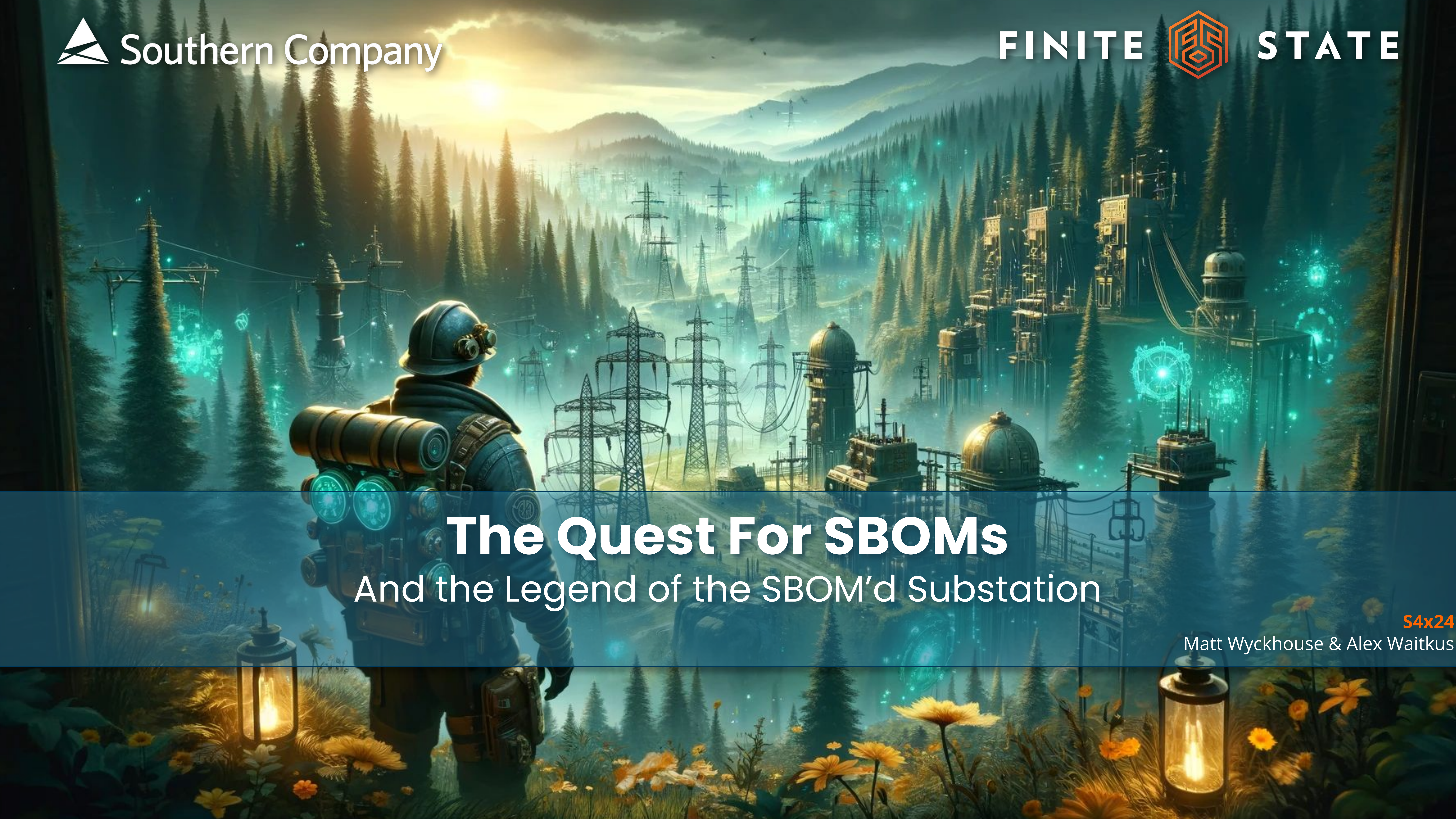
Southern Company

FINITE STATE



The Quest For SBOMs

And the Legend of the SBOM’d Substation

S4x24

Matt Wyckhouse & Alex Waitkus

S4x23: Create The Future

Finite State hosted a roundtable with OT vendors, manufacturers, and utility asset owners

We developed a plan for utilities to begin collecting SBOMs for a specific environment

The purpose was to gain better visibility and awareness into:

- Software subcomponents
- Risk posture/tech debt
- N-day vulnerabilities
- Vendor risk management

Your mission is to "SBOM" an Industrial Facility at Mississippi Power (MPC). We know it contains:

- Protection Devices
- Network Devices
- Cybersecurity Devices
- Physical Security Devices
- Condition Based Maintenance Devices
- And more…

Southern Company

S4x23 Roundtable Session

FINITE STATE

The “Ideal” Quest for SBOMs

Generate Inventory
of Devices and Software in Substation

Request SBOMs
& Receive Security Data from Vendors

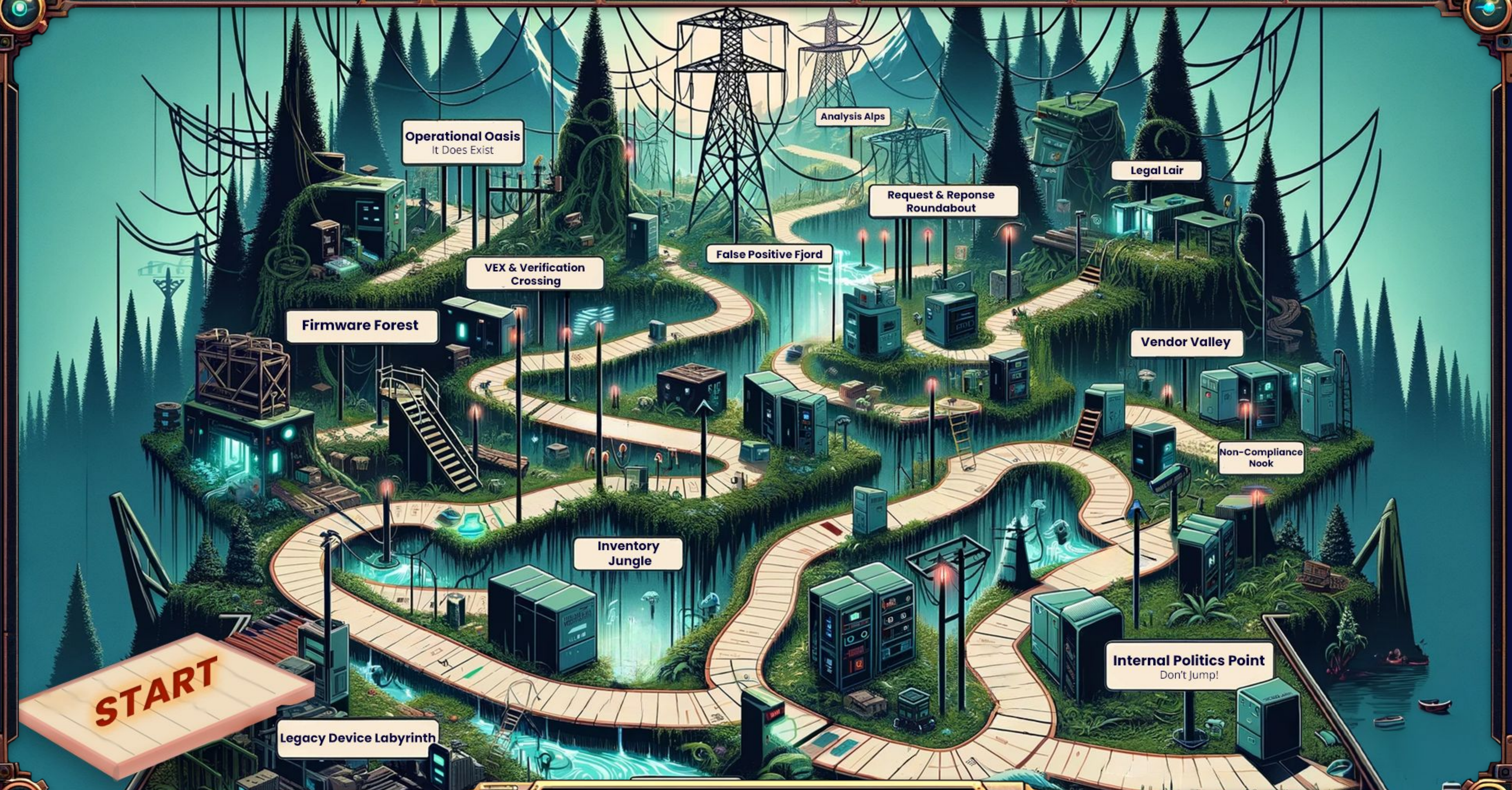
Verify & Validate
through Testing of Devices and Software

