Cyberbit Overview

Adam Aizenberg
EMEA Director

About Us

The Group: Elbit Systems

ISRAEL'S #1 DEFENSE SYSTEMS PROVIDER

$3.1B YEARLY REVENUES NASDAQ: ESLT

12,000 EMPLOYEES

MILITARY COMMAND AND CONTROL SYSTEMS

UAV SYSTEMS

Cyber Intelligence (Cyberbit)

ADVANCED FLIGHT SIMULATORS

INELLIGENCE AND CYBER

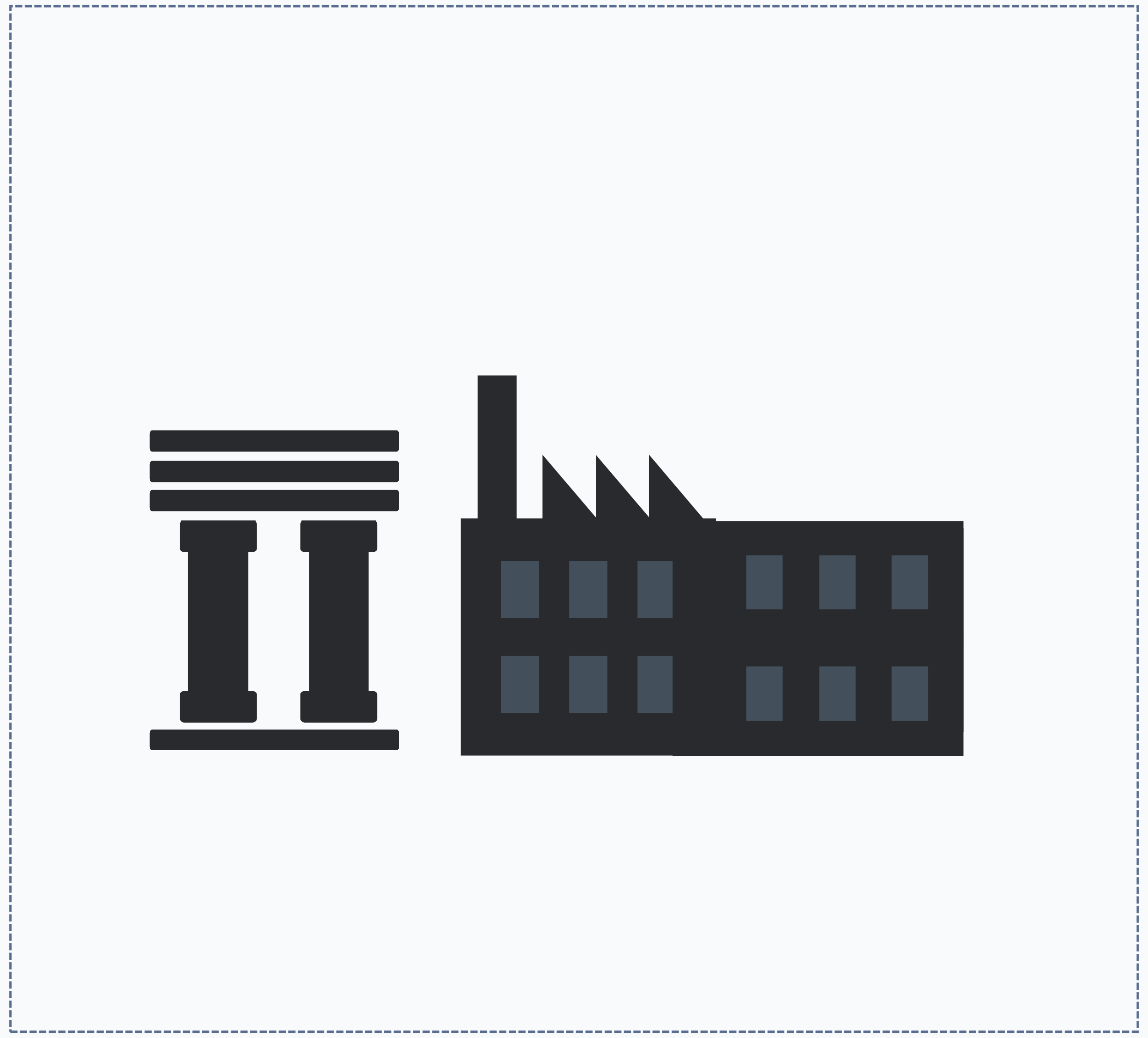
CYBERBIT

- **500 employees**
- **FY’16 sales over $150M**
- **Global support and deployment**
- **Startup culture with corporate DNA**
- **4 Products:**
  - Endpoint Security (EDR)
  - SOC Automation & Orchestration (SOC 3D)
  - ICS/SCADA Security (SCADAShield)
  - Security Training (Cyber Range)

Cyberbit Products

SCADAShield

Protecting ICS/SCADA networks and Critical Infrastructure



Cyberbit EDR

Protecting Enterprise Endpoints from ZeroDays / APTs / Ransomware

SOC 3D

Efficient and Centralized SOC Management & Automation (above SIEM)

