WHITEPAPER

Enhancing Cybersecurity Through Interoperability:

Trends, Technologies, and Challenges

Authored by:
Juan Vargas,
Cybersecurity and Engineering Consultant,
Artech L.L.C

Executive Summary

The importance of interoperability in cybersecurity cannot be overstated, especially its role in creating adaptive strategies for organizations. Interoperability allows seamless integration of diverse security solutions, enhancing threat detection, response capabilities, and compliance. There are several key technologies driving interoperability trends and also challenges in implementing it, such as lack of industry standards and balancing security and privacy concerns. By adopting interoperability, organizations can ensure their cybersecurity products adapt to their existing security architecture rather than forcing the organization to adapt to the limitations of a single product or vendor. Then with collaboration and standardization within the cybersecurity industry, a more robust, interconnected security infrastructure can be developed.

Contents

Introduction

As the digital landscape becomes more complex and cyber threats continue to evolve, organizations must employ a comprehensive and adaptive cybersecurity strategy. This often involves integrating a wide range of applications and security solutions, regardless of the software company that developed them. Interoperability enables the seamless sharing of information and the integration of security systems from different vendors. It is the key to achieving this integration, as interoperability allows organizations to create a holistic cybersecurity approach that adapts to their unique security architecture.

Although the objective of achieving comprehensive cybersecurity measures is not a recent one, it remains an ongoing challenge. Software developers frequently view cybersecurity as a potential market opportunity, motivated to develop an integrated suite of applications that they believe can satisfy their customers' security requirements. In this pursuit, interoperability with other software is relegated to a secondary consideration and is given inadequate attention during the development process.

Corporations often hold different perspectives on cybersecurity. For these entities, cybersecurity encompasses the entire company's security architecture, which can be complex due to the diverse business needs of multiple units that may not integrate easily. This is particularly relevant in critical national infrastructure, such as power plants, where automation systems are utilized and may be compatible with some cybersecurity solutions, but not others. As a result, these systems must undergo rigorous validation processes to ensure operations won't be affected by the installation of new cybersecurity solutions.

One approach to addressing interoperability challenges in cybersecurity is to redefine the concept of "cybersecurity architecture" and think of it as if it was a single, comprehensive "cybersecurity product." This can be compared to building a car, where the end product is not just a collection of individual components (such as windows or an engine), but rather the fully assembled vehicle. Unfortunately, achieving this level of integration has proven to be a significant challenge for the cybersecurity industry, mostly because the ultimate nature of the "cybersecurity product" is still undefined. In other words, there is no clear consensus on what constitutes a truly comprehensive cybersecurity solution, and as a result, new products are continually being developed with claims of addressing novel security concerns.

Interoperability is a necessary requirement in cybersecurity precisely because the problem of cyber threats remains unresolved. Even if all available cybersecurity software is integrated, new vulnerabilities are discovered daily, prompting the need for innovative solutions. In the previous example, a car solves the problem of mobility, whereas cybersecurity applications cannot entirely rectify the problem of cyberattacks. It is possible that a future may exist where the problem is mostly resolved, but that day has not yet arrived.

Because of this unresolved cybersecurity problem, organizations are less likely to settle on a single solution when they invest in cybersecurity solutions. While it's in their best interest to do so, they worry they will need the newest features advertised by the newest companies coming into the marketplace. Or worse, they fear that if they are subject to a cyberattack, they will have to answer to the court of public opinion for not implementing the latest solutions.

When asked about this in a recent survey, 77% of respondents stated they would like to see more support for open standards, and 83% believe that a product's integration capabilities are important (ESG & ISSA Research, 2022). Yet, in the cybersecurity market, two costly mistakes are commonly observed. First, competitors frequently develop similar functionalities to offer a comprehensive solution that displaces all other options. Second, these companies fail to recognize that their competitive interests often hinder their own innovation processes, resulting in the development of software that is neither new nor innovative. This approach creates a "moat" around their solutions, which ultimately slows down the development of additional solutions by other third-party providers. In the cybersecurity industry, there is often a disconnect between the intended audience for cybersecurity software and who their vendors believe the customers at the organization are. While many agree that IT personnel should be the primary end-users of such software, we can't have IT people everywhere; cybersecurity is needed. For instance, certain organizations, such as critical national infrastructure and industrial systems, rely on non-IT experts to run their cybersecurity programs. It's also important to recognize that the ultimate end-user of the "cybersecurity product" is neither IT or other operations personnel, but rather corporate executives and government authorities who conduct cybersecurity investigations.

