
Visualizing your security posture from link, to gateway, and beyond..
MIND THE GAP
CYBERNETIQ.ca

Joe Cummins

CTO / Founder

CYBERNETIQ

Cyber Security is a series of interconnected & complex challenges

CYBERNETIQ

#thechallenge

SITUATION

01

CURRENT

02

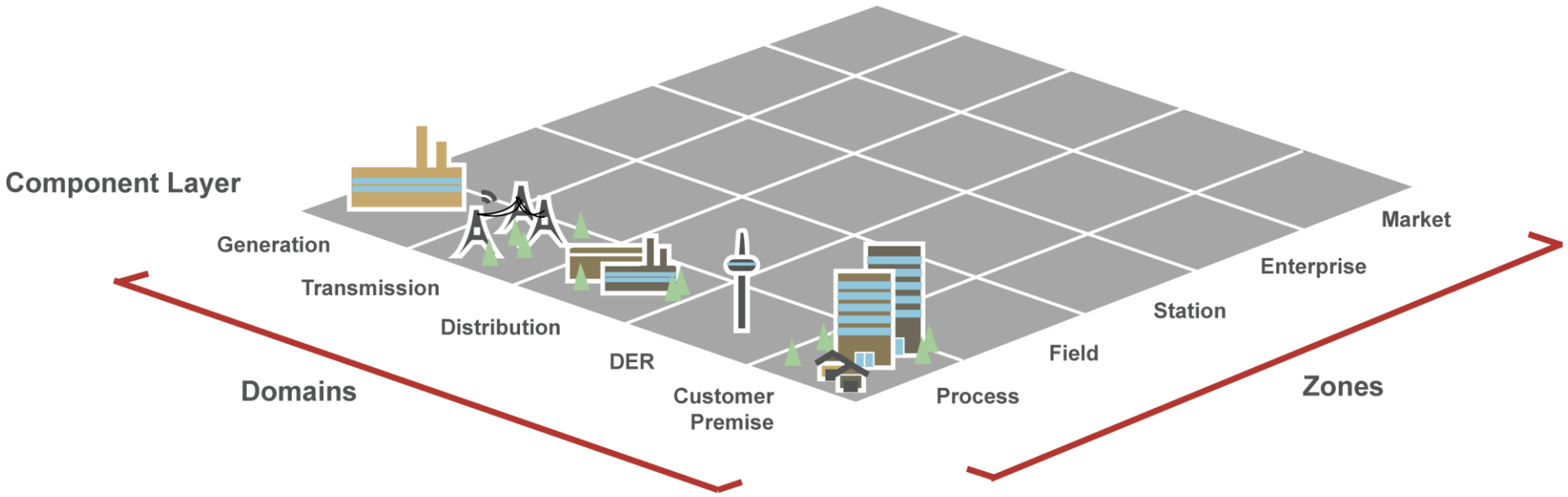
FUTURE

CYBERNETIQ

#thechallenge

SITUATION

CURRENT

