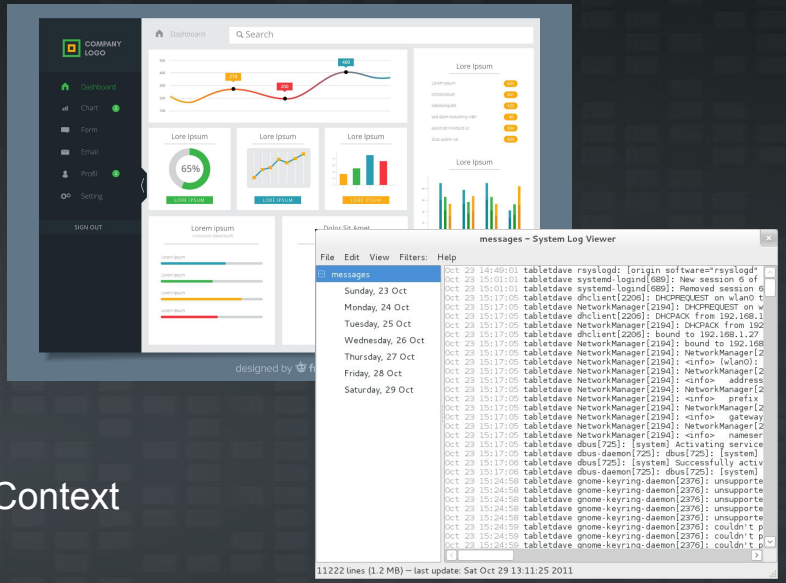
Unlock the Threat
Apply Storyboarding to the Cyber Arena

Aaron Boteler
Chief Technology Officer

CLOUDCURRENT
REVOLUTIONIZING CYBERSECURITY

Introduction

- Cybertool Market Forensics
  - Mixture of SIEMs and Traffic Sensors
  - Time-stamped Log Views / Alerts
  - Labor-intensive Incident Analysis

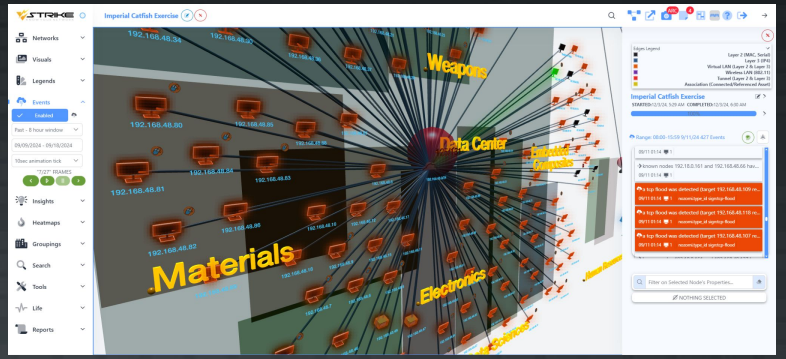


- Where is the picture?
  - Clustered Static Network Views 👉 Lose the Context
  - Dynamic-nature is lost handicapping analysis

- What if a dynamic visible storyline of cyber incidents is available?
  - Power of a Cyber Picture 👉 upskill all stakeholders to a clear understanding

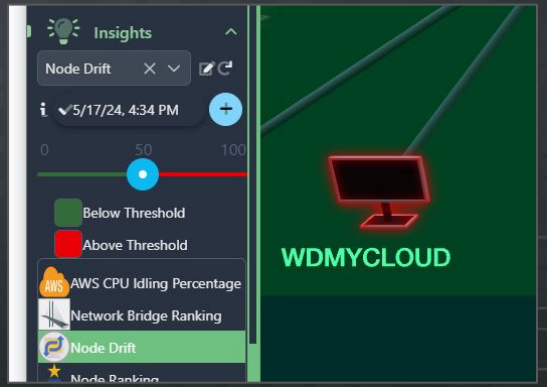
Cyber Arena

- How to develop that picture?
  - Ingest device configurations/asset scans
  - Ingest temporal events/alerts
  - Real Physical Layout Algorithm 👉Context!!!

