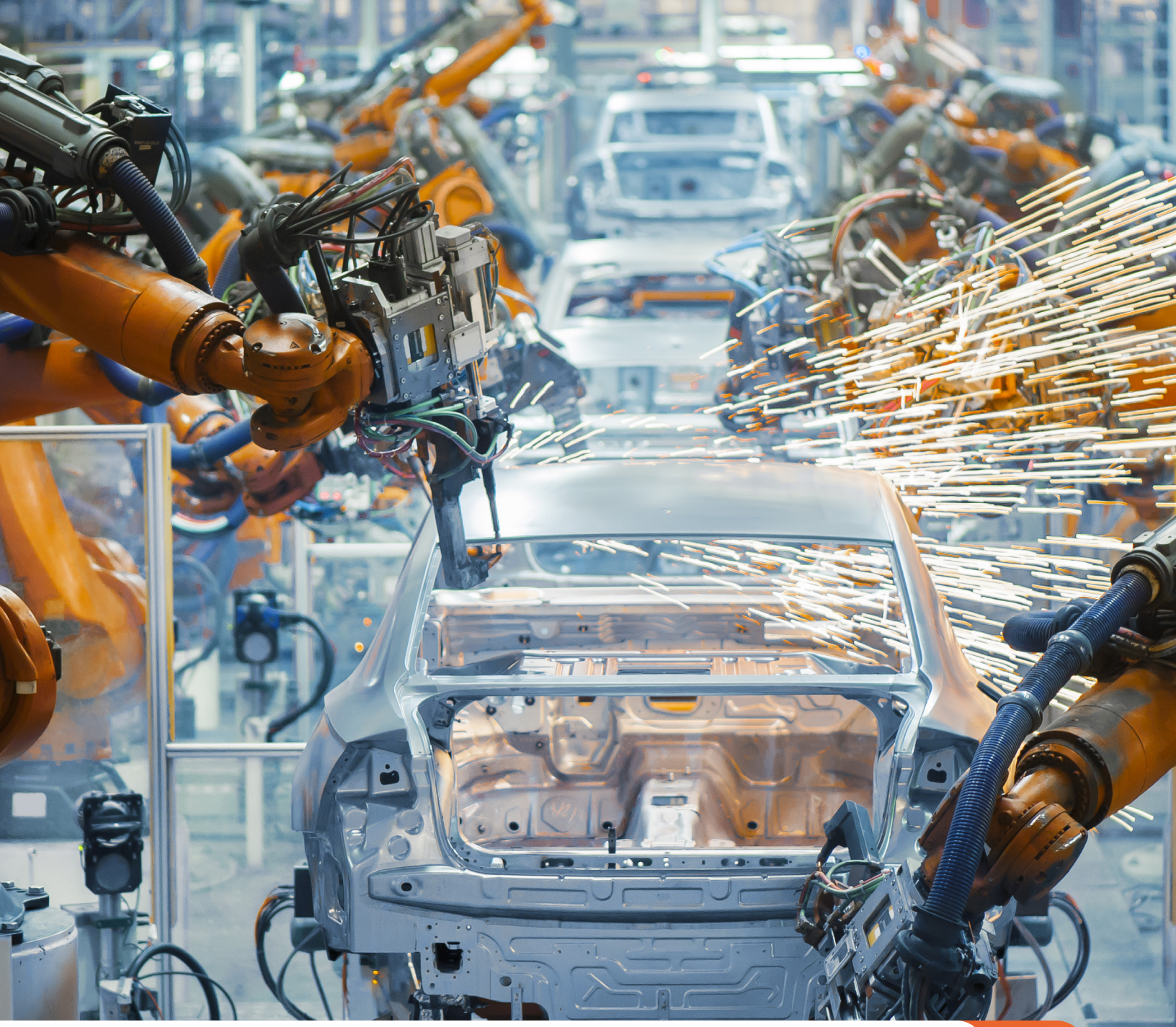

Rockwell Automation

The Next Generation of Smart Automobile Manufacturing Demands Proactive Cybersecurity

