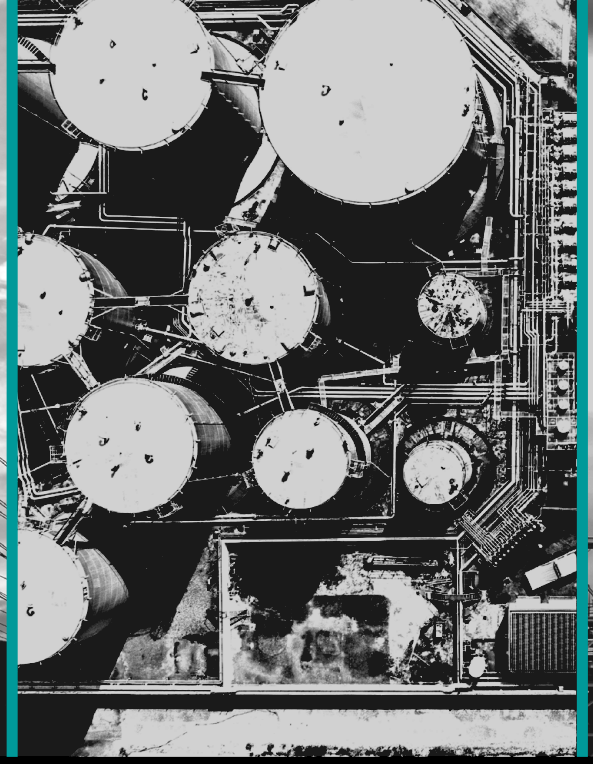


DRAGOS
SAFEGUARDING CIVILIZATION

10 Ways Asset Visibility Builds The Foundation For OT Cybersecurity

How well do you know your OT assets?

WHITEPAPER

Asset visibility is at the foundation of all effective operational technology (OT) cybersecurity programs. After all, industrial organizations can't effectively protect the OT assets they don't know about. This is true no matter whether your company is producing ethylene downstream, distributing renewable energy to residential customers, or distributing vaccines to fight a global pandemic — all share the same asset visibility challenge.

From turbines to temperature controllers and everything in between, asset owners know that safety, uptime, and reliability can all be impacted by cyber attacks. When organizations lay the groundwork by fully identifying and inventorying their OT assets, every cybersecurity process becomes easier, whether it is leveraging threat detection, initiating incident response, actively managing assets for vulnerabilities and weaknesses, or implementing overarching strategic OT security initiatives.

HOW WELL DO YOU KNOW YOUR OT ASSETS?

Often one of the most eye-opening early experiments a company can make about asset visibility is simply asking each group of relevant stakeholders how many assets they have. Quite often organizations find that they'll get a different answer from each group, be it IT, security, or operations — a red flag that nobody has a clear picture of what's on the network.

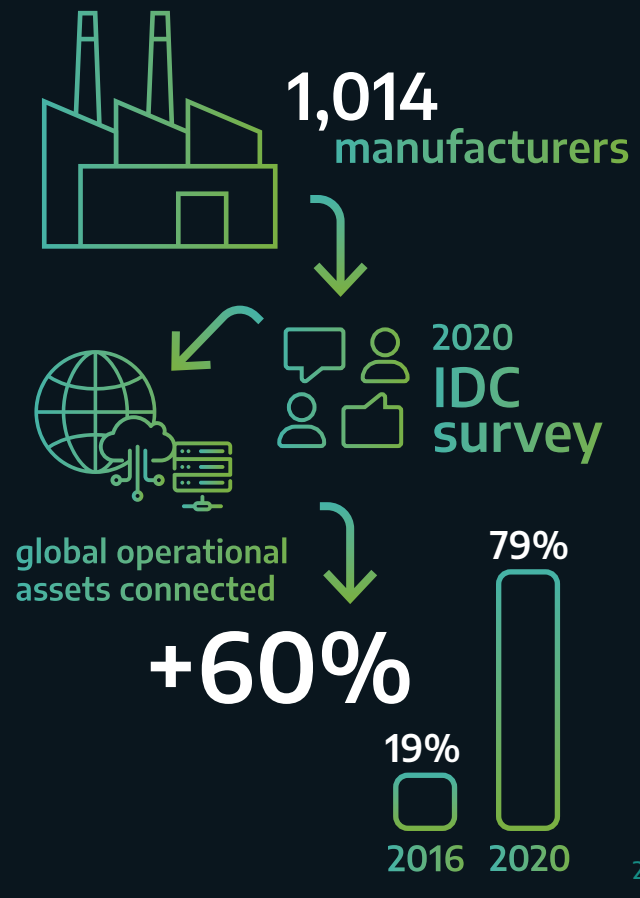
Think about it: when executives hear about new OT threats in the wild that could impact anything from gas crackers to safety instrumented systems, how can they even get their arms around the relevance of these emerging OT risks to their business if they don't have an inventory of assets identified and classified?