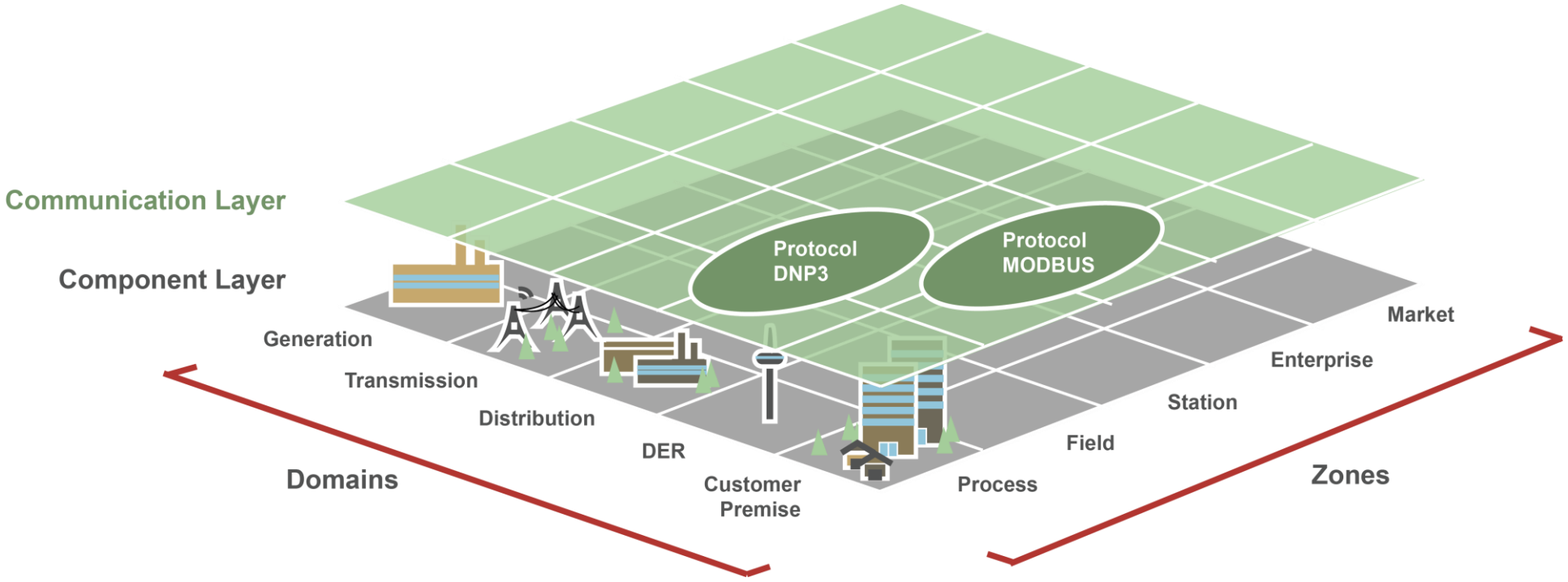


CYBERNETIQ

#thechallenge

SITUATION

CURRENT

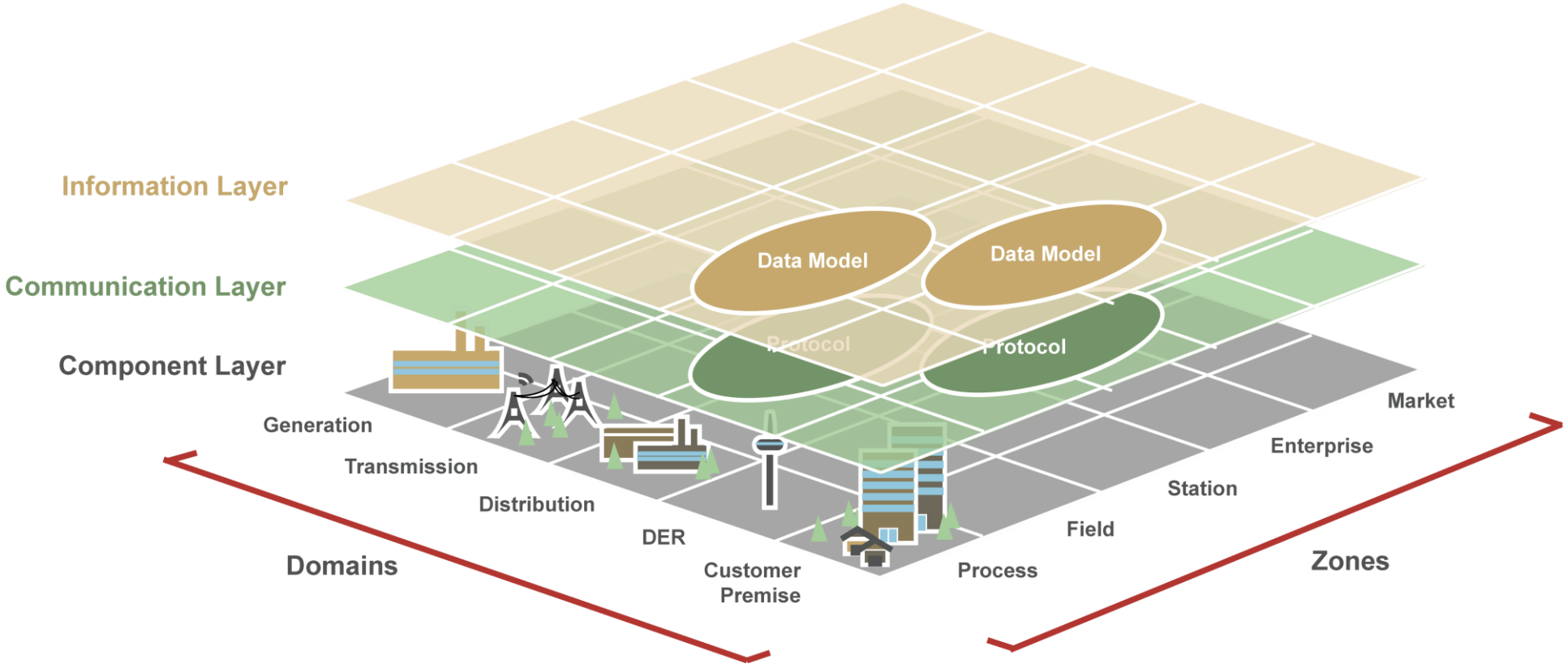


CYBERNETIQ

#thechallenge

SITUATION

CURRENT

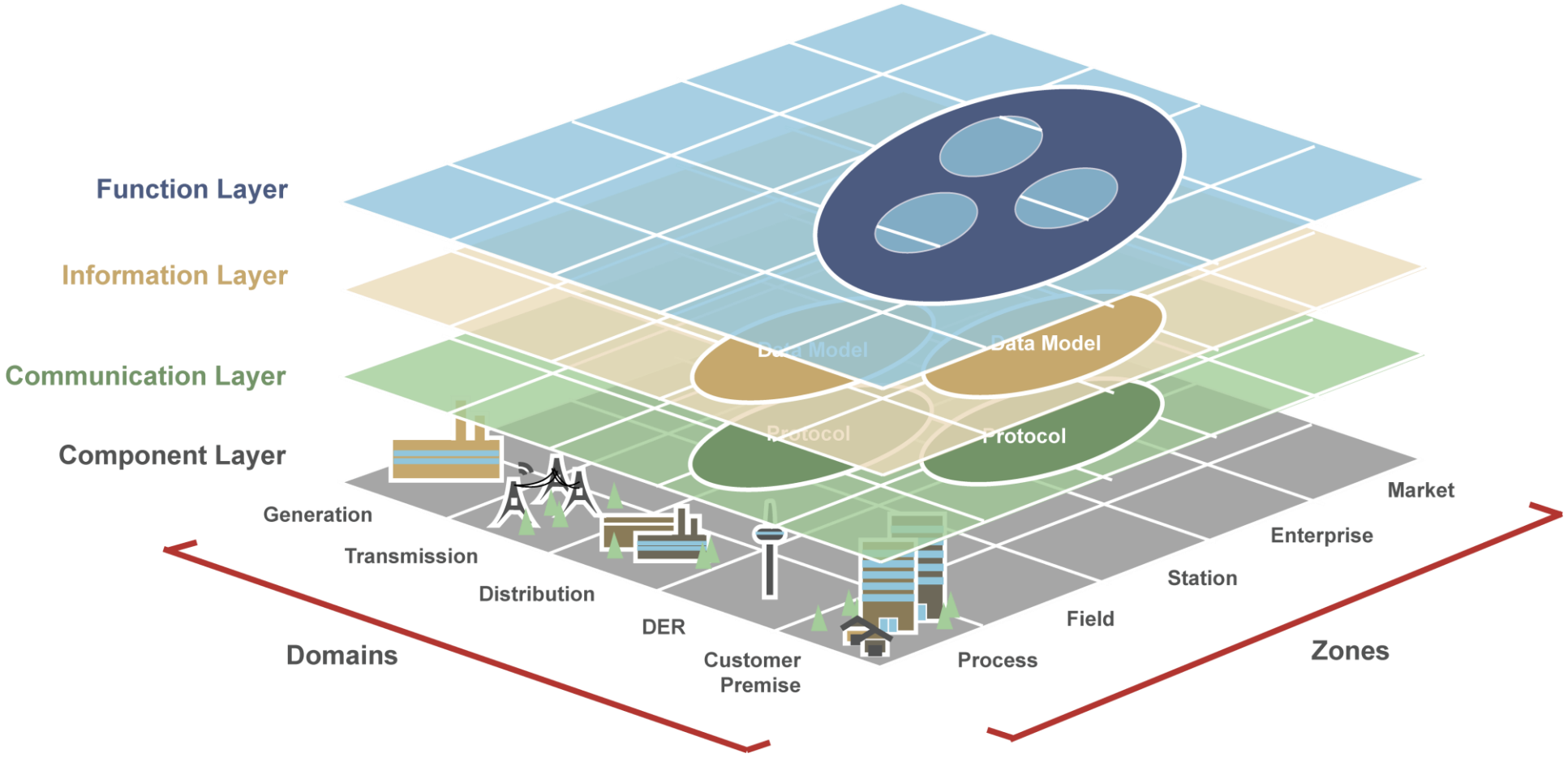


CYBERNETIQ

#thechallenge

SITUATION

CURRENT

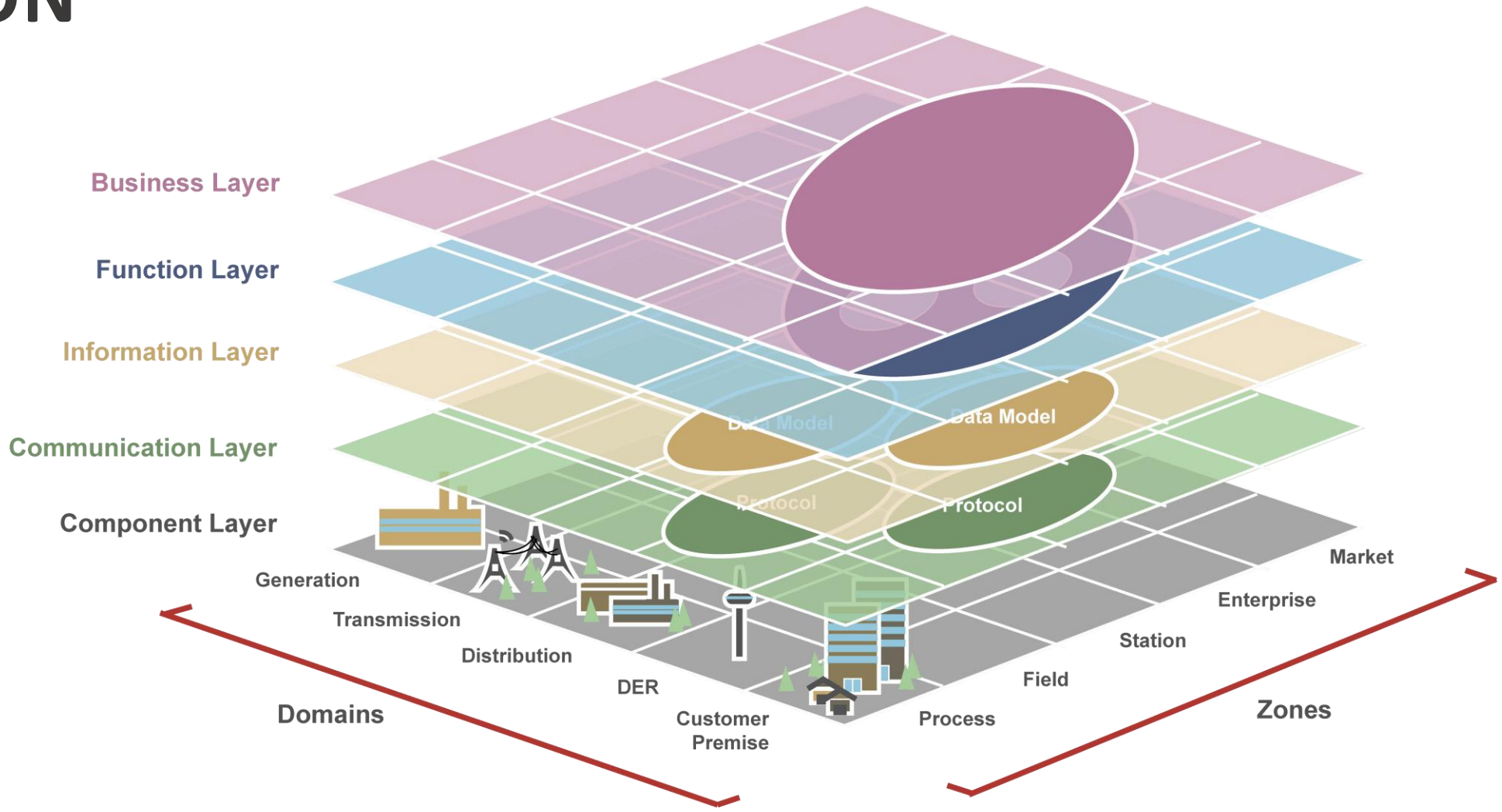


CYBERNETIQ

#thechallenge

SITUATION

CURRENT

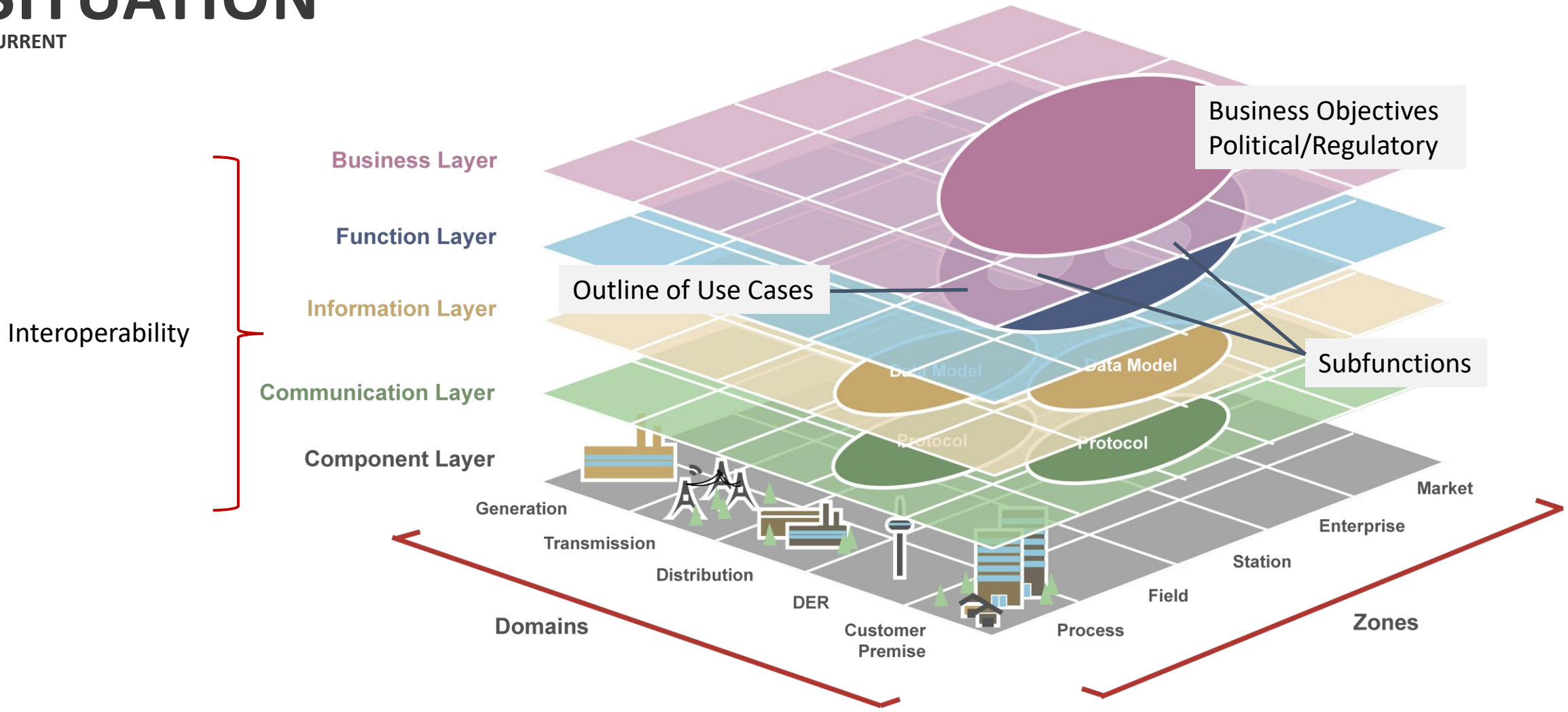