Table of Contents

Introduction 01

Why Auto Manufacturers are Susceptible to Cyberattack 02

Security During Rapid Digital Transformation 02

FUTURE FOCUS: Securing Connected Vehicles
is Essential for Winning the Trust of Today's Consumers 03

The Greatest Cyber Threats to the Automotive Industry Today 04

Common Cybersecurity Attacks on Automotive Manufacturers 04

The Changing Nature of What Must Be Protected 06

Cybercrime on the Rise: Major Attacks Targeting Auto Manufacturers 07

Building a Rock-Solid Approach to Automotive Cybersecurity 06

The NIST Cybersecurity Framework 08

Zero Trust for Automakers 10

How Rockwell Automation Can Help 11

Introduction

From the adoption of driverless cars to the push for battery-powered vehicles, the automotive industry is currently experiencing change that's faster-paced and more sweeping than at any previous time in its history. Industry leaders are innovating to make all-electric and hybrid cars more fun to drive, while internal combustion engine redesigns are decreasing emissions and boosting performance. At the same time, automakers have an unprecedented opportunity to introduce new efficiencies into their operations by increasing automation, digitization and connectivity on the plant floor.

This rapid pace of digital transformation — together with the auto industry's high profile — is making automotive manufacturing an increasingly attractive target for cybercrime. Malicious actors are well aware of the high cost of downtime in auto factories, and they know that these costs can tempt ransomware victims to consider making large payments in order to resume production quickly.

Cybercriminals also know that the installed base of automotive assembly equipment, including industrial control systems (ICS) and manufacturing execution systems (MES), tends to have a long lifecycle and that vulnerability management is a perpetual challenge in operational technology (OT).

In today's world, the cyber risks that automakers confront are major and significant. The threat landscape remains challenging, with damages from cybercrime forecast to cost the world more than $10.5 trillion annually by 2025, with costs growing 15% year-over-year.[1] Meanwhile, the most sophisticated and best-funded malicious actors, those sponsored by nation-states, are becoming more capable and more brazen. Researchers estimate that "significant" state-sponsored cyberattacks doubled in frequency between 2017 and 2021.[2] Among industrial manufacturers, at least 53% have experienced a cybersecurity breach in one of their facilities within the past two years.[3]

[1]*Cybersecurity Ventures*, [2]*States, Cyberconflict and the Web of Profit*, [3]*LNS Research*

Why Auto Manufacturers are Susceptible to Cyberattack

Automotive manufacturers are a top target for cybercriminals, in part because they share many traits with other manufacturers including legacy infrastructures that often remain unpatched, along with a lack of skilled resources for managing risks. Recent studies show that among the top 100 automakers, 49% are "highly susceptible" to ransomware attacks. Leaked passwords or stolen credentials from 91% of these companies were found to be readily available on the Dark Web, while 79% of the automakers and Tier-1 suppliers received poor ratings for patch management. 90% were rated "highly susceptible" to phishing attacks.[4]

Automakers are also a prime target because they face unique industry-specific risks. Automotive supply chains are inherently complex, with automotive OEMs relying upon globally-distributed networks of third-party manufacturers for a vast array of parts, including software and electronic hardware components. Because today's vehicles include growing numbers of software-controlled and internet-connected systems, ensuring the integrity of supply chains is critical for maintaining the functional safety of vehicles — and protecting the lives of their occupants.

Security During Rapid Digital Transformation

Digital transformation is taking place across the industrial landscape. The automotive sector is among the fastest moving. Digitization of auto manufacturing processes is driving greater productivity, improving product quality and consistency, and optimizing workflows that enhance plant safety and efficiency. The ability to share data between IT and OT systems is enabling analytics that are improving operations, creating better business outcomes for automakers.

