Microsoft Security

IT and OT convergence is happening, but is security ready? What is a CISO to do?

Table of Contents

When hackers inflicted a ransomware attack on Colonial Pipeline, shutting down fuel lines across the southeastern United States and costing the company $4.4 million in ransom alone, the world took notice. From startups to corporate conglomerates, and from entry-level IT employees all the way up to the C-suite and boards, no one wanted to have another attack take place on their watch.

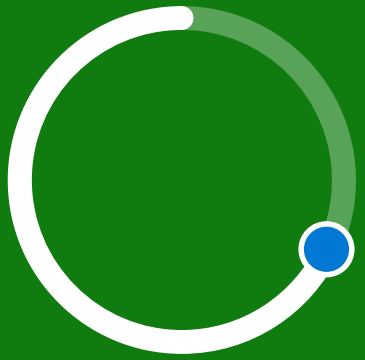
The costs to companies who are attacked go far beyond just the ransoms paid. Colonial Pipeline paid the ransom within hours of being attacked but was not fully operational until more than a week had passed. The shutdown caused widespread fuel shortages, panic buying, rescheduled flights, and increased gas prices. Whatever the industry, the risk to companies and their partners both upstream and downstream is real.

There is a massive growth trajectory for ransomware and extortion attacks in the coming years. The explosion of unmanaged devices and operational technology (OT) employed within organizations has dramatically increased the surface area for hackers to attack, and the often-mistaken belief among some C-suite executives is that the industrial systems have a similar level of protection as the rest of their IT network is only exacerbating matters. Of course, the CISO knows better!

The costs to companies who are attacked go far beyond just the ransoms paid.

According to a report from Enterprise Strategy Group (ESG), 18% of companies say they experience ransomware attacks on a daily basis, and the risks are getting worse as attackable surface areas grow. 68% of executives believe that adding new IoT and OT devices to their environments is critical to innovation and growth but, according to Ponemon, less than 30% of them even have visibility to the devices they already have. Rare is the corporate security professional who can even identify every last endpoint touching their network, much less identify where the gaps are and begin to protect them.

Beyond ransomware attacks, porous cyber borders leave organizations vulnerable to corporate espionage and even physical attacks. A petrochemical plant in Saudi Arabia was targeted in 2018 with the intention of triggering an explosion. When Merck was targeted the next year by a nation-state threat actor some questioned whether it was an act of war. Risks abound across state and local governments, retail, transportation, food and beverage, mining, smart buildings, manufacturing and more are forcing us to think differently and take new approaches. Hackers can extort huge sums of money, but they can also cause untold damage to brands, equipment, and they can even lead to significant safety issues.



68% of executives believe that adding new IoT and OT devices to their environments is critical to innovation and growth.

In a world of IT/OT convergence, **CISO's security concerns multiply**

Traditionally, chief information security officers (CISOs) focused on data security, while industrial control systems were the province of chief operating officers (COOs). In the days when OT consisted of discrete, independent, non-networked components, this arraignment was fine. Today, however, OT devices are integral parts of many companies' overall networks, providing entry points and lateral pathways for attackers to infiltrate and sabotage networks.

