citizens.

Risks to these systems range from disruption to destruction of critical assets with the potential for collateral impact to the safety of employees and citizens.

Historically, ICS threats emanated from well-equipped nation states that steered clear of destructive attacks, which were viewed as "red lines" that couldn't be crossed without a retaliatory response. With Stuxnet and attacks on the Ukrainian power grid, to name just a few, the proverbial red lines have clearly been crossed. But new threats, beyond nation states, are also emerging.

Cybercriminals are exploring ways to extend ransomware campaigns from grandma's photos, which may command a few hundred shekels, to holding a production line hostage, which can be much more lucrative. Meanwhile, terrorist organizations can now engage a burgeoning underground market to buy or rent the skills, tools and infrastructure necessary to launch a campaign focused on destroying infrastructure or harming people.

One clear effect has a been a dramatic uptick in the attention corporate boards and C-level executives are now paying to the cyber risks associated with the industrial assets they are responsible for. This attention has spurred many organizations to review governance plans–with a clear trend towards accountability for protecting ICS networks being assigned to a Chief Information Security Officer (CISO). These events have spawned keen interest in tools that can provide CISOs and security teams with the same level of visibility into ICS networks that they are accustomed to with traditional IT networks.
This paper explores key selection criteria leading organizations are using to evaluate and select an appropriate monitoring system for industrial networks. It is based on hundreds of discussions with customers, prospects, industry analysts and ICS security luminaries.

KEY REQUIREMENTS–AN OUTCOMES PERSPECTIVE

As with any technology selection, there are layers of requirements that teams need to wade through before choosing an ideal solution. Selecting a monitoring system to protect some of the most critical assets the organization owns is no different. It is, however, important to focus on the most important criteria first so the team can narrow the field and choose a solution that addresses the essential objectives. Otherwise it is easy to get lost in a plethora of low-level requirements and miss the proverbial "forest for the trees".

A particularly useful exercise in refining the list of requirements is to flip the discussion from a "requirements view" to an "outcomes perspective". That is, express the key outcomes you want to ensure that the system can deliver. This view will help the team cut through the clutter and focus in on the important goals.

A particularly useful exercise in refining the list of requirements is to flip the discussion from a "requirements view" to an "outcomes perspective". This view will help the team cut through the clutter and focus in on the important goals.

The "top five" most important outcomes for ICS monitoring systems include:

1. Do No Harm and Require No Downtime
2. Give Complete Visibility
3. Provide Early Warning
4. Detect Malicious and Accidental Threats
5. Enable Rapid Response (Reduce Mean Time Resolution)

Below we explore each of these key outcomes in more detail.

DO NO HARM AND REQUIRE NO DOWNTIME

Mixing metaphors, if the proverbial "pill is worse than the ill, then we have a problem Houston". Many industrial networks are fifteen, twenty or even thirty years old. The industrial assets and the underlying networks in many of these environments are quite brittle compared with today's standards. And while newer plants, with modern network equipment and contemporary industrial assets are often more robust and resilient to network traffic delays or other unexpected interruptions, even modern ICS networks can be finicky.

Therefore, ICS monitoring systems need to be designed to ensure they don't harm industrial networks or adversely impact the industrial process. Many traditional IT vendors and security teams learned hard lessons when they tried to run, for example, vulnerability scanning systems that queried control assets that were simply not designed to be interrogated and added traffic to the network. ICS devices sometimes failed, and not gracefully, occasionally taking plants offline in the process.

As we noted earlier, systems that actively poll (or query) endpoints such as controllers can harm the process. This can be a somewhat less severe risk in modern networks or at the upper layers of the Purdue Model where the workstations or servers are more resilient to interrogation.

Another important consideration is whether the solution requires plant downtime for installation or maintenance. Systems that need to be installed on endpoints or systems that need to be placed "in line" on the ICS network require downtime to set up or must be installed, configured and modified only during plant maintenance windows. This can cause significant implementation project delays or emergency downtime to fix issues.

GIVE COMPLETE VISIBILITY

Out of the hundreds of discussions we have had with security teams over the last few years, we have never heard "we only want visibility and monitoring for a portion of our industrial network."

> Providing visibility across the length, width and depth of an ICS network is a foundational outcome and important prerequisite for other key requirements.

In fact, this requirement is now simply "table stakes" for any vendor competing in this market. If the solution can't meet this requirement then the others don't much matter. This requirement has multiple dimensions.