Cyberbit RANGE – Cyber Training Simulator

CYBERBIT
PROTECTING A NEW DIMENSION

EDR

Endpoint Detection and Response for IT

70%-90%

of malwares found in breach investigations

Are unique to that organization

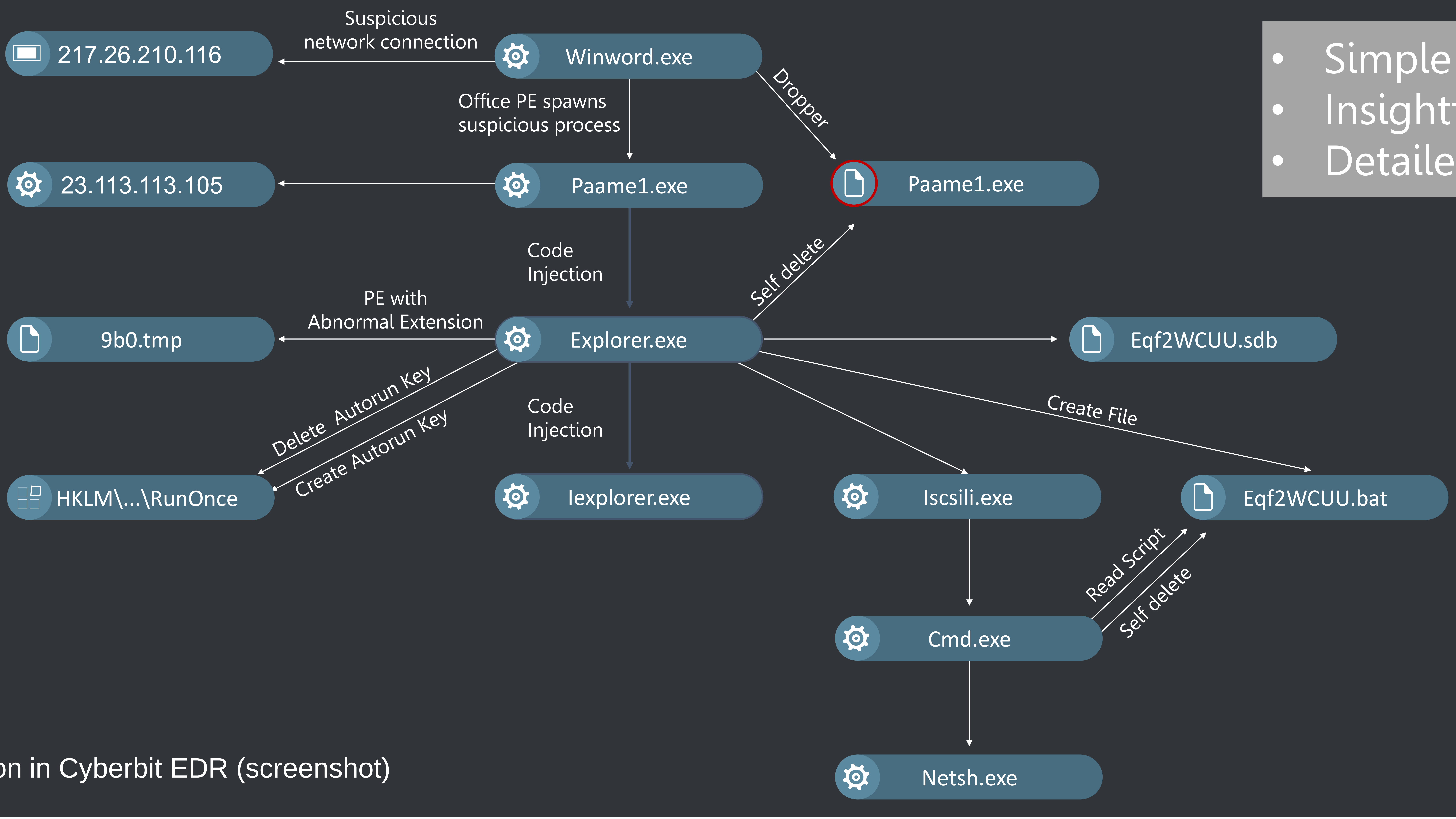
201 days

Mean time to identify

70 days

Mean time to contain

Telling the Attack Story