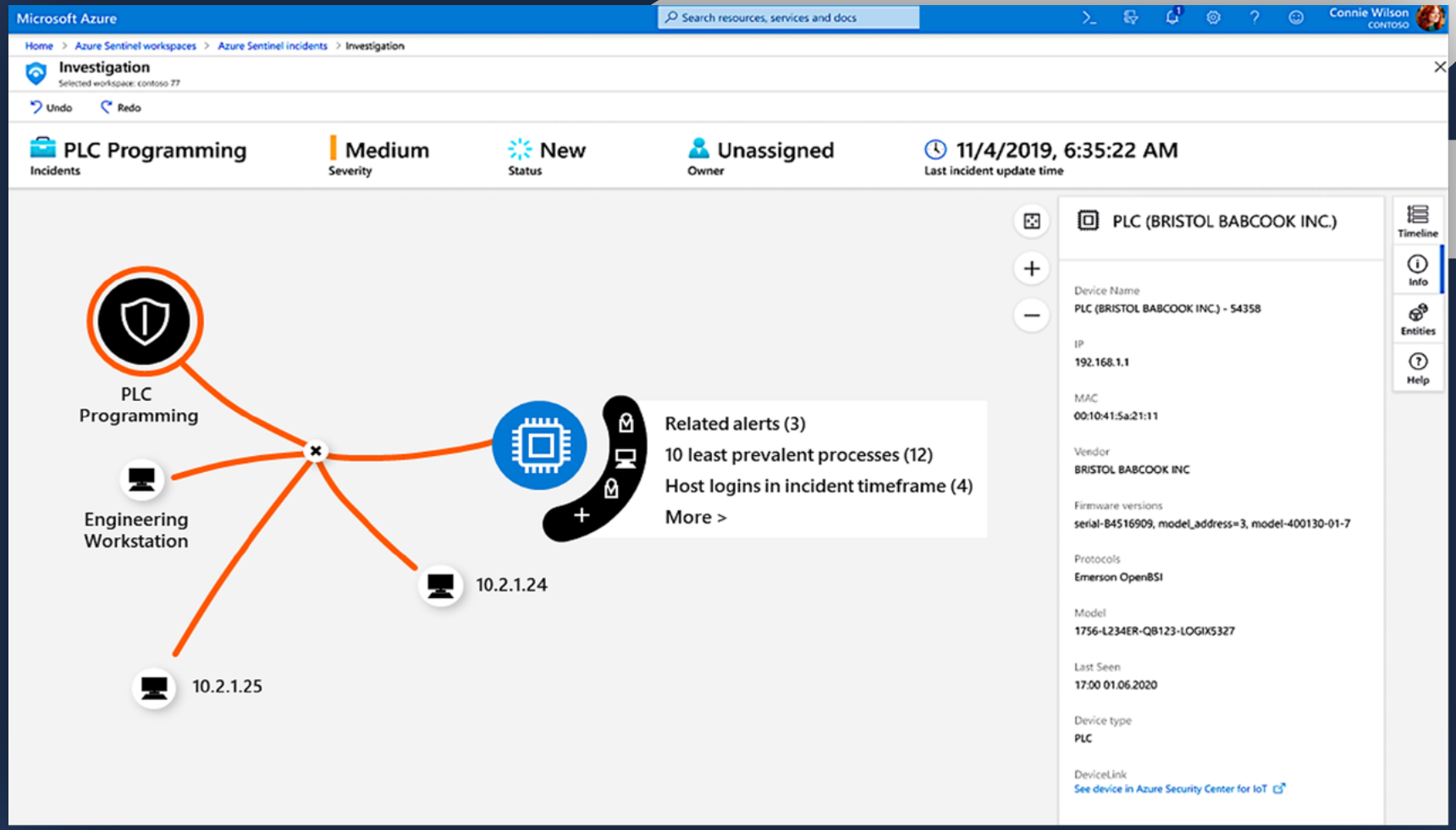
CISOs and other security leaders must now contend with an attack surface area that has more than tripled in size, in terms of devices, in just the past few years. For most enterprises, the security that has been deployed is not keeping pace with rapidly growing threats. For forward-thinking CISOs and other security professionals, there are five primary considerations when securing IT and OT networks including: visibility, protection, detection, response and recovery. And of course, a realistic plan to achieve these objectives must be created and that plan must be cognizant of IT/OT convergence happening within the organization.

You can’t defend what you don’t know exists

OT assets and industrial systems are all too frequently a security blind spot. Companies often don’t have a complete view, or even have no way of knowing, what OT and IoT devices they have currently in their networks. With the right solution all endpoints can be brought into a single, integrated view, and security professionals can gain visibility to all of their devices, they can learn to whom they are communicating with and from here they can identify where the security gaps are.

With a visual map in hand, companies can also trace an attack if one occurs. Having this level of visibility allows security teams to see where hackers entered, follow the attack vector through the network and understand how the attack ultimately took form.

With Microsoft Sentinel working in concert with Microsoft Defender for IoT, network defenders can see the kill chain of the entire attack even when the attack includes devices on both IT and OT networks.



