Protecting Industrial Assets with Cybersecurity Solutions in Converging OT/IT/IIoT Environments

Voith Group and Kudelski Security

Rene St-Pierre – Voith – Director of Cyber Security, North America
Eric Johansen, CISSP – Kudelski Security – Director, US Business Development
John Hellickson – Kudelski Security – VP CISO Advisory, US Advisory Services

Table of Contents

1: Introduction

Security has always been an important topic for companies protecting their physical, financial and information assets. Internal and external threats to the security of the business have been important considerations when assembling and implementing security plans. Before computers, security plans were more straightforward given that the majority of threats were visible and had to present themselves physically at a geographical location to accomplish their intended purpose. The nature of these threats led to a more physical approach to security and served vigilant companies well – but even the most vigilant were sometimes compromised by both subtle and not so subtle attacks. In these cases, catching the bad guys before they could get away or before they could do any damage became priority number one. And those prepared to respond quickly were usually rewarded with containing the threat and minimizing losses while continuing operations.

The introduction of computers to the back office, to the operations, and to the daily lives of all employees and suppliers added a digital (or “cyber”) dimension to the physical challenges of security. No longer did threats have to show up in person to impact the business or operations, bad actors could formulate and execute their attacks from remote locations anywhere in the world through any number of communications channels that existed anywhere in the organization. Some of the most clever attackers could exploit the least obvious paths to get connected to the assets they were interested in compromising. In the cyber world, the rate of innovation via networks of information

sharing has provided the bad actors a huge advantage over companies trying to implement, sustain, and evolve their cyber/physical security infrastructure on their own.

Adding to the challenge of cyber/physical security is the growing trend towards massive integration of data across systems, facilities, and supply chains. In this new "cloud" environment, security isn't limited to just the company's assets but also the assets stored and managed by third party providers. These providers who provide significant value through connectivity (Industrial Internet of Things) also bring a need for increased vigilance, planning, and monitoring.

As every company has unique sets of resources, unique constraints, and unique objectives, so too are the security planning, prioritizing and deployment needed to face the challenge. Furthermore, a holistic approach should be aligned with the business goals today and into the future.

Some recent examples and data highlight the vulnerabilities:

July 24, 2018

Russian Hackers Breach US Utility Networks via Trusted Vendors

Hackers were able to access confidential information, such as the equipment being used and how utility networks are configured.

From <https://www.greentechmedia.com/articles/read/russian-hackers-us-utility-power-grid-trusted-vendors

August 7, 2018

Utilities Prepare for Increased Cyber attacks on the Electric Grid

More electric utilities and energy companies are turning to cybersecurity vendors for protection against attempted attacks, a growing threat highlighted by the recent disclosure of Russian hacking into their communications networks last year. Duke Energy, reported more than 650 million attempted cyber attacks in 2017 alone.

From <https://www.bna.com/utilities-prepare-increased-n73014481471/>

Critical Infrastructure Cyber Incidents Reported to DHS ICS-CERT (2013-2015)

Energy	**35%**
Critical Manufacturing	26%
Water	6%
Transportation	6%
Communications	4%
Healthcare	4%
Government Facilities	5%
All Others	14 %

Source: DOE Multi-Year Plan for Energy Sector Cybersecurity

Average Annualized Cost of Cyber Crime by Industry Sector in 2015 ($ millions)

Financial Services	$28.33
Energy & Utilities	**$27.62**
Defense	$23.18
Technology	$16.45
Communications	$14.90
Services	$12.93
Transportation	$12.08
Retail	$11.96

Source: DOE Multi-Year Plan for Energy Sector Cybersecurity

2: Real World Cyber Security Solutions

Practical security plans that work in the real world have to consider real world global realities. These realities include, but are not limited to many of the following:

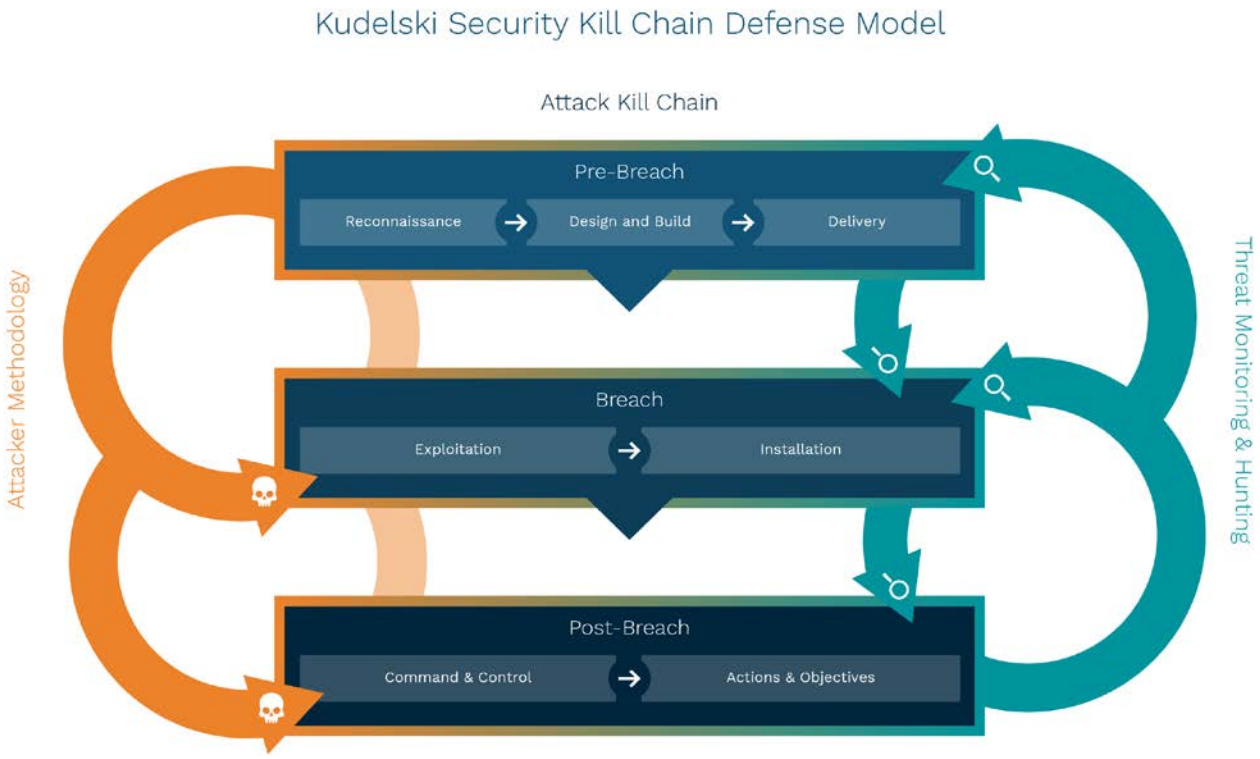
- A wide variety of vendor products operate in most facilities
- A wide range of ages of equipment and controls exist in many facilities
- Many different software systems have accumulated through acquisitions
- Limited budgets and resources typically limit the rate of upgrades/updates
- Business growth drives prioritization of new initiatives
- The complexities of dealing with external pressures to business are increasing
- No one's reputation or profitability has time for unplanned outages of any kind

Which leads to the conclusion that in security planning there is no "one size fits all" solution that will address all of the unique elements of all businesses. In fact, the issues that need to be addressed by industrial facilities are even more challenging due to the "industrial" nature of the assets and impacts to the supply chains to which they are integral parts.

Understanding that organizations usually have to work with what they have as the starting point helps to ground the Gap analysis between the current and future desired states for an enterprise solution to security. Recognizing and addressing the trend toward pervasive ubiquitous interconnectivity between all digital assets informs the need for thoughtful integrated solutions that address today's inefficiencies while leveraging any and all efficiencies where they can be identified and leveraged as they become available.

In the case of Voith and Kudelski, the philosophy and methodologies employed are at the core of the solution(s) and expectation(s). Kudelski provides a core philosophy of the Kill Chain Defense Model (see figure 1) whereby threats are proactively sought out and blocked, threats are addressed and thwarted, and threats are contained and addressed in the case of a breach. Throughout the multi-tiered iterative philosophy (reminiscent of the OODA loop), learning is constant and leveraged to inform and fortify from future threats.

Figure 1



Translating the philosophy into operational excellence requires that the planning considers the assets, existing capabilities, risk areas, available resources and priorities and integrates them into an approach that is deployable, sustainable, and adaptive. The solution is ideally vendor agnostic and can scale with the organization and its growth while delivering extremely high confidence of thwarting almost all threats and containing any threats that are able to breach the primary protective measures. All of this without disrupting the business and its customers.