CYBERNETIQ

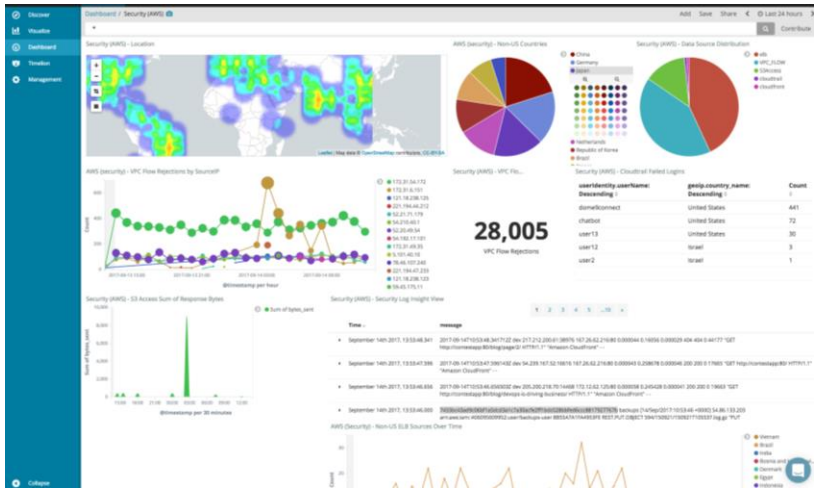
#thechallenge

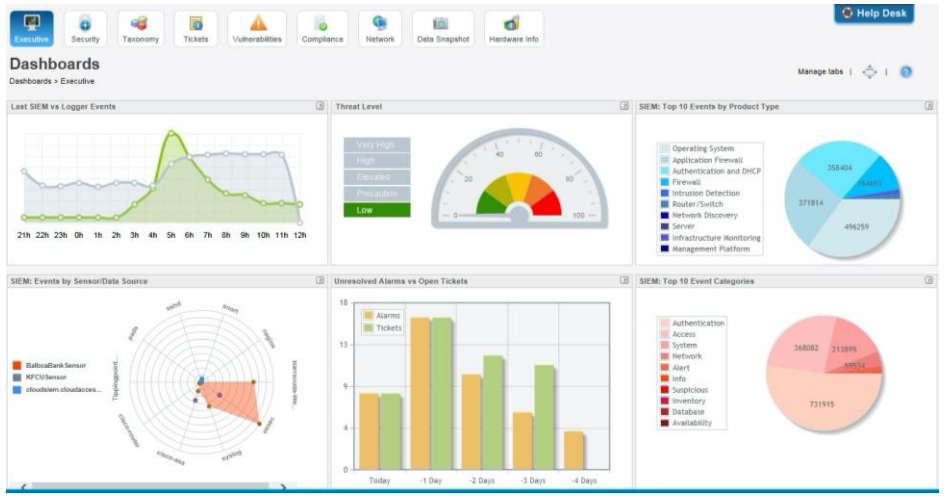
SITUATION

CURRENT



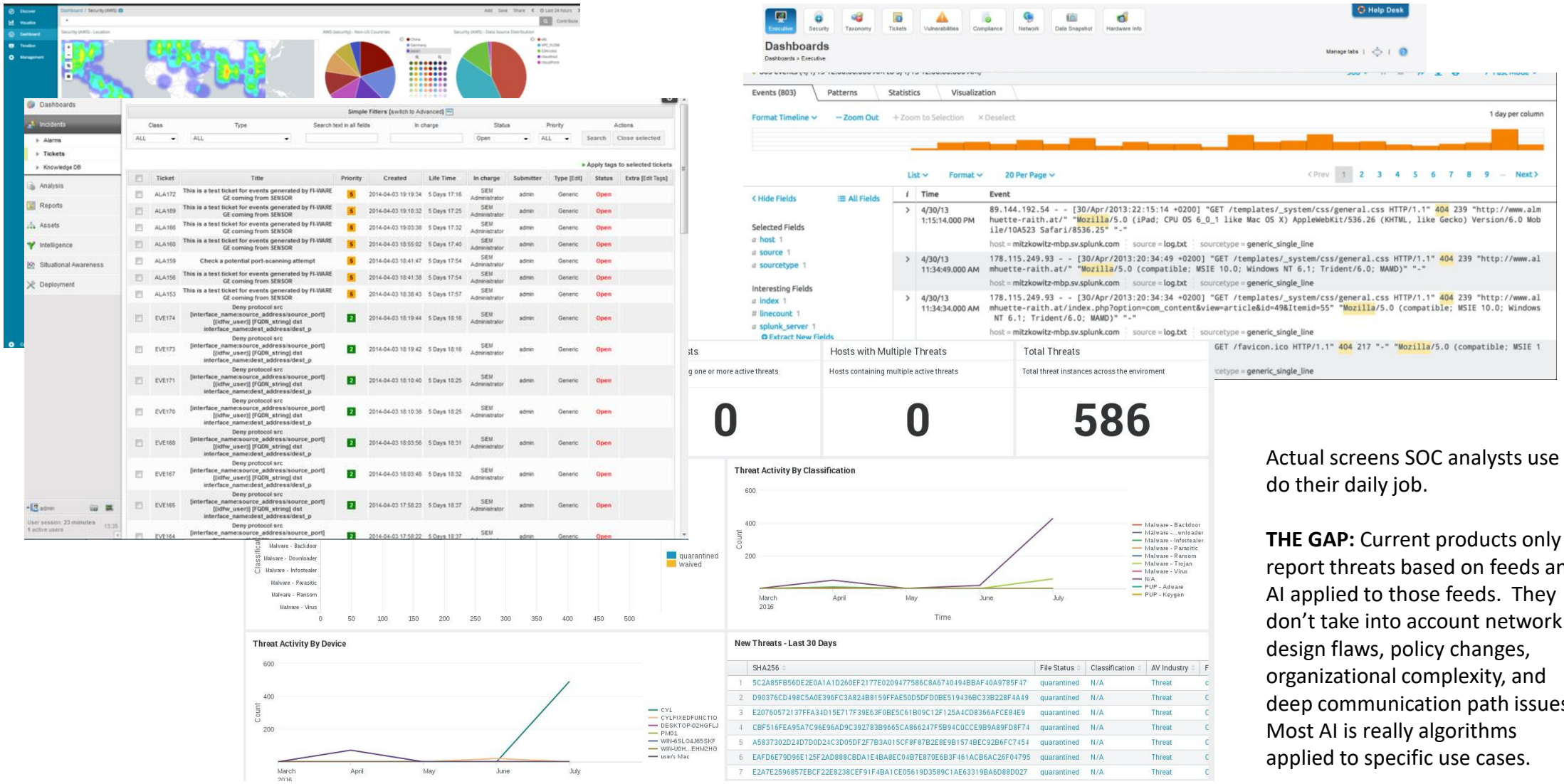
CYBERNETIQ





Typical SIEM interfaces when they're being marketed. "Pretty screens" appear to make cyber security simple. These are great for executive summaries and seeing trends.