Picking up the signal in the noise

The number of signals transmitted back and forth between devices in even a small network can be mind-boggling and far exceed the ability of teams to perform even a cursory manual review. Without continuous automated monitoring, companies are unable to clearly see, manage and defend their vulnerable industrial assets.

All too often, CISOs are not able to determine when a connection is safe, when it is suspicious, and when it is an attack, even if they have records of the signals themselves. Is this new connection authorized? Is it an outside vendor trying to gain access for legitimate business purposes? Or is this a hacker trying to gain access for nefarious purposes? Without continuous monitoring and an AI-backed platform to analyze the data collected, CISOs have no way of knowing.

The future is now: IT/OT convergence

The traditional air gap between IT and OT networks is increasingly a thing of the past and unless a specific regulation prohibits it, most industries have IT and OT networks that are connected. Unfortunately, security for OT devices has not kept pace with their IT counterparts. As a result, these hybrid networks have become a soft, and thus favorite, vector of attack for cybercriminals who know that devices on the OT network are frequently not as secure.

Just as these connected networks improve operational efficiency and assist executives in gaining a more complete view of each aspect of their operation, so too does comprehensive signal monitoring provide better, real-time data on security.

IT and OT convergence forces silos and cultural gaps to be addressed within organizations by facilitating working relationships between employees in different parts of the house. To ensure device security without causing unnecessary downtime, both SecOps staff and their colleagues on the operations side need to understand each other's roles and concerns, as well as insight into how each uses various tools and what metrics guide their performance.

For companies large and small, cyber attacks pose a very real and potentially devastating threat.

Microsoft Security

From here to there: protecting the organization at every step of the journey

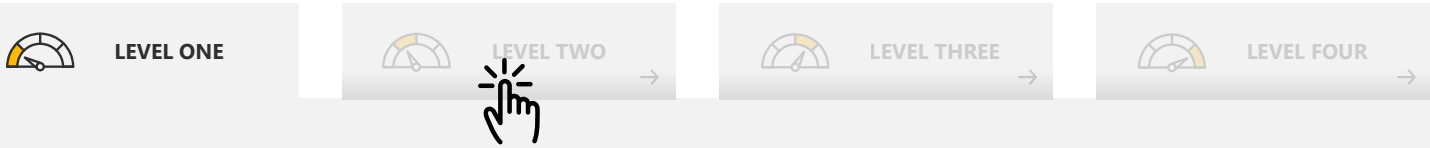
Just as companies vary in size and revenue, so too do they range in security maturity. For companies large and small, cyber attacks pose a very real and potentially devastating threat. Fortunately, there is also a solution for all, that can be used no matter what level of maturity an organization possesses.

Even companies with relatively mature security policies still need to remain vigilant against emerging threats. For those not as far along the journey, small investments can pay large dividends.

A company with a completely opaque view of their connected assets, for example, would benefit from a simple inventory. From there, having a dynamic list that automatically updated when devices were added or removed would be a next step. Proactively notifying SecOps teams of changes and then integrating it would complete the organization's journey towards more secure asset management. Similarly, small steps in threat detection and device integration can result in tremendous security benefits.