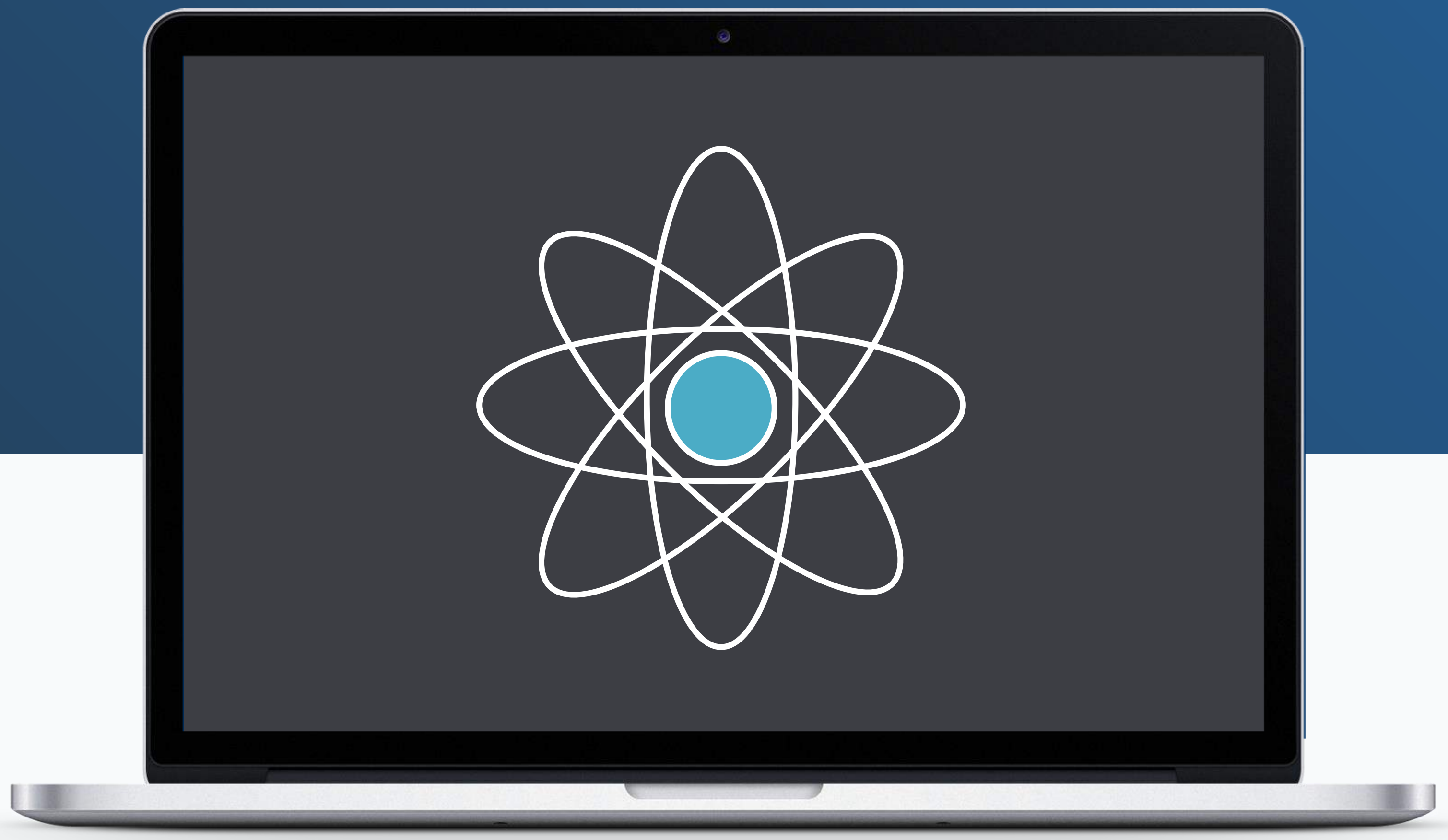


- Simple
- Insightful
- Detailed

Dridex Investigation in Cyberbit EDR (screenshot)

Detection, Forensics and Response

Kernel-Based
Endpoint Agent

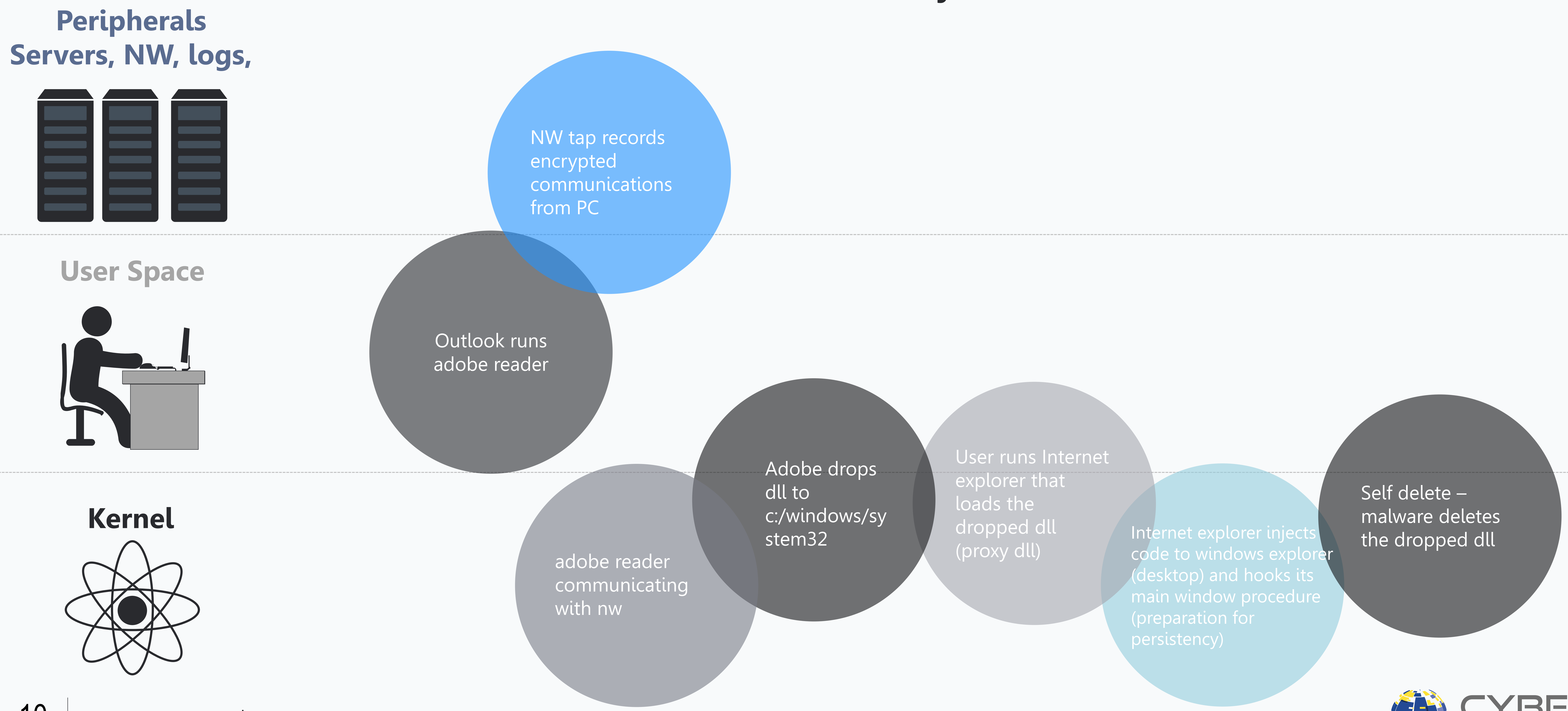


Big Data Analytics

Centralized
Investigation & Response

Why Endpoint? Why Kernel?