Continuous OT asset visibility capabilities make it possible to discover:

- connectivity and communications channels operators didn't know existed,
- active threats operating quietly in the environment,
- insecure configurations,
- latent vulnerabilities,
- rogue assets and more.

Let's explore why and how this should be done:

OT Connectedness Is Growing



BRIDGING THE IT-OT VISIBILITY DIVIDE

Most companies understand the need to inventory their assets, but a methodical approach will have a huge impact on the efficacy of data collection in actually helping to solve security and business issues. The amount of data generated can quickly overwhelm analyst resources so understanding critical requirements and desired business or risk management goals is essential to think through up front.

IT has a long history and legacy in asset management and asset inventorying at this point, which means that the tools, frameworks, and practices around gaining asset visibility are very well tuned to their use cases. But OT has unique environmental challenges that need to be managed across industrial assets — ones to which IT's tools, integrations, and processes are not designed to meet. Office workers are often familiar with forced reboots of their desktop computers for patch installations, but in an industrial environment rebooting a workstation connected to a smelting furnace could result in weeks of unplanned downtime to cool, empty, and reheat the furnace.

Many IT asset visibility tools and tactics do not translate well to the OT environment — for example, you can't put an agent on a PLC because they often run firmware or operating systems that agents aren't compatible with. An IT administrator who performs a network scan using NMAP in an industrial environment runs the risk of knocking sensitive devices offline like older controllers that could disrupt or halt production. In traditional IT environments, it would be perfectly normal to use active scanning tools for asset discovery and monitoring, but in industrial scenarios, passive techniques are often preferred if not required because of the level of safety they provide. Organizations need to take a different approach that's specific to OT environments in order to achieve a level of asset visibility that corresponds to what their security team may be used to seeing from IT assets.


Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats

Executive Summary

One guide that we recommend to OT asset owners is the Collection Management Framework for ICS Security Operations and Incident Response. It provides a prescriptive, impact-driven reference based on years of customer experience that's uniquely suited for the realities of the OT environment.

We'll dig into the basics of the Collection Management Framework and how to get started establishing asset visibility in a moment, but first let's explore why this work needs to be done.

ONLY 10%

of enterprises have a **COMPLETE INVENTORY OF THEIR OT ASSETS** COVERED by their SOC

— SANS Institute 2019 SOC Survey

90%

of Dragos's professional services engagements find that industrial organizations have **EXTREMELY LOW OR NO VISIBILITY** into the assets in their OT environment

— Dragos 2020 ICS Cybersecurity Year in Review

> "An inventory of assets important to the delivery of the function is an important resource in managing cybersecurity risk. Recording important information, such as software version, physical location, asset owner, and priority, enables many other cybersecurity management activities."

THE 10 WAYS

1. Understanding Normal

Knowing the real state of the environment – which assets are where and how they're operating on the network – establishes a baseline of what 'normal' looks like. You wouldn't expect to see a historian pop up on L1, nor would you want to see a patch management server suddenly start beaconing out to an Internet location. This provides a reality check for how processes and workflows really execute in the operational environment. It also adds valuable context and a higher fidelity of information to accelerate a range of security activities from monitoring and threat detection to change management to incident response.

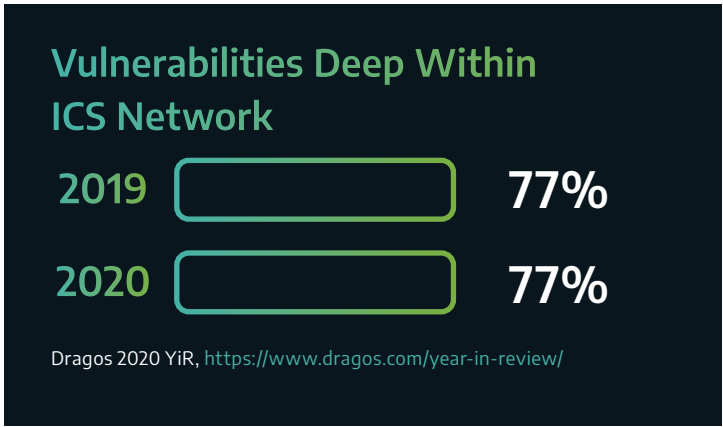
Establishing this baseline isn't necessarily an exercise in chasing the brass ring of anomaly detection. Relying singularly on anomaly detection can introduce a host of problems and alert fatigue, as anomalies are not always synonymous with threats. However, tracking the norm and noting deviations from it can provide another dimension of data and a historical record for security analysts to lean on during investigation and remediation.

Operators require tools that make their jobs more efficient, and the easier it is to establish baselines, the quicker they can spot deviations. This can take the form of alerts or notifications, but also in more graphical formats where colors represent operational health. For example, at shift start having the ability to view a simple dashboard that highlights any problematic PLCS in red while displaying stable operator consoles in green, makes it easier to focus on areas requiring attention. The aggressive trend towards connected digital operations is accelerating the need to have centralized views across OT environments.