3: Cyber Security Health Check

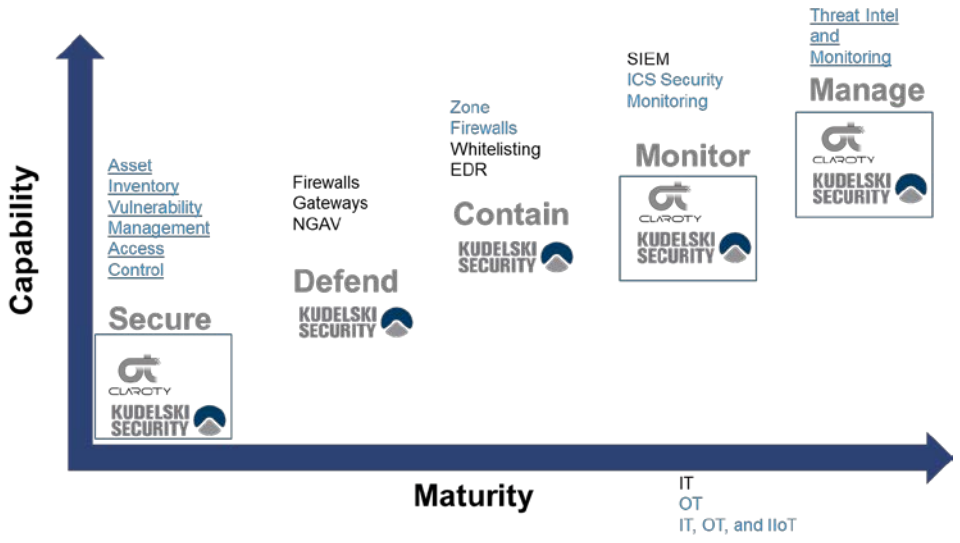
All good plans start with knowing where and who you are today. Knowing where you are starting from reduces the chances of choosing the wrong plan to the destination you desire. The Gap between these two points (today and future) informed by experienced professionals who have worked with almost every size and nature of company to develop workable plans is a critical factor to succeeding in implementing an optimal solution to address security needs today and tomorrow. As the saying goes "you can have it all, you just can't have it all at once."

In fact, there are known steps of Capability and Maturity (see Figure 2) that organizations go through on their way to establishing a robust cybersecurity system that addresses their OT, IT and IIoT security needs. These steps include (in order of increasing capability and increasing maturity):

- Secure
- Defend
- Contain
- Monitor
- Manage

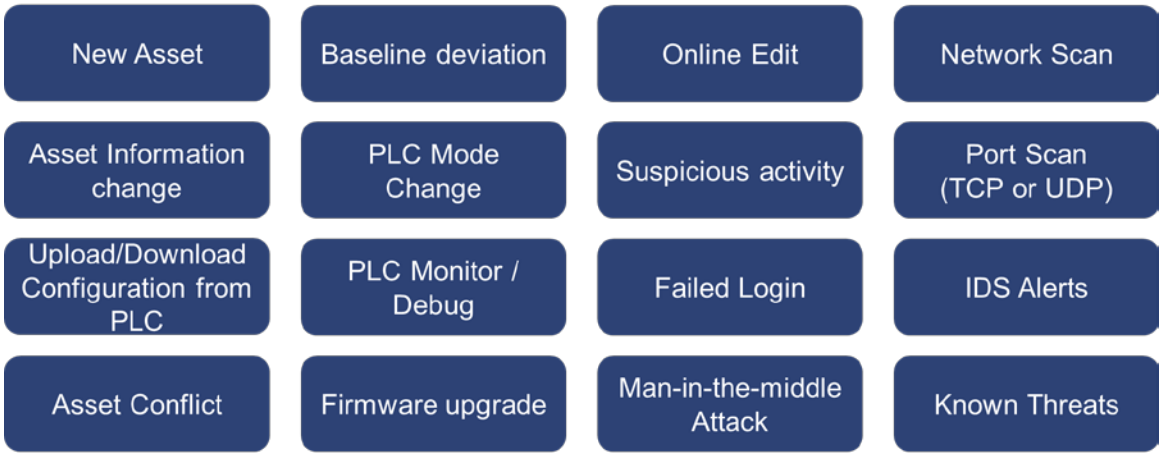
These follow the underlying philosophy show in Figure 1 very closely and ultimately lead to an end state of constant vigilance and iterative shared learning to get out ahead of the attackers and leverage a world class offense as proactive defense. In this way, the burden of the protection is shared amongst partners who all have a common goal – to protect your business so that you can focus on serving your customers and stakeholders.