First the solution must be able to monitor both TCP/IP and non-IP nodes–for example, serial connections such as Profibus or Modbus–that are a critical part of many industrial environments. Further, the system needs to be able to understand network topology and provide visibility into the "other side" of gateway devices. For example, this could be a programmable logic controller (PLC) with a network card that is a gateway to a potentially expansive segment of the network on the other side of the device. IT teams will often assume that they have a secure network perimeter, but fail to understand that assets on the other side of gateway may be connected to a network that is connected directly to the internet or DMZ. This is not a theoretical case. We have observed this type of network configuration issue in multiple implementations. In a nutshell, blind spots are bad because they limit the team's visibility into potential attack vectors and make good hiding places for adversaries seeking persistence.

Secondly, the system must cover the full range of ICS protocols that are present in your specific environment. This does not mean cursory coverage where the system can simply identify the presence of a specific ICS protocol, or systems that only understand the network address of the nodes involved in the conversation. This means a deep understanding of the open and proprietary protocols, so the tool can discern type of devices that are communicating and understand the actual conversations. Otherwise the system will not be able to provide important insights, detect anomalies or provide rich alerts and the contextual information you will need to meet other very important objectives as noted below.

Many IT security vendors have tried to repurpose traditional security tools for use in ICS networks (e.g., IDS/IPS, next gen firewalls, etc.). For these limited protocol devices, being implemented in an ICS network is like being dropped into a United Nations session without the special translation headphones. You know there are many conversations going on but can only really understand one or maybe two. A tool that is ICS protocol blind means it cannot understand the important industrial control conversations that need to be monitored for anomalous behavior or other important activities that may pose a risk to industrial assets, the industrial process or the safety of personnel. The degree to which the system can provide insights into network configuration issues or build a fine grain anomaly detection model is directly proportional to the depth of understanding that the given system has into the protocols being used in the network. Stated more succinctly, without significant protocol inspection depth, the monitoring system's detection and alerting capability will be conspicuously limited.

PROVIDE EARLY WARNING

An attack on a system requires that the adversary successfully execute multiple steps in a process. The steps an adversary takes to execute a cyber-attack were well documented by a team at Lockheed Martin, using the established kill chain model employed by the military. A key premise of the Lockheed Martin Cyber Kill Chain is that if you can detect a threat early in the chain, you can disrupt (kill) it before it has its intended impact.

With this as a premise, it is very important for the ICS monitoring technology to be able to identify an attack as early as possible in the kill chain–for example when the attacker is trying to establish a foothold on the industrial network or working to enumerate the network to identify key targets such as controllers. Because early detection is not ensured and response times often vary, it is also important for a monitoring tool to be able to detect adversary activity all along the kill chain–up to and including attempts to manipulate settings to impact the underlying process (e.g., changing a controller settings).

Early warning is very important. Using a video game analogy, if the red dot on your chest is the first warning you receive that someone is trying to shoot you, then it is likely too late.

DETECT MALICIOUS AND ACCIDENTAL THREATS

Industrial systems and the processes they control face many different types of issues. As any well-schooled ICS security practitioner (unfortunately there are not enough of them) or plant floor operator can tell you, human error and accidents are far more common (at least today) than actual cyber-attacks trying to inflict harm. Thus, ICS monitoring solutions must be capable of alerting security and shop floor teams about both malicious activity and other actions that could potentially harm assets, process or people.

ICS monitoring solutions must be capable of alerting security and shop floor teams about both malicious activity and other actions that could potentially harm assets, process or people.

On the malicious side of the equation there are two main categories – external and insider threats. External threats must gain a footprint on the network or coopt an insider to have an adverse impact. In the former case, we discussed detection throughout the kill chain steps. The insider is the most difficult case–where an external actor coopts an insider, or where a disgruntled employee is acting on their own. In this situation, the insider would typically have legitimate credentials (if credentials are even required) and be authorized to make changes to the network environment or controllers that could harm the process. Thus, the monitoring tool must be able to detect obviously malicious activity as well as high-risk changes that may be perfectly legitimate but could also be initiated by an insider attempting to do harm.

ENABLE RAPID RESPONSE (REDUCE MEAN TIME RESOLUTION)

This is an easily stated, but often very hard to deliver outcome for many systems. To achieve this outcome there are a few underlying requirements that need to be addressed.

First, the system needs to provide security operations center (SOC) analysts–typically the primary user–immediate "situational awareness". To achieve this requirement the system must provide concise, wellcrafted, human understandable alerts that shorten the time and effort needed to investigate and resolve alerts.

Rather than a single, consolidated alert that indicates exactly what is going on, far too many systems provide SOC analysts with a long stream of anomalous events–often requiring significant effort just to understand what is happening and whether it is important. Assembling a stream of alerts for an ICS network that SOC analysts are often unfamiliar with, into something meaningful, is beyond the skill set of most analysts. Even if the team has the skills, the extra cycles are something that these teams certainly don't have and the lost time can prove critical during an attack.