2. Asset Verification

Gaining full visibility into OT assets like HMIs, historians, and controllers, gives organizations a true lay of the land of what really resides within their facilities. A complete asset inventory provides a clear-eyed understanding that's essential for identifying misconfigurations, vulnerabilities, and other weaknesses across an industrial control environment.

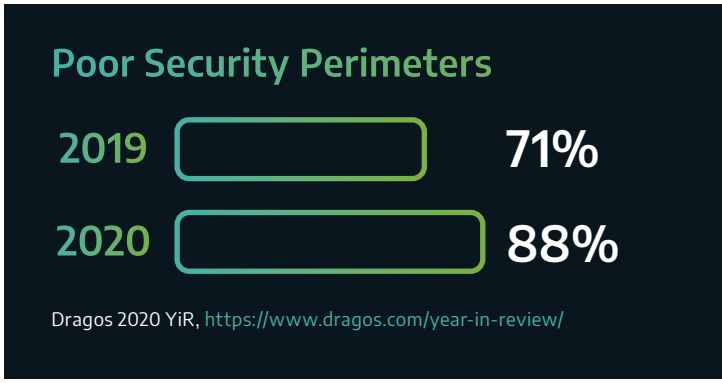
When done well, asset visibility should provide insight into not just the existence of the asset but also its version, firmware status, and configuration state. It would be important to know if a controller is running a vulnerable firmware version and whether an update is available from the vendor.



Too often, asset owners spend valuable resources walking the floor to manually identify connected devices like network switches, workstations, or even process controllers — a method that is both inefficient and subject to significant errors. Automated collection and updating of this information ensures a consistent and continuous inventory across facilities that scales. It also opens up a world of possibilities for verifying the state of assets when operations teams are in the heat of the moment — whether it is in a planned infrastructure upgrade in which vendors may be tweaking configurations or an unplanned outage or potential security incident.

3. Identify And Visualize Asset Relationships And Communication Pathways

Asset visibility not only provides insight into the assets themselves, but the relationships they have with one another and communication pathways they establish. Mature asset visibility capabilities makes it easier to monitor an organization's OEM and third-party management communication channels to ensure they're adhering to their scope of contract and not introducing unnecessary risk to the ICS ecosystem. This includes keeping eyes out that communication paths aren't touching other systems, only doing work during approved change control windows, and so on. If an engineering workstation suddenly starts sending commands to a controller in Zone 2 when it is only supposed to talk to devices in Zone 1, then investigation is needed.



Asset mapping can show pivot paths that illustrate how many hops away assets are from one another to easily offer security analysts and operators a visualization of network segmentation to identify zoning issues and how an adversary could potentially move around the network. Similarly, this kind of information can help validate firewall rules. If a contractor installed an unauthorized cellular modem for remote support, you would want to know about that — especially if it provided a path to an engineering workstation and allowed an attacker to pivot to a domain controller.

Not only do these logical representations of operating environments provide critical visibility into network activity, they also expose potential misconfigurations and gaps in architecture. Identifying these gaps gives asset owners the advantage of implementing defense controls proactively. Why wait to fall victim to a ransomware attack when there are simple steps that can be taken like monitoring Active Directory or remote connections and hardening the environment to produce a more defensible architecture?

4. Threat Detection

A passive network detection approach doesn't necessarily require complete asset visibility or a baseline for normal to pick up on threat activity operating between assets. And as we've said before, anomalies in asset status, like a workstation being offline when it may have intentionally been taken down for maintenance, don't directly denote that a threat is present.

However, it's definitely easier to identify threats operating within fully visible assets. For example, large .iso files with a file name that closely resembles an OEM update but a hash value that matches a known malicious file can key a team into suspicious activity.

DETECTION AND VISIBILITY – TWO SIDES OF THE SAME COIN

Not all vendors provide comprehensive solutions that reflect this important point. A threat detection rule that fires because of east-west traffic flow has an entirely different context if that traffic is to an HMI vs a Safety Instrumented System (SIS). Asset discovery and visibility alone isn't enough. Threat detection alone isn't enough. The two must be coupled for proper threat visibility.

Visibility and an established baseline for asset inventory and behaviors adds crucial contextual clues to speed up threat detection. Those changes themselves could be good or bad, and the deviation wouldn't necessarily be something on which an organization would want to trigger an alert. If a port needed for remote access is opened up during a routine vendor support window there wouldn't be cause for alarm, but if the same port allowed a connection from an unauthorized remote system, the conditions are quite different. Environmental information coupled with threat behavior data, provides valuable additional context on whether changes are related to adversary tactics, techniques, and procedures (TTP) as opposed to planned infrastructure changes.

