Open Cybersecurity Alliance

We're Making Standards-Based, Interoperable Cybersecurity a Reality

Cybersecurity Imperative

Cybersecurity consistently ranks as a top concern for organizations of all sizes. Constantly changing threats and expanding challenges of protecting people, resources and corporate data result in frequent breaches. Almost daily, governments and organizations issue public notifications on losses of data and money.

Your IT environment undergoes constant changes. New digital assets, such as Internet of Things (IoT) devices, get added to your items that need to be protected. Your IT employees are constantly updating and reconfiguring the systems involved to adjust to new workloads and users. This is accentuated with the global COVID-19 pandemic accelerating cloud usage among remote workers.

Fragmented & Complex Security Hinders Effectiveness

In addition, your security infrastructure is marred by security complexity. The security technology market in general is in a state of overload, with pressure on budgets, staff shortages and too many point solutions. ESG Research notes the average number of tools for cybersecurity organizations is 25 to 49, with 20 vendors providing the various components. Customers often cite problems with an overload

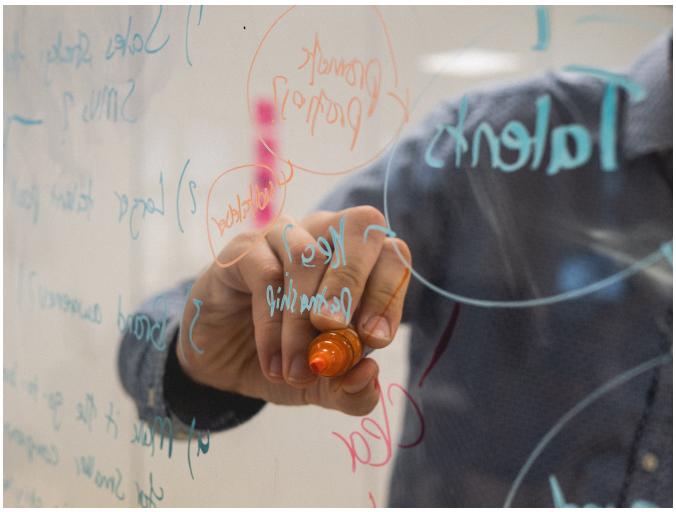
Key Highlights

Remove Cyber Security Complexity with Industry-Driven Interoperability

Empower Security Working Together with Common Architecture, Language & Messaging, and more

Leverage and Contribute to the OCA Open Projects

of events or alerts, complexity and duplication of tools.[1] The current approach of purchasing multiple separate leads to problems like different user interfaces and databases that require unique configurations, and constant maintenance, support and training to use and connect these products as needed.



Fragmented security hinders effectiveness

Security Operations Center (SOC) teams are stretched

Typically, cybersecurity organizations use a large number of products from multiple technology providers, including the following offerings:

- A security information and event management (SIEM) solution for centralizing the security events for correlation and prioritization
- A security orchestration, automation and response (SOAR) solution to improve the processes around detection and response by context enrichment and better downstream prioritization and efficiency

[1] ESG Master Survey Results, 2018 Data Protection Landscape Survey

- Email security systems
- Endpoint detection and response systems
- Network security systems, such as firewalls, routers and so on
- Products that cover the attack surface of a corporation's IT systems and provide visibility to all systems and users, such as IoT systems, cloud systems, databases, identity and access systems and so on

Security operations teams struggle with navigating across these systems to determine if and when an attack has occurred and if a breach has happened. The complexity of today's defense approach, with a tool for each domain, risk analysis, threat detection and independent domains of knowledge, isn't interoperable.

The problem with this approach is your security defense doesn't act like a system but as a collection of separate independent parts. The ideal cybersecurity defense platform has interoperable components that can be centrally managed using a common command and control system and centrally monitored using a well-defined ontology of objects and events. This platform approach creates a united front of tools working together to defend and secure critical assets.

Disconnected security tools introduce complexity

Open Cybersecurity Alliance

The establishment of the Open Cybersecurity Alliance (OCA) is built on the realization that security tools need to communicate with a common language so that interoperability can be achieved at the communication and data levels. The goal of OCA is to enhance interoperability and collaboration around different standards, tools, procedures and open-source libraries. Using OCA tools and standards, organizations will be able to easily create a more sustainable approach to addressing the increasing volume and sophistication of cybersecurity threats by being better able to identify, analyze and remediate more effectively.