These advances can also increase cyber risk, especially when automakers haven't developed a comprehensive enterprise industrial cybersecurity program. Taking a defense-in-depth approach that aligns with the NIST Cybersecurity Framework is essential for securing networks and individual devices to defend systems against external attacks.

Auto manufacturers must also develop continuous, rapid detection and response capabilities, identifying anomalous activities and blocking attacks before they cause serious downtime, or financial and equipment losses. And they must become capable of recovering from cyber incidents quickly. This demands a multi-layered approach with the right people, processes and technologies in place, including secure-by-design ICS products and robust security solutions that are purpose-built for industrial environments.

[4] Black Kite

FUTURE FOCUS:

Securing Connected Vehicles is Essential for Winning the Trust of Today's Consumers

Connected vehicles are those that share data with cloud-based systems, in-vehicle applications and other systems including road infrastructure, other vehicles, mobile devices or telematics services. Since GM introduced the first automatic in-car emergency call system in 1996, the connectivity of passenger vehicles has grown by leaps and bounds. **It's estimated that connected vehicles will make up more than 25% of the global automotive market by the end of 2023, and over 75% by 2025.**[5]

Today's most technologically-sophisticated vehicles incorporating advanced driver-assist systems (ADAS) contain more than 150 microprocessor-based electronic control units (ECUs) and over 150 million lines of code.[6] Deloitte estimates that as much as 40% of the cost of a new car can be attributed to semiconductor-based electronic systems,[7] and how well software works is often a key determinant of vehicle performance and efficiency – and thus, consumer preferences for a particular car model or automotive brand.

It's estimated that connected vehicles will make up more than 25% of the global automotive market by the end of 2023, and over 75% by 2025.

Autos are Now 'Born Listening'

Many drivers now expect their cars to run on software and behave like fast-moving mobile data centers. They're also paying more attention to in-vehicle cybersecurity. When security researchers demonstrated they could remotely take control of a Jeep going at highway speed, hijacking its onboard systems via the internet, the incident led Chrysler to recall 1.4 million vehicles. Mainstream media outlets also took notice.[8]

In another proof-of-concept demonstration, hackers were able to open a popular electric vehicle's doors using a drone carrying a WiFi dongle, and even break into the central Command-and-Control (C2) server used to communicate with the maker's entire customer fleet.[9]

More than ever before, rigorous connected vehicle cybersecurity is imperative for automotive brands wanting to win and retain consumer trust. According to one recent survey, 80% of car buyers would never purchase a vehicle from an automaker if that brand had experienced a vehicle hack.[10] And another survey found that 84% of consumers would not buy a car again from a dealership where they'd purchased a vehicle in the past if they discovered that their data had been compromised in a breach.[11]

[5] Capgemini , [6] IEEE Future Directions, [7] Deloitte, [8] Wired, [9] Electrek, [10] After Market News, [11] Total Dealer Compliance

The Automotive Industry's Biggest Cybersecurity Threats

Digital transformation is taking place across the industrial landscape. The automotive sector is among the fastest moving. Digitization of auto manufacturing processes is driving greater productivity, improving product quality and consistency, and optimizing workflows that enhance plant safety and efficiency. The ability to share data between IT and OT systems is enabling analytics that are improving operations, creating better business outcomes for automakers.

These advances can also increase cyber risk, especially when automakers haven't developed a comprehensive enterprise industrial cybersecurity program. Taking a defense-in-depth approach that aligns with the NIST Cybersecurity Framework is essential for securing networks and individual devices to defend systems against external attacks.

Auto manufacturers must also develop continuous, rapid detection and response capabilities, identifying anomalous activities and blocking attacks before they cause serious downtime, or financial and equipment losses. And they must become capable of recovering from cyber incidents quickly. This demands a multi-layered approach with the right people, processes and technologies in place, including secure-by-design ICS products and robust security solutions that are purpose-built for industrial environments.