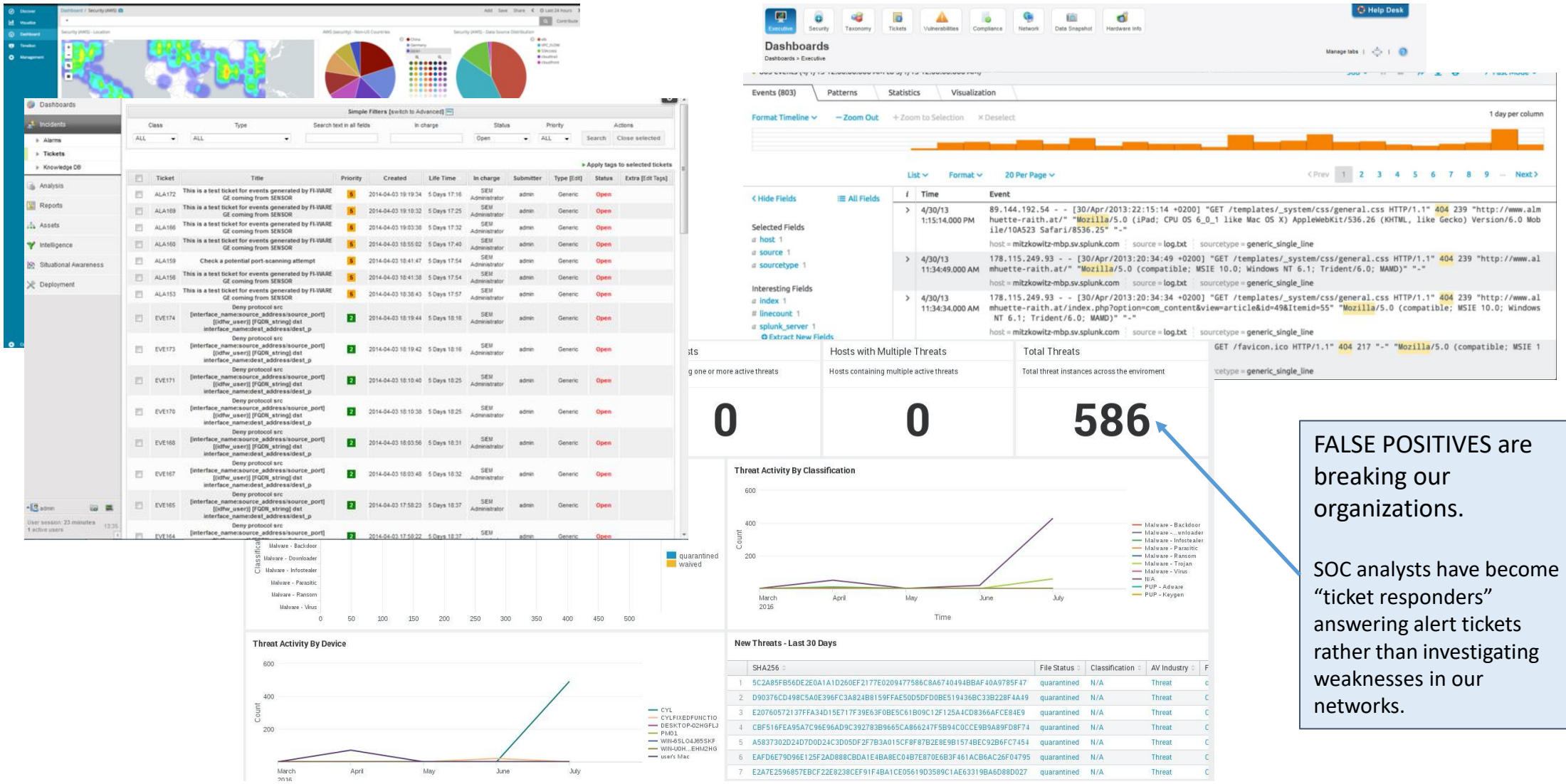
CYBERNETIQ



Actual screens SOC analysts use to do their daily job.

THE GAP: Current products only report threats based on feeds and AI applied to those feeds. They don't take into account network design flaws, policy changes, organizational complexity, and deep communication path issues. Most AI is really algorithms applied to specific use cases.

CYBERNETIQ



FALSE POSITIVES are breaking our organizations.

SOC analysts have become “ticket responders” answering alert tickets rather than investigating weaknesses in our networks.