5. Spotting Rogue Assets

Most operators know all of the assets attached to their core processes, but may not necessarily be aware of rogue or hidden assets that open the environment to risk. This is particularly challenging for companies with remote sites or large, sprawling facilities with varying levels of physical security. This could be a stray laptop that someone has hooked into the network at a far-flung facility for a technician to provide on-site troubleshooting, an old, retired device that remains plugged into the network like an external USB storage drive for backups, or even maliciously implanted devices like a camera that is monitoring shop floor activity.

These are the kind of assets that are most likely to surprise operators, and they are also the ones that adversaries are most likely to sink their teeth into. Adversaries seek to target assets that organizations don't know about like undocumented engineering workstations as a way to quietly persist on the network.

Short of automated asset identification, the most traditional way to find these rogue assets is via a painstaking walkdown process. In fact, even with automation regular facility walk throughs are an important backstop for security assurance. However, there's only so many resources to go around and most organizations are likely to do this only annually, semi-annually, or quarterly at best across all of their sites. Having an automated method for spotting rogue assets in between those checks can make a big difference for continuously hardening OT environments.

6. Incident Response

Thorough, up-to-date asset visibility can serve a vital role in incident response across the entire lifecycle of an incident. Responders armed with accurate asset inventories are able to confirm threats and identify incidents more quickly. As they carry out their investigations, asset visibility can make all the difference in accurately scoping the spread of an incident and fully understanding the systems affected by the adversary's actions. Knowing which site a compromised HMI is located at, and where it physically sits at a plant can expedite access for the purpose of forensics.

Similarly, visibility supports insights that can lead to a plan for system or network containment and remediation. And once an incident is ready to be closed, greater visibility gives responders greater peace of mind that they've been able to fully eradicate a threat.

7. Mitigating New Critical Vulnerabilities And Threats

Can you quickly answer executives when they want to know whether your infrastructure is impacted by a new vulnerability or a new threat group's TTP? A searchable, easily accessible asset inventory can help quickly rule out irrelevant threat intelligence or calm fears of a new vulnerability.

Conversely, it can help teams pinpoint where relevant assets are if they need to be patched — or secured through compensating controls if a patch is not available or impractical to deploy for operational reasons. This can not only help speed up mitigation of new highly critical risks, but also generally streamline day-to-day vulnerability management and patch management practices. Security teams in manufacturing environments need to have a clear understanding of exactly which vulnerabilities can and should be patched to maximize schedules that are already high pressure during infrequent events like shut down.

VULNERABILITY MANAGEMENT WITHOUT AUTOMATION IS A RESOURCE KILLER

Without central visibility into asset vulnerabilities, and a closed loop to manage the controls which address them, whether they include patching, configuration changes, or port/protocol/routing changes, cybersecurity teams will be spread thin if they are relying on offline

8. Supplementing Change Management With Configuration Detection

Setting internal security configuration standards for OT assets and sticking with these policies is easier said than done. Configuration drift is inevitable in a dynamic industrial network and it can be difficult to track and manage changes as they occur in real-time.

The right asset visibility capabilities can make it easier to detect changes in configurations that makes infrastructure weaker or even knock it out of compliance with regulatory mandates. They provide the building blocks for improving change management and asset management maturity — a key element not just for security but also operational integrity. A patching server with access logs disabled by an attacker could result in regulatory fines for non-compliance, not to mention the potential for operational disruption.

9. Minimizing Impact Of Compliance Reporting

Asset visibility can also provide a huge win for cybersecurity staff and operators alike on the compliance front. Operators are typically under tremendous pressure to meet regulatory mandates such as NERC CIP and ISA 99/IEC-62443 to regularly report their security and asset controls to auditors. At many organizations this process takes a significant amount of manual labor and interruptions to daily work.

Automated discovery, analysis, and mapping of assets can minimize the impact of compliance reporting for the entire team and free up resources to make security or operational improvements through more meaningful avenues.

> **“Managing asset configuration involves defining a configuration baseline for information assets, IT assets, and OT assets and ensuring that these assets are configured according to the baseline. Most commonly, this practice applies to ensuring that similar assets are configured in the same way. However, in cases where assets are either unique or must have individual configurations, managing asset configuration involves controlling the configuration baseline of the asset when it is deployed for operation and ensuring that the asset remains configured according to the baseline.”**

10. Justifying Security Investments

Understanding the complexity of an OT asset portfolio is one of the first steps that security strategists must take to engage in a robust risk assessment. Knowing where and how assets are deployed and what the extended security controls around them look like is necessary to identify gaps in controls and processes. When it comes to critical infrastructure or industrial operations, one compromised asset could have major safety or revenue consequences that greatly exceed most IT devices.