Figure 2



OT

Industrial facilities and operations, as noted previously, have unique characteristics due to the nature of the equipment, the controls, and the impacts they have on the supply chains to which they are connected. Many of the issues with OT resources have to do with both physical and cyber aspects of equipment that is connected (and not connected) to intranets which are then connected to larger networks that may be internal or external. Connectivity is not inherently good or bad but does come with trade-offs. While connectivity could provide access to attackers, it can also provide increased operational efficiency. Connectivity also offers protection from attackers if OT is updated with the latest and greatest security upgrades and configured properly. Ultimately, OT assets have to have the appropriate level of visibility and management applied to them to assure they are brought up to a level required by business objectives and risk tolerance over their life cycle.



IT

Traditionally, Information Technology (IT) resources and systems have been the domain of administrative/management/corporate groups given the origin of these systems and the nature of the information that has been leveraged to support office workers. However, traditional IT resources have naturally, but slowly, emerged in OT environments where they are typically providing greater amounts of storage, processing power, or connectivity to the larger networks. Thus, the IT resources in organizations can span from early CPM-like operating systems to the most current Linux based Raspberry PI hacks utilized by workers trying to get things done. Many of the challenges today are based on not having a comprehensive view of all the IT systems – both traditional as well as IT living in the OT environments. An accurate picture and robust plan requires an understanding of these combined systems.

IIoT

Whether kept on premises or off loaded to the cloud (via the internet), IIoT connectivity, storage and data processing/analytics can leverage the expertise, infrastructure and best practices of third party providers. However, each of these elements and their impacts need to be assessed, evaluated, and addressed in the overall plan to assure that the appropriate level of security is in place and adhered to while minimizing the chances that these connections or resources are exploited in an attack on the enterprise and its various sites.

Cyber Security Health Check

Together, Voith and Kudelski provide a comprehensive strategic assessment and evaluation of OT, IT, and IIoT resources while considering the variety of sources of potential threats (see Figure 3).

Figure 3

Common Threat Impacts	Typical Attacks	Cyber Threat Actor
Theft of IP	Phishing / Spear-phishing	Insider
Theft of PII	Malware	Cyber Criminal
Fraud	Web Application Attack	Hactivist
Business Disruption	Brute Force	State Sponsored Entity
Financial Loss	Business Process Compromise	Thief
Public Release of Sensitive Information	Drive-by Download	
Data Loss	Distributed Denial of Service (DDoS)	
	Advanced Persistent Threat (APT)	
	Ransomware	
	Third Party Access	
	Social Engineering	
	User Error	
	Physical Theft	
	Hardware / IoT Intrusion	
	Virus / Worm	
	Cyber Fraud	

The assessment and proposed roadmap consider the following dimensions when working with organizations on a comprehensive integrated plan for Cyber Security:

- Architecture and Design
- Assets
- Budget and Investment
- Business Continuity
- Cloud Security
- Communications
- Configuration and Patching
- Cyber Operations
- Facilities
- Human Resource
- Identify and Access
- Incidents
- Information Risk and Compliance
- Logs and Analytics
- Policy and Standards
- Privacy and Data
- Security Awareness and Training
- Software Assurance
- Strategic Planning
- Threat and Vulnerability
- Threat ID and Intelligence
- Vendor and Third Parties

The assessment, evaluation, and recommendations result in a dashboard that can be used by executive management, security professionals, and other stakeholders who need to have access to the insights and plans for the organization. As the organization matures, the dashboard demonstrates progress towards the goals and security posture desired by the organization.