From Infection to Persistency in 2 seconds



Peripherals
Servers, NW, logs,

User Space

Kernel

NW tap records encrypted communications from PC

Outlook runs adobe reader

adobe reader communicating with nw

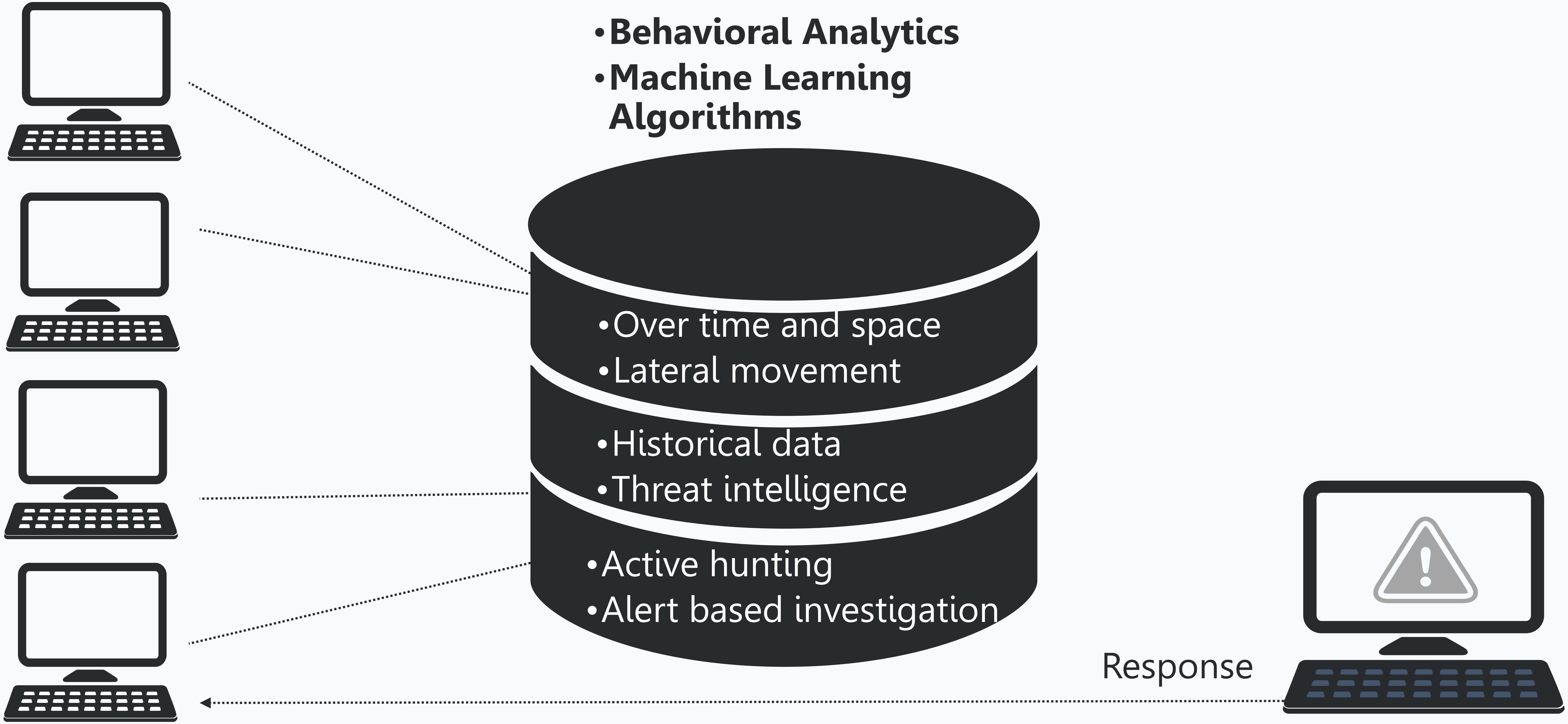
Adobe drops dll to c:/windows/system32

User runs Internet explorer that loads the dropped dll (proxy dll)

Internet explorer injects code to windows explorer (desktop) and hooks its main window procedure (preparation for persistency)

Self delete – malware deletes the dropped dll

Continuous Big Data Analytics



- **Behavioral Analytics**
- **Machine Learning Algorithms**

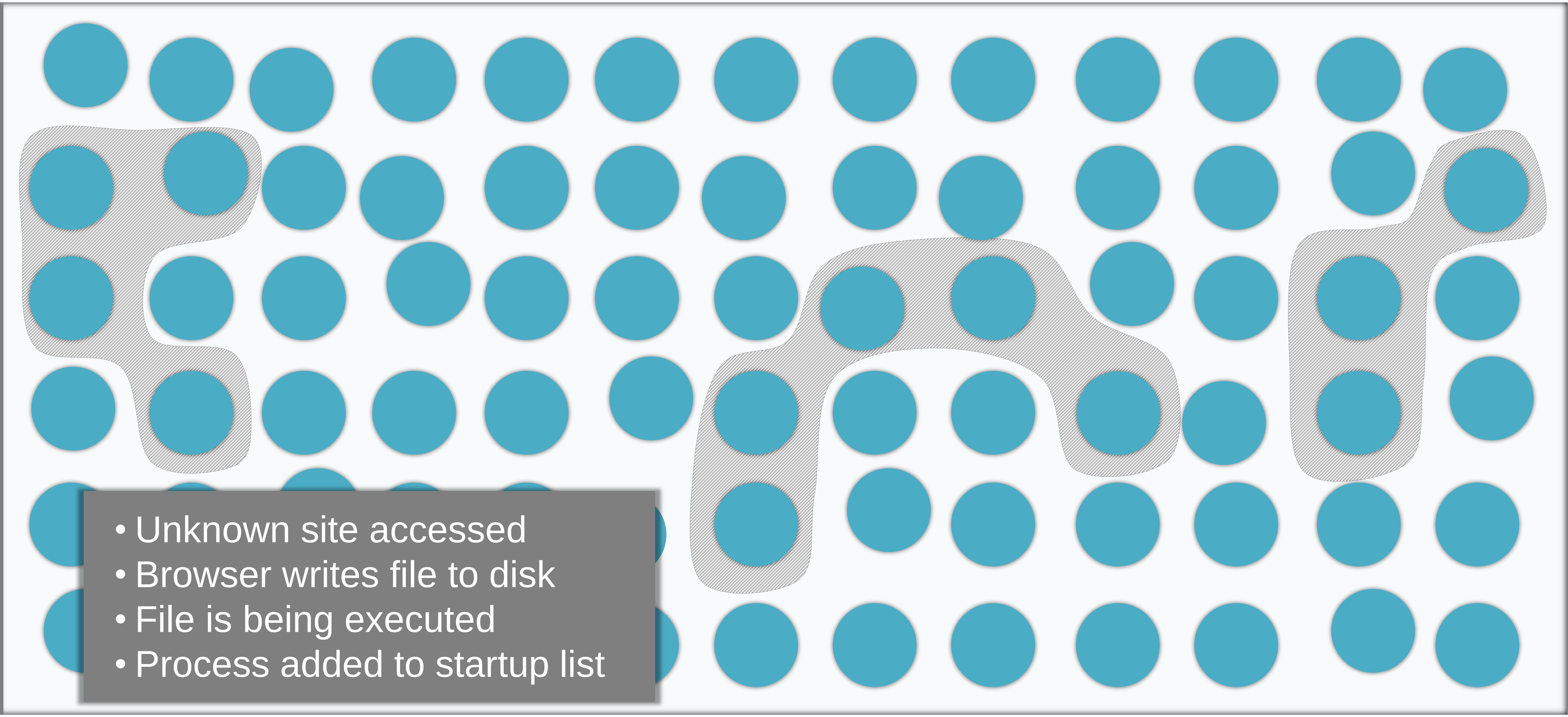
- Over time and space
- Lateral movement