Common Cybersecurity Attacks on Automotive Manufacturers

The three most prevalent attack scenarios today include ransomware attacks, phishing attacks (resulting in credential theft) and the exploitation of unpatched vulnerabilities in plant-floor devices.

THE RANSOMWARE THREAT

Ransomware attacks are the world's fastest-growing type of cybercrime, with global damages caused by ransomware currently forecast to exceed $20 billion. Researchers estimate that a business is now impacted by a ransomware attack every 11 seconds.[12]

Manufacturing is among the sectors most likely to be targeted by ransomware operators, with industrial organizations seeing almost twice as much ransomware-related network traffic as the next most-targeted industry.[13] And among manufacturers, automakers are an especially attractive target because the costs associated with stopped production are so high. In fact, the same phenomenon that makes automakers more likely to consider paying ransoms — intolerance of downtime — also makes many of them slow to remediate vulnerabilities.

Ransomware attacks often begin with successful phishing attempts. Ransomware operators also frequently exploit publicly-visible critical ports to upload malware into the environment, or leverage stolen credentials to gain remote access to systems. Properly **segmenting** industrial and enterprise networks is essential for preventing ransomware from spreading from the initial point of infection. Ensuring that industrial DMZs (Demilitarized Zones) and critical security zones are logically isolated from enterprise IT networks can block attempts to move laterally across OT environments, if access is gained in IT or OT.

[12] Cybersecurity Ventures, [13] Cisco

PHISHING ATTACKS TARGET AUTOMAKERS

Email-based attacks specifically targeting automakers are pervasive. Threat researchers evaluating the automotive industry's phishing risk exposure discovered more than 18,000 fake or phishing domains that were created explicitly to target the top 100 automakers and OEMs.[14] Phishing is a highly effective tactic for cybercriminals to employ because it can yield IT or ICS insider-level privileges, including administrative credentials.

Once a phishing attempt succeeds, it can be difficult for defenders to detect subsequent attack stages since threat actor activities will look like those of an insider. Their ability to do immediate harm will be limited only by their knowledge of how to operate plant systems and manipulate ICS components to achieve specific goals. Guarding against these types of threats requires network, application and device-level controls, as well as ongoing IT/OT security monitoring to quickly detect behavioral anomalies or unusual login attempts.

A comprehensive **security awareness training program** teaching employees to identify and avoid phishing attempts can mitigate these risks, as can implementing appropriate policies controlling administrative access to manufacturing and industrial operating systems. Investing in the education and training that will keep workers up-to-date on current security threats and best practices is also key.

UNPATCHED VULNERABILITIES IN THE INSTALLED BASE

Patch management of the installed base is very challenging for automotive companies, but those that remain unable to mitigate vulnerabilities in plant floor systems quickly will find themselves facing unacceptable risk.

In one recent research report, as many as 91% of auto manufacturers were found to have at least one high-severity vulnerability within their OT or ICS software.[15] Some were exposed on the open internet, and many could not be patched because updates to post end-of-life hardware were no longer being supplied by manufacturers.

Developing an effective and well-understood process for handling vulnerabilities in the installed base and meeting patching requirements is essential. **Identifying and inventorying all network assets** throughout the OT environment, including hardware, equipment, servers, sensors, and mobile devices and performing **continuous asset monitoring** to detect unauthorized assets or users on networks - is a vital step.

Regular **penetration testing** is also crucial. Experts attempt to breach systems and can provide a true assessment of weaknesses and vulnerabilities, enabling their remediation.

[14] *Intsights*, [15] *Black Kite*

The Changing Nature of What Must Be Protected

In the past, automakers' IT networks needed to be protected and defended, as did programmable logic controllers (PLCs) and ICSs on the plant floor.