Analyze & Monitor
Vulnerabilities and Risks

Operationalize
SBOMs & Supply Chain Risk Management

Southern Company

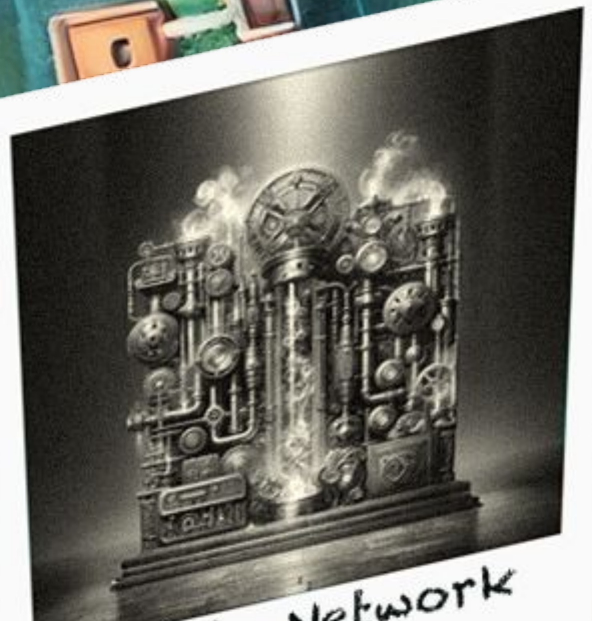
FINITE STATE



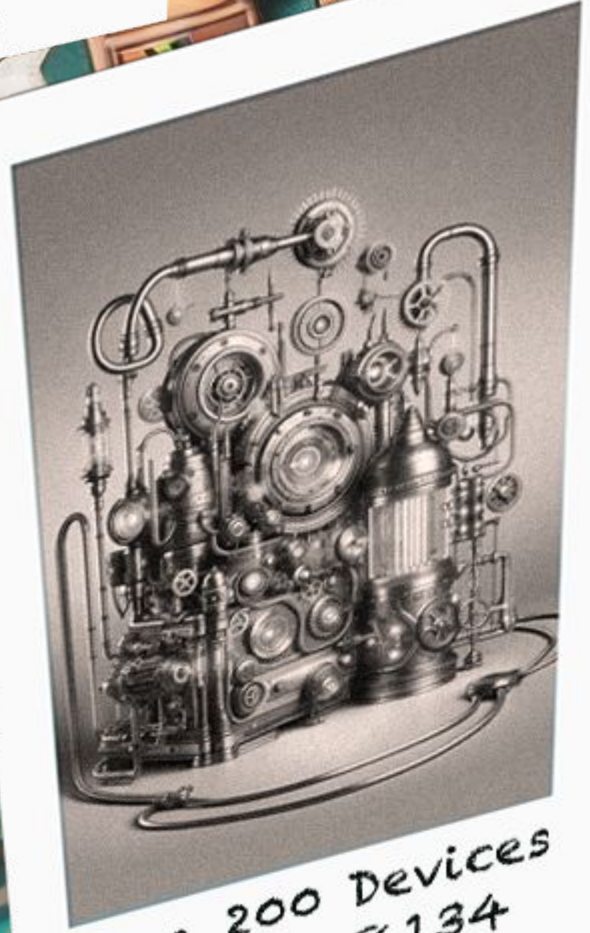
Southern Company

The "Real" Quest for SBOMs

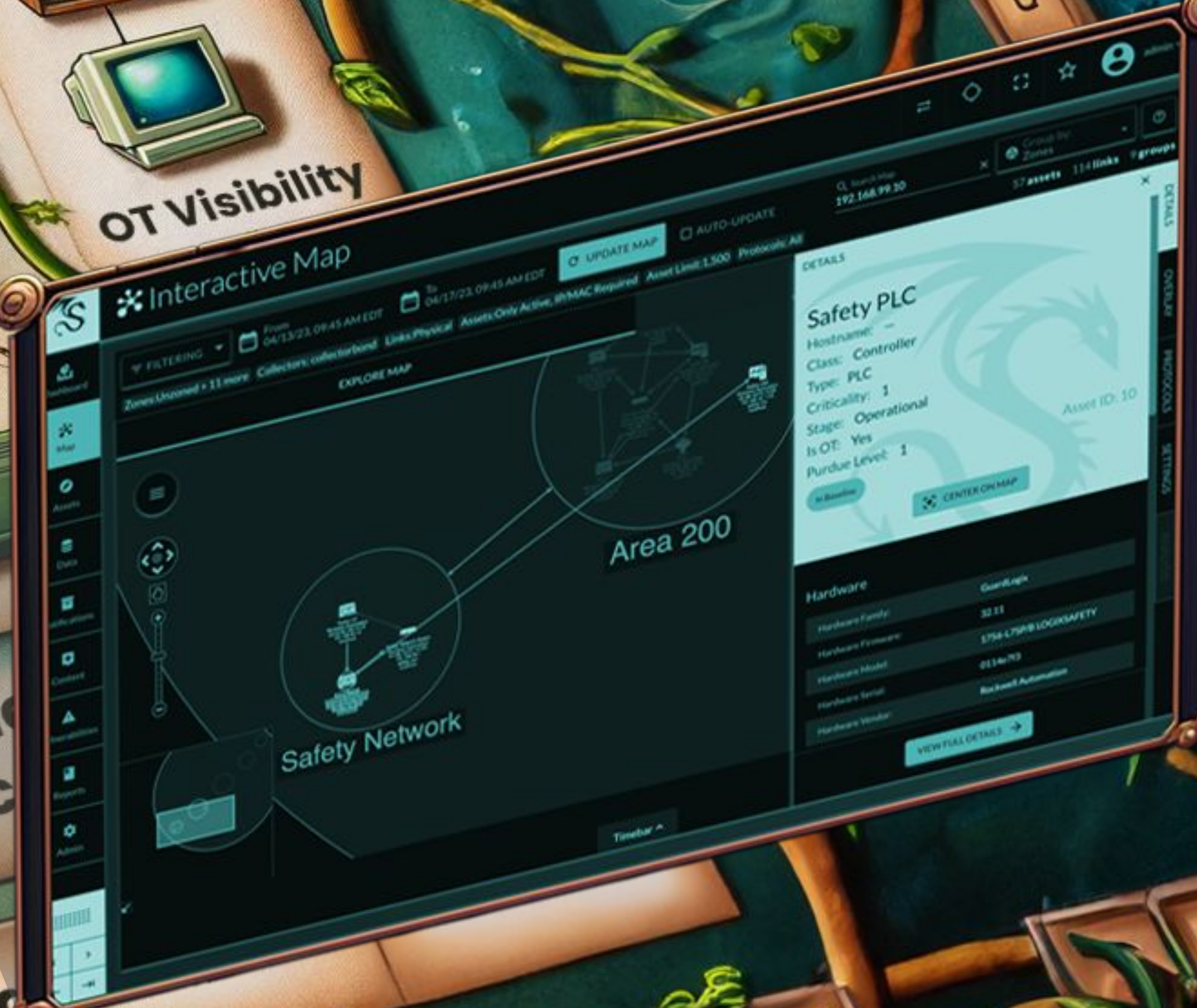
FINITE STATE



Safety Network
192.168.28.5



Area 200 Devices
192.168.118.134



From 04/13/23, 09:45 AM EDT

To 04/17/23, 09:45 AM EDT

Zones: Unzoned + 11 more · Collectors: collectorbond · Links: Physical · Assets: Only Active, IP/MAC Required · Asset Limit: 1,500 · Protocols: All

Search Map: 192.168.99.30

Group by: Zones

57 assets · 114 links · 9 groups

Safety PLC

Hostname: –
Class: Controller
Type: PLC
Criticality: 1
Stage: Operational
Is OT: Yes
Purdue Level: 1

