Building Cyber Resilience

Jim Richberg, Public Sector Field CISO & VP Information Security

June 2023

Agenda

- Introduction: Why does cyber resilience matter and how can you build it?
- Focus area: *building integrated/federated operations*
  - Defining the problem
  - Approaches to addressing each element of the problem
  - Key Questions to consider
- Key building blocks to integrating security

Why is Cyber Resilience such a Hot Topic?

- A key focus for government (e.g., 2023 US Cyber Strategy)
- Increased interest among organizations and coalitions in integrating operations across and within security, IT, and OT
- Technology and conceptual convergence (e.g., SASE, Zero Trust)
- Worsening threat environment (nation-state and criminal)
- Potential for increased funding and multiple approaches and options to choose from (‘People, Process, Technology’)

My Perspective and Advice

My perspective is shaped by:

- Overseeing U.S. ‘Comprehensive National Cybersecurity Initiative’, building and connecting major Federal cybersecurity centers
- Work as a CISO at one of the world’s leading cybersecurity firms

Lessons learned:

- **Identify and partner with key stakeholders** (internal and external)
- **Understand and leverage key trends** (e.g., the technological ‘art of the possible’, convergence of networking and security, changing regulatory and conceptual landscape)
- **Leverage ongoing or planned upgrades** to maximize their benefit on enhancing resilience

Focus of this Talk:

- A key part of building organizational cyber resilience is improving effectiveness of cybersecurity, and a simple way to frame this is as a two-part problem:
  - **Establishing situational awareness** (building a Common Operating Picture)
  - **Driving integrated response**
- Integrating security operations across multiple/disparate organizational elements or missions is more complicated than securing a simpler environment but leverages the same underlying core building blocks

Situational Awareness

- Situational Awareness consists of:
    - **Perception** / gathering information
    - **Comprehension** / understanding the state of the environment
    - ***Predicting*** future near-term states of the environment
- *Humans* –not machines-- need a 'dashboard' to understand and organize situational awareness
- *Communication* and c*ohesion* pose challenges in establishing shared situational awareness *within* an Ops Center but especially *between* them

Generating shared situational awareness consumes most of the available time and attention (and places a premium on efficiency of response)

Pluses and Minuses to Different Approaches to *Building Situational Awareness*

Federating awareness <u>across</u> Centers or **<u>within</u>** a central one either by:

1. Generating a <u>single</u> shared view

    \+ User friendly, can supplement or replace subordinate Center perspectives
    \- Likely requires a bespoke solution built from scratch

    Easier to do when the standards/views of the subordinate Centers can be controlled

2. Sharing <u>separate</u> <u>perspectives</u>
   (e.g., each Center has a 'repeater' of the views from the others)

    \+ Easier to implement, but harder to do so successfully
    \- Requires ongoing manual (human analyst/operator) integration
    \- Integration becomes harder as number/diversity of perspectives grows

Key design decision – *who is the audience for this situational awareness?*
(Executives or network defenders)

Three Approaches for *Enabling Integrated Response*

1. **Data**-driven: building from standardized formats (e.g., log files, STIX-TAXII for cyber threat intelligence)
2. **Function or product**-driven: leveraging key capabilities and commercial products such as multifunctional hardware or SIEM and SOAR
3. **Architecture**-driven: leveraging Mesh Architecture-level interoperability across functions and vendors

These approaches are not mutually exclusive

Key Questions / High level Roadmap

FRAMING QUESTIONS:

- Establish the *RELATIVE PRIORITY* of shared Situational Awareness vs. Response
- *Is anyone in charge?* (i.e., have directive authority)
- What are the available *resources?*
- *How much* data will be available?
- *How fast* does processing need to occur?

Situational Awareness

- *Current capabilities*: does every member have a common operating picture?
- *How many views* need to be integrated?
- *Who is the customer*?

Integration of response

- *Does every member have a Center*?
- How do needs and current member capabilities map to *commercial solutions*?
- *What are timelines*/deadlines for implementation?