- Historical data
- Threat intelligence

- Active hunting
- Alert based investigation

Detecting by Context

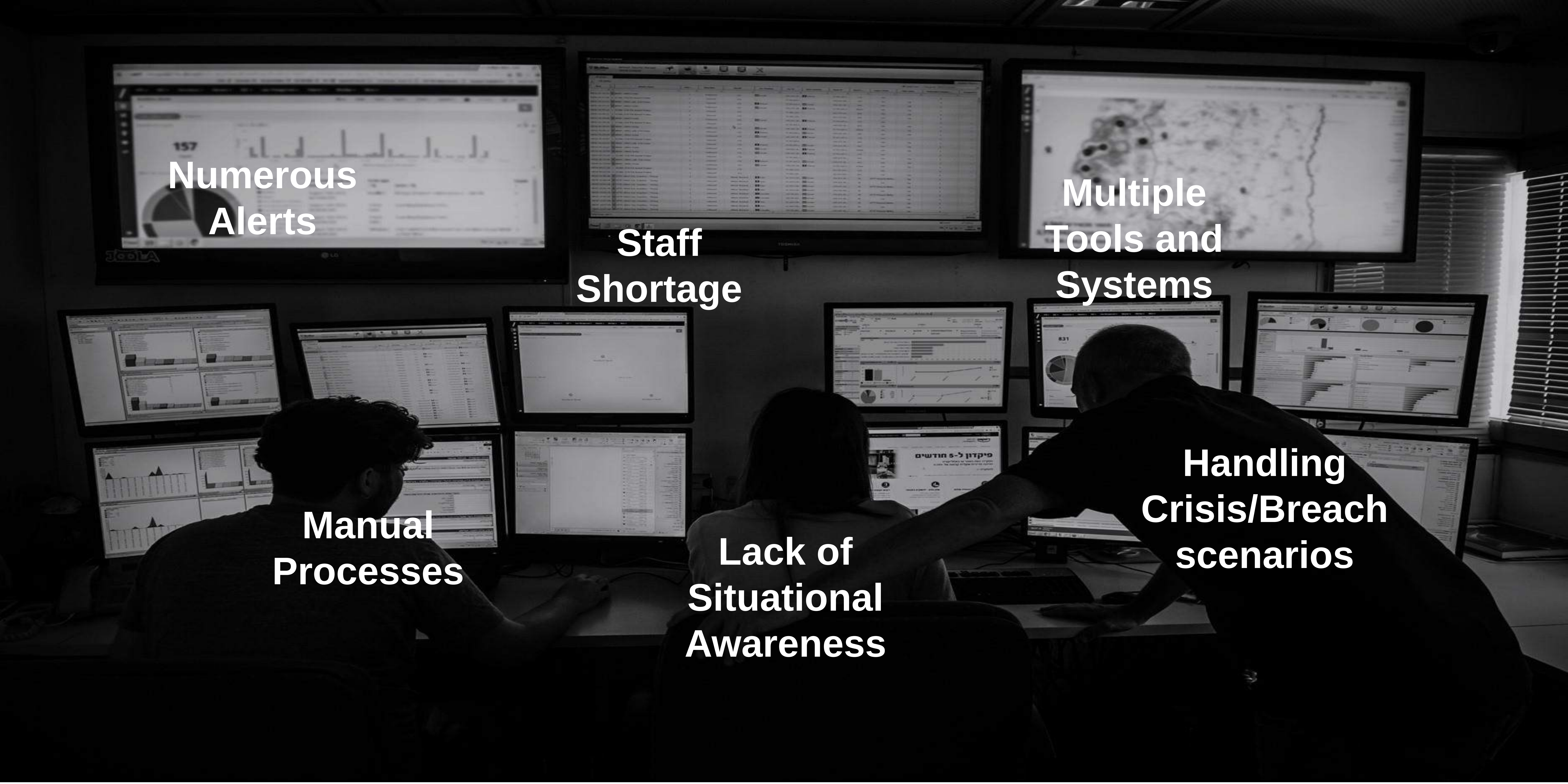
● Behavior ● Suspicious Behavior ▨ Malware activity



- Unknown site accessed
- Browser writes file to disk
- File is being executed
- Process added to startup list