CYBERNETIQ

#reports

PSC CCRR

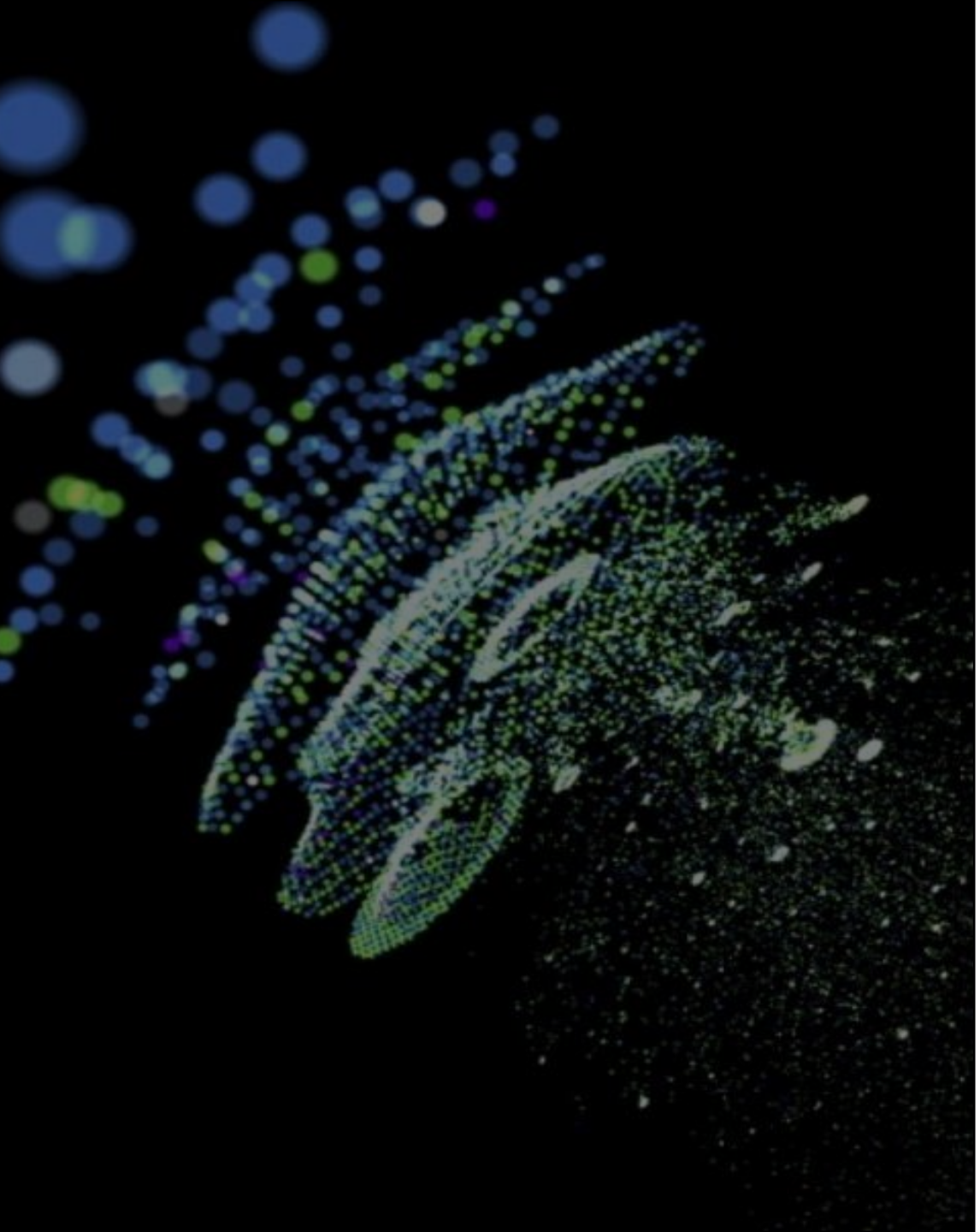
01

Objective

02

Findings

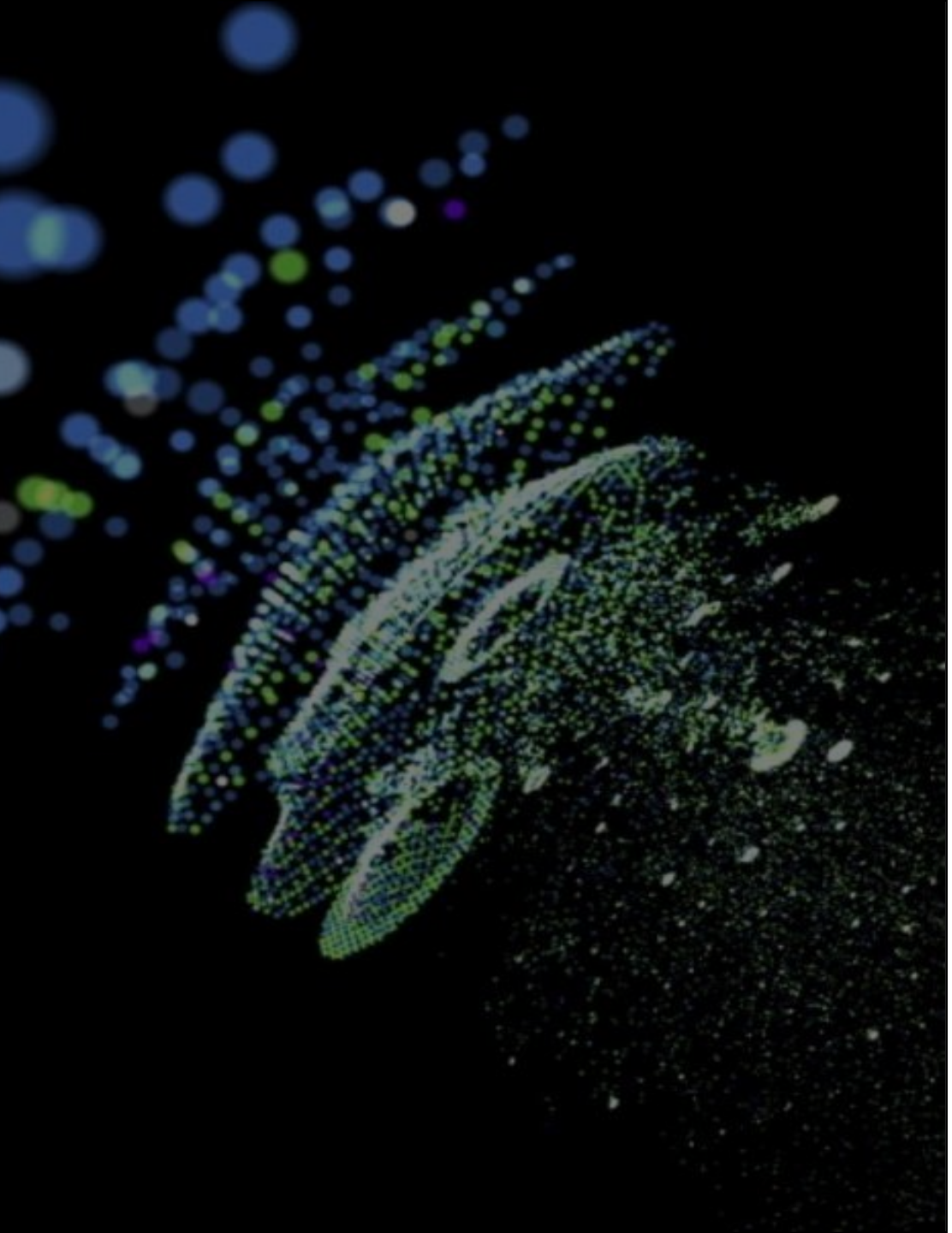
CYBERNETIQ



Universal Information Security Challenges

- Performance of IT Assessments of Enterprise and Automation networks is unpredictable, delicate, and risky!
- Requires in-depth understandings of:
  - Protocols, Devices, and entire Systems
- Existing tools:
  - bulky, costly, do not meet baselines
  - Generic Standards
  - Generate too many false positives
- Needed:
  - Lightweight, Risk Analysis Framework
  - Repeatable (Trending / Metrics)
  - Gap / Overlap analysis (Functionality / Optimization)
  - Identify exposures (Security / Awareness)
  - Business Value Proposition / Procurement

- **Simple** unified solution for mapping Resilience!



Universal Information Security Outcomes

- Contain, Identify, Control – 100% of Client network Ecosystem through “multiple source” inclusion
  - Overlap / Overlay
  - Network Architecture, Network Configuration
  - Vulnerability data / Network Mapping
  - Traffic / Syslogs / Netmon / Netflow
- Integrate existing security appliances
  - Network Traffic / System Applications
  - Network Vulnerability Management
  - Network Architecture / Endpoint
- Instantly Locate system / network gaps
  - Remediate weaknesses
  - Isolate Segmentation gaps
  - Define actionable mitigations
- Build / Change / Expand / Evaluate
  - Network Infrastructure modifications
  - Network Segmentations failures
  - Effective Network Security Posture

#thechallenge

FUTURE- is NOW!

01

Problem Analysis

02

CLAW - a 3D Virtual Cyber Solution

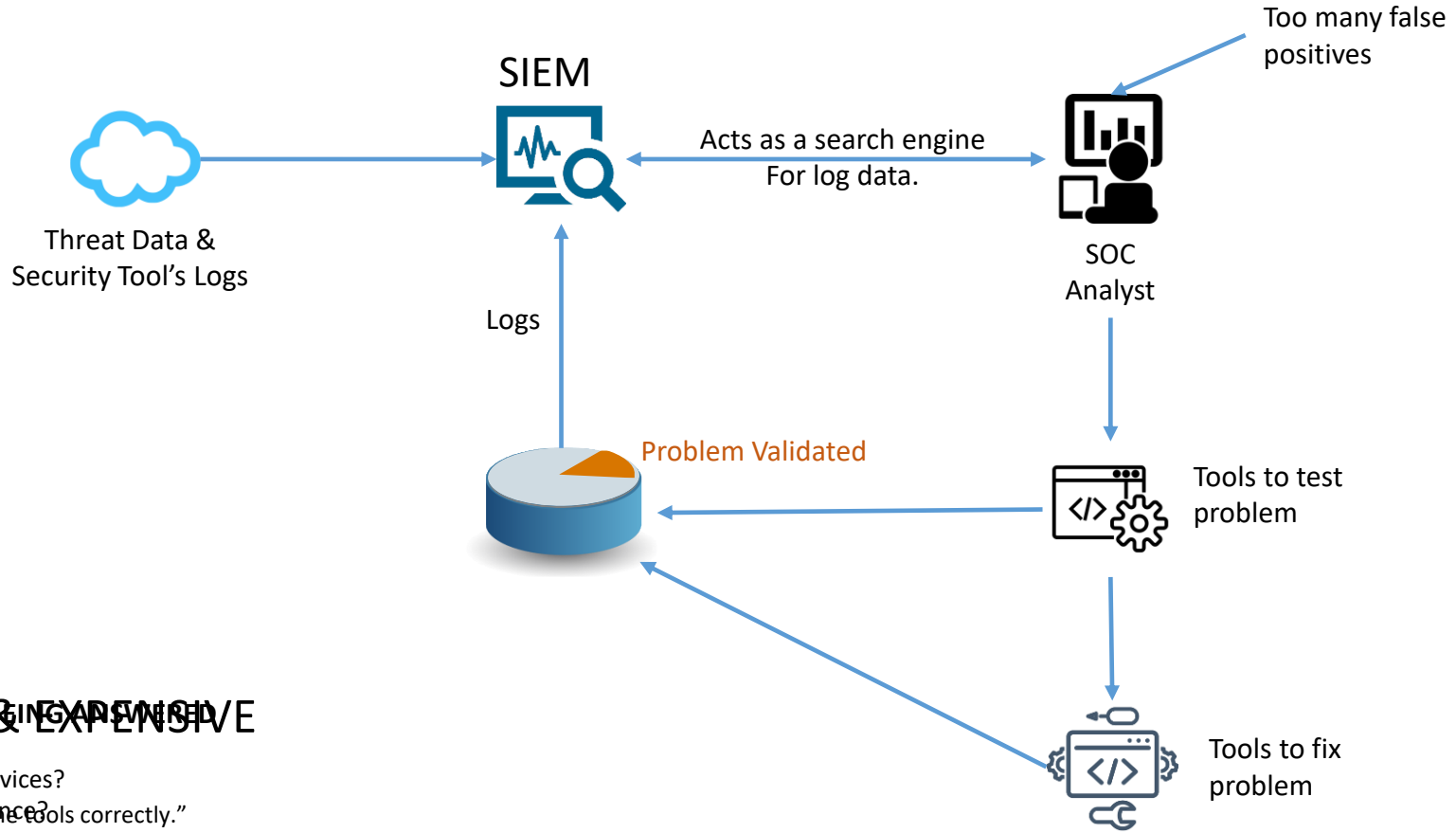
CYBERNETIQ

#thechallenge

FUTURE- is NOW!

Problem Analysis

“We treat security as device-centric weaknesses”



COMPLEXITY = SLOW & EXPENSIVE

OTHER CRITICAL QUESTIONS NOT BEING ANSWERED

- Where is this device in my network?
- How is it communicating to other devices?
- Is it functioning at optimal performance?
- How is interacting with my firewall rules?
- What protocols is the device using?
- Are these devices different from other similar devices?
- Where is this device in proximity to my sensitive data?