Key Building Blocks of Cyber Resilience

Building Block #1: Cyber Threat Intelligence

Different levels are key to both Situational Awareness and Response

- Tactical intelligence (‘turning data into dots’)
  - Production and use is *largely automated*
  - The largest category by volume and variety of data sources
- Operational intelligence (‘connecting the dots’)
  - *Human curated*; quality and focus often uneven
- Strategic intelligence (‘making patterns or pictures’ out of the dots)
  - *Human generated;* relatively uncommon

Operational* level info *is key for federated Situational Awareness while Federating Response relies largely on tactical information

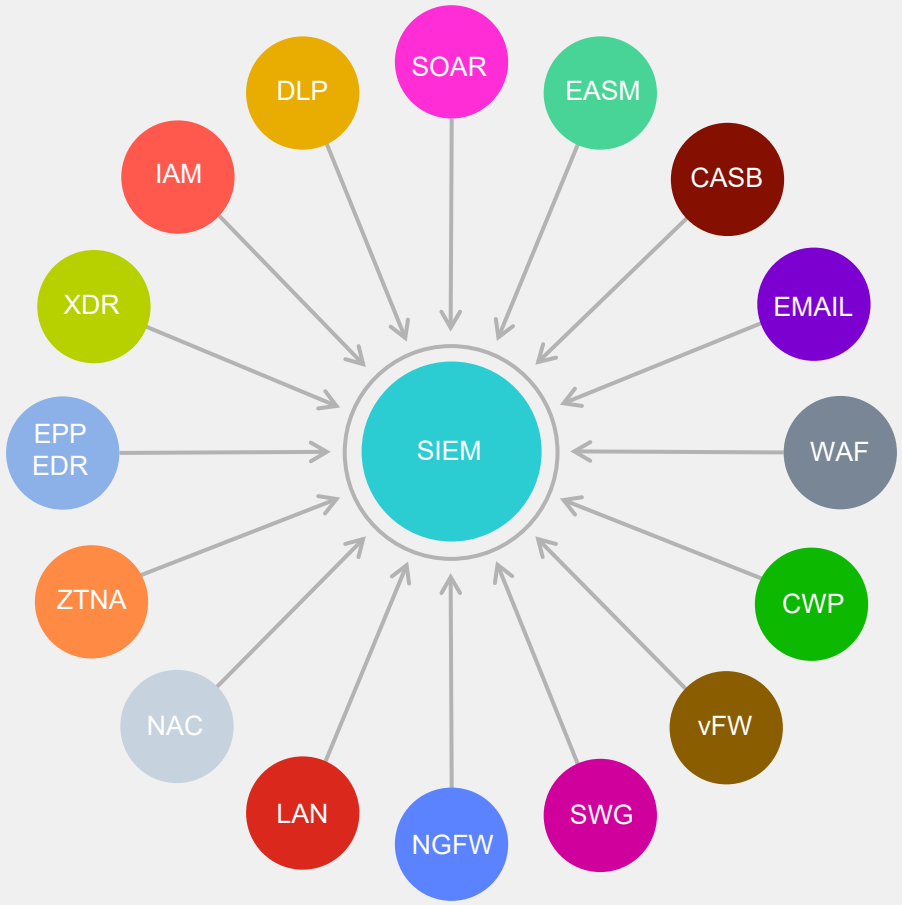
Building Block #2: AI/ML-driven automation

- Major OEM's have been using Artificial Intelligence and Machine Learning in threat detection for over a decade
- Growing maturity of deep learning/neural network capability enables new use options including standalone deployment within IT networks and in OT
- Some AI/ML tools are focused specifically on supporting SOC analysts and network operators
- AI/ML is fueling the ability to leverage large data sets to drive real-time automation. ***This has the potential to turn size and complexity from a liability into a net advantage***

Building Block #3: Replacement of Siloed Solutions with Ecosystems of Interoperable Capability