The four levels of IT/OT security maturity

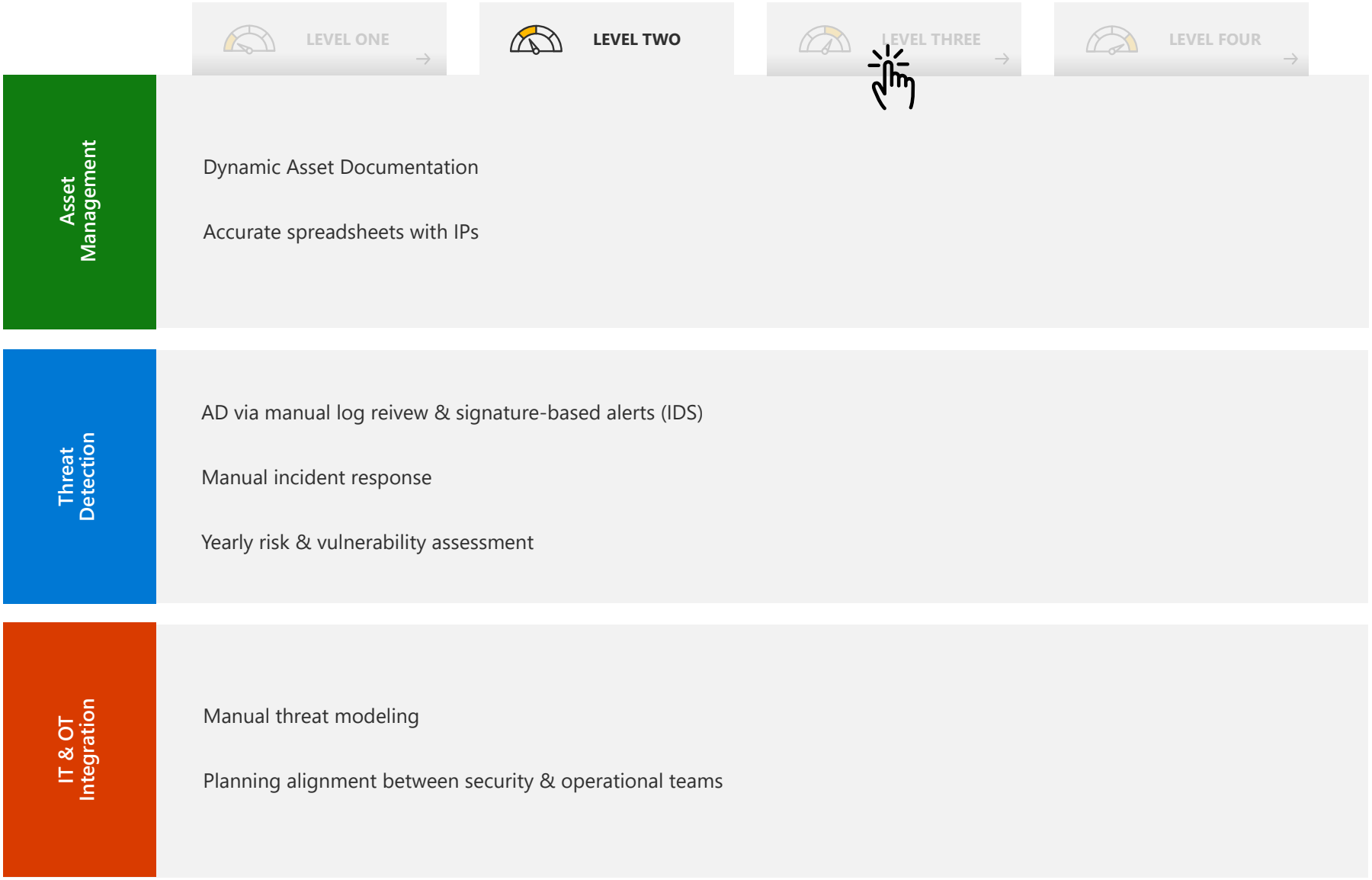
The four levels of IT/OT security maturity charts are a great way for you to identify your current level of maturity and define a plan to get to higher levels.



	LEVEL ONE
Asset Management	Asset documentation spreadsheet Static network map
Threat Detection	No Anomaly Detection (AD) No indicent response No risk & vulnerability assessment
IT & OT Integration	No threat modeling No alignment between security & operational teams

The four levels of IT/OT security maturity

The four levels of IT/OT security maturity charts are a great way for you to identify your current level of maturity and define a plan to get to higher levels.