Today, these systems must be secured, but so must increasingly complex and interconnected IT/IoT/IIoT ecosystems, along with connected vehicles that rely on software. This raises a whole new set of questions for carmakers:

- How can a manufacturer patch software in a vehicle that's already on the road?
- Do automakers need to build new security operations centers (SOCs) just to be able to monitor the fleet of vehicles they've already produced?
- What sorts of new regulatory oversight will the auto industry face in the coming years?
- How can automakers gain better visibility into the security practices of their third-party ECU suppliers?

Building a Rock-Solid Approach to Automotive Cybersecurity

As automakers increasingly embrace end-to-end connectivity across their production facilities and enterprise computing ecosystems, there's a growing need to adopt a comprehensive approach to cybersecurity in order to protect people, intellectual property, productivity and operational continuity.

OT networks are inherently complex; there's no silver bullet or simple, one-time fix that can guarantee a permanently secure environment.

Instead, it's essential to take an ongoing risk-based approach, identifying the unique people, process and technology risks faced by the enterprise. A clear assessment of vulnerabilities and associated risks can help the organization allocate the right resources, implement the right policies and procedures, and deploy the right technologies.

Automotive manufacturers should begin by understanding their installed base's security posture by conducting a thorough asset inventory and comprehensive risk assessment.

Timeline of Major Attacks Targeting Auto Manufacturers

March 2019

In a highly targeted attack likely conducted by an advanced persistent threat (APT) group, cybercriminals gained access to servers containing customer data in a breach that may have impacted as many as 3.1 million people.[16]

December 2019

An APT group suspected of having ties to the Vietnamese government, APT 32 (Ocean Lotus) is reported to have breached networks at two major car manufacturers.[17]

February 2020

Security researchers found 19 vulnerabilities in vehicles, enabling them to communicate with the manufacturer's backend servers to open car doors and start engines remotely.[18]

April 2020

By reverse-engineering the telematics control unit (TCU) of an individual vehicle, security researchers were able to utilize the telematics connection to infiltrate the OEM's corporate network and gain access with full administrative privileges.[19]

May 2020

Source code for connected components installed in an athis auto maker's vans was leaked after Git repositories containing images, code, detailed documentation and development environments for the vans' onboard logic units (OLUs) were made public.[20]

June 2020

A targeted ransomware attack on a the Japanese automaker infected internal servers and led the company to suspend production at plants around the globe.[21]

August 2020

A security researcher was able to gain control over an automotivethe company's entire connected vehicle fleet by exploiting a server-side vulnerability on the OEM's network.[22]

August 2020

A dealership fell victim to the group operating Ryuk ransomware. The attackers stole corporate data during the incident and published it to their dedicated leaks portal.[23]

February 2021

An automaker suffered an alleged DoppelPaymer ransomware attack that impacted internal and customer-facing systems and led to an extended outage.[24]

May 2021

A parts-manufacturing subsidiary of a large auto manufacturer suffered a targeted ransomware attack. Financial and customer data was exfiltrated and exposed while the organization's parent company struggled with production stoppages due to supply chain problems.[25]

[16] CPO Magazine, [17] ZD Net, [18] Upstream, [19] Pen Test Partners, [20] ZDNet,
[21] Dark Reading, [22] Electrek, [23] TechNadu, [24] CPO Magazine, [25] The Register

The NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a set of guidelines and best practices that have been adopted as a standard across a wide variety of sectors and industries. The NIST Cybersecurity Framework offers guidance on how organizations can manage and mitigate cybersecurity risk, and includes a set of recommendations on how to prevent, detect and respond to cybersecurity events to enable rapid recovery. It's broadly understood as the gold standard foundation upon which an organization can build a solid security program.

The Framework includes five key Functions: **Identify, Protect, Detect, Respond and Recover.** Together, they encompass the entire attack continuum and security management lifecycle. The five Functions organize key areas auto manufacturers can address to improve their overall security posture, reduce the number of exploitable attack vulnerabilities, and minimize the damage that an OT cybersecurity event could cause.