Asset ID: 10

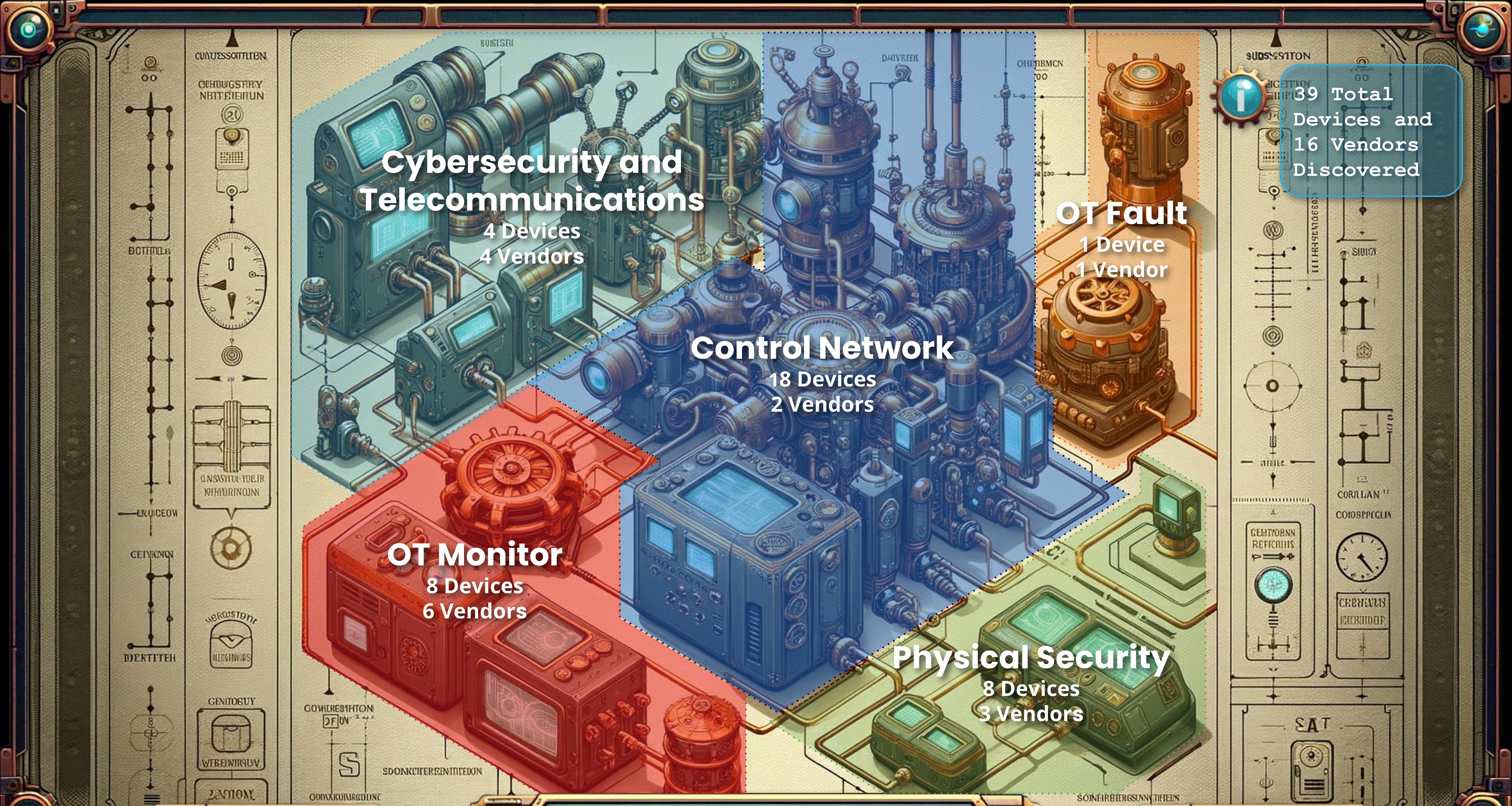
Hardware

Hardware Family:	GuardLogix
Hardware Firmware:	32.11
Hardware Model:	1756-L73SP/B LOGIXSAFETY
Hardware Serial:	0114c7f3
Hardware Vendor:	Rockwell Automation

Southern Company

Level 1: Inventory Jungle

FINITE STATE



39 Total Devices and 16 Vendors Discovered

Cybersecurity and Telecommunications
4 Devices
4 Vendors

Control Network
18 Devices
2 Vendors

OT Fault
1 Device
1 Vendor

OT Monitor
8 Devices
6 Vendors

Physical Security
8 Devices
3 Vendors

Level 1: Complete

Southern Company

FINITE STATE

Southern Company

Level 2: Vendor Valley

FINITE STATE

Hello [redacted]

Regarding [redacted], we regret to inform you that we are unable to provide the requested Software Bill of Materials (SBOM) at this time.

In May 2021, the Biden Administration issued an Executive Order on Improving the Nation’s Critical Infrastructure. [redacted] supports the U.S. government’s directives to improve critical infrastructure cybersecurity and to address complex multidimensional cybersecurity challenges affecting the world, the SBOM information is only available for certain product software released after September 14, 2022, in line with memorandum M-22-18 from the Office of Management and Budget.

The file image associated with the SHA-512 hash for which the SBOM was requested falls outside of this timeframe, and thus is unavailable for download.

Regards,

[redacted]

Side Quest: SBOM Drama

Hello [redacted]

Thank you for your request. We have provided your SBOMs, and they are available to download from our portal over the internet at the following link: [redacted].

Please remember that you are not allowed to load the SBOMs into any software or database that is connected to the internet, as it would be a violation of our legal agreement.