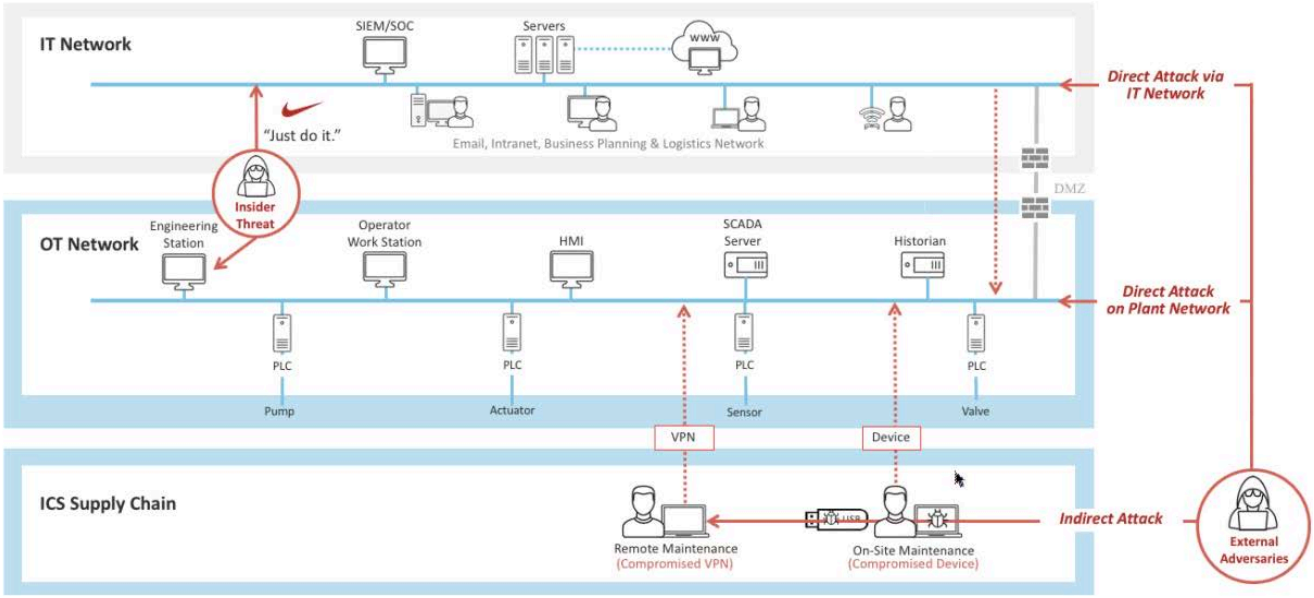
4: Managed Services / Security Ops Center

The fastest, and many times most cost effective, path to having mature capabilities added to an organization's portfolio is bringing them in from the outside. This use of third party offerings to augment an organization's operations where the capability is not the core expertise of the organization can be both prudent and efficient. Given the required investments, timing, talent recruitment and retention issues, and ongoing operating costs associated with 24x7x365 operations providing 99.999% availability – many companies opt to have a small security staff of their own and outsource the rest to companies like Voith/Kudelski.

OT

Traditionally, OT resources have been somewhat isolated from the larger networks using “air gaps” with the ability to disconnect them or keep them offline with little impact to the rest of the operations. However, there is a growing demand to have more information from all of the equipment in operations in a more real time manner in order to monitor the performance of operations, adjust to client demands, and optimize efficiencies given the dynamic environments in which many of these assets and businesses operate. Along with this increased connectivity comes the need to proactively address potential threats (see Figure 4). As noted earlier, the OT network has a variety of areas of risk and ideally a robust cybersecurity plan would be vigilantly watching for any and all anomalous activity in and around the equipment, its data, and its controls.