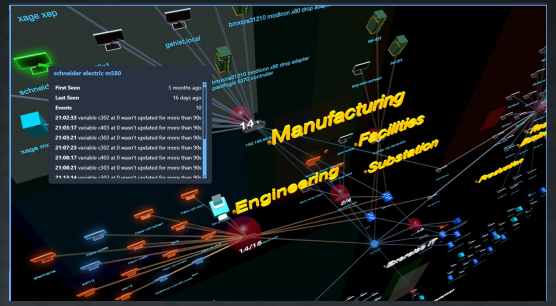


- VStrike's Cyber Platform is the Answer
  - Immersive 3D Dynamic Rendering Engine
  - Flexible Open Plugin Architecture
  - Data Fusion Engine

- VStrike's Visual Storyboarding
  - Create Visible Actionable Intelligence
  - Forward, Backward, Pivot Timeline 👉 Understand!!!



Cyber Storyboarding



- Overlay Time-stamp Key Activities
  - From SIEMs, Sensors, Windows Defender Logs, and more
  - Tcpfloods, Encrypted Comms, Login Failures, Risky URLs, and more
  - CPU Spikes, Ingress Spikes, Logins, and more

- Develop a Storyline with pause, step back, step forward, animate, and timeline pivot

Our Storyboarding offers a way to pause, step, reflect, and share evolving intuition and thoughts leveraging the power of visual representation giving brain-boosting benefits that upskill the entire team

- Storyboard live activity hunting for bad actor, bots, and other security incidents
  - See the beginning, middle, and end of the incident story unfold - valuable threat intelligence
  - Gain time and space with early threat detections as they develop
  - Develop actionable intelligence to create realistic false targets and decoys