Regards,

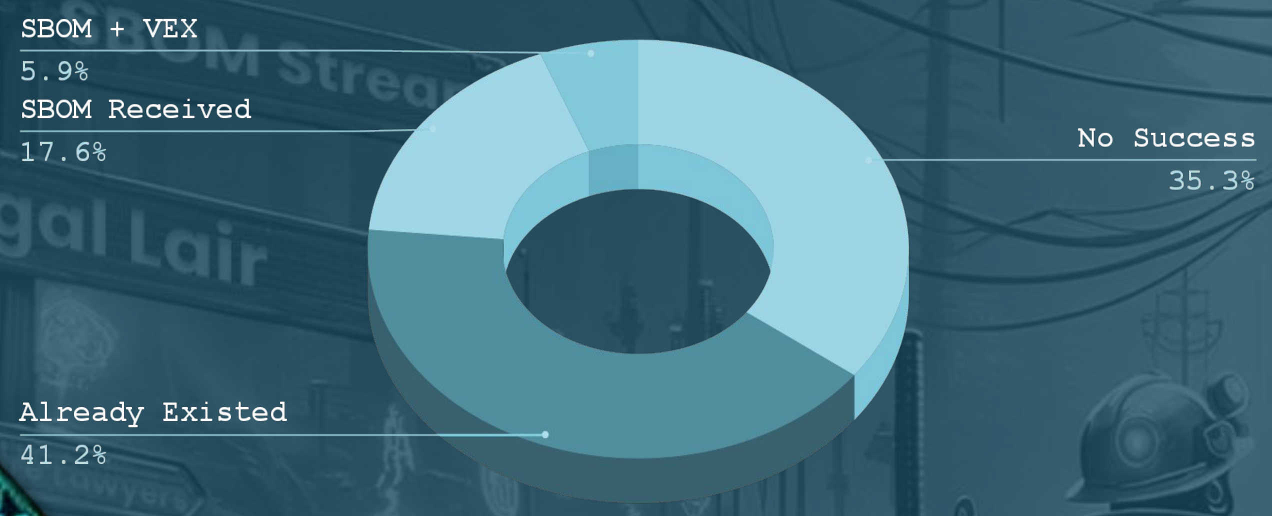
[redacted]

Southern Company

Side Quest: Restrictions

FINITE STATE

LEVEL 2 STATISTICS



- Average Days to Receive SBOM = 60 days
- Average Number of Emails / Meetings to Request SBOM = 12
- Percentage of Products Where SBOM Request was Denied = 58%

