White Paper

6 BEST PRACTICES FOR SECURING INDUSTRIAL ENVIRONMENTS

Essential Practices for Better Visibility, Control, and Security

CrowdStrike and Claroty have partnered to secure industrial environments. This guide leverages both trusted cybersecurity firms' successes and learnings from years spent helping secure industrial operations around the globe, across a vast variety of differing and challenging environments. The rapid growth in risks and vulnerabilities these environments are encountering demands a measured and effective response.

While every industrial environment can pose unique challenges, the following best practices apply broadly to anyone looking to effectively manage and secure industrial networks.

1. Secure the Known

Industrial environments often encompass networks, assets, and systems with unknown components, but there are also many components everyone knows about — securing these should be the first step. Common examples include:

- **Human-Machine Interfaces (HMI)**
- **Active directory controllers**
- **Engineering workstations**
- **Historians**

Installing an Endpoint Detection and Response (EDR) solution, such as the market-leading CrowdStrike Falcon platform, begins to limit the attack landscape and provides an early warning for malicious activity. It is critical to the success of any EDR deployment that the solution provider clearly indicates which devices are suitable for installation of an EDR solution, as not every device is capable of hosting an endpoint protection agent.

2. Discover the Unknown & Build Comprehensive Visibility

Once the "known" environment is secure, the next concern should be to discover everything else. 100% visibility should be achieved quickly and without a high degree of effort, it just takes the right approach. Solutions providing this visibility need to be built to interpret a broad array of protocols — including those that are niche, uncommon, or unique to their environment — and provide an actionable degree of depth and breadth in the network insights provided. This understanding of industrial environments is essential, but gathering the necessary information also needs to be done in a safe, controlled manner so as to not disturb the operations and processes connected devices support.

The fastest and most effective route to a more secure industrial environment demands an integrated approach to OT visibility, as with CrowdStrike Falcon with Claroty Edge — a joint solution built to discover unknown network components quickly, easily, and safely.

Previously unknown network components may include:

- Unmanaged systems
- IoT devices
- Medical devices
- Random active directories
- PLCs
- HMIs
- Connected vehicles
- Building systems

3. Build a Vulnerability Management Plan

Vulnerability management is only as good as the data provided in the discovery phase, so getting the exact model, firmware, and attached modules is key to reducing noise and false positives. (see figure 1 below)

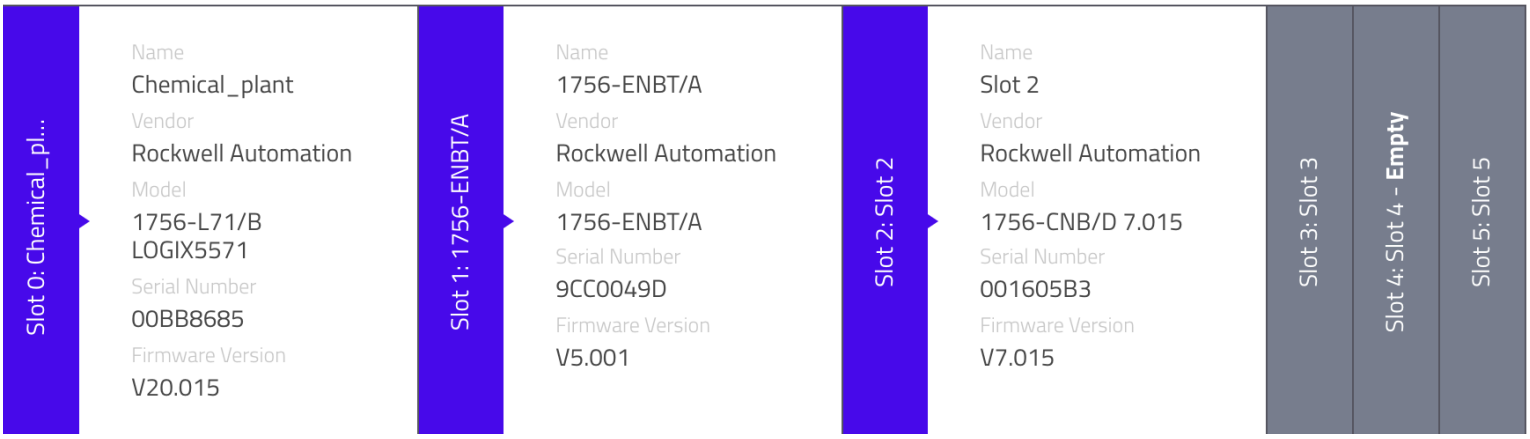

Figure 1: A view of sample discovery data provided within the Claroty Platform. The necessity of this best practice is not impacted by tool selection.

This is even true for CVE 3.0. Many industrial networks are simply left to run and are only upgraded when something breaks — leaving a large number of outstanding vulnerabilities unchecked for both known and unknown network components. With full visibility of all assets, the accumulated vulnerability data may seem daunting to take on.

The list of "High" risk vulnerabilities may be long so it's critical to triage and seek out common mitigation steps, for example blocking Ethernet over IP from exiting the network on port 44818. It is especially vital to take vulnerability risk levels and the criticality of systems into account when planning remediation. Figure 2 below shows the massive reduction in effort necessary when a plan is formulated and mitigation steps are unified.