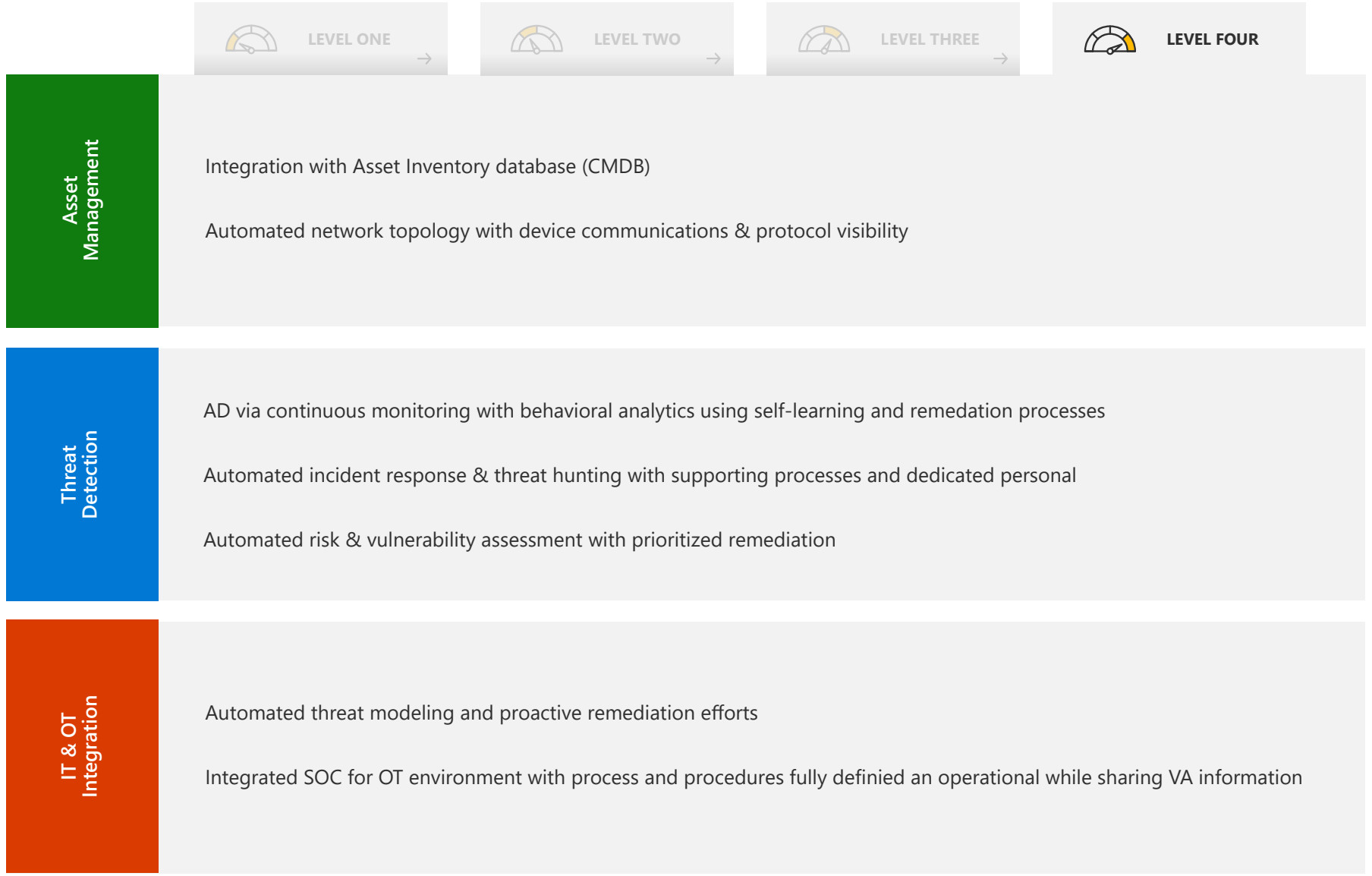
The four levels of IT/OT security maturity

The four levels of IT/OT security maturity charts are a great way for you to identify your current level of maturity and define a plan to get to higher levels.

	LEVEL ONE	LEVEL TWO	LEVEL THREE	LEVEL FOUR
Asset Management			Alerting when new assets appear and retire Accurate network map with all assets in network topology	
Threat Detection			AD via continuous monitoring with behaviorial analytics using self-learning Automatated incident response & threat hunting. Reviewed occasionally Automated risk & vulnerability assessment	
IT & OT Integration			Automated threat modeling Basic integration of SOC for OT environment	

The four levels of IT/OT security maturity

The four levels of IT/OT security maturity charts are a great way for you to identify your current level of maturity and define a plan to get to higher levels.