With asset visibility it becomes much easier to find areas where security controls are lacking and start prioritizing investments and future initiatives. Asset inventories and mapping provide the security team with an accessible and updatable source of information for developing and tweaking their roadmap. Similarly, they give everyone hard evidence to present to business and operational stakeholders when it comes time to justify spending requests or process changes.

OTHER OPERATIONAL BENEFITS

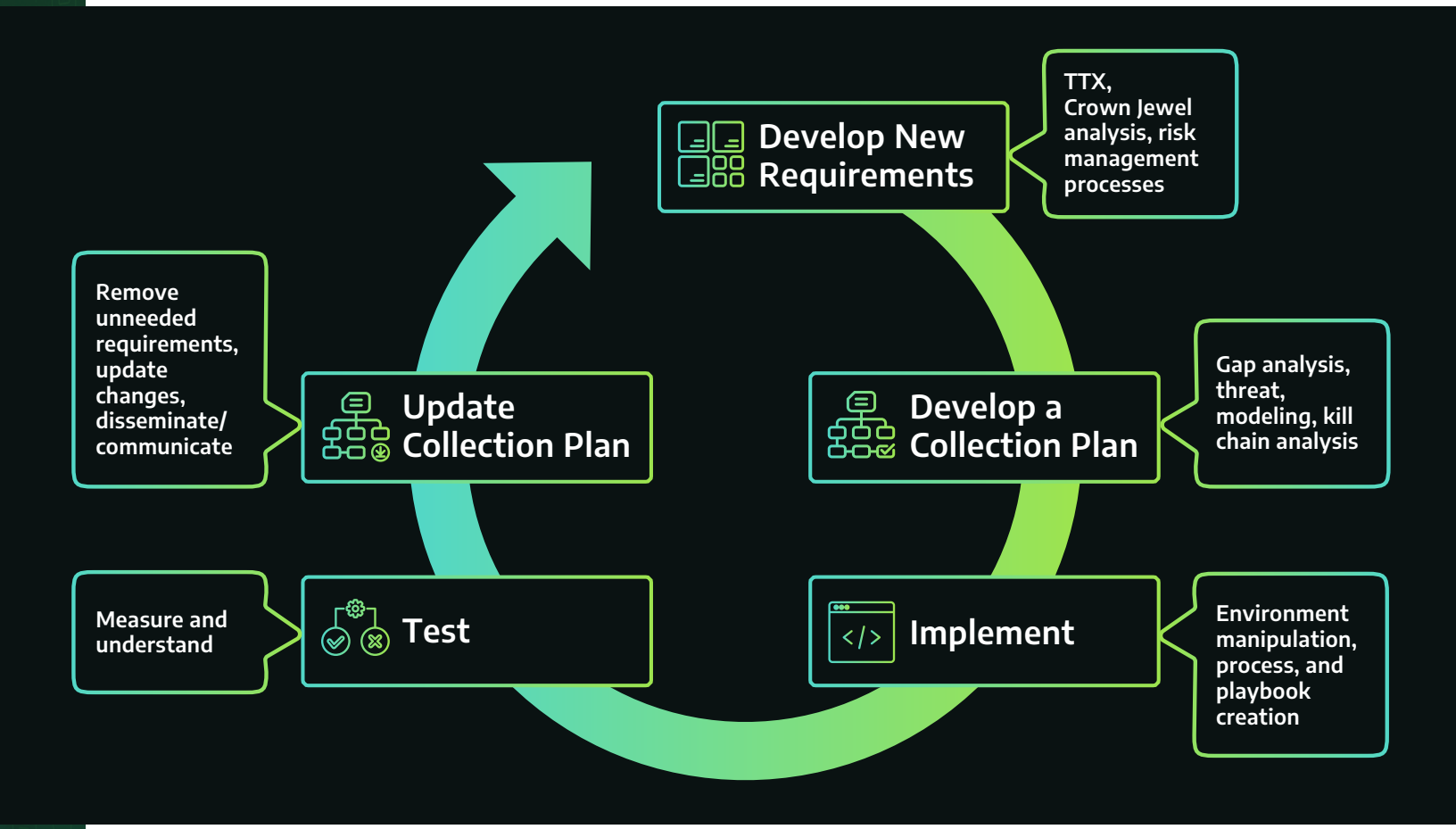
While we have focused primarily on security benefits and use cases for asset visibility in these 10 ways, it's important to remember that the positive influences of visibility extend well into the operational realm. Shorter time to resolution when an asset is offline, improvements in predictive maintenance because of better data visibility, and more efficient turnaround during planned shutdown can all have a direct lift to bottom line revenue from a faster return to production.

One of the most obvious areas that can benefit is performance management. With OT asset visibility maximized it becomes easier for operations teams to identify areas of network over-utilization and pinpoint communication issues before they cause operational impact. An overloaded switch that started dropping packets and interrupted data collection would make it almost impossible for operators to know whether they were seeing the true status of a process. Imagine a water utility that released contaminated water because a flow control valve issue didn't trigger an expected alert. Similarly, visibility simplifies the process of identifying when asset service issues may impact operational processes, such as if a gas monitoring system goes offline or network time servers go offline.