Southern Company

Level 2: Complete

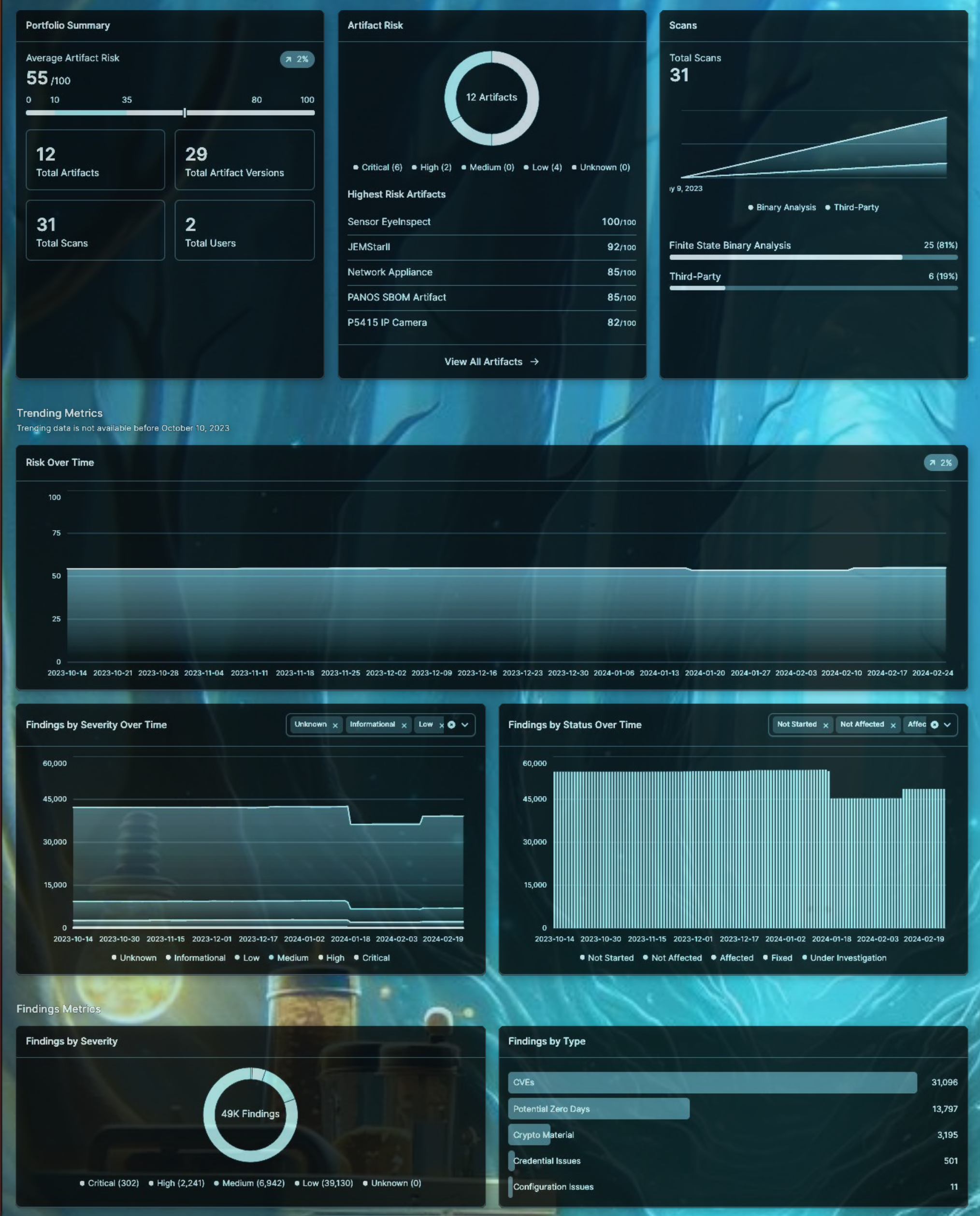
FINITE STATE

Level 3: The SBOM Enigma

SBOM Quality Metrics:

- SBOM Quality Scores:
  - Firmware 1 = 6.3/10
  - Firmware 2 = 6.3/10
  - Firmware 3 = 6.5/10
  - Firmware 4 = 6.5/10
  - Firmware 5 = 6.3/10
  - Firmware 6 = 6.3/10
- Errors:
  - Did not meet NTIA minimum SBOM requirements
  - Missing proper component identifiers

Firmware Analysis Report:



Portfolio Summary

Average Artifact Risk ↗ 2%

55 /100

0 10 35 80 100

12 Total Artifacts

29 Total Artifact Versions

31 Total Scans

2 Total Users

Artifact Risk

12 Artifacts

● Critical (6) ● High (2) ● Medium (0) ● Low (4) ● Unknown (0)

Highest Risk Artifacts

Sensor EyeInspect	100/100
JEMStarII	92/100
Network Appliance	85/100
PANOS SBOM Artifact	85/100
P5415 IP Camera	82/100

View All Artifacts →

Scans

Total Scans

31

Finite State Binary Analysis	25 (81%)
Third-Party	6 (19%)

Trending Metrics

Trending data is not available before October 10, 2023

Risk Over Time ↗ 2%

Findings by Severity Over Time

Unknown × Informational × Low ×

Findings by Status Over Time

Not Started × Not Affected × Affec

Findings Metrics

Findings by Severity

49K Findings

● Critical (302) ● High (2,241) ● Medium (6,942) ● Low (39,130) ● Unknown (0)

Findings by Type

CVEs	31,096
Potential Zero Days	13,797
Crypto Material	3,195
Credential Issues	501
Configuration Issues	11

Warning:
SBOM Mismatch

Firmware analysis found 72 more components than vendor SBOM.

Southern Company

Level 4: Verifying SBOM Truths

FINITE STATE

Level 5: The Vulnerability Hoard

Southern Company

FINITE STATE

Exploitability Analysis now activated. Collect VEX documents to reduce vulnerabilities.

Total vulnerabilities reduced by 99%.

Now showing only exploitable vulnerabilities.

Critical: 0

High: 3

Medium: 14

Low: 64

Level 6: Exploitability Enclave

Error: VEX exploitability data mismatch on CVE-2022-ABCDE. Inconsistent with penetration testing and threat intel results!

Side Quest: VEX Truth?