We'll explore each of these areas in greater depth below, providing a roadmap of the steps involved in building a defense-in-depth security strategy aligning with the NIST Cybersecurity Framework.

IDENTIFY

In the first of the NIST Framework's functions, organizations are advised to discover business-critical processes and assets, as well as to inventory the systems and software in their IT and OT environments. This makes it possible to better understand sources of cybersecurity risk by mapping it onto systems, assets, data and capabilities. With this understanding, an organization can focus and prioritize its efforts consistently with the business's objectives and risk management strategy.

As newly connected devices come online at rapid rates in today's manufacturing facilities, it can become more and more challenging for security teams to understand which OT hardware is networked. It's near-impossible to protect what you cannot see.

Maintaining a current and accurate asset inventory (including information about device specifics such as connectivity and risks or vulnerabilities that are present within assets) is essential. When security teams understand what's on the network, they can document system architectures and data flows using standard representations that will allow global teams to compare hardware topologies — and risks — across multiple sites.

A comprehensive asset inventory provides a baseline to identify deficiencies, and design and implement a security program to address them. After completing an initial asset inventory, automakers should plan for ongoing security assessments that can ensure that security objectives are continuing to be met, and that compliance with industry standards is being maintained. Asset inventories also help reveal unauthorized assets, or those being used in unauthorized ways.

Security assessments are also essential for identifying software vulnerabilities (CVEs). They provide a foundation for mitigating existing vulnerabilities now, while enabling organizations to build a proactive approach to discovering and patching future vulnerabilities.

PROTECT

The Protect function includes activities that improve cyber hygiene and enable defense-in-depth. This provides a set of safeguards that lessen cyber risk and protect the integrity and confidentiality of high-value data along with the availability of business-critical systems. Such safeguards include identity and access management controls, network segmentation, CIP Security, CPwE architecture, vulnerability management programs, backup solutions, security awareness training for employees and device-based configuration controls.

Network segmentation is a key consideration for automakers and other industrial manufacturers. Legacy OT network designs tended to be flat, but improperly segmented IT and OT networks makes it possible for attackers who gain access to IT systems to move laterally across plant environments quickly, potentially disseminating ransomware, gaining access to proprietary information, or compromising production.

Proper network design and effective segmentation of industrial DMZs and security zones enables security teams to rapidly isolate impacted systems in the event of an attack. This allows normal production to continue elsewhere in the facility.

Manufacturers deploying new automated or connected solutions can leverage a validated reference architecture to ensure that they're designing a future-ready network, appropriately segmented and tested for performance, availability and security. Using an architecture comprised of previously validated designs, with documentation on best practices and configuration settings, lets organizations implement a robust converged IT/OT network that meets all performance, scalability and security requirements.

DETECT

The activities within the Detect function allow cybersecurity teams to quickly identify the anomalous network behaviors or data flows that may signal that an attack has occurred. These activities include collecting and monitoring logs and continuously monitoring the logical and physical security of IT and OT environments. A 24x7 security operations center (SOC) will provide the requisite alerting and event investigation and response capabilities.

Third-party threat detection services can provide access to anomaly and breach detection technologies. Their use enables defenders to establish normal operational baselines and identify and investigate situations that do not conform to these expected patterns.

To determine the impact a security event might have on plant operations, it's vital to have consistent and thorough documentation for all plant systems, OT networks and IoT/IIoT devices, including those that are potentially insecure. In many manufacturing environments, an understanding of OT system architectures — and which systems are exposed to external networks — was maintained as "tribal knowledge" among plant personnel. Formal documentation enables stronger and more productive collaboration between plant engineers and security operations teams.

RESPOND

When a cybersecurity incident is detected, organizations that have performed the activities within the Respond function will be able to take action quickly to contain the incident and reduce its impact. The Respond function incorporates both technical capabilities and processes and communication flows. Organizations should proactively identify the roles and responsibilities of key stakeholders who would be called into action in the event of an OT cyber incident.