SOC 3D

SOC Automation and Orchestration



Numerous Alerts

Staff Shortage

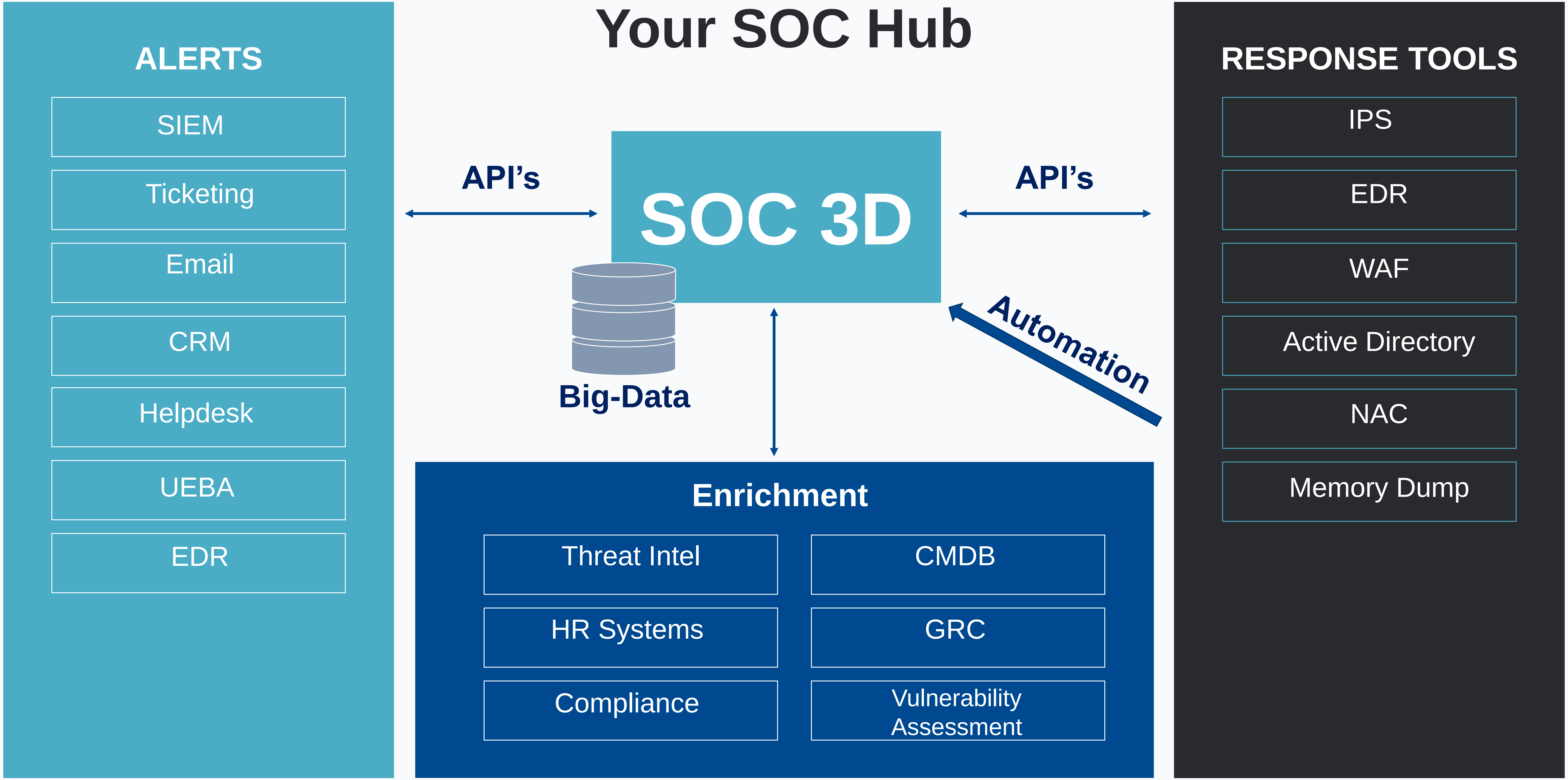
Multiple Tools and Systems

Manual Processes

Lack of Situational Awareness

Handling Crisis/Breach scenarios

Your SOC Hub



ALERTS

- SIEM
- Ticketing
- Email
- CRM
- Helpdesk
- UEBA
- EDR

API's

SOC 3D

Big-Data

API's

Automation

RESPONSE TOOLS

- IPS
- EDR
- WAF
- Active Directory
- NAC
- Memory Dump

Enrichment

- Threat Intel
- CMDB
- HR Systems
- GRC
- Compliance
- Vulnerability Assessment

How can we manage thousands of incidents, with dozens of tools, within severe skill shortage constraints

From managing dozens of screens → to a centralized “single pane of glass”

From trying to make sense out of multiple data feeds → to centralized data enrichment

From manual response → to automated playbook enforcement

Double your SOC’s incident response capacity

Case study: NASDAQ traded enterprise

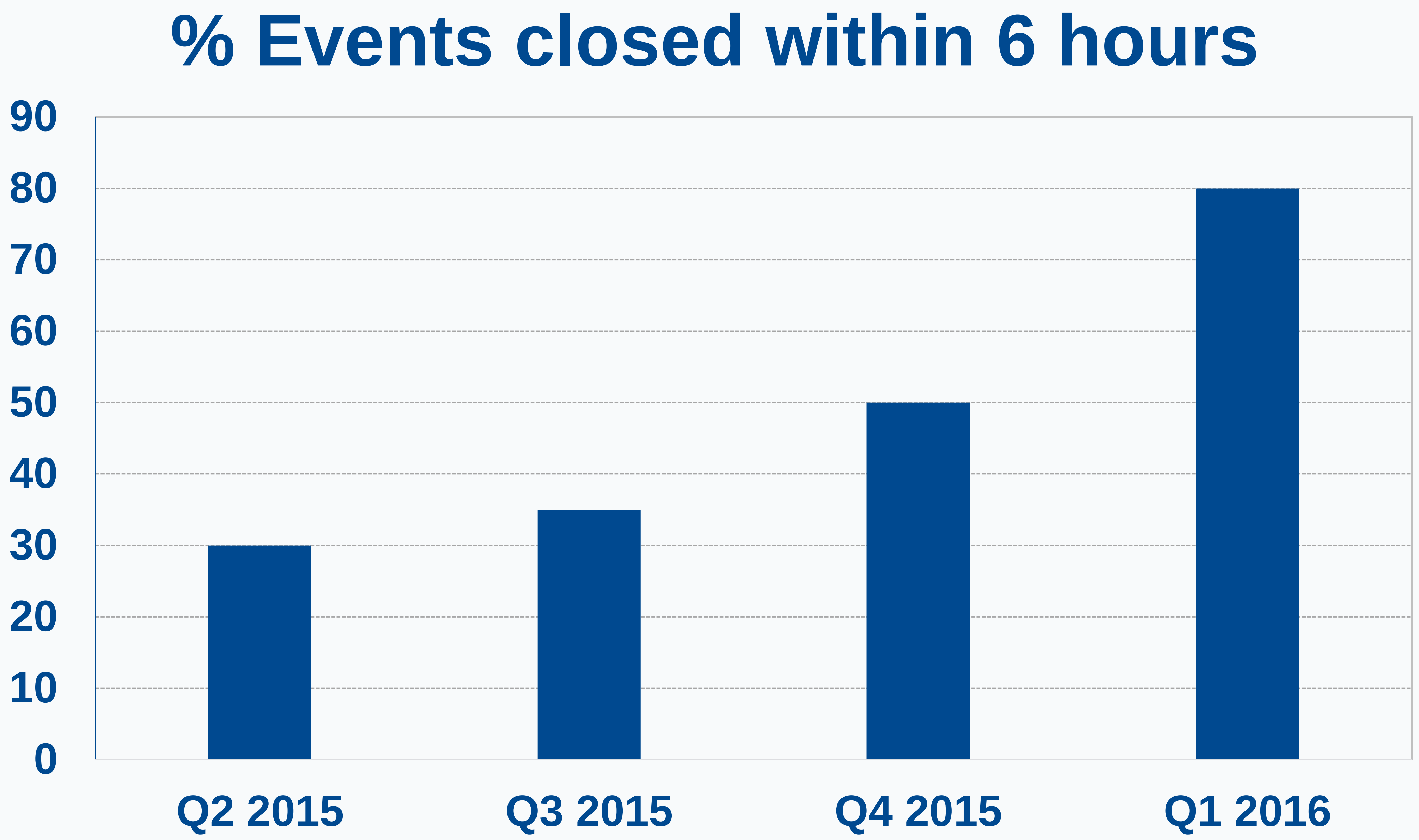
20,000 SIEM incidents/month (average)