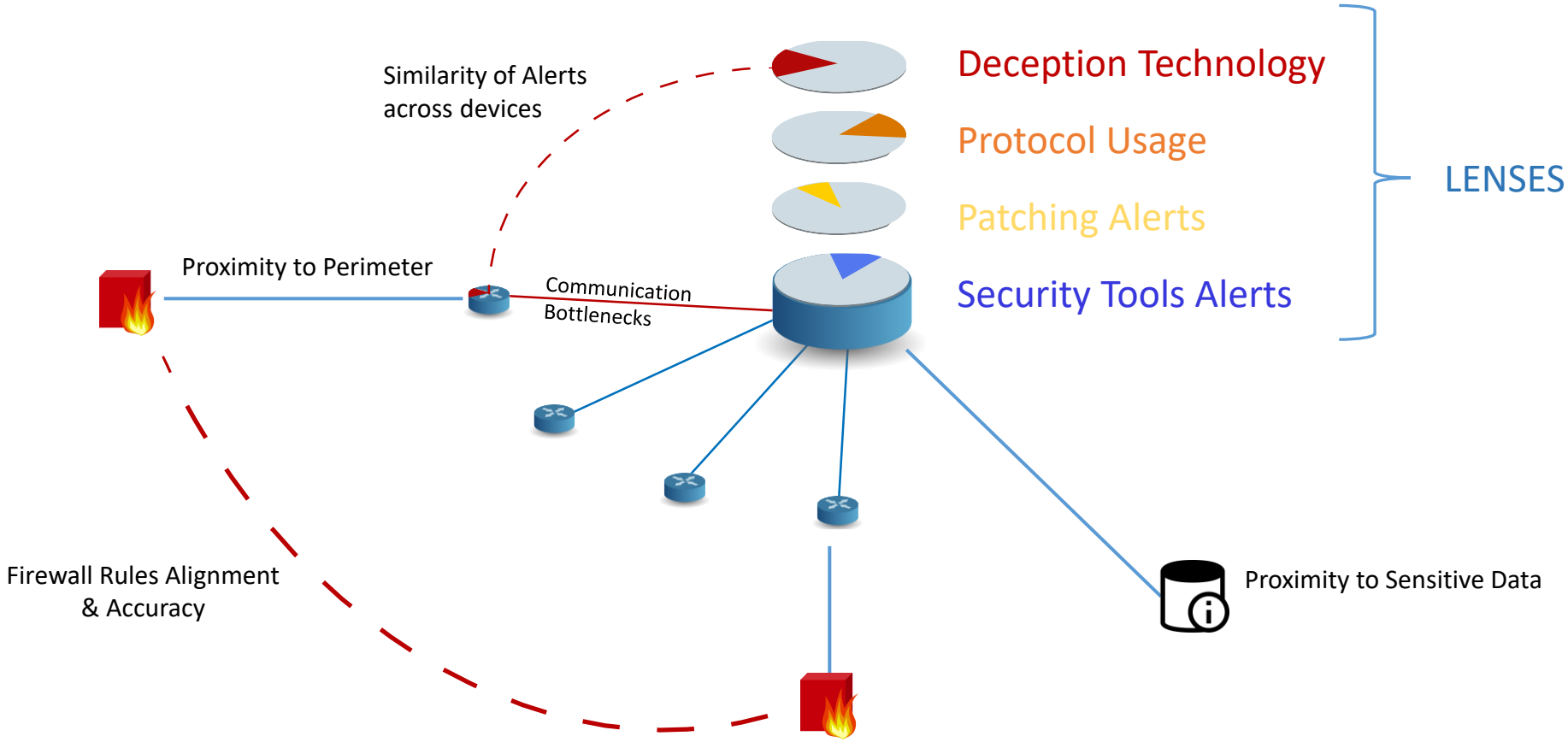
- “We have too many products”
- “I don’t even know if we are using the tools correctly.”
- “Too many false positives”
- “I can’t tune this tool, EVER!”
- “My security budget is out of control.”
- “I can’t keep qualified people.”
- ”I just need to meet compliance.”

CYBERNETIQ

#thechallenge

FUTURE- is NOW!