Industry-Driven Platform Approach for More Effective Security

By defining an architecture to support communications across cybersecurity technologies, cybersecurity defense can be more efficient and effective. Laying out a common communications bus, where security technology can share information and interact, eliminates the need to create multiple, distinct point-to-point connections to carry the same information. By defining common commands and response formats, interactions among products are consistent, eliminating the need for product-specific context and content.

Using this approach, cybersecurity solutions can be deployed anywhere and connect into the common communications bus to be part of the overall cybersecurity system. This setup is especially important as the current security market is evolving and security functions and capabilities are constantly moving and changing.

Collaborative approach for a stronger security

Critical OCA solution components and their outcomes

STIX and STIX-shifter

Structured Threat Information eXpression (STIX™) originally evolved out of discussions among the security operations and cyber threat intelligence experts on the IDXWG email list regarding the development of a standardized representation for cyberthreat indicators. Members of US-CERT and CERT.org established the IDXWG email list in 2010 to discuss automated data exchange for cyber incidents.

STIX is a structured language for describing cyber threat information so it can be shared, stored and analyzed in a consistent manner. The STIX language conveys the full range of cyber threat information and strives to be expressive, flexible, extensible, automatable and readable by humans.

Cyberthreat information being managed and exchanged today is typically inconsistent and very limited in sophistication and expressivity. Where standardized structures are used, they're

typically focused on only an individual portion of the overall problem, don't integrate well with each other, or lack coherent flexibility. STIX aims to extend indicator sharing to enable the management and widespread exchange of significantly more expressive sets of indicators as well as other cyberthreat information.

One of OCA's objectives is to leverage existing standards. STIX establishes a data model for threats and provides a unifying architecture tying together a diverse set of cyberthreat information including the following items:

- Cyber observables
- Indicators
- Incidents
- Adversary tactics, techniques and procedures, including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting and so on
- Exploit targets, such as vulnerabilities, weaknesses or configurations
- Courses of action, incident response or vulnerability and weakness remedies or mitigations
- Cyberattack campaigns
- Cyberthreat actors
- Relationships between objects

OCA is leveraging STIX and has created a project called STIX-shifter.

STIX-shifter is an open-source Python library that translates between STIX and common cybersecurity data formats. By doing so, STIX-shifter allows software to connect to products that house data repositories by using STIX Patterning and return results as STIX Observations.

STIX 2 Patterning is a part of STIX that deals with the “matching things” part of STIX, which is an integral component of STIX Indicators.

An example of STIX 2 pattern is [url:value = 'http://www.testaddress.com'] OR [ipv4-addr:value = '192.168.122.84']

This library ingests STIX 2 patterns as input and searches for data that matches the patterns inside various products that house repositories of cybersecurity data. Examples of such products include SIEM systems, endpoint management systems, threat intelligence platforms, orchestration platforms, network control points, data lakes and more.

In addition to searching the data by using these patterns, STIX-shifter uniquely also **transforms the output** into STIX 2 Observations. You want to have this process so that all of your security data, regardless of the source, mostly looks and behaves the same.

Anyone with experience in data science will tell you that cleansing and normalizing of data across domains is a large hurdle to overcome with attempting to build cross-platform security analytics. OCA is attempting to break down this barrier with STIX-shifter.

Open DXL and OpenDXL Ontology

One of the primary needs to building a collaborative system is to define a communications model that enables security components to communicate with each other effectively. Selected to move and evolve from the current one-to-one model where each security component establishes its own connection with all the other components is the Open Data Exchange Layers (OpenDXL). OpenDXL allows organizations to efficiently create once and connect to many or selected connections.

The goal of OpenDXL is to enable security devices to share intelligence and orchestrate security operations in real time.

OpenDXL lets developers join an adaptive system of interconnected services that communicate and share information to make real-time, accurate security decisions. OpenDXL leverages the Data Exchange Layer that many vendors and enterprises already use and delivers a simple, open path for integrating security technologies regardless of vendor.

While OpenDXL can provide the communications layer, a need exists to establish defined commands and messages. OCA has an existing project called OpenC2 that is creating a standardized language for the command and control of technologies that provide or support cyber defense.