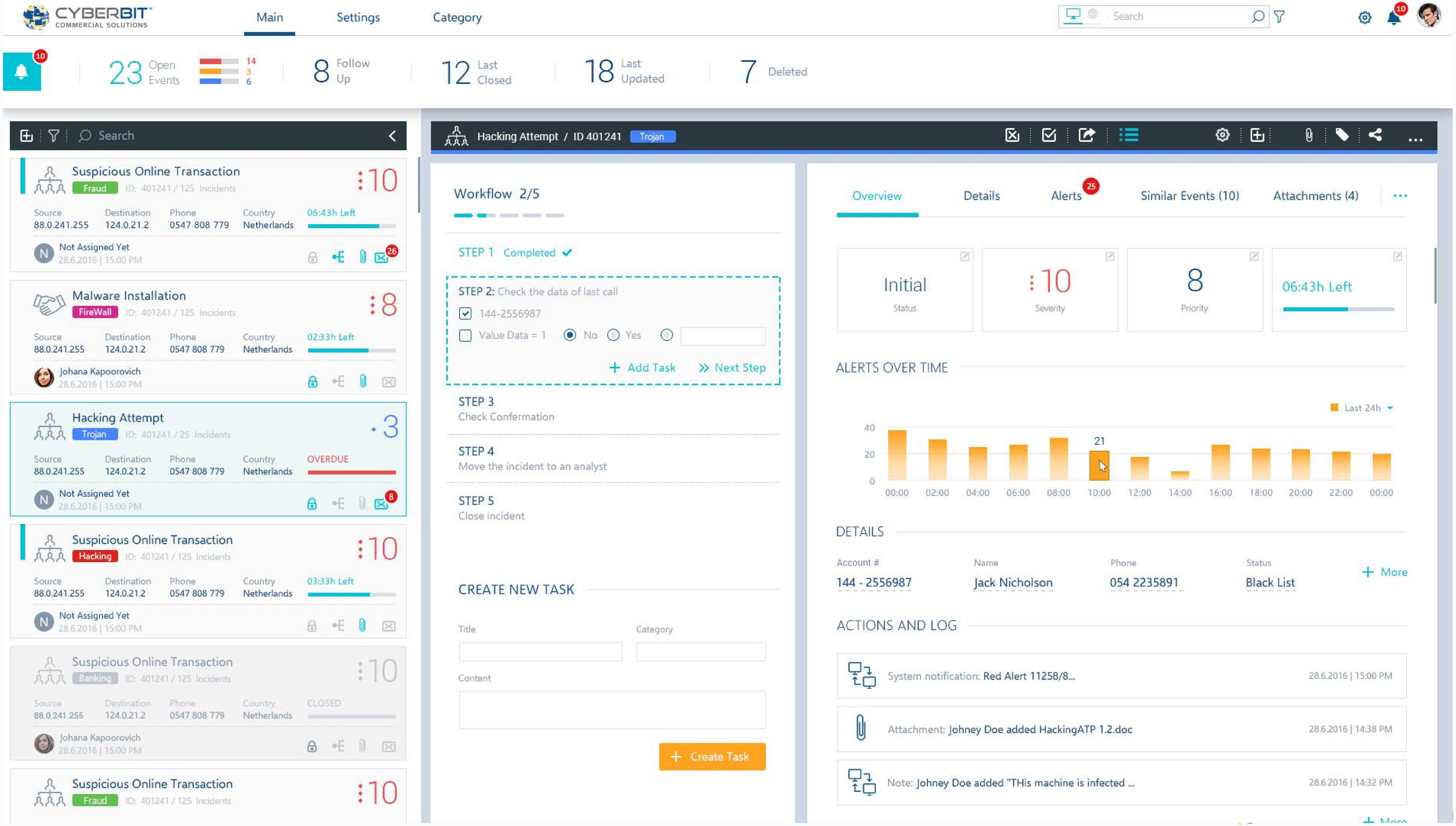
25 targeted threats (APTs) since SOC establishment

80% of events are handled within 6 hours

50 long-duration events per month (over a week)

150 unknown attacks per month





CYBERBIT COMMERCIAL SOLUTIONS

Main | Settings | Category

Search

23 Open Events — 14, 3, 6

8 Follow Up

12 Last Closed

18 Last Updated

7 Deleted

Search

Suspicious Online Transaction — Fraud — ID: 401241 / 125 Incidents — 10

Source	Destination	Phone	Country	
88.0.241.255	124.0.21.2	0547 808 779	Netherlands	06:43h Left

Not Assigned Yet 28.6.2016 | 15:00 PM — 26

Malware Installation — FireWall — ID: 401241 / 125 Incidents — 8

Source	Destination	Phone	Country	
88.0.241.255	124.0.21.2	0547 808 779	Netherlands	02:33h Left