Problem Analysis



CYBERNETIQ

#reports

Discoveries

01

Problem Analysis

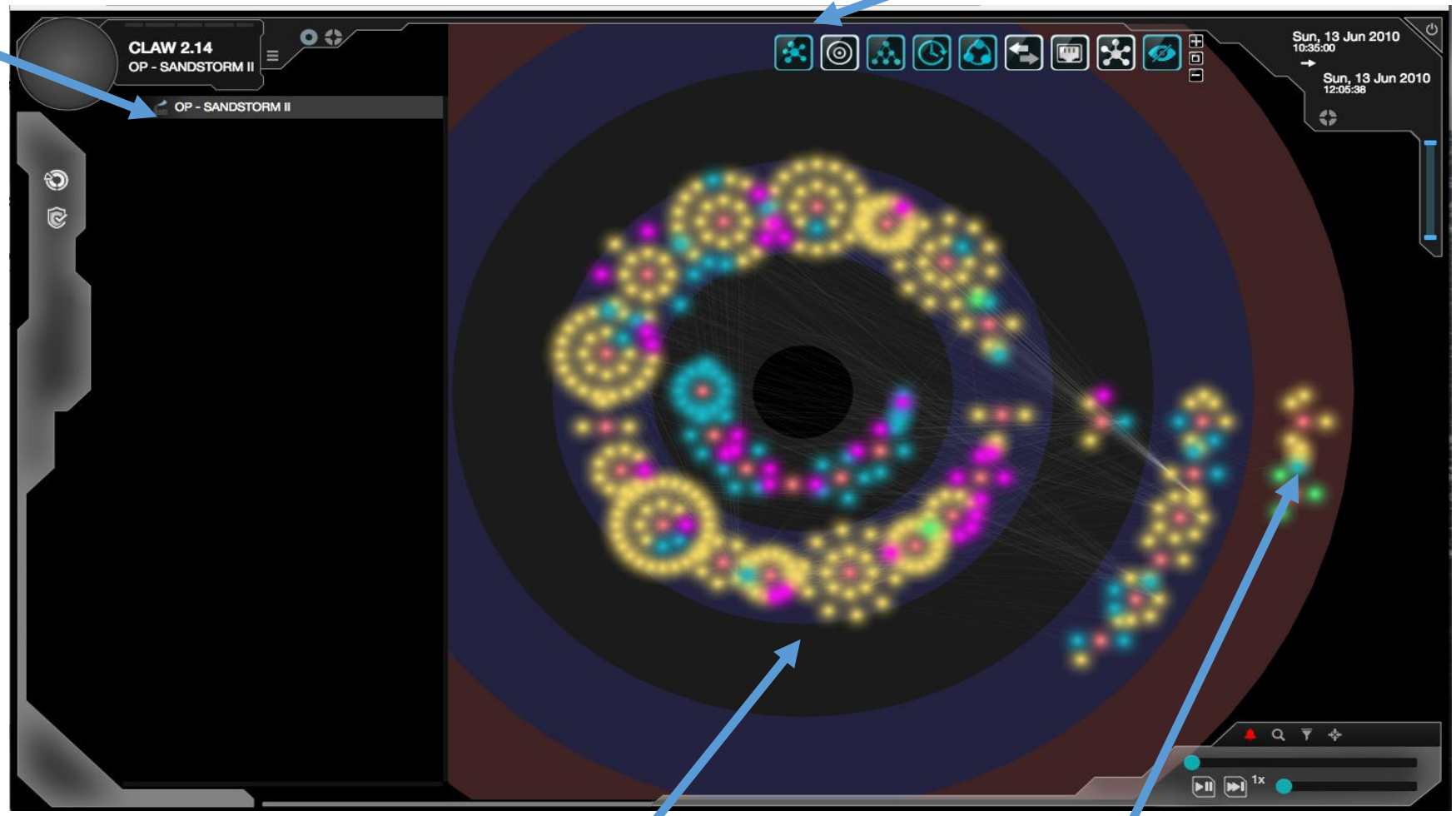
02

CLAW - a 3D Virtual Cyber Solution

CYBERNETIQ

Select from multiple “lenses” and Models to animate the dataset

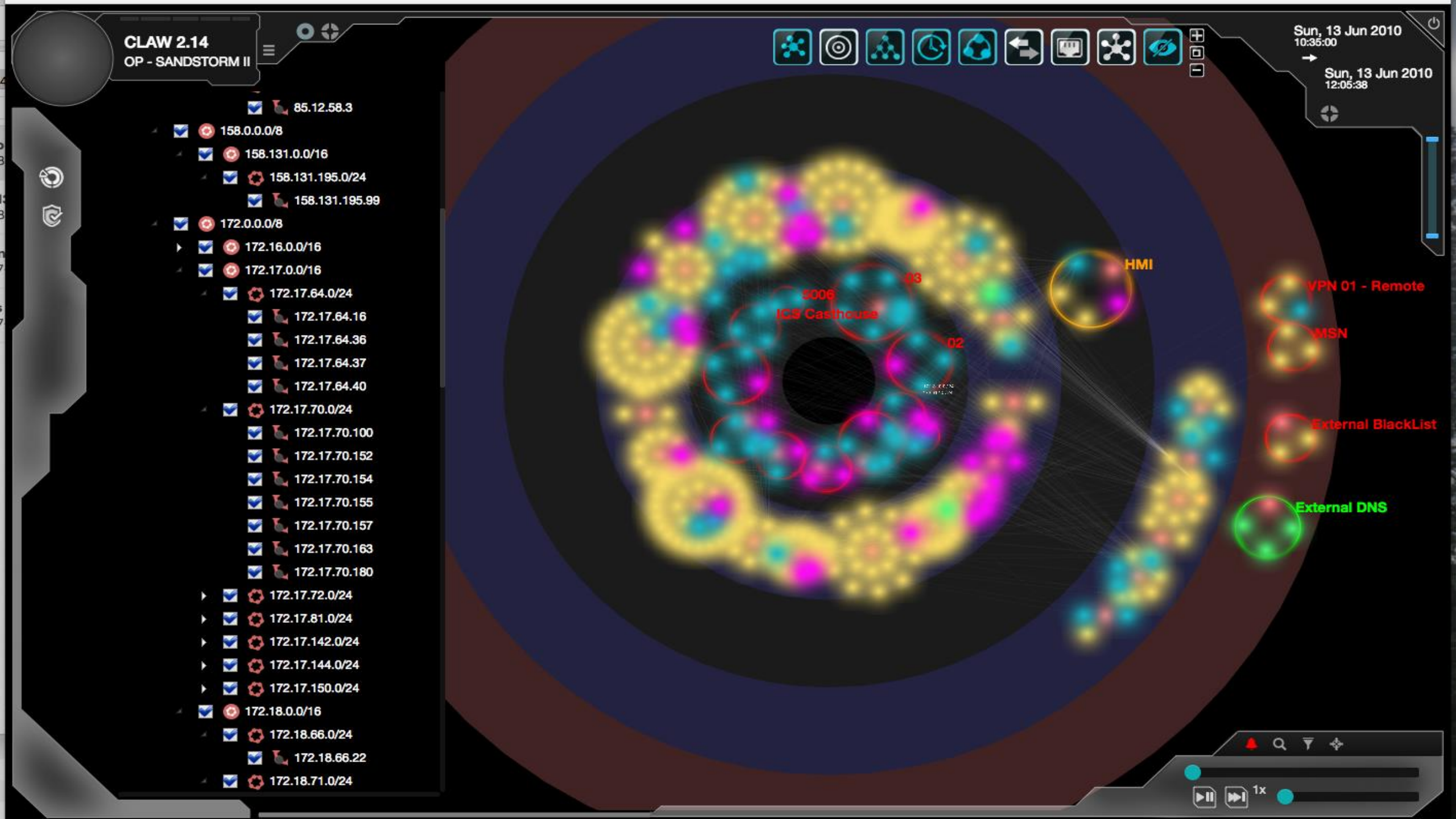
Tree View
Org, Location, Netblock, Subnet, Device