Secondly, in addition to immediate situational awareness, advanced systems will provide the contextual security data required for SOC teams leading the investigation of alerts in the early part of the kill chain. SOC teams understand security events associated with adversaries gaining a foothold, enumerating the network and attempting to move laterally. This activity is directly in their "wheel house" and the more contextual information the analyst has regarding the attack the more quickly and efficiently they can investigate and resolve the issue.

The same applies for alerts associated with the latter stages of the kill chain, for example where an adversary may be trying to change controller settings to impact the underlying industrial process. In these cases, the SOC team will most likely need to interact with their counterparts at the plant. For this conversation to be efficient and productive, the SOC analyst will need to provide shop floor personnel contextual information associated with the process itself.

For example, instead of relaying network addresses of the assets involved, which plant personnel may or may not be able to quickly associate, the SOC analyst can improve the situation by providing asset names. Further, to ensure that plant personnel can efficiently investigate issues, SOC teams can provide information such as the set points being manipulated and other contextual information the operations and engineering teams need. Armed with actual process related context, plant personnel can readily query SCADA and DCS systems, understand the potential impact and take steps to mitigate the attack.

To help SOC teams collaboratively investigate and solve these later stage, process affecting alerts with the shop floor teams, the system must provide detailed process context. This same context is also required when shop floor teams need to investigate whether alarms associated with high-risk, process impacting changes to the industrial environment are:

- appropriate and authorized
- caused by human error
- work of an insider threat

In each of these scenarios the ability to rapidly understand the situation that caused the alarm and the ability to quickly and efficiently investigate the issue is crucial.

In each of these scenarios the ability to rapidly understand the situation that caused the alarm and the ability to quickly and efficiently investigate the issue is crucial.

SUMMARY

With the list of the top five outcomes ICS monitoring systems need to deliver, teams can focus on the most important requirements–those that deliver true risk management ROI. In Appendix A we summarized additional requirements which many organizations we have worked with include in their selection criteria. We hope this white paper helps and would love to hear your feedback.

APPENDIX – DETAILED SELECTION CRITERIA FOR ICS MONITORING SYSTEMS

Visibility

- Visibility across and into the complete ICS network
  - Ethernet-connected nodes which are assigned an explicit IP address.
  - Serially connected nodes (e.g., Modbus, Profibus)
  - PLCs that reside behind PLC that functions as a gateway (serial and Ethernet)
  - Remote I\O that communicate with a PLC through network cards (serial and Ethernet).
- Ability to accurately express the network topology
- Detailed filtering of assets based on multiple different asset attributes (type, IP address, protocols being communicated, etc.)
- Visualization of network configuration errors such as:
  - Communications crossing network zones
  - Communications/attempted communication with external networks/internet
- Show ghost assets" - Ghost assets are communications targeted at assets that are not on the network or not responding to requests and other rogue assets that should not be on the ICS network at all
- Comprehensive asset discovery – discover all different types of assets on an ICS network and provide in-depth information about each asset – name, type, manufacturer, model, network addresses, serial numbers, firmware/software versions, etc.)
- Comprehensive communications discovery – discover details of the communications between assets (type, frequency, temporal context, etc.) and distinguish the different types of communication (reads, writes, programming, file transfers, etc.) for all protocols "spoken" in the environment

Detection/Alerting Capabilities

- Develop a fine-grain model of assets on the network and their legitimate communication patterns
- Detect anomalous network behavior – ability to see anomalous network activities and detect attacks at any stage in the kill chain. Detect new assets on network, new communication patterns.
- Detect high risk changes – detect changes that may be normal but are nonetheless high-risk enabling the team to spot potential human errors or possible insider threats
- Detect and alert on both security related threats and threats to the integrity of the underlying industrial process
- Alert filtering
- Support for work-flow and assignment of different alert types to different people/groups
- Alert/event consolidation – provide single roll-up alert verses stream of events
- Generate well-crafted alerts that are human understandable to provide immediate situational awareness
- Context rich alerts – provide the alert details needed for security and/or plant operations/engineering team to rapidly discern impact and quickly and efficiently investigate issues
- Alert archival