Figure 4



IT

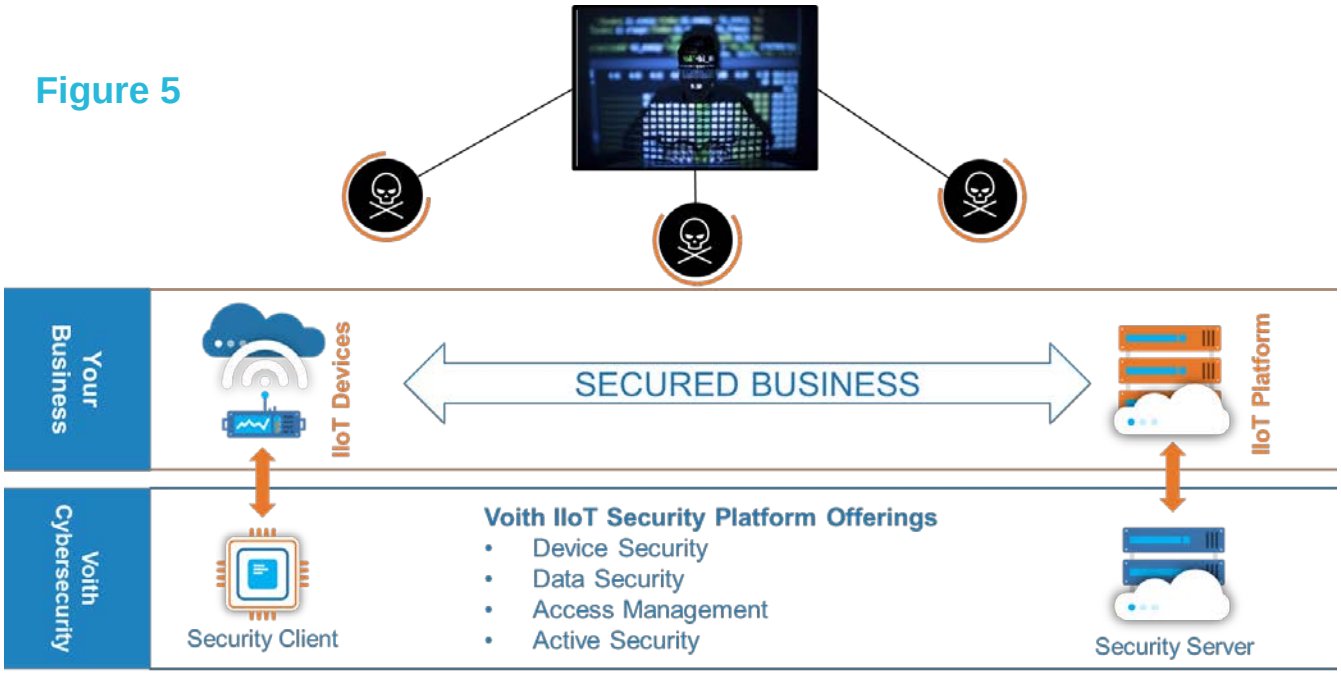
Similar to the OT assets, the IT assets at plant facilities have been more isolated than most consumer focused business operations. As plants become more connected via the IT resources, there is a known need to assure that external parties are not able to negatively impact the operations from remote (or internal) locations. As noted in Figure 4, this also results in the need for 24x7x365 monitoring and proactively seeking bad actors who may have been “casing” the operations for some time as well as identifying and watching for new attempts to breach and learn

about the network topology. In these cases, we want to identify the intruder, while learning their behavior along the way, and securing the information the intruder intends to exploit in the future.

IIoT

Due to the connectivity expectations and demands, Voith and Kudelski employ an approach that places “agents” throughout the operations in order to have the ability to monitor and thwart potential attacks in near real time, (see Figure 5). This approach provides Voith and Kudelski the opportunity to provide the greatest value and visibility to ongoing attempts by external parties who may be trying to breach the security of connected devices.

