THE EVOLUTION OF "NEXT-GENERATION" MANUFACTURING AND THE NEED FOR NETWORK SECURITY

By MixMode & RAVENii

Contents

Key Takeaways

1. Implementing a security platform that supports an evolving (as opposed to static) network baseline using unsupervised AI is critical to catching anomalous behavior and avoiding attacks.
2. Ongoing need for maintenance, configuration and training of the security tooling decreases security efficacy.
3. Anomaly detection across SCADA and automated manufacturing network devices, and correlation with alerts on the corporate network, mitigates risk of an impactful breach.

The Evolution of "Next-Generation" Manufacturing and the Need for Network Security

Industry 4.0 is changing the way products are being manufactured around the world. This new manufacturing era is increasing automation and enhancing smart technology. Because Industry 4.0 is built on connected devices and machines, it is inherently vulnerable to network security threats.

Historical Background

Manufacturing has evolved significantly since the first industrial revolution, which was marked by advances in mechanization driven by water and steam power.

Assembly lines and mass production were emblematic of the second industrial revolution, while computers and early automation marked the third.

The fourth industrial revolution, or Industry 4.0, builds on the third, featuring increasingly digitized, autonomous processes that are rapidly changing the manufacturing industry and the way products are being produced all over the world.

Benefits of Industry 4.0

Industry 4.0 is ushering in a new era of manufacturing, one centered on connected machines that communicate with one another. These networked components make up what is called the Internet of Things (IoT).

Essentially, Industry 4.0 describes an environment where IoT smart machines work together to optimize manufacturing procedures. The result is a potential improvement to various key manufacturing processes:

- Logistics and supply chains can self-adjust to changing conditions like weather delays.
- Equipment and vehicles are being automated to accept shipping containers from ships and road-based cargo trailers.
- Robotics are benefitting from autonomous tech - factory robots can complete more tasks that reduce costs and optimize warehouse floor space.

Industry 4.0 Risks

IoT and cloud technology significantly impact Industry 4.0 manufacturing. Increasing use of these technologies has led to cybersecurity risks that didn't exist just a few years ago.

Industry 4.0 era manufacturing tech is just as vulnerable to security breaches as a corporate network. Employees can inadvertently expose the network to exploitation by skilled hackers, leaving manufacturing data insecure.

Because supply chains are increasingly integrated, third-party vendors, contractors and vendors need access to client data. This has increased the attack surface of the manufacturing network as suppliers and service providers need access to sensitive data.

Disruption to the manufacturing process is another risk unique to Industry 4.0 environments. Data loss can be damaging in the long run, but hackers who gain control over these environments can slow down or even stop active production.

The potential costs of a cyberattack, including damage to company finances and reputations, can be very high.

NIST Recommendations for Mitigating malware attacks

According to the National Institute of Standards and Technology (NIST), the vulnerability of industrial control systems (ICS) to cybersecurity threats is increasing because of the adoption of commercially available information technology to promote business systems' connectivity and remote access.

To address these threats, NIST has demonstrated a set of capabilities that mitigate malware attacks and other threats by detecting anomalous behaviors in operating environments.[1]

NIST has mapped these demonstrated capabilities to the Cybersecurity Framework and documented how this set of standards-based controls can address the anomaly scenarios that manufacturers face:

[1] *"Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection," NIST, Accessed November 2019, https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf*

***"Zero-Day exploits, and their underlying vulnerabilities, have a 6.9 year life expectancy, on average"* - Rand Corporation**

A typical threat doesn't show up on an intel feed until 3 years after it's created. MixMode can detect and surface zero day attacks or threats not listed on intel feeds by monitoring network behavior and using our Context-Aware Third-Wave AI to perform advanced anomaly detection.

1. Unauthorized Device is Connected to the Network

It is important to identify all devices on the ICS network for a complete risk analysis and to minimize potential attack vectors. The presence of unauthorized devices may indicate anomalous activity.

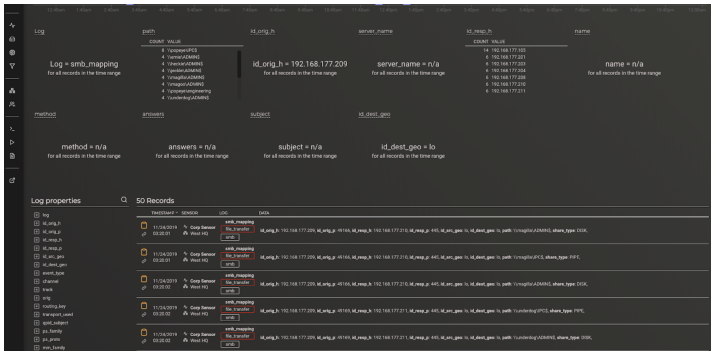
2. Unencrypted HTTP Credentials are Detected on the Network

Unencrypted or plaintext credentials transmitted over a network are a vulnerability for ICS networks. If packets containing these credentials are intercepted, then the credentials can be used to access to the devices or services.

3. Unauthorized Ethernet/IP Scan of the Network

During the reconnaissance phase, an attacker may attempt to locate vulnerable services in an ICS network and will likely probe for ICS-specific services (e.g., Ethernet/IP). Once a vulnerable service, host, or device is discovered, an attacker may attempt to exploit that entity. (See Figure 1)

Figure 1



4. Unauthorized SSH Session Is Enabled with Internet-based Server

A Secure Shell (SSH) session is an encrypted and secure connection for remotely sending commands over a network. However, unauthorized SSH sessions with internet-based servers could indicate malicious activity. Attackers can use an SSH session to gain access to the ICS device and network. (See Figure 2)

Figure 2

5. Data Exfiltration to the Internet via DNS Tunneling

Attacks against ICS with the goal of information gathering must attempt to exfiltrate sensitive or proprietary data from the ICS network, potentially utilizing the Internet as a transport mechanism. Monitoring for ICS devices communicating to other devices over the Internet can help detect data exfiltration events, especially if the affected device does not normally communicate over the Internet.

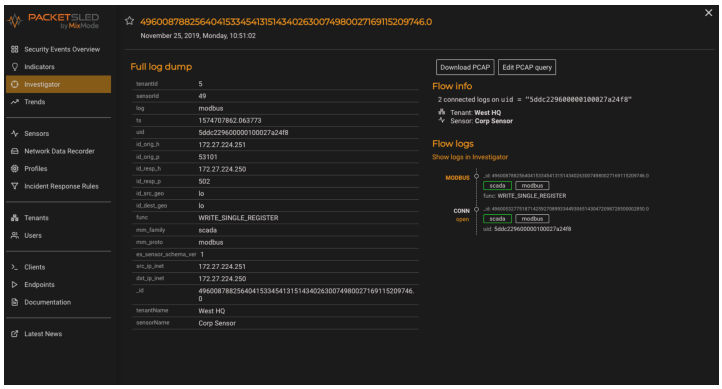
6. Unauthorized ICS Logic Download

Many ICS devices provide services to remotely update control logic over the network. These network services can also provide a mechanism for attackers to replace valid control logic with malicious logic if the device is unprotected.

7. Undefined Modbus TCP Function Codes Transmitted to PLC

Communications that do not conform to the defined specifications of the industrial protocol may cause an ICS device to act in an undefined or unsafe manner. Depending on the manufacturing process and the ICS device, the nonconforming communications may or may not be impactful, but investigation into the cause is warranted. (See Figure 3)

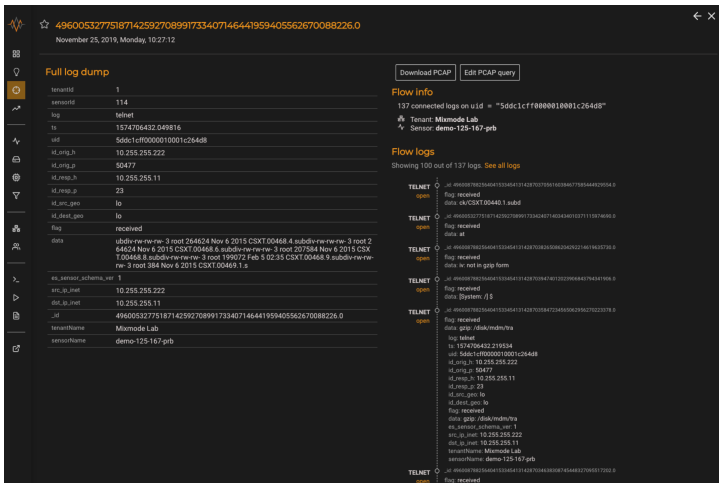
Figure 3



8. Brute-Force Password Attack Against a Networking Device

Authentication systems that are not rate-restricted may be vulnerable to password-guessing attacks, especially if the default credentials of the device have not been changed. Given enough time, an attacker may be able to access vulnerable systems by using a brute-force password attack. (See Figure 4)

Figure 4



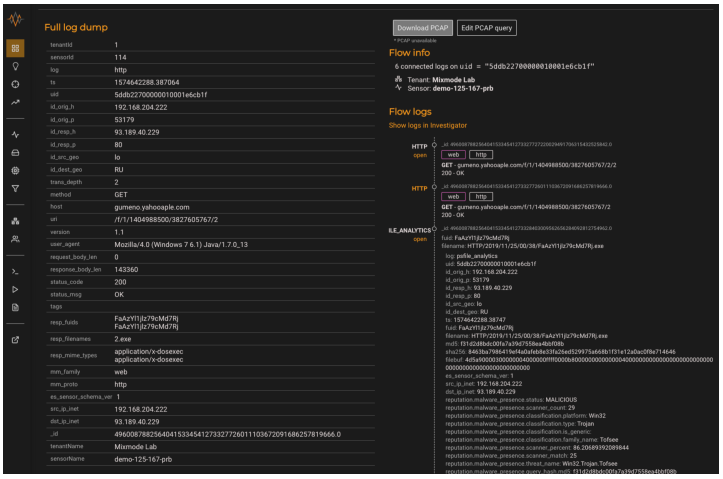
9. Data Exfiltration to the Internet via Secure Copy Protocol

As previously mentioned, attacks against ICS, with the goal of information gathering, must (at some point) attempt to exfiltrate the data from the ICS network, potentially utilizing the internet as a transport mechanism. Monitoring for ICS devices communicating to other devices over the internet can help detect data exfiltration events, especially if the affected device does not normally communicate over the internet. Depending on the protocol used for exfiltration, the file contents and/or data being exfiltrated may be ascertainable (e.g., specific file types transferred using the File Transfer Protocol [FTP] protocol), providing insight into the impact of the event.

10. Virus Test File Is Detected on the Network

Malware and computer viruses can undermine ICS security, confidentiality, and stability, with the potential to sabotage the ICS. The ability to detect viruses and malware in the ICS network is important for minimizing risk to the manufacturing system. (See Figure 10)

Figure 5



Addressing Industry 4.0 vulnerabilities with MixMode

Smart networks require smart security measures. Comprehensive security for an Industry 4.0 manufacturing environment must include technology that can protect against a wide range of potential vulnerabilities in a constantly-evolving network.
To address the scenarios above, manufacturers need a set of common and critical capabilities that protect SCADA and automated manufacturing networks, including the ability to:

1. **Baseline normal network activity**
2. **Inventory assets and devices**
3. **Validate common alert and controls**

MixMode is a network data detection and response platform that provides context-based security founded on an evolving baseline of network behavior. Using this baseline, the platform mitigates risk by monitoring endpoint devices and identifying anomalies in network traffic.

Using MixMode, manufacturers can uncover typical vulnerabilities in an Industry 4.0 operation, including:

- **Open ports**
- **Unencrypted traffic**
- **Passwords in clear text**
- **Unexpected communications between IPs or departments**
- **Rogue machines on network**

By drastically reducing false-positive alerts, MixMode also enhances the performance of cybersecurity teams.

Unlike other security platforms, MixMode leverages a form of AI called unsupervised learning, which uses the context of network-specific inputs to develop a generative model. The AI uses this model to decide whether a threat or anomaly is valid or a false positive.

Because MixMode uses an AI built on unsupervised learning, the platform is more effective at detecting zero-day attacks than other cybersecurity platforms.

MixMode Capabilities Include:

- **Easy integrations** - API allows for simple integration with SIEM, orchestration
- **Reduction in false positive alerts by 90%** so you can focus on actual threats
- **Full visibility** - See all the traffic on your network and on the factory floor
- **Multi-tenancy** - Manage all facilities from a single pane of glass

NISTIR 8219 Behavioral Anomaly Detection Capabilities

MixMode provides capabilities that detect the following anomalies:

Plaintext passwords
User authentication failures
New network devices
Abnormal network traffic between devices Internet connectivity
Data exfiltration
File transfers between devices
Abnormal ICS protocol communications malware
Denial of service (DoS)
Abnormal manufacturing system operations port scans/probes
Environmental changes

MixMode network analytics go far beyond basic threat detection. The platform's AI dives deep to quickly establish a baseline snapshot of the network and then uses that baseline to predict threats before they happen.

Case Study: Improving security by increasing OT network traffic visibility

MixMode is currently helping manufacturers protect their Industry 4.0 operations against a wide range of cyberthreats. As part of its digital transformation, a leading manufacturer of electrical metering equipment and enclosures sought to proactively improve cybersecurity by gaining visibility into its OT network traffic.

Working with RAVENii, a cybersecurity service provider, the company developed a tactical security plan built around the MixMode vCISO program. During a review of the company's security gap analysis, the CIO confided that she was losing sleep because of her lack of visibility into what was happening across the company's network, especially in the OT environment.

Within 7 days, RAVENii was able to provide network visibility by deploying MixMode sensors, including a vulnerability scanner, at all of the firm's manufacturing sites. Because it monitors traffic with passive sensors, MixMode doesn't impact the function of the client network. As part of its ongoing service agreement, RAVENii works closely with the company to investigate MixMode alarms, remediate vulnerabilities, and perform periodic threat-hunting activities.

- **Established baseline of the customer network within 7 days.**
- **No configuration or training for AI needed.**
- **Visibility into factory level data through SCADA/Modbus protocols.**
- **Anomaly detection, including surfacing threats not seen in intel feeds, misconfigured SIEM or firewall, rogue machines on-network, clear text passwords.**
- **Correlation of alerts across on-premise and cloud environments.**
- **Reduction of alerts for on-premise traffic by 95% versus previous open source network traffic analytics.**
- **Delivered ROI within 7 days.**

About MixMode

MixMode is a revolutionary AI focused Cybersecurity Company using patented third-wave AI originally developed for projects at DARPA and the DoD. MixMode's AI-Powered Network Traffic Analytics Platform provides deep network visibility and predictive threat detection capabilities, enabling your security team to efficiently perform real-time and retrospective threat detection and visualization. Used by breach response teams worldwide, security analysts and SOC teams can integrate MixMode into their playbooks, SIEMs, or utilize MixMode on a standalone basis to dramatically reduce investigation time, cost and expertise required to respond to persistent threats, malware, insider attacks and nation state espionage efforts. Based in Santa Barbara with an additional office in San Diego, the company is backed by investors including Keshif Ventures and Blu Venture Investors.

About RAVENii

RAVENii is transforming cybersecurity by "Humanizing the Hunt". We apply experienced human intuition to existing security solutions because we believe "Gray Matter" matters. Most organizations have made significant investments in security tools; however, have lacked the time, resources or expertise to implement and realize the full value of these investments. RAVENii is tool agnostic which allows us to utilize and optimize our client's previous technology investments to achieve their cybersecurity requirements. RAVENii was launched in 2014 bringing decades of front-line experience across many domains of cybersecurity; while harnessing the power of its global network of seasoned security experts to keep abreast of the ever-changing threat landscape. Today, RAVENii supports data centers, school districts, public municipalities, non-profit organizations, transportation, utilities, manufacturing, financial, and healthcare organizations with its "Gray Matter" approach to cybersecurity in an unceasing effort to improve our customer's security posture.