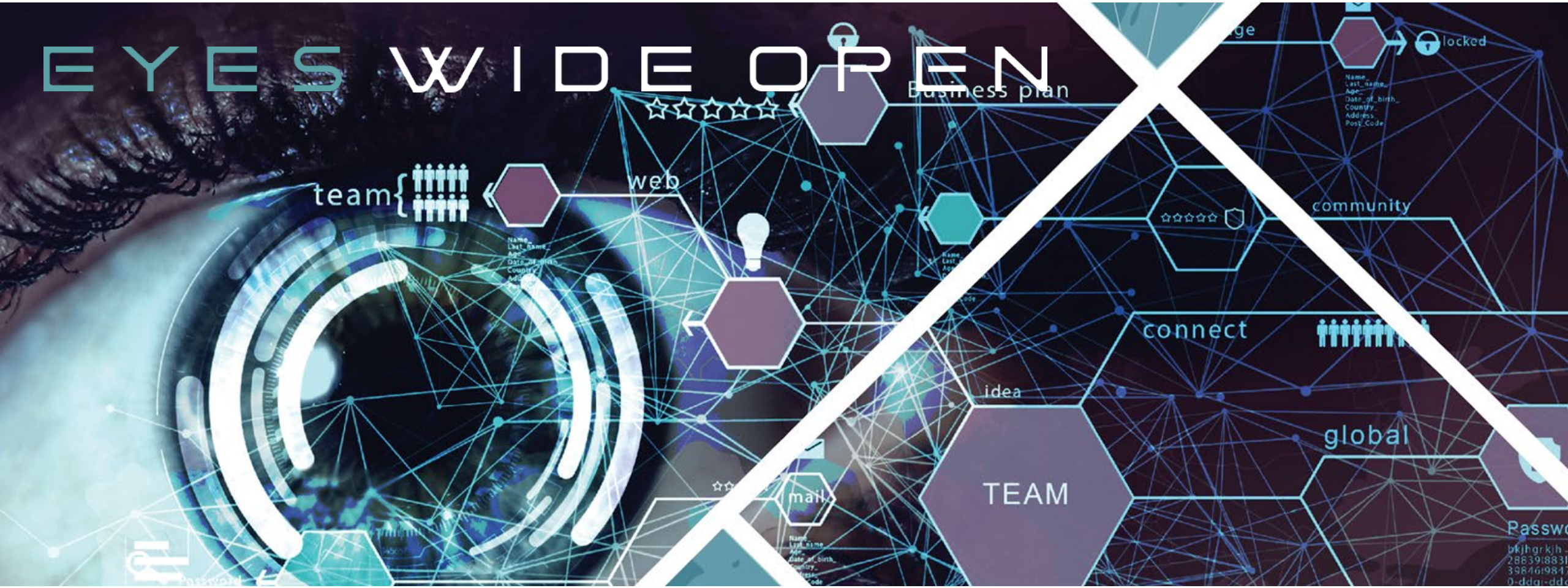
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



The Role of Modern Asset Management in Cybersecurity

Lenny Zeltser

CISO, Axonius

AXONIUS

What's the deal with asset management for IT and security?

- Maintain an "inventory of information and other associated assets" (ISO)
- "Actively manage (inventory, track, and correct) all enterprise assets" (CIS)
- "Provide management with a complete picture of what, where, and how assets are being used." (NIST)
- "Perform automated asset discovery every 7 days." (CISA)

Important question to consider for today's IT and security leaders:

- Why haven't we solved the asset management challenge yet, after all these years?
- What's in scope of asset management practices today?
- How can security and IT stakeholders benefit from well-functioning approaches to asset management?

Challenges and Opportunities of Asset Management Today

Enterprises expect IT and security to address business needs quickly.

- IaaS/cloud resources can quickly appear and disappear.
- SaaS products allow business users to provision resources even without IT and security.
- Security can no longer be a gatekeeper for deploying IT infrastructure.
- Manual data entry for the asset inventory into, say CMDB, is no longer practical.

IT assets are spread across many domains and teams.

- Multiple IaaS/cloud service providers
- Self-hosted infrastructure
- Remote offices
- People's homes
- SaaS products

Cybersecurity teams expect higher asset management visibility than IT (sometimes).

- What percent of coverage is good enough for you?
- Audits and security frameworks have high expectations for comprehensive, full coverage.
- Security incidents are likely to involve unmanaged or unknown assets.
- Leading asset management improvements can position the security team in a favorable light.

We want to track multiple types of IT assets in a useful inventory.

- Applications (installed and SaaS)
- Network devices
- Physical systems
- Virtual machines
- User accounts

Merely knowing about the existence of the IT asset is insufficient.

- What is its configuration state?
- What OS and software is installed there?
- Is it consistent with our security expectations?
- If there are any gaps, how might we address them?
- Who is responsible for it—tech and business owner?

Look at multiple tools as data sources for an accurate asset inventory.

- Network and vulnerability scanners
- User directories and identity services
- System and device management solutions
- Endpoint security software
- Network and cloud management tools
- Financial systems

Gartner coined the term Cyberasset Attack Surface Management (CAASM).

- Focuses “on enabling security teams to overcome asset visibility and exposure challenges.”
- Gathers data “primarily through API integrations with existing tools.”
- Allows querying consolidated data to identify gaps in security controls.

Useful Cybersecurity and IT Scenarios for Asset Management

Device and System Discovery

- Unmanaged devices and systems
- Movement of devices and systems across networks or physical locations

Sample data sources:

- Network management
- System and device management

Endpoint Protection

- Missing or non-functioning security agents
- Details about installed software

Sample data sources:

- Endpoint security
- System and device management

Vulnerability Management

- Devices or systems not being scanned
- Prioritization of vulnerability data based on context (e.g., internet exposure or business role)

Sample data sources:

- Network and vulnerability scanners
- Network and cloud management tools

Cloud Security

- Ephemeral workload oversight
- Configuration gaps in the IaaT/cloud infrastructure

Sample data sources:

- Network and vulnerability scanners
- Network and cloud management tools

Investigations and incident response:

- The state of the affected devices or systems
- Awareness of the affected environment and context

Sample data sources:

- Network and cloud management tools
- User directories and identity services

GRC and audits:

- Accurate asset inventory
- Evidence of controls tied to asset management

Sample data sources:

- Network and cloud management tools
- User directories and identity services

Systems management and support:

- Validation of software distribution and patches
- The state of the affected devices or systems

Sample data sources:

- Endpoint security
- System and device management

Modern asset management acts the nexus for cybersecurity and IT workflows.

- Having a single place for all asset data saves time and offers useful context for data-based decisions.
- Correlating data from multiple tools can answer questions a single tool cannot.
- Answers to these questions also provide metrics and help track progress of cybersecurity projects.

A Few Takeaways for You

How do “legacy” and “modern” asset management approaches compare?

Legacy:

- Focuses on devices
- Manual CMDB data entry
- Stale and incomplete data
- Helps with hardware and software inventory

Modern:

- Tracks all asset types
- Data from multiple sources
- Accurate, comprehensive
- Helps with device discovery, network management, endpoint security, incident response, cloud oversight, config management, etc.

When devising your security asset management strategy:

- Assume that most of your asset data will come from diverse sources and not from manual entry.
- Decide what data sources can give you sufficient visibility into the assets as a starting point.
- Bring the data together, then create a process for examining it to find security gaps.
- Design scenarios for using the data that benefit your stakeholders.

Security can build good will with multiple stakeholders through asset management.

- Corporate IT
- DevOps
- Network administrators
- Auditors
- Finance analysts