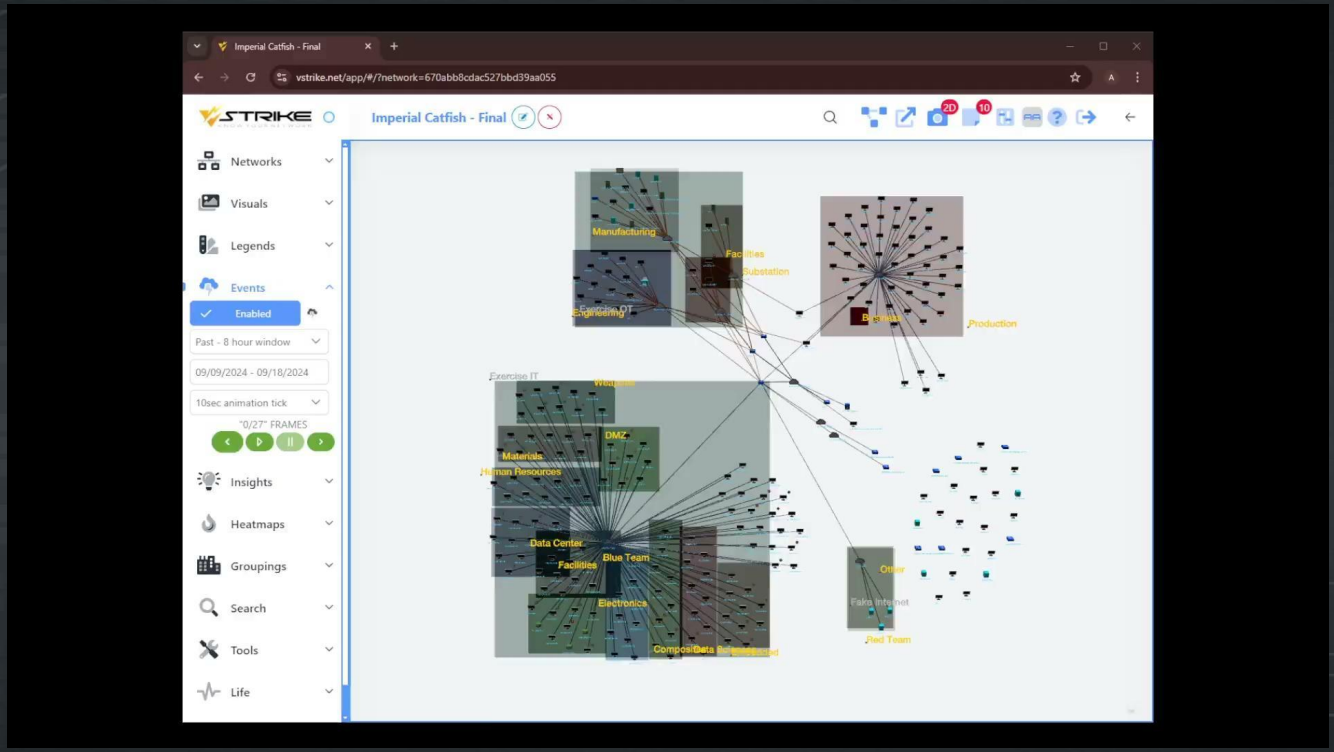
VStrike’s Success

VStrike Pilot Deployment in NNSA/DOE Imperial Catfish Exercise 2024 in a Mixed IT/OT Energy infrastructure with the Red Team simulating a Volt Typhoon-like attack.

- Provided Situational Awareness of all Major Network Activities
  - Leveraged the other cyber tool and sensor data feeds to create the visual storyboard

- Provided animation of the Key Events
  - Provided a clear understanding through the storyboarding (unique among the vendors)

Exercise Key Events Video

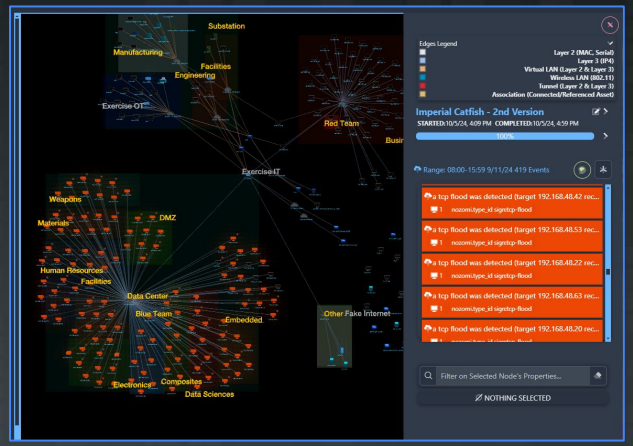


Exercise Key Events

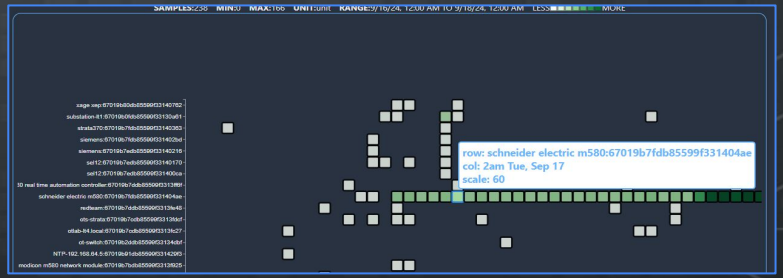
Exercise Period from 9/9/2024 to 9/20/2024

To 9/11 07:59	Initial scanning IPs of Interest - 192.168.67.104, 162.159.36.2
To 9/13 15:59	Heavy TCP Flooding Heavy IP Spoofing OT Consumer Reconfiguration Blue Team responds to tcpflooding from haw-dmz-wks5 Few SSH Links
To 9/18 23:59	Heavy TCP Flooding tails off Continuous tcp/443 links established Continuous Network Scanning IPs of Interest - 192.168.65.17 (substation-lt1), 192.168.48.24 (haw-dmz-wks5), 192.168.48.16, 192.168.48.150, USB Detection at haw-ef-wks5 OT Device Affected - schneider electric m580

9/14 0800 to 1559 - TCP Flooding



Hour-by-Hour Behavioral Event Activity



Summary

- One-of-a-kind Cyber Storyboarding Capability in a 3D Cyber Arena
- Proven breakthrough with the right data and plugins
- Powerful Cyber Forensics unveiling the digital trails for real Threat Intelligence
- Provides Dynamic Security Posture

With the right data, VStrike uncovers what is going-on, upskills the team, and provides insights to the defenders, managers, and maintainers

DEMO

NEXT STEPS?

Thank You!

Available for Further Discussions
Flyers Are Available