Even so, many Chief Information Security Officers (CISOs) are primarily trained to focus on new software features and assume that if a solution works for IT, it works for the organization as a whole. This approach is misguided and will need to be corrected. Cybersecurity is not merely about features; it is primarily about ensuring compliance, managing risk, and mitigating liabilities. In addition, cybersecurity plays a critical role in helping authorities prosecute cybercrime cases. As such, if a cybersecurity solution doesn't work for these authorities, then the solution doesn't work at all.

While corporate executives and government authorities are ultimately responsible for ensuring effective cybersecurity measures, IT personnel are crucial in configuring and maintaining complex software solutions. In other words, IT is an essential component of the "cybersecurity product" and not the end-user—it's part of the car, not the driver of the car.

In addition, cybersecurity measures are essential for ensuring the security of national resources and maintaining critical infrastructure, such as the availability of electricity, water, and communication services. If the national infrastructure is not protected, the country may be unable to defend itself in future conflicts, thereby impeding the growth of the entire cybersecurity ecosystem.

State-of-the-art in Interoperability

The cybersecurity landscape has seen an increasing trend towards interoperability, driven by the adoption of various technologies. While a fully interoperable architecture has not been achieved, these technologies have laid the groundwork for future advancement. A few notable examples are:

1. OpenAPI technology

Many vendors offer third-party access to a limited set of resources in their software products through application programming interfaces (APIs). However, there is no standardization in message structures or responses, leading to differences in design and feature sets across vendors.

2. SIEM technologies

Security information and event management (SIEM) systems collect logs from diverse devices, ranging from Windows machines to network devices and programmable logic controllers (PLCs). SIEM technologies contribute to interoperability by standardizing logs using filtering techniques.

3. SOAR Technologies

Security orchestration, automation, and response (SOAR) technologies use APIs to automate specific cybersecurity responses based on known scenarios (Microsoft, n.d.). While these technologies demonstrate the potential of interoperability, the underlying APIs are heterogeneous, resulting in rigid automation processes that require considerable effort to implement and maintain.

4. STIX and TAXII

Structured threat information expression (STIX) and trusted automated exchange of intelligence information (TAXII) facilitates the exchange of threat information across multiple vendors, enabling rapid sharing of actionable intelligence about emerging threats (ThreatConnect, n.d.).

5. EDR/XDR Technologies

Endpoint detection and response (EDR) and extended detection and response (XDR) technologies are designed to capture information from multiple sources, provide threat intelligence, and facilitate response actions (Microsoft, n.d.). Similar to SIEM, these technologies contribute to interoperability by consolidating data from diverse sources.

Benefits of Interoperability in Cybersecurity

One of the primary benefits of interoperability in cybersecurity is the enhancement of threat detection and response capabilities. The seamless exchange of information across systems facilitated by interoperability allows organizations to share critical threat intelligence, enabling them to detect and respond to threats more effectively. As security solutions identify patterns, correlate data, and provide a more comprehensive view of potential risks, organizations are better equipped to promptly identify, mitigate, and remediate cyberattacks.

The concept of sharing threat intelligence is not new. For example, the previously mentioned STIX and TAXII are of interest because they are two standards developed by the cybersecurity community to improve the sharing of threat intelligence between organizations. They were developed by the MITRE Corporation and the Department of Homeland Security with the help of the private sector. As of 2015, both standards transitioned to OASIS Cyber Threat Intelligence Technical Committee.

STIX is a language to describe cyber threat intelligence in a structured and standardized way. It provides a common language for indicators of compromise (IOCs), tactics, techniques, procedures (TTPs), and other types of threat intelligence. TAXII is a protocol for exchanging cyber threat intelligence. It allows organizations to share threat intelligence in real-time and in a machine-readable format, making detecting and responding to new threats easier.

This improved ability to detect and respond to threats is closely related to the streamlining of security operations made possible by interoperability. By reducing the time and effort required to manage multiple disparate systems, organizations can establish more efficient workflows and simplify the management of security tools. This enables security teams to focus on higher-priority tasks, such as analyzing threats and developing proactive defense strategies, ultimately enhancing the organization's overall security.