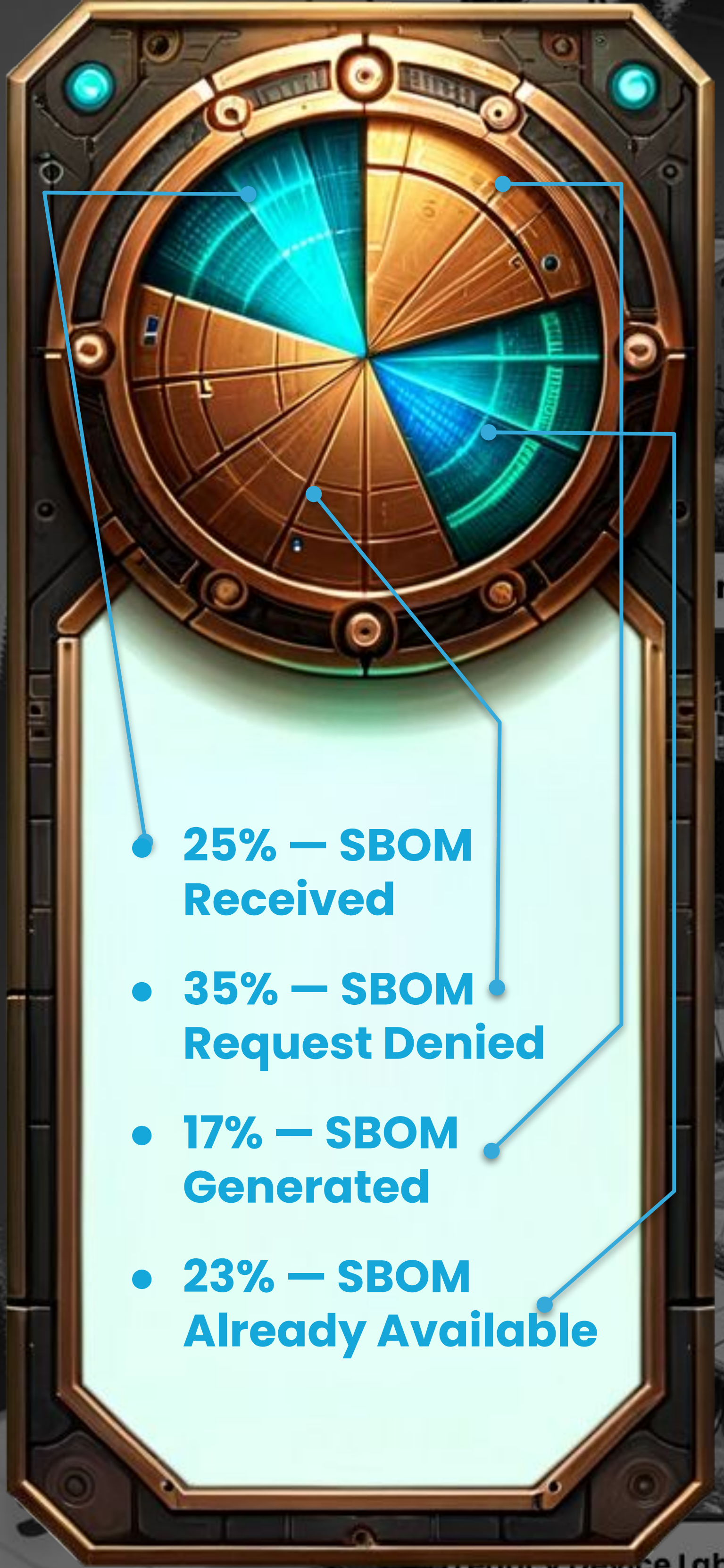
Stage 1: Mission Accomplished

- Enhanced Visibility Achieved
- Vulnerability Management Program Upgraded
- Regulatory Compliance Unlocked
- Supply Chain Risk Management Program Enhanced
- Vendor Accountability and Collaboration Achievement
- Community Engagement Activated

Southern Company

FINITE STATE

Gameplay Stats



Summary Statistics:

Average Time to Get SBOM

- 60 days from request to receipt

Average # of Components

- Linux-based Systems: 1,807
- Bare Metal / RTOS: 21

Average # of Vulnerabilities

- Linux-based Systems: 2,084
- Bare Metal / RTOS: 9

Average # of Emails/Meetings to request SBOM

- 12

Average numbers of vulnerabilities after VEX provided from Vendor

- 10 (according to Vendor)

Southern Company

FINITE STATE

Players and NPCs

Vendor Risk Management Team
Legal Team
Legal Team
Sales Team
OT Security Team
Telco Team
Substation Engineering Team
Product Engineering Team
Sales / Field Engineering Team
Cyber Security Team
Product Security Team
CEO / Executive Team
Condition Based Maintenance Team
Physical Security Team

Warp Speed Activated

Auto - Exploitability Potion Added

MITRE Entered the Game

Ameren Entered the Game

Scythe Entered the Game

Schneider Electric Entered the Game

EPRI Entered the Game

Southern Company

Stage 2: Coming Soon

FINITE STATE

Thank You!

- Number of vendors
- Time to respond
- Response rate
- SBOM quality vs. firmware analysis findings
- Exploitable vulnerabilities vs. non-exploitable

Ending Credits

Southern Company

FINITE STATE