HOW TO GET STARTED

Before starting, make sure a plan is established that determines data collection requirements through a structured approach like Dragos's **Collection Management Framework**. A good plan will lay the foundation for a successful outcome that creates a sustainable, scalable, and efficient Asset Visibility program.

Typically the planning and implementation stages as guided by the Collection Management Framework will be a continuous process that looks something like this.



As organizations go through the journey of establishing asset visibility, they should anticipate potential stages of the maturation process.

Be Prepared For Surprises

As organizations begin the process of maturing their asset visibility and management capabilities, step one is mental preparation. The process can often uncover surprising insights about infrastructure that may make some people uncomfortable, whether they're about connectivity and communications channels they didn't know existed, active threats operating quietly in the environment, insecure configurations, latent vulnerabilities, or rogue assets. But knowing about these problems is the first step toward fixing them.

Discovery and Asset Identification

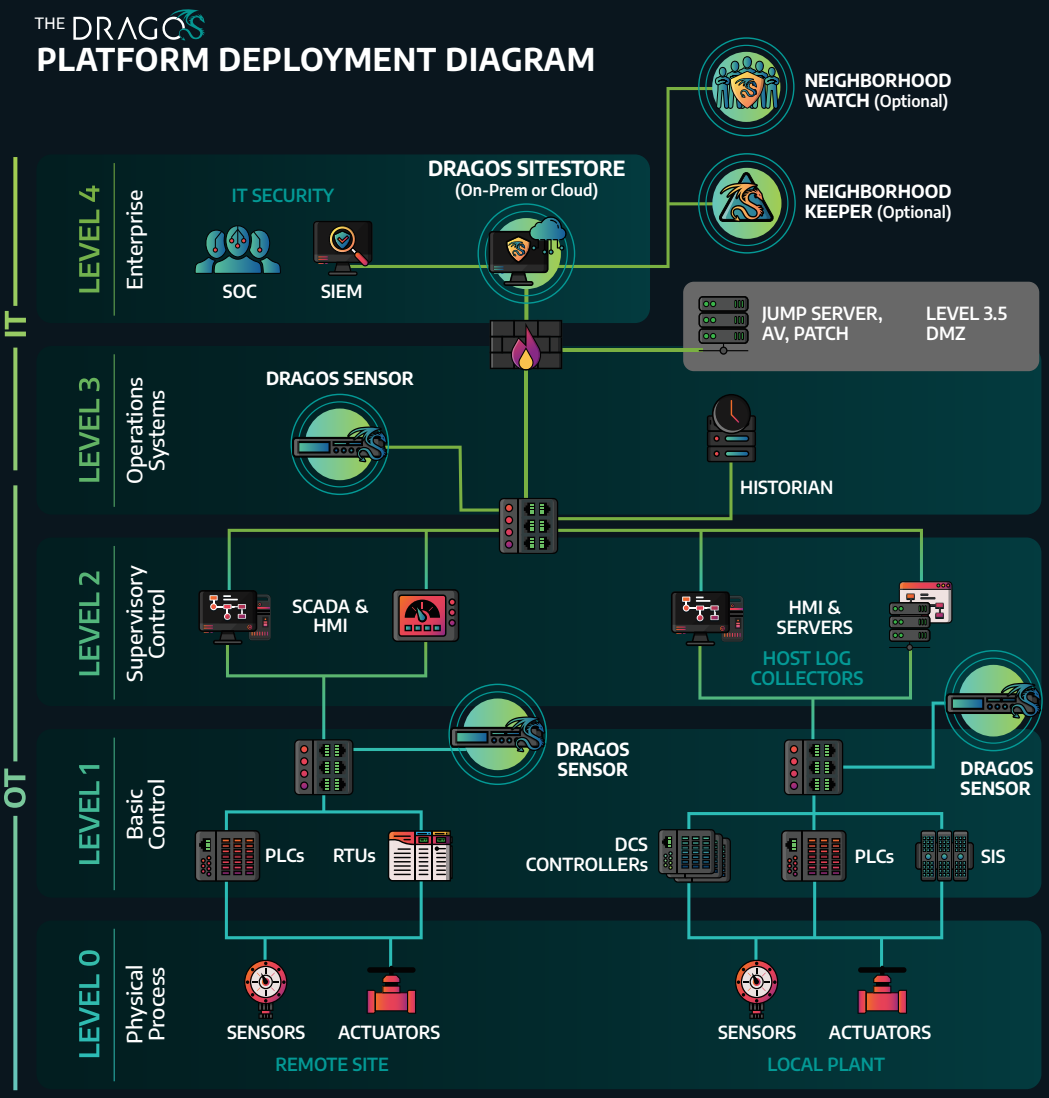
Asset discovery and asset identification are fundamental to establishing solid visibility across OT asset portfolios. Sometimes it can be difficult getting started with automated discovery because an organization may have unrecognized blind spots about its infrastructure. As organizations consolidate within industries through acquisitions, and as aging workforces retire and take tribal knowledge with them out the door, gaps in documentation become problematic. Even if the gaps aren't overt, system documentation can quickly go out of date if not maintained. That wireless access point that was set up in an emergency and not properly documented, or the backup engineering workstation that came online and wasn't properly decommissioned can turn into industrial nightmares if not properly dealt with. This is why it can be valuable to kick off the initiative with manual discovery. Start first by mapping high-level architectures and performing comprehensive facility walkdowns to start physically identifying hidden assets that will need to be accounted for.