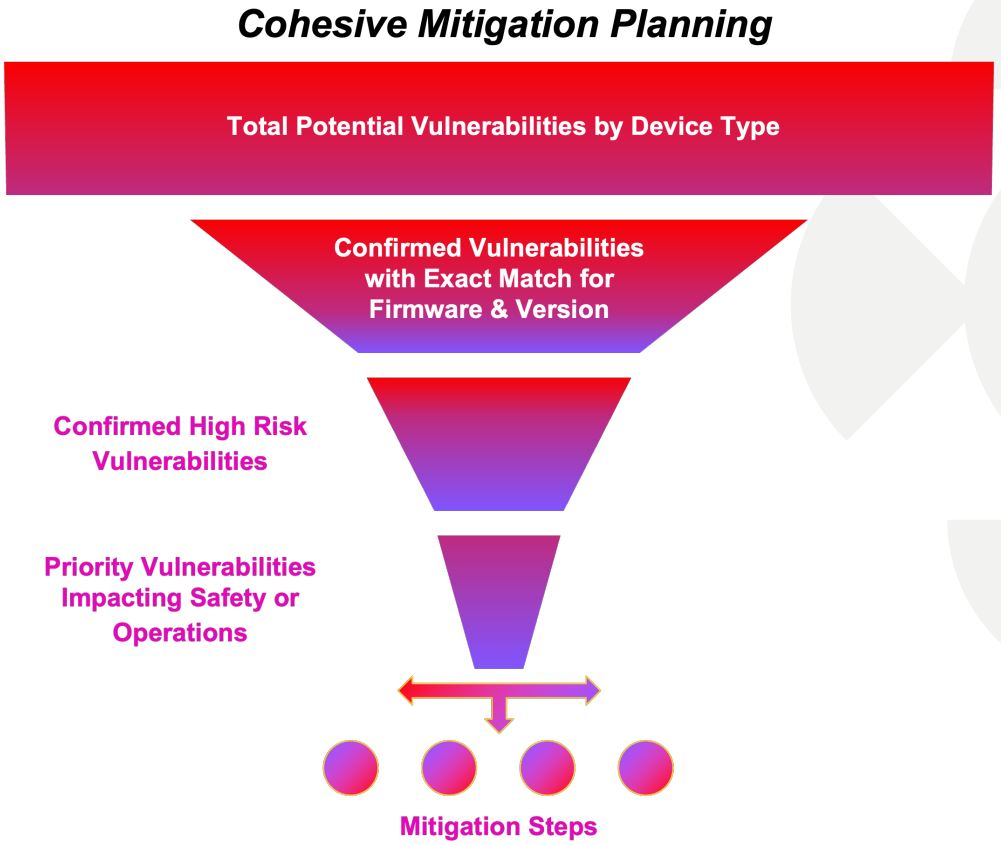

Figure 2: Actionable next steps for mitigating the greatest risks quickly and efficiently can be identified through a tiered process of prioritization.

4. Secure the Unknown

Systems uncovered in the discovery phase now need to be protected and monitored. Some exposed network components will be able to have an EDR installed, for example unmanaged Windows systems. Others like PLCs, old HMIs, and IoT devices may not be able to install an EDR agent, and in these cases a broader network protection solution like Claroty Continuous Threat Detection (CTD) is required. It's important to make sure both the endpoint and network protection devices work together in a single ecosystem, preventing the requirement for tool swivel seating. With a fully integrated EDR and network protection solution, network protection can be anchored across every endpoint and effectively provide security coverage for the many gaps between secured endpoints.

5. Control Access

Controlling access to industrial networks is a vital next step on the path to a secure industrial environment. It is critical to formally establish and enforce policies controlling access to the network and assessments have to be undertaken to discover local accounts, determine privilege, and understand normal behavior. Serious concerns should be raised around any standing practices involving the use of vulnerable access options not intended for use in industrial environments. These legacy options, such as VPNs, should be considered a direct risk to any systems accessible via those methods.

Secondary, external access should be controlled, documented, vaulted, and recorded with an industrial platform tailored to the OT environment. It is essential that any access to the environment is within controlled, established processes and organizations must have the capability to monitor access and enforce policies. This capability can only be securely enabled with solutions built for the complicated realities of industrial environments, such as Claroty Secure Remote Access (SRA) and CrowdStrike Identity Threat Detection (ITD).

6. Enable Anomaly Detection

With visibility in place and the environment secure, the final step is to protect against advanced threats, whether malicious or inadvertent. Allowing the EDR and network protection components to work together — as with the CrowdStrike-Claroty joint solution — creates a network DNA and establishes baselines for behavior. These baselines aid in the enforcement of policies governing optimal and safe operations — typically including critical details like production values and communication patterns. A pair of examples:

- **A pipeline has never exceeded 48PSI and a value of 90PSI is suddenly seen**
- **RDP session from a line on the manufacturing floor to another line, where this request had never been seen before**

While these anomalies may produce some false positives, it also forms the foundation for detecting unknown threats — especially the hardest to detect and most advanced threats. It's vital to keep in mind information security is a continuous practice that requires repeated assessment and planning to adjust for new and unexpected threats. Having a foundation established with the above 6 best practices gives organizations the best chance of avoiding the exposure, lost productivity, and costs associated with under-secured industrial environments.

CLAROTY

CROWDSTRIKE

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), CrowdStrike is a global cybersecurity leader that has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud, the Falcon platform enables partners to rapidly build best-in-class integrations to deliver customer-focused solutions that provide scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value. Learn more: https://www.CrowdStrike.com/

About Claroty

Claroty is on a mission to secure all cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). Our platform is deployed by hundreds of organizations at thousands of sites across all seven continents. Claroty is headquartered in New York City, with employees across the Americas, Europe, Asia-Pacific, and Tel Aviv. Since being launched by the famed Team8 foundry in 2015, Claroty has raised $635 million in funding from the world's largest investment firms and industrial automation vendors, making it the most well-funded industrial cybersecurity company.

To learn more, visit **www.claroty.com**.

CONTACT US

contact@claroty.com