With Microsoft Defender for IoT, organizations with a low level of maturity for Asset Management can quickly get to the highest levels with an easy-to-use user experience that supports modern accessibility requirements.

What are CISOs to do? **Best practices to secure OT**

Microsoft periodically gathers CISOs to gain real-world insights and ensure that new initiatives meet the challenges they are facing. During the in-depth CISO roundtables held in Q4 of 2021, 34 security executives from 28 companies gathered to discuss best practices for removing silos between IT and OT professionals and to ensure the security of the entire enterprise. All generally agreed that a ransomware attack attempt was a matter of when, not if.

Strengthen security in alignment with NIST framework recommendations

Knowing how critical our national cyber security is, Microsoft supports the National Institute of Standards and Technology's (NIST) and its recommendations from the NIST Cyber Security Framework. Microsoft's Defender for IoT aligns with the five pillars they suggest to protect corporate networks.

Identify

Microsoft Defender for IoT automatically discovers and displays assets the moment they are connected. Security practitioners gain complete visibility and can validate whether or not a new device is authorized to connect to the network.

Protect

Once vulnerable assets are identified, security practitioners can take steps to secure them using attack vector analysis, vulnerability management, network segmentation and instituting Zero Trust security architectures. Networks segmentation is a powerful approach that makes lateral steps through the network more difficult, giving additional security to data and devices.

Detect

With continuous monitoring of all assets for unusual or suspicious activity, threats can be detected and neutralized before any material harm is done to the business.

Respond

If a cyber criminal does breach the network, Microsoft Defender for IoT's playbooks outline the steps that are taken to automatically shut them down before additional devices or data are compromised.

Recover

Gartner has given Microsoft the highest rank for execution among all competitors in their magic quadrant evaluations of endpoint protection platforms. In the unlikely event that an attack does occur, however, Microsoft Defender for IoT creates a detailed attack plan so that security practitioners can understand what took place and restore systems to their pre-attack state.

Defend complex networks with an easier, faster, less expensive solution

At the same time companies are providing more soft targets for cyber criminals to exploit, the tools they use are becoming cheaper and easier than ever. Phishing and related attacks are easy and on the rise, and distributed denial of service (DDoS) attacks can cost as little as $300 a month. Some hackers are even running affiliate programs where they provide kits to low-skill attackers in return for a share of the ransoms. With each passing day, the risk of an attack grows and the need for quick and easy-to-deploy solutions rises.

With over 24 trillion signals collected daily across the global Microsoft ecosystem (such as endpoints, apps, data cloud, etc), augmented by the threat intelligence produced by Microsoft's Section 52, an inhouse IoT and ICS/OT specialized security research team, Microsoft Defender for IoT can produce high impact insights and efficacy.

Microsoft Defender for IoT can also usually be deployed in less than a day, due in large part to its agentless nature. This allows for a passive system to monitor all network activity without impacting OT devices nor the need for local agents. No matter the topology or regulations governing an industry, Microsoft Defender for IoT can begin reducing complexity and providing value within minutes with less CPU usage and lower maintenance costs.

Success is achievable, **the impact considerable**

"One hour of downtime is more costly than the entire annual cost of Microsoft Defender for IoT. The solution pays for itself many times over."

Before hackers attack a network, they perform external reconnaissance to determine the potential value of the target. They'll first examine public financial documents, try and determine whether they have cyber-insurance policies, determine how large the company is and demand a ransom large enough to severely hurt but small enough to be paid. While the ransoms demanded thus vary in size, they averaged nearly $2 million in 2021.

The hard costs of downtime are often even more expensive. In a recent ESG report, *Analyzing the Economic Benefits of Microsoft Defender for IoT*, finds that the average downtime duration is 21 days per attack, resulting in downstream costs can dwarf the ransom paid. Reputations suffer as well with existing customers losing trust and new customers harder to come by. Even after eradicating attackers and remediating the environment, rarely will it be the same company when everything shakes out.