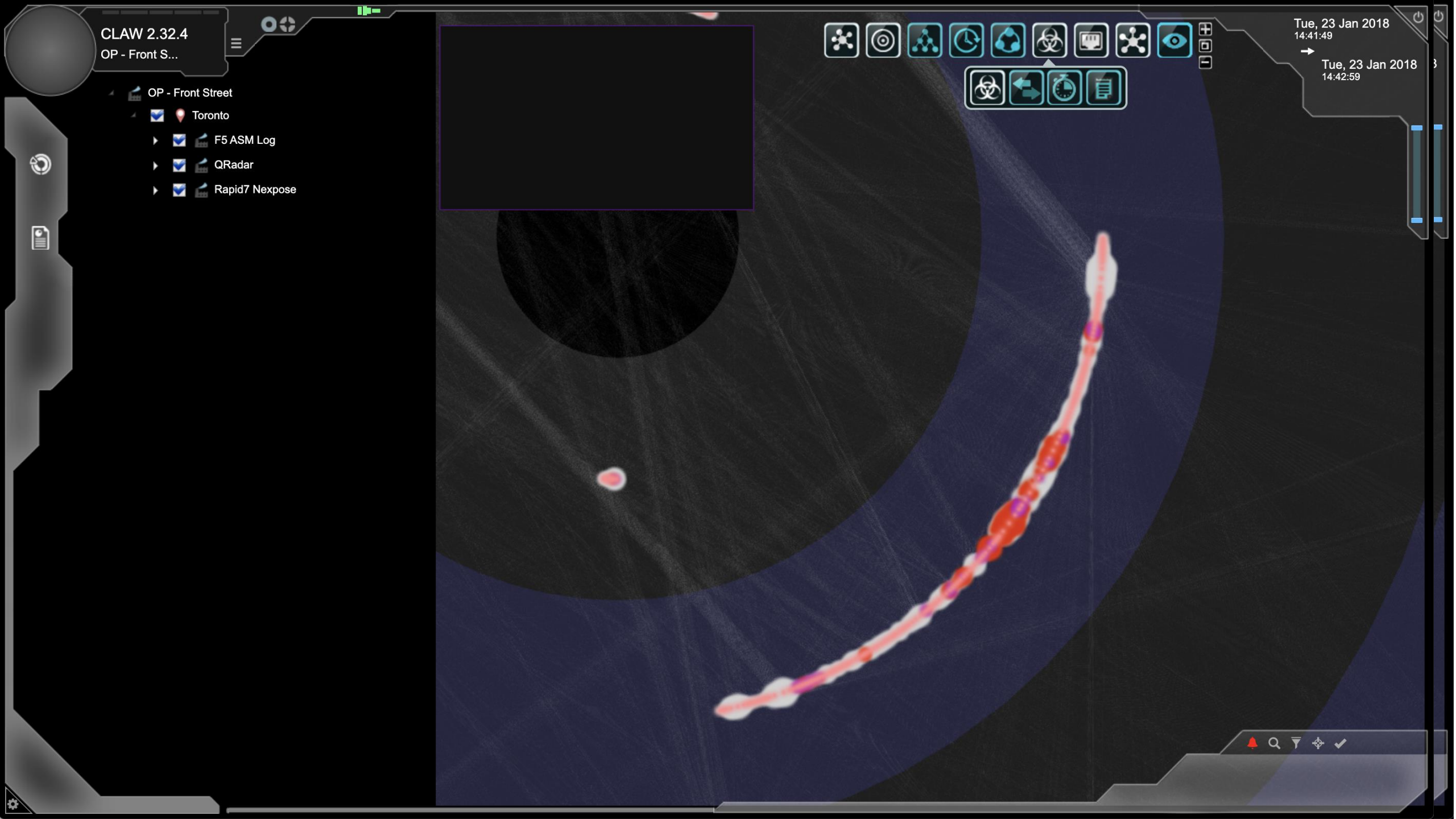


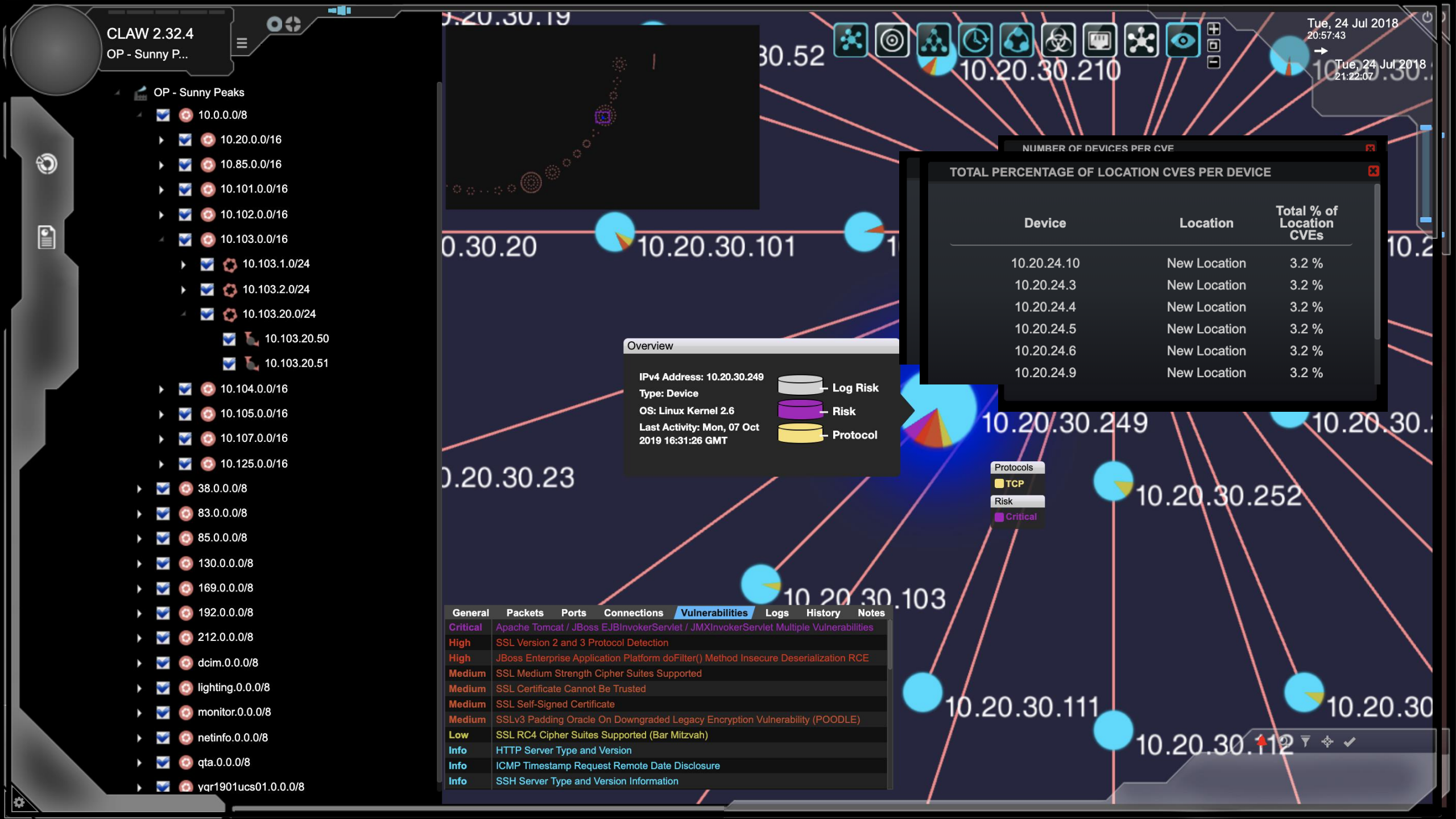
Defence In Depth
Lens Canvas

Interactive Nodes

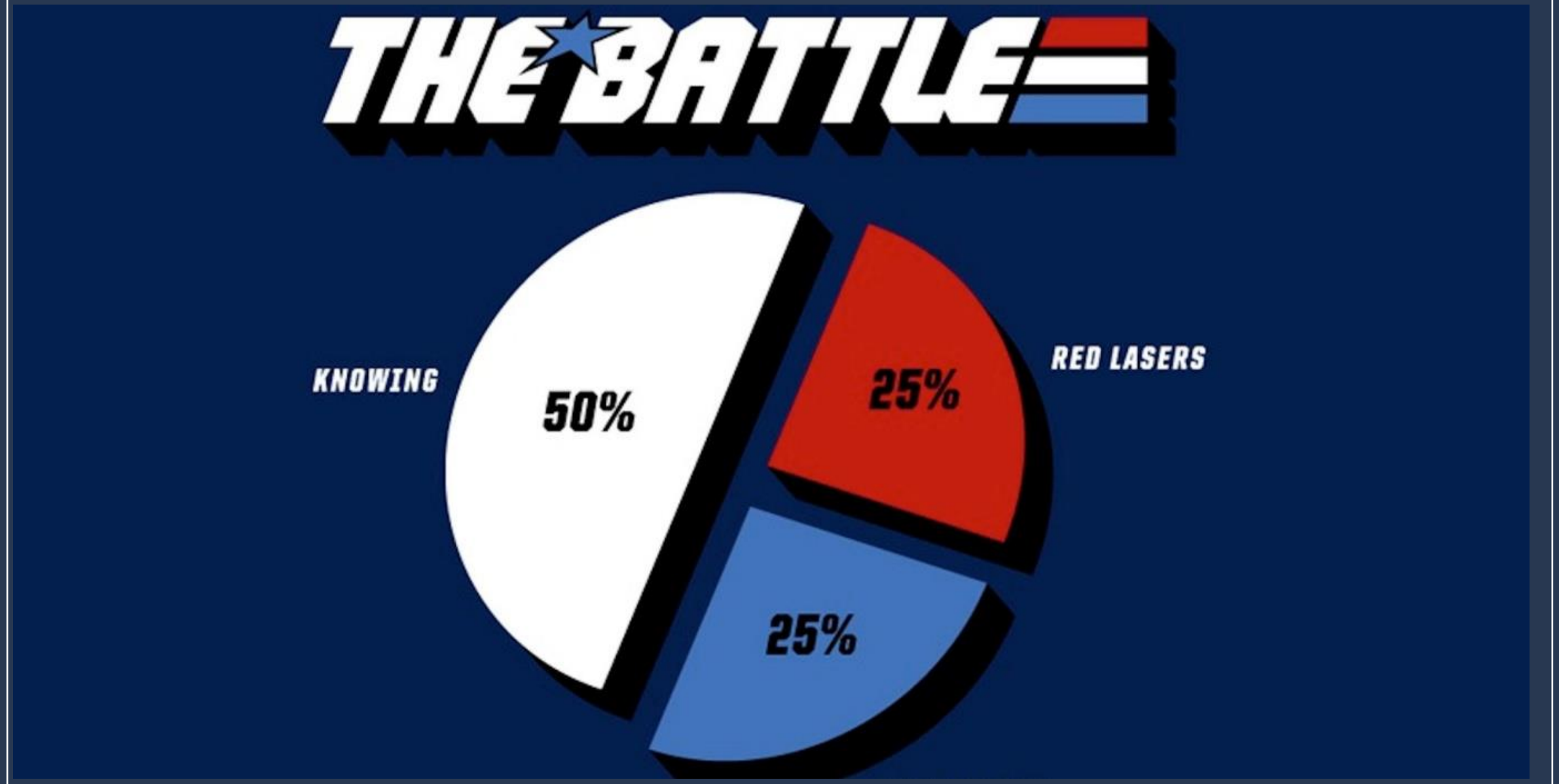
CYBERNETIQ


CLAW 2.14
OP - SANDSTORM II
85.12.58.3
158.0.0.0/8
158.131.0.0/16
158.131.195.0/24
158.131.195.99
172.0.0.0/8
172.16.0.0/16
172.17.0.0/16
172.17.64.0/24
172.17.64.16
172.17.64.36
172.17.64.37
172.17.64.40
172.17.70.0/24
172.17.70.100
172.17.70.152
172.17.70.154
172.17.70.155
172.17.70.157
172.17.70.163
172.17.70.180
172.17.72.0/24
172.17.81.0/24
172.17.142.0/24
172.17.144.0/24
172.17.150.0/24
172.18.0.0/16
172.18.66.0/24
172.18.66.22
172.18.71.0/24
Sun, 13 Jun 2010
10:35:00
Sun, 13 Jun 2010
12:05:38
HMI
03
5006
ICS Casthouse
02
VPN 01 - Remote
MSN
External BlackList
External DNS
1x


CLAW 2.32.4
OP - Front S...
OP - Front Street
Toronto
F5 ASM Log
QRadar
Rapid7 Nexpose
Tue, 23 Jan 2018
14:41:49
Tue, 23 Jan 2018
14:42:59


CLAW 2.32.4
OP - Sunny P...
OP - Sunny Peaks
10.0.0.0/8
10.20.0.0/16
10.85.0.0/16
10.101.0.0/16
10.102.0.0/16
10.103.0.0/16
10.103.1.0/24
10.103.2.0/24
10.103.20.0/24
10.103.20.50
10.103.20.51
10.104.0.0/16
10.105.0.0/16
10.107.0.0/16
10.125.0.0/16
38.0.0.0/8
83.0.0.0/8
85.0.0.0/8
130.0.0.0/8
169.0.0.0/8
192.0.0.0/8
212.0.0.0/8
dcim.0.0.0/8
lighting.0.0.0/8
monitor.0.0.0/8
netinfo.0.0.0/8
qta.0.0.0/8
yqr1901ucs01.0.0.0/8
Tue, 24 Jul 2018
20:57:43
Tue, 24 Jul 2018
21:22:07
10.20.30.210
10.20.30.101
10.20.30.249
10.20.30.252
10.20.30.103
10.20.30.111
10.20.30.112
NUMBER OF DEVICES PER CVE
TOTAL PERCENTAGE OF LOCATION CVES PER DEVICE
Device
Location
Total % of Location CVEs
10.20.24.10 New Location 3.2 %
10.20.24.3 New Location 3.2 %
10.20.24.4 New Location 3.2 %
10.20.24.5 New Location 3.2 %
10.20.24.6 New Location 3.2 %
10.20.24.9 New Location 3.2 %
Overview
IPv4 Address: 10.20.30.249
Type: Device
OS: Linux Kernel 2.6
Last Activity: Mon, 07 Oct 2019 16:31:26 GMT
Log Risk
Risk
Protocol
Protocols
TCP
Risk
Critical
General
Packets
Ports
Connections
Vulnerabilities
Logs
History
Notes
Critical Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities
High SSL Version 2 and 3 Protocol Detection
High JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE
Medium SSL Medium Strength Cipher Suites Supported
Medium SSL Certificate Cannot Be Trusted
Medium SSL Self-Signed Certificate
Medium SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Info HTTP Server Type and Version
Info ICMP Timestamp Request Remote Date Disclosure
Info SSH Server Type and Version Information


CLAW 2.32.4
OP - Grassy ...
Routes
Allowed
Blocked
Enabled Rules
Disabled Rules
Source Addresses
0.0.0.0/0
Destination Addresses
0.0.0.0/0
ethernet1/3
ethernet1/4
ethernet1/5
ethernet1/6
ethernet1/7
0.0.0.0
0.0.0.0
0.0.0.0
192.168.216.0
TCP 0.0.0.0
TCP 0.0.0.0
UDP 0.0.0.0
localhost.localdomain - Firewall Configuration Vulnerabilities
Vulnerability Details
Synopsis: Any to Any Permitted
Severity: Low
Affected Interfaces: ethernet1/11 (1), ethernet1/13 (1), ethernet1/2 (13), ethernet1/3 (2), ethernet1/4 (1), ethernet1/5 (1), ethernet1/7 (9), ethernet1/8 (1), ethernet1/9 (1)
Description
Allowing access to all destinations provides access to all the hosts inside the perimeter, including the firewall itself, and to all Internet hosts. Traffic should be carefully filtered to meet the organization's requirements.


THE BATTLE
KNOWING
50%
RED LASERS
25%
25%

CLAW-CE
cybernetiq.ca/register

cybernetIQ.ca

info@CybernetIQ.ca

(877) 236-6996