Johana Kapoorovich 28.6.2016 | 15:00 PM

Hacking Attempt — Trojan — ID: 401241 / 25 Incidents — 3

Source	Destination	Phone	Country	
88.0.241.255	124.0.21.2	0547 808 779	Netherlands	OVERDUE

Not Assigned Yet 28.6.2016 | 15:00 PM — 8

Suspicious Online Transaction — Hacking — ID: 401241 / 125 Incidents — 10

Source	Destination	Phone	Country	
88.0.241.255	124.0.21.2	0547 808 779	Netherlands	03:33h Left

Not Assigned Yet 28.6.2016 | 15:00 PM

Suspicious Online Transaction — Banking — ID: 401241 / 125 Incidents — 10

Source	Destination	Phone	Country	
88.0.241.255	124.0.21.2	0547 808 779	Netherlands	CLOSED

Johana Kapoorovich 28.6.2016 | 15:00 PM

Suspicious Online Transaction — Fraud — ID: 401241 / 125 Incidents — 10

Hacking Attempt / ID 401241 — Trojan

Workflow 2/5

STEP 1 Completed ✓

STEP 2: Check the data of last call

☑ 144-2556987

☐ Value Data = 1 ● No ○ Yes ○

+ Add Task   >> Next Step

STEP 3
Check Confermation

STEP 4
Move the incident to an analyst

STEP 5
Close incident

CREATE NEW TASK

Title

Category

Content

+ Create Task

Overview | Details | Alerts 25 | Similar Events (10) | Attachments (4)

Initial — Status

10 — Severity

8 — Priority

06:43h Left

ALERTS OVER TIME

DETAILS

Account #	Name	Phone	Status
144 - 2556987	Jack Nicholson	054 2235891	Black List

+ More

ACTIONS AND LOG

System notification: Red Alert 11258/8... 28.6.2016 | 15:00 PM

Attachment: Johney Doe added HackingATP 1.2.doc 28.6.2016 | 14:38 PM

Note: Johney Doe added "THis machine is infected ... 28.6.2016 | 14:32 PM

+ More

SCADAShield

Protecting Critical & Manufacturing Infrastructure (ICS)

Simplifying Operations, Increasing Security

visibility, discovery and security of ICS networks

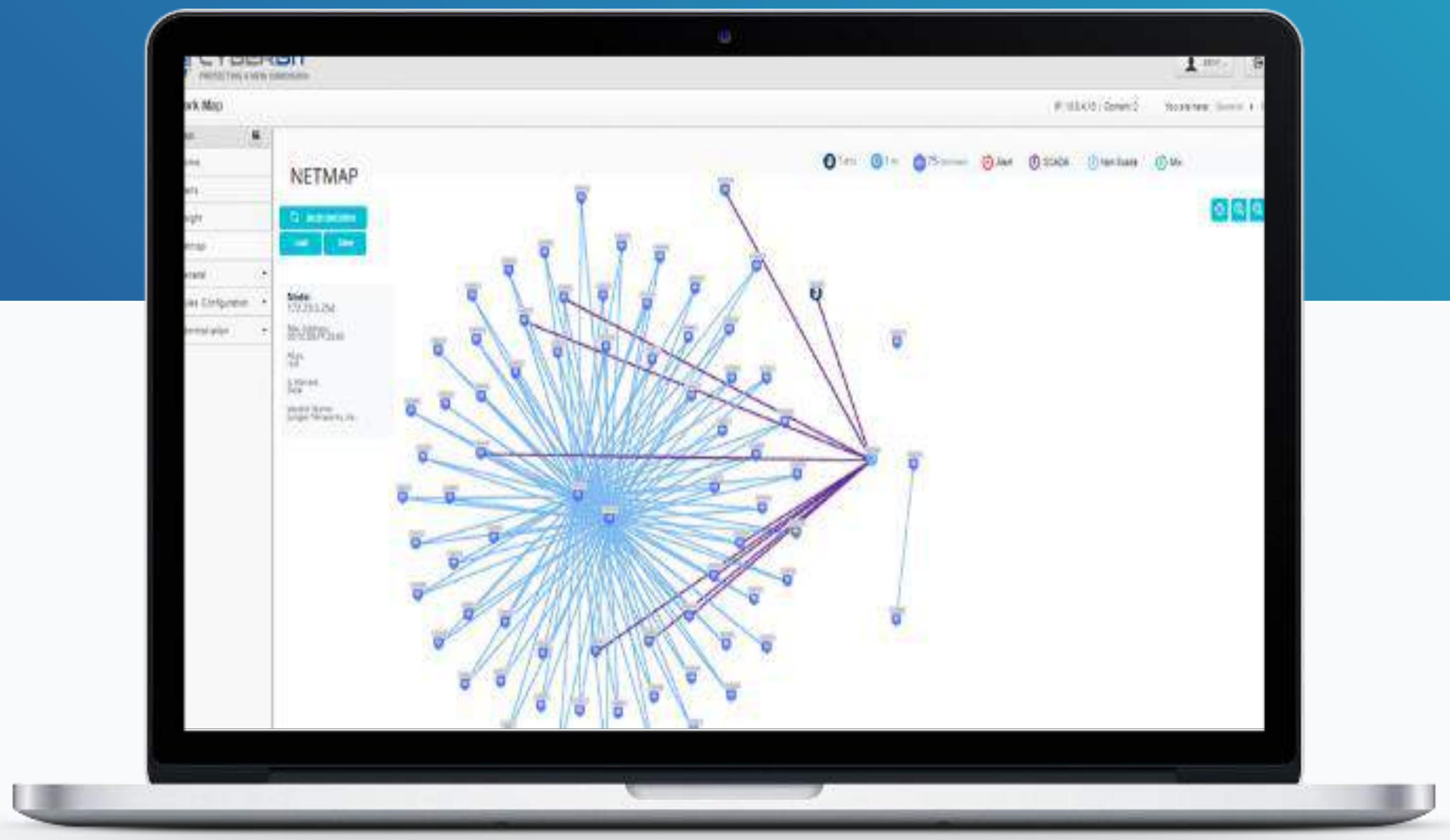
NETWORK G-DPI SENSOR