ESG estimates that avoiding a ransomware attack can save a company with 32,500 devices more than $35 million over three years. Or, as a CISO of a major manufacturing company put it, "One hour of downtime is more costly than the entire annual cost of Microsoft Defender for IoT. The solution pays for itself many times over."

Securing unmanaged industrial systems and **connected devices starts today**

For some threat actors, their intent is purely mercenary. They will shut down a manufacturing facility until a ransom is paid and then go on to the next victim. Some may cause catastrophic damage at a critical energy facility in order to further their political goals. These are just a few examples.

Whatever their reason, and no matter the target, it is now the responsibility of CISOs everywhere to secure not only their IT environments, but their vulnerable industrial OT assets as well. They must communicate to their boards they can no longer afford to wait to make the investments necessary to secure their OT environments and that there are solutions that can meet their needs no matter where they are currently at on the IT/OT security maturity model. With Microsoft Defender for IoT there is a viable path forward to gain complete visibility to all of your ISC/OT assets, to improve your security posture and to monitor and stop attacks by the most sophisticated attackers.

Success story no. 1

Lhoist stops attack during proof of concept demo

With more than 100 facilities in over 25 countries around the world, Lhoist is a global leader in the mineral industry. The company typically builds a processing plant on site at their quarries and produces materials that end up in a variety of everyday consumer and industrial goods.

Like many companies, their IT and operations professionals traditionally stayed in their own lanes. The lines began to blur, however, as more of their industrial automation equipment was connected to the local network, which in turn was connected to the larger corporate network.

When a related organization was brought to its knees by a ransomware attack, shutting down operations, causing missed deliveries and costing millions in damages, the Lhoist board took immediate notice. Clément Herssens, Lhoist's CISO, began testing solutions to protect the company's crown jewel assets. After Microsoft Defender for IoT detected a malware outbreak during the proof of concept stage and alerted the team before it caused any damage or stopped production, the choice was clear.

Beyond the benefits of the security detections Microsoft Defender for IoT provided, the team said turning it on was like bringing a blurry picture into focus. All the nodes and activity on their OT network—the devices, traffic, bandwidth usage, protocols and all the links between different zones—were shown together for the first time. The automation team even found major operational benefits from their enhanced ability to optimize device performance and identify malfunctioning devices before they failed.

Mining minerals from the earth is an industry that dates back to the stone age. With their adoption of a cutting-edge security package, Lhoist has firmly placed itself in the vanguard of modern industrial enterprises.

Success story no. 2

Interoperability and AI boost Rudin Management's ROI

Across three centuries, Rudin Management has amassed a portfolio of 10 million square feet of office space and 5 million square feet of residential space in New York City. Managing this much real estate is a challenge by itself, but trying to gain visibility into its IoT/OT networks, and then adequately securing them, added an entirely new level of complexity.

From steam pipes to elevator shafts, many of the OT devices on the Rudin network not only posed network security risks, but risks to the life and safety of their tenants as well if compromised. Further complicating matters was trying to find a solution that would meet all of the company's asset visibility and risk reduction needs across a wide range of equipment suppliers.

Soon after deploying Microsoft Defender for IoT, the platform flagged 60 new unauthorized IoT/OT devices that suddenly appeared on one of Rudin's many OT networks and were trying to connect to the internet. Microsoft Sentinel, which shares data with Defender out of the box, immediately isolated the devices by changing policies on the company's next-generation firewalls to make sure that the unauthorized devices didn't send or receive data from the internet.

Microsoft Defender for IoT later identified these new devices as legitimate, but unauthorized, components brought in by an outside contractor. The system's AI capabilities were also able to learn from the experience, making all Microsoft Defender for IoT customers more secure in the future. With their plans to adopt Azure Digital Twins, Rubin Management is building and securing an entire digital security ecosystem that will serve them well in the years, and centuries, to come.

Microsoft Defender for IoT helped Rubin Management monitor, defend and control essential systems:

- fire safety
- elevators
- building access controls
- CCTV cameras
- heating
- ventilation
- air conditioning
- lighting
- occupancy sensors and energy and water consumption

Microsoft Security

To learn more about Microsoft Defender for IoT and how you can be fearless with OT security, visit Defender for IoT landing page today.