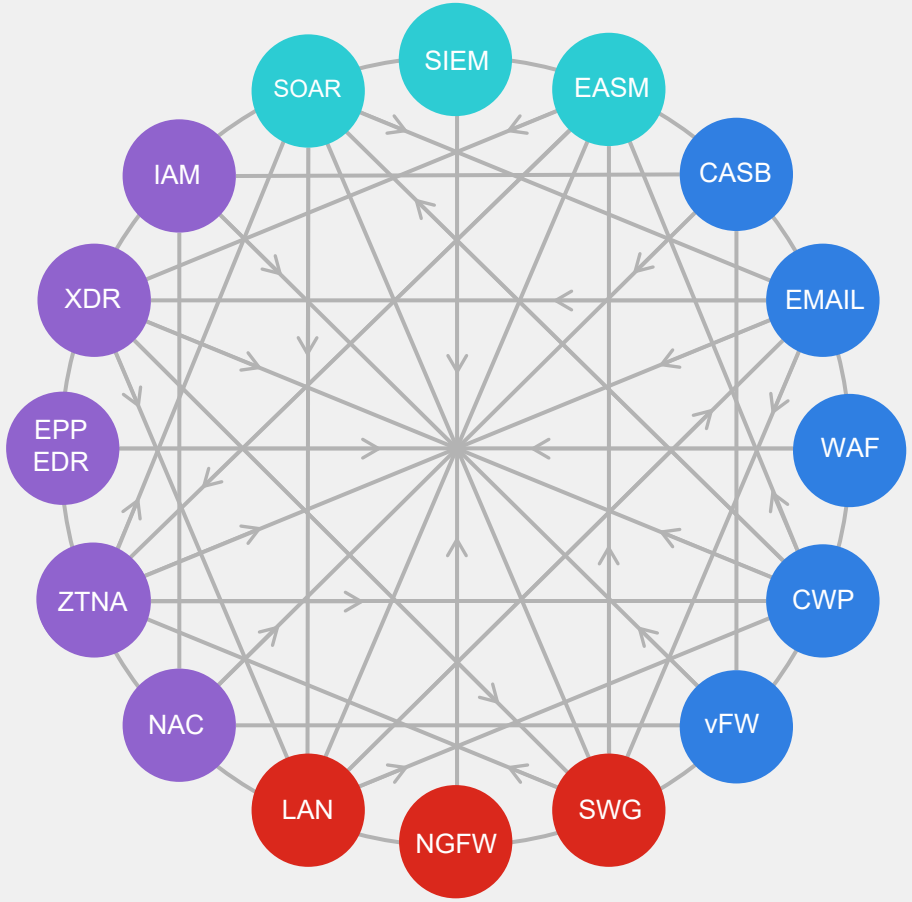
Gartner Cybersecurity MESH Architecture (CMSA)

Cybersecurity Point Products



20 Vendors

Cybersecurity Platform Approach



4-6 Platforms

These Ecosystems can be broad

For example, Fortinet's has 500+ best-in-class integrated external solutions

Fabric Connectors	Fortinet-developed deep integration automating security operations and policies	aws, aruba (a Hewlett Packard Enterprise company), cisco, Google Cloud, IBM Cloud, Microsoft Azure, ORACLE, servicenow, Symantec.
Fabric APIs	Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions	ARISTA, ASAVIE, DELL, DRAGOS, EQUINIX, intel, SIEMENS (Ingenuity for life), splunk>, TIGERA, tufin
Fabric DevOps	Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration	aws, Google Cloud, HashiCorp, Microsoft Azure, openstack., ORACLE, RED HAT ANSIBLE Automation, refactr, vmware
Extended Ecosystem	Integrations with threat sharing initiatives and other vendor technologies	CYBER THREAT ALLIANCE, MITRE, STIX, INTERPOL, OT CSA, Firewalls, Switching, Wireless, Endpoint Security

Figures as of March 31, 2021
Note: Logos are a representative subset of the Security Fabric Ecosystem

Building Block #4: Start with COTS Solutions

Next Gen Products can help Federate Operations

SIEM (Security Information and Event Management)

- AI/ML-driven User and Behavior Analytics support asset baselining and anomaly-based triggers
- Level setting/normalizing of data across multiple domains to support complex pattern discovery
- High speed log parsing and use of threat intelligence
- Work processes, functions, and roles can be pre-defined

SOAR

- Playbook designer for integrating products and common actions
- Facilitates SOP creation and process automation for managing multiple incidents and types of SOC response simultaneously
- Can perform services remotely for member organizations
- Role-based incident management including a “virtual War Room” with access control and organizational activity templates

Thank you!

Please direct any questions to:

Jrichberg@Fortinet.com


FORTINET