OpenC2 defines a language at a level of abstraction that will enable unambiguous command and control of cyber defense technologies.

This project is broad enough to provide flexibility in the implementation of devices and accommodate future products. OpenC2 will have the precision necessary to achieve the desired effect as well.

In addition to OpenC2, OCA created the OpenDXL Ontology project, focused on the development of an open and interoperable cybersecurity messaging format for use with the OpenDXL messaging bus. OpenDXL Ontology enables any tool to automatically gain the ability to communicate and interoperate with all other technologies using this language. This development helps eliminate the need for custom integrations between individual products.

Let’s consider a use case. An infected endpoint reaches out to a malicious site. Network security flags the effort and communicates with endpoint security and vulnerability management to query and

scan the device to determine if infected. Endpoint security and vulnerability management determines the device is infected and advises network access to quarantine the device until malware is removed. Endpoint security removes malware. Network access is updated, and quarantine is expired.

OpenDXL, OpenC2 and OpenDXL Ontology all work together to form the OCA communications layer, enabling collaboration across security components.

Security Content Automation Protocol (SCAP) v2

The Security Content Automation Protocol (SCAP) v2 Data Collection architecture focuses on the capabilities needed for the following activities:

- Task the cybersecurity architecture with collection of asset information from or about a managed asset.
- Store collected asset information that may be used to quickly respond to future queries without engaging with an asset.
- Compile and deliver reports containing requested asset information.

SCAP v2 provides an asset monitoring service that can be leveraged by all security components. This service eliminates the need for multiple independent agents from each security component to collect this information.

SCAP v2 Use Cases

Point-in-time information collection

The data collection architecture collects specific information about certain enterprise assets, to the extent that its capabilities allow. The data collection architecture then compiles its findings into a report

that is returned to the requester. At this point, the action is complete. The data collection architecture will retain the collected information for a period of time so it can be used to support future requests but otherwise has no further responsibilities regarding the request.

Ongoing monitoring against a baseline

The data collection architecture collects information about certain enterprise assets, just as in use case 1, but then monitors those assets for changes in the collected information. The tasking party learns of any detected changes in the reported information. This way, data collection architecture provides an ongoing picture of the changing state of the enterprise.

Benefits of OCA

A system is a group of interacting or interrelated entities that form a unified whole. By approaching security as a system composed of collaborative components, you can achieve more efficient and effective security operations. The OCA approach provides the following benefits:

Better orchestration of your security operations and incident response

- Information sharing across multiple components at the same time
- Better context sharing across components to more quickly identify risks
- Ability to drive actions across security components at the same time
- Increased automation capabilities with the ability to drive multiple components with a single action

Elimination of the need for product-by-product redundancies

- Definition of unique communications between each product

- Deployment of multiple agents to collect security data

Simplification of your security operations center

- Elimination of the need for the security administrators to navigate and analyze separate product information individually
- Simplification of the maintenance of your security products (less connections to define, less agents to deploy and manage)

Benefits for Security Practitioners

- Share information, analytics, and orchestrated response between products
- Discover critical insights and findings you're missing now
- Avoid buying unnecessary tools
- Free yourself from vendor lock-in

Benefits for Security Vendor community

- Increase integration exposure and reduce engineering
- Leverage opensource connectors and add value to your products
- Deliver more robust data integrations
- Allow clients to extract more value from your tools

More Efficient and Effective Security Operations

Take the next step

Our networks and systems have evolved over time. Each network device used to have its own console, configuration requirements and logs and operated independently. Now, networks have developed many open standards and protocols and can be operated and managed efficiently. This ability exists even though our networks have grown significantly in the number and types of devices and the types of connections.

Security systems need to evolve in the same way. OCA has taken the next step to provide the necessary open standards and tools to bring security operations forward and offer a more effective way to defend your business from risks.

- Review your current security approach and how it Is affecting your costs. Are you achieving your goals on threat detection and response times? Do you feel the current approach could be simplified and more effective?
- Does approaching security as a system of collaborative security products as opposed to acquiring individual products make you rethink your current approach?

Join us at Open Cybersecurity Alliance to help us simplify security and support the development of interoperability and collaboration.

Learn more at https://opencybersecurityalliance.org