This early manual work will make it easier to prioritize and decide where to establish telemetry first for continuous, automated discovery. At Dragos we call this process the Crown Jewel Analysis, whereby an organization looks at its high-level architecture it can start identifying the crown jewels — facilities, networks, and systems crucial to business missions or under high safety thresholds — which would be the natural place to start implementing the capability for automating discovery and identification of assets.

Thoughts from a consultant in the field:

"A lot of times, people will say, 'Well, I don't have that data to really identify my high value assets that need to be monitored.' Well, sometimes it's a lot easier than you think. I would be surprised at any manufacturing facility or industrial facility that doesn't have insurance on their turbine for instance. If that turbine breaks, it's a big problem. So what systems control the turbine? A lot of times that information has already been identified for the business continuity risk plan or insurance."

Many industrial companies are familiar with the Purdue Model as both a logical and conceptual way to organize and operate their OT environments – all the way from business or IT systems at Level 4, down to PLCs and the physical processes they control and monitor at Level 0. Whether a downstream petrochemical company, or an electrical utility operator, the structure and architectural framework provided by the Purdue Model makes it easier align with the planning and execution of security controls.

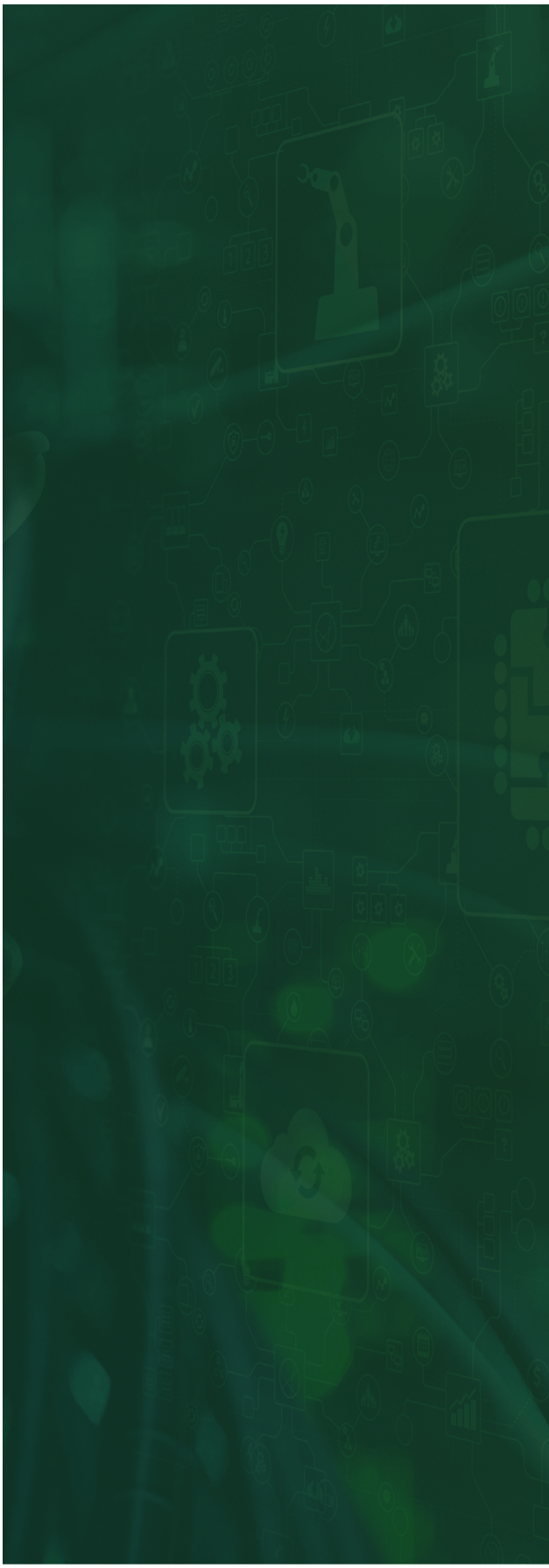


As organizations progress to implementing monitoring and automation to improve visibility, many find a land-and-expand approach to be the most effective way to roll out their technology and processes. Many start first by landing in the network—examining East-West traffic in the Level 1 and 2 networks, North-South to Level 3/3.5, and traversal to the IT networks. Then they expand by moving down layers in the Purdue model and adding in host traffic and OT device logs. There's no one-size-fits-all approach – the point is that it will be a gradual process of broadening the scope of deployed visibility tools.