Figure 5

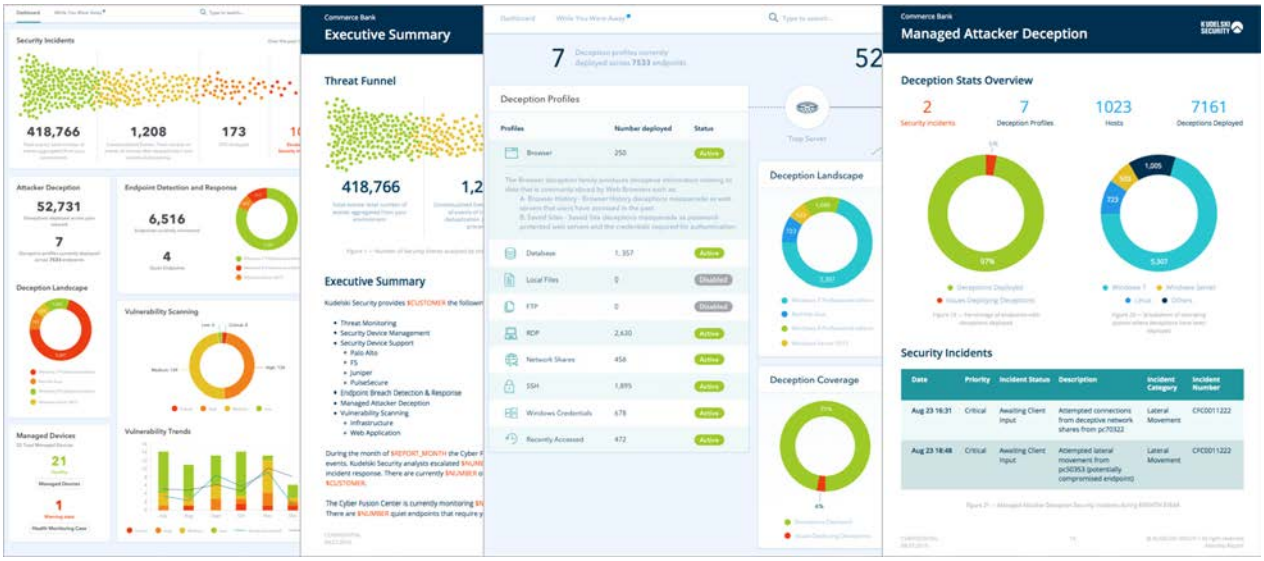


5: Conclusion

The convergence of OT/IT/IIoT in business and industrial operations requires a highly integrated and holistic solution. Solutions need to consider all of the existing conditions, the desired future state, and have a path to systematically provide value with each step – while providing the maximum security possible. Given the increasingly complex demands placed on IT, OT, IIoT, and security staff within companies, it is critical to have external white hat assessment and planning support to address any potential blind spots. The external strategy assessment also brings the accumulated knowledge of experts working across a wide range of businesses and business requirements. The outcome of the assessment, a Cybersecurity Health Check, is a view that can be updated and refreshed on a regular basis, with the plan and associated benefits clearly communicated with all stakeholders. The plan and dashboard also help to share progress on a regular basis and provide a basis upon which new requests can be compared and prioritized.

In order to assure that no one falls asleep at the switch, an approach is needed to monitor, analyze, and identify any potential threats 24x7x365. The bad guys definitely don't sleep or follow any rules so the solutions have to be ready for any attack at any time, with responses established in advance so that appropriate action is taken as quickly as possible to block, retard, or contain threats that are able to breach the outermost defenses. Just as important as thwarting active attacks is addressing identified weaknesses and potential future threats. To support these activities as a force multiplier, issues and activity have to be made visible so that the most important issues can be addressed by internal staff (or assigned to external parties). Monitoring and reporting/visualizing security related activities is critical to the success of programs that have as many facets as a cybersecurity program. As noted in Figure 6, we provide notifications of urgent activity and incidents to manage, and report the daily efforts required of the security related staff. Additionally, the visualizing and underlying analytics can surface patterns of behavior that indicate threats typically well in advance of a coordinated attack. With the integrated ability to proactively "hunt" for threats internally and externally, the business gets the maximum protection for current and future threats.

Figure 6



The pace of integration, data generation and aggregation, and analysis of data for business benefit from all potential sources of value is increasing at an exponential rate. The velocity of data, the volume of the data, and consumption of data is moving to real time analysis and reporting. With these increased business demands and related ability to more effectively compete in the marketplace, there is every reason to make sure that the security needs for all associated assets are addressed in a comprehensive way that doesn't leave an easy entry point for malicious actors. The Cybersecurity Health Check and Managed Services from Voith/Kudelski are the most important assurances that you and your organization can have to minimize the impacts of threats against your enterprise – today and for the future.

About

Voith Group

The Voith Group is a global technology company. With its broad portfolio of systems, products, services and digital applications, Voith sets standards in the markets of energy, oil & gas, paper, raw materials and transport & automotive. Founded in 1867, the company today has more than 19,000 employees, sales of € 4.2 billion and locations in over 60 countries worldwide and is thus one of the large family-owned companies in Europe. RSP: We should mention something about our Digital push/agenda, our AUT/OT/IIOT capabilities.
RSP: www.Voith.com

Kudelski Security

Kudelski Security is the premier advisor and cybersecurity innovator for today's most security-conscious organizations. Our long-term approach to client partnerships enables us to continuously evaluate their security posture to recommend solutions that reduce business risk, maintain compliance and increase overall security effectiveness. With clients that include Fortune 500 enterprises and government organizations in Europe and across the United States, we address the most complex environments through an unparalleled set of solution capabilities including consulting, technology, managed security services and custom innovation. For more information, visit www.kudelskisecurity.com.

Too many people say their company will get to securing their digital assets "tomorrow", only to find out that they waited one day too many. Every day hackers and bad actors get more sophisticated– visualize these threats to help amplify your sense of urgency because it's only a matter of when.

For More Information

Please contact:

Rene St-Pierre
Director of Cyber Security, North America
Voith Digital Ventures
Rene.St-Pierre@Voith.com
905-287-5845