Initial Deployment/Plant Changes

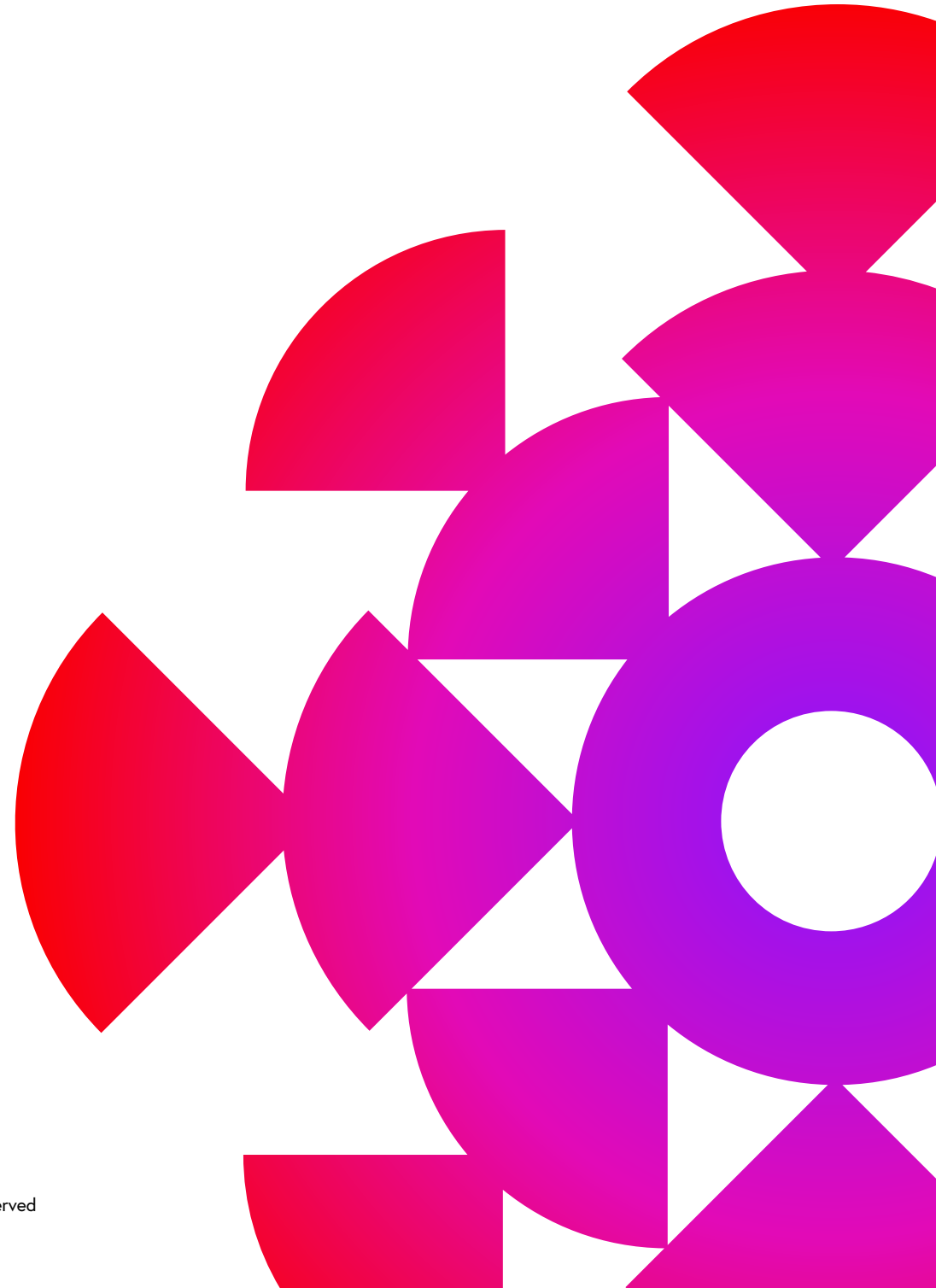
- Fast deployment that requires no production-line/plant downtime
- Automated asset discovery – no need to type, import or otherwise "hand jam" asset and other ICS network configuration into the system
- Ability to generate initial asset priorities/risk ratings for each asset
- Seamless connection, discovery and monitoring across both Ethernet and serial networks
- Plant/network change management - enable plant asset/network configuration changes without causing a stream of alerts or requiring wholesale retraining of the system

Integration

- Active Directory/LDAP
- Syslog output for alerts
- SIEM & Log Management Systems – incorporation of alerts into existing IT Security Operations Center (SOC) workflows

Systems Management/Operations/Secure Configuration

- Central multi-site management – ability to aggregate multiple plants/operational segments into a single pane of glass for enterprise-level visibility across sites.
- Manage users with varied privilege levels
- Ability to run over data diode/one way communications
- Ability to work over low-bandwidth connections – e.g., satellite communications or other QOS configurations.



CLAROTY