Planning for Asset Management

The endgame for all of this work isn't visibility for visibility's sake. It's a journey, and asset visibility is the starting point. Ultimately, the goal should be to start operationalizing those findings and moving toward more advanced asset management — including internal inspection of control systems, patch management, and full lifecycle management.

As industrial organizations plan ahead for asset management, they should be strategizing ways to avoid information overload from the data streaming out of their monitored assets. Ideally a phased rollout will consider not only deployment logistics, but also how and by whom the monitoring data will be ingested. Organizations should plan to have a team of analysts available to manage data, inventory assets, assess, and monitor the OT environment. That team can be run in-house through an existing SOC functionality or maybe a new OT SOC team, or outsourced via a specialized managed service. As the organization deploys, it should also consider how much telemetry it puts out in the environment as bounded by the team's ability to keep tabs on the data.



OVERCOMING IT-OT CULTURAL CONFLICT

Often times some of the biggest challenges and points of friction in getting monitoring in place for automated asset visibility stems from the IT-OT cultural divide. In a recent talk about their lessons learned from its asset visibility and monitoring journey, two experts from a major Southwestern USA utility company distilled some insight on how to get buy-in from operators:

Bring Barbecue:

"Early on, we learned that we needed to listen a lot. The (operations) engineers are smart. What we found successful is quite by happenstance, we went for a tour and kind of prepping to go in we brought barbecue. As the barbecue smell wafted out across the control room, more and more people started showing up, and we had some really good conversations with some very smart people who knew things about that plant that nobody else would have known. It helped us plan. Get out there, build those relationships, take the barbecue, do whatever you need to do to actually get in and talk to those people."

— IT-OT Cybersecurity Architect

Get Some Early Wins:

"We started getting some wins with asset verification, just identifying things that were there. A lot of times, if you've ever been out at one of these locations during an outage, it's busy, and people are up till midnight. At some of these generation facilities, people bring their trailers and go to sleep overnight in their trailer so they can get up early the next morning to work. Well, when they're that busy, there are things, especially documentation, that goes by the wayside, and having the asset verification where we can see things coming and going as they're being added to the network has been actually very useful for them and for us."

— IT-OT Cybersecurity Architect

Give Operators Visibility, Too:

"Our SOC is going to be the ones that are in the platform doing a lot of the security tasks, of course working with the OT teams as needed. The idea is that we do want to take security monitoring off of their plate. But we want to give them access because we don't want to remove them completely from it if they are interested. Through that, it's been awesome to watch our operators and how they come up with operational use cases within the platform and with that visibility. A lot of these guys have been blown away by the visibility that they now have, and many of them, either they'll come to us, or they'll use the platform themselves for troubleshooting."

— IT-OT Cybersecurity Architect

HOW DRAGOS HELPS ORGANIZATIONS OVERCOME OT VISIBILITY CHALLENGES

Dragos helps industrial organizations get a handle on their OT asset inventories and mature their asset management practices with the most effective OT cybersecurity on the market and the industry's largest team of ICS/OT practitioners. Dragos can help organizations at any maturity level improve their asset visibility from ICS management infrastructure, to controllers to safety systems, and everything in between. We do this through:

Dragos Platform:

- Fully identify assets on monitored networks and gain a visual representation of the environment including OT systems and devices like PLCs and RTUs
- Leverage the flexibility of passive scanning and host log analysis as determined by the needs of the business and realities of the network
- Establish a baseline for your environment and focus attention on deviations that could signal malicious activity
- Contextualize asset data with four types of threat detection to minimize alert fatigue: configuration, modeling/anomaly detection, indicators of compromise, and behavioral analytics.

Professional Services:

- Initiate an asset visibility program with an architectural review and crown jewel analysis
- Lean on experienced ICS security practitioners to develop a tailored sensor deployment strategy
- Gain insights on how to get the most out of OT asset monitoring infrastructure

Neighborhood Watch:

- Augment your cybersecurity operations with our team of ICS cybersecurity experts — performing comprehensive asset identification, threat detection, and incident triage with the cloud-deployed Dragos Platform to ensure threats don't get overlooked.
- Routine threat hunts based on newest adversary tactics, techniques, and procedures (TTPs)
- Immediate support for critical situations — only a phone call or email away

READY BEFORE HELP IS NEEDED

Are you ready to get your cybersecurity challenges under control?

Contact us at sales@dragos.com or request a demo.

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT WWW.DRAGOS.COM.