SOC teams and plant engineers will need to share responsibilities for event investigation. All on-site and offsite personnel will benefit from regular tabletop scenario exercises to review the procedures in place and ensure they're ready to make quick and accurate decisions should a crisis occur.

RECOVER

The Recover function goes beyond immediate, short-term response activities. Organizations should develop plans that will enable them to rapidly restore capabilities or services that are impacted by cybersecurity incidents. This enhances resilience and protects operational continuity.

All industrial manufacturers should not only maintain comprehensive backups, but also ensure that a full restore can be completed within a timeframe short enough that there won't be severe operational impacts. Testing backup capabilities is essential, as is performing regular tabletop exercises to identify and remediate gaps in business process resilience.

ICS recovery requires specialized skills and capabilities. Not only do security teams need to complete forensics and damage assessment and ensure that all malicious software has been removed, but they also need to re-commission drives and re-establish PLC processes so that they're fully operational. Teams should have experience in getting processes back up and running quickly.

The core concept of Zero Trust is "never trust, always verify."

Zero Trust for Automakers

Zero Trust is an approach to network security that was first outlined by John Kindervag at Forrester Research more than a decade ago. Since then, it's gained traction among IT security professionals, in large part because it's ideally suited for securing modern cloud-first and remote-enabled IT environments. Today, it's beginning to see wider adoption among OT security professionals as well.

The core concept of Zero Trust is "never trust, always verify." The underlying assumption is that no user, machine identity, traffic flow or application should be inherently trusted. Instead, identities and risk levels should be verified on an ongoing basis, with continuous policy enforcement for every connection.

In today's world, where attacks are incessant, adopting a Zero Trust approach will mitigate risks and lower the chances that any attack might be successful. Zero Trust can benefit automotive manufacturers by:

- Reducing the size of the attack surface through the establishment of granular access controls for critical assets.
- Greatly reducing the number of malicious intrusions into the network by making authentication and identity validation requirements more stringent
- Removing excessive trust from network architecture designs to make attackers' jobs far more difficult

Today's Zero Trust strategies are best designed through another methodology provided by Kindervag, focusing on identifying the organization's Protect Surfaces – the Data, Assets, Applications and Services (DAAS) elements most critical to operations, and protecting them with Zero Trust controls in priority order.

How Rockwell Automation Can Help

Rockwell Automation is the world leader in industrial automation, with over a hundred years of experience designing and building OT systems.

The company leverages this deep expertise to secure the world's critical plants, assets, networks. Having served thousands of ICS and automation clients around the world, Rockwell Automation knows what it takes to protect infrastructures, prevent downtime and mitigate damage from cyberattacks. Rockwell Automation provides industrial-strength cybersecurity services that protect the production operations you and your customers rely on daily – from plant floor to cloud.

Rockwell Automation provides managed services that encompass the activities within all five Functions within the NIST Cybersecurity Framework, including asset identification, penetration testing and assessment, vulnerability monitoring and patching, security program design and implementation, threat detection and backup, and incident response and recovery services.

In addition, Rockwell Automation offers a full complement of project-based services to enable clients to accelerate their OT security maturity. Rockwell Automation also maintains close partnerships with industry leaders in IT and security such as Cisco, Claroty, Microsoft, Dragos and Crowdstrike. They co-developed the Converged Plantwide Ethernet (CPwE) architecture with Cisco to offer clients a set of pre-validated and documented architectural plans alongside practical guidance for implementing and configuring them.

The Rockwell Automation product portfolio includes secure-by-design industrial control solutions as well as security technologies that were created especially to add additional layers of protection to Rockwell's products. These purpose-built security solutions provide perimeter protection, network segmentation, secure communications between control elements, and data protection for users of their devices.

To learn more about how automotive manufacturers can take the next step toward building cyber resilient production facilities, contact an expert at Rockwell Automation today.

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-BR004A-EN-P-May 2022