Another notable benefit of interoperability is improved accountability in cybersecurity. Frequently, it is difficult to determine when a cybersecurity application is not functioning correctly, leading to misplaced blame on individuals who may have disabled security features or failed to use the software correctly. Interoperability makes it easier to identify when software is not working, as other applications actively use this information for their functionality, thus promoting a culture of accountability and transparency.

Interoperability also plays a crucial role in meeting regulatory compliance requirements by streamlining security-related data collection, analysis, and reporting. An interconnected security infrastructure ensures that all relevant information is readily available and can be consolidated into comprehensive reports, simplifying compliance with various industry standards and regulations. Compliance is a critical aspect of cybersecurity, and the enhanced reporting capabilities provided by interoperability contribute to more robust overall security.

Lastly, interoperability fosters a culture of collaboration and information sharing with third parties that want to use the existing cybersecurity infrastructure to build their applications. Similar to how applications are built for phones, developers would build specific functionalities if they were presented with a straightforward way to exchange information with other applications, regardless of who is the software vendor.

Challenges of Implementing Interoperability

The diverse and constantly evolving nature of the cybersecurity landscape poses significant challenges for creating security tools that can interoperate seamlessly with one another. Achieving interoperability among newly developed cybersecurity tools involves addressing several interconnected challenges, such as the lack of industry-wide standards, balancing security and privacy concerns, overcoming resistance to change and legacy systems, and navigating vendor lock-in and proprietary solutions.

An interesting comparison can be made between the situation in the cybersecurity domain and the development of the structured query language (SQL) for data management. SQL emerged as a standardized way to access and manipulate data in relational databases, regardless of the vendor (IEEE, 2012). This standardization facilitated continuous communication and data sharing among various database systems, streamlining operations and increasing efficiency across different platforms.

Nevertheless, the equivalent of SQL does not currently exist for cybersecurity tools. One primary challenge in creating interoperable cybersecurity tools is the absence of universally accepted standards and protocols. Without clear guidelines or a common language for designing and integrating various security solutions, developers may struggle to create tools to communicate and share data without interruption with other systems. Developing and adopting industry-wide standards, similar to the role SQL has played in the field of data management, would facilitate interoperability.

The need for industry-wide standards in cybersecurity underscores the importance of encouraging collaboration within the ecosystem. Stakeholders, including organizations, vendors, and regulators, should work together to establish universally accepted standards and protocols that enable seamless communication and data sharing among security tools, similar to how SQL has standardized data access and manipulation.

Additionally, addressing other interoperability challenges is crucial for developing interoperable cybersecurity tools. By learning from the success of SQL in the data management domain and promoting collaboration, innovation, and standardization, the cybersecurity industry can draw valuable lessons and insights to address the challenges of creating interoperable tools and work towards creating a more robust and interconnected security infrastructure.

Clear guidelines and best practices need to be established to balance security and privacy concerns while developing interoperable cybersecurity tools. Borrowing from SQL's example, developers can create standardized methods for securely sharing data between tools while adhering to privacy regulations, such as the General Data Protection Regulation (GDPR). This would protect sensitive information while enabling seamless communication between security solutions.

Overcoming resistance to change and addressing the challenges posed by legacy systems is another critical aspect to consider. Just as SQL revolutionized data management by providing a standard interface to interact with different databases, the cybersecurity industry must promote the benefits of interoperable tools to enhance security and efficiency. Encouraging organizations to upgrade or replace legacy systems with solutions that support open standards and interoperability can lead to more resilient security infrastructure.

Compelling Use Cases for Interoperability

Developing interoperability standards would allow for better outcomes that are very hard to achieve today. Here are a few examples of what could be achieved in the short term with a collaborative approach to cybersecurity.

Case Study 1:
Enhancing Adaptability with Small Innovative Solutions

Background: A large financial institution with an established cybersecurity platform faced the challenge of keeping up with rapidly evolving cyber threats. The organization needed a solution to integrate cutting-edge security tools from smaller, innovative vendors.

Implementation: The financial institution embraced these small innovative solutions and integrated them into its existing cybersecurity solution to address emerging threats without a significant redesign.

Results: The financial institution experienced a significant improvement in its overall security posture. The organization's ability to adapt and respond to evolving cyber threats increased, and a culture of continuous improvement and innovation was developed.

Case Study 2:
Streamlining Security Management with a Unified Strategy

Background: A multinational corporation struggled with managing a complex cybersecurity infrastructure consisting of solutions from multiple vendors. The organization needed to streamline security management and enforce consistent policies across the entire infrastructure.

Implementation: The corporation focused on creating a unified, flexible cybersecurity strategy encompassing multiple vendors.

Results: The organization's security management became more efficient, resulting in a more cohesive defense strategy. Adopting interoperable tools allowed the corporation to tailor its security infrastructure to its unique needs, making it robust and adaptable.

Case Study 3:
Enhancing Upper Management Visibility for Informed Decision-Making

Background: A large utility company needed a way to provide its upper management with comprehensive visibility into the organization's cybersecurity landscape for informed decision-making and resource allocation.

Implementation: The company focused on seamless communication and data sharing among various security solutions to provide executives with a holistic view of the organization's security posture.

Results: Upper management gained comprehensive visibility into the company's cybersecurity landscape, leading to more effective distribution of resources and alignment of its security strategy with its overall business objectives.

Case Study 4:
Supporting Law Enforcement Efforts through Efficient Data Retrieval

Background: An e-commerce platform faced a significant cyberattack that led to losing sensitive customer data. Law enforcement needed access to data from crucial company security systems for their investigation and prosecution efforts.

Implementation: The e-commerce platform used an application to rapidly collect information from different sources to help law enforcement during the investigation.

Results: The efficient retrieval of data expedited the investigation and prosecution of the cybercriminals responsible for the attack. The collaboration between the e-commerce platform and law enforcement also helped to show a united front against cyber threats, leading to the appropriate handling of the situation.

A Realistic Solution: A Comprehensive Framework for Adaptive Cybersecurity

To address the interoperability challenge in cybersecurity, a promising solution is the development of an open and common framework. This framework would encompass several key aspects, fostering integration and collaboration between various cybersecurity components:

1. Unified agent.

The industry has long recognized the value of using a single agent to manage endpoints. By adopting a common agent, organizations can streamline endpoint management and avoid the unnecessary development of multiple agents that perform similar tasks.

2. Transport layer.

This open standard would facilitate communication between cybersecurity components, such as agents, endpoint applications, and orchestrators. Inspired by the approach taken by Mitre and the Department of Homeland Security with STIX, the transport layer can employ a well-defined API conforming to specific data architectures and sharing models, enabling seamless interactions between different cybersecurity elements, as well as supporting customizations for extended functionality.

3. Native support for common functions.

The framework should provide native support for essential functions, including orchestration, data stores, SIEM, antivirus, application, and device control, among others. While applications can vary in functionality and build upon the framework, they should all support a core set of common functions.

4. Third-party app integration.

Encouraging software applications to utilize this common platform for solution deployment would foster innovation and expand functionality. By adopting a modular approach and a common protocol for endpoint interrogation, applications can more easily integrate with the framework, even when functionality is specific to a particular solution.

5. Cybersecurity architecture.

The framework should incorporate a well-defined architecture to avoid conflicts and ensure seamless integration. For example, an endpoint agent would be designed to support only one antivirus product running at the same time, preventing potential issues arising from multiple, conflicting products.

Conclusion

Addressing interoperability challenges in cybersecurity is crucial for developing effective security strategies. A comprehensive framework for adaptive cybersecurity, consisting of a unified agent, transport layer, native support for common functions, third-party app integration, and a well-defined architecture, offers a promising solution. By adopting this framework and promoting open standards, stakeholders can create a resilient, interconnected security infrastructure to better defend against evolving cyber threats, ultimately fostering a more secure digital landscape.

References

ESG & ISSA Research. (2022, July). Security process and technology trends. Retrieved from https://issawebstite.wpenginepowered.com/wp-content/uploads/2022/07/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf

IEEE. (2012, November 21). Early History of SQL. IEEE Annals of the History of Computing, 34(4), pp.78-82. Doi:10.1109/MAHC.2012.61.

McAfee. (2019, June 11). Interoperability is key to cybersecurity: A conversation at CSIS. Retrieved from https://www.mcafee.com/blogs/other-blogs/executive-perspectives/interoperability-is-key-to-cybersecurity-a-conversation-at-csis/

Microsoft. (n.d.). What is SOAR? Retrieved from https://www.microsoft.com/en-us/security/business/security-101/what-is-soar

Microsoft. (n.d.). What is XDR? Retrieved from https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr

ThreatConnect. (n.d.). Why STIX/TAXII is important. Retrieved from https://threatconnect.com/blog/why-stix-taxii-is-important/