Modernize Manufacturing Security Operations

Insights from Splunk and Adarma

Over the last few years, manufacturers have faced an onslaught of supply chain challenges, labor constraints, inflation pressures, and shifting regulatory requirements. Those that embraced new technologies — like AI, automation, and digital-to-physical conversion — weathered it better by driving digitization forward and opening new doors to operational excellence and production efficiency.

They're propelling improvements in critical key performance indicators (KPIs), like overall equipment effectiveness (OEE) and uptime.

But, advancing digitization is dissolving the protective "air gap" between IT and operational technology (OT), creating new entry points for cybersecurity threats.

Building digital resilience from carpet to concrete

Previously, manufacturers believed they could secure both the carpeted (IT) and concrete (OT) environments by keeping OT and industry control systems (ICS) autonomous, offline, and outside the purview of IT. That approach — with minimal connection between enterprise IT systems and OT on the factory floor — worked until digital transformation on the production line changed everything.

Today's cyber criminals see IT/OT convergence as an opportunity and view manufacturers as lucrative attack targets. Attacks can bring down production lines, and manufacturers will pay (often significantly) to get operations back online. The rise of AI brings additional promise and problems, with security teams recognizing that it can expand the attack surface to a concerning degree and be a potent tool for adversaries.

Manufacturing security leaders are extending visibility across their entire technology landscape to detect, investigate, and respond to threats — faster.

Detect threats at scale

Unify security operations

Empower security innovation

> Manufacturers are resilience experts. I'm confident in this industry's ability to not just navigate an evolving cyber threat landscape, but to harness it to fuel a smarter, more efficient manufacturing future.
>
> **Ewald Munz,**
> Head of Manufacturing Automotive and Sustainability, EMEA, Splunk

1

Detect threats at scale

Keeping up with security requirements is daunting. Half (51%) of manufacturing security professionals report that security requirements have become harder over the last 12 months.*

In manufacturing, the attack surface is wide: it includes all the enterprise IT of a modern business and an entire universe of business-critical OT. To stay one step ahead of bad actors, manufacturers are prioritizing efforts to gain improved visibility into the hard-to-see corners of their networks.

Manufacturers want to be able to see IT and OT risks (and connection points) in one place, so they can:

Secure an expanded attack surface
Proactively monitor for threats and anomalous activity — from signs of new cybersecurity threats to any new risks introduced by ongoing IT/OT integration.

Prioritize incidents and standardize workflows
Coordinate response and mitigation plans to reduce the time it takes to detect and repair and keep systems and equipment up and running.

Minimize security breaches
Gain a comprehensive view of digital systems.

> Manufacturers who have long relied on obscurity, siloed segmentations, and air-gapped methodologies are racing to build real, resilient defenses in a transformed environment.
>
> **Tom Harrop,**
> Director of Manufacturing & IoT Specialization, Splunk

* Splunk, *The State of Security 2024*.

2

Power a unified IT/OT SOC

Silos between IT and OT obscure sightlines and limit the reach of enterprise security into a growing catalog of point solutions on the factory floor. The evolution to hybrid, multi-cloud infrastructure further compounds complexity and reduces visibility, at the same time as interconnected supply chain networks and direct-to-consumer sales increase the industry's threat vortices.

Manufacturers are extending unified visibility — the kind previously reserved for corporate IT — onto the factory floor. New tools and processes better identify risks, deploy critical resources, and gain the insights needed to launch defensive pivots and flexible recoveries that boost uptime.

While OT visibility is a major achievement, some manufacturers are taking futureproofing to the next level with centralized IT/OT security operation centers (SOCs). Rather than grapple with underused, poorly connected data, SOC teams can more efficiently remediate threats with features like automated investigations and risk-based alerting at their disposal.

Security leaders are bridging traditional silos so SOC teams can pursue threat detection, investigation, and response (TDIR) faster to counter cybersecurity threats across IT and OT.

> While most attacks originate in IT, they don't stay there. It's time for all manufacturing leaders to connect and leverage IT and OT in a unified fight for more secure, efficient operations, from the boardroom to the production line, and everywhere in between.
>
> **Tom Harrop,**
> Director of Manufacturing & IoT Specialization, Splunk

3

Empower security innovation

The manufacturing industry is under pressure to transform at rapid speeds to create smart factories and power digital transformation. But that need to innovate isn't limited to the factory floor. Cybersecurity teams are looking to extend their limited bandwidth to help modernize the SOC and build custom capabilities to tackle the latest threats.

Digital resilience is a catalyst to driving SOC enhancements that address today's challenges head on. Manufacturers are building toward the SOC of the future, where unified TDIR drives critical outcomes: mitigating the impact of security incidents, shifting to more proactive security, driving higher uptime, and unleashing the full potential of digitized operations.

With the Splunk platform, manufacturers can experience:*

90%

faster identification of root cause and remediation

50%

increase in alert fidelity

30%

increase in operational efficiency

> Unifying data from IT and OT networks in a single platform allows traditionally siloed teams to collaborate in new ways. The result is proactive security, faster innovation, and a more resourceful manufacturing business.

* ESG Economic Summary, *Analyzing the Economic Benefits of Splunk Security.*

Adarma and Splunk can guide manufacturers on a journey to improved digital resilience. With our security solutions, organizations gain an unmatched breadth of technology, expertise, and community to reduce risks, modernize the SOCs, and propel ongoing innovation.

By unifying data across systems to drive faster detection, investigation, and response, manufacturers can rise above today's pressures and lead the digitization charge.

splunk> a CISCO company

Learn more: www.splunk.com/manufacturing

www.splunk.com

ADARMA
TOGETHER WE'VE GOT THIS

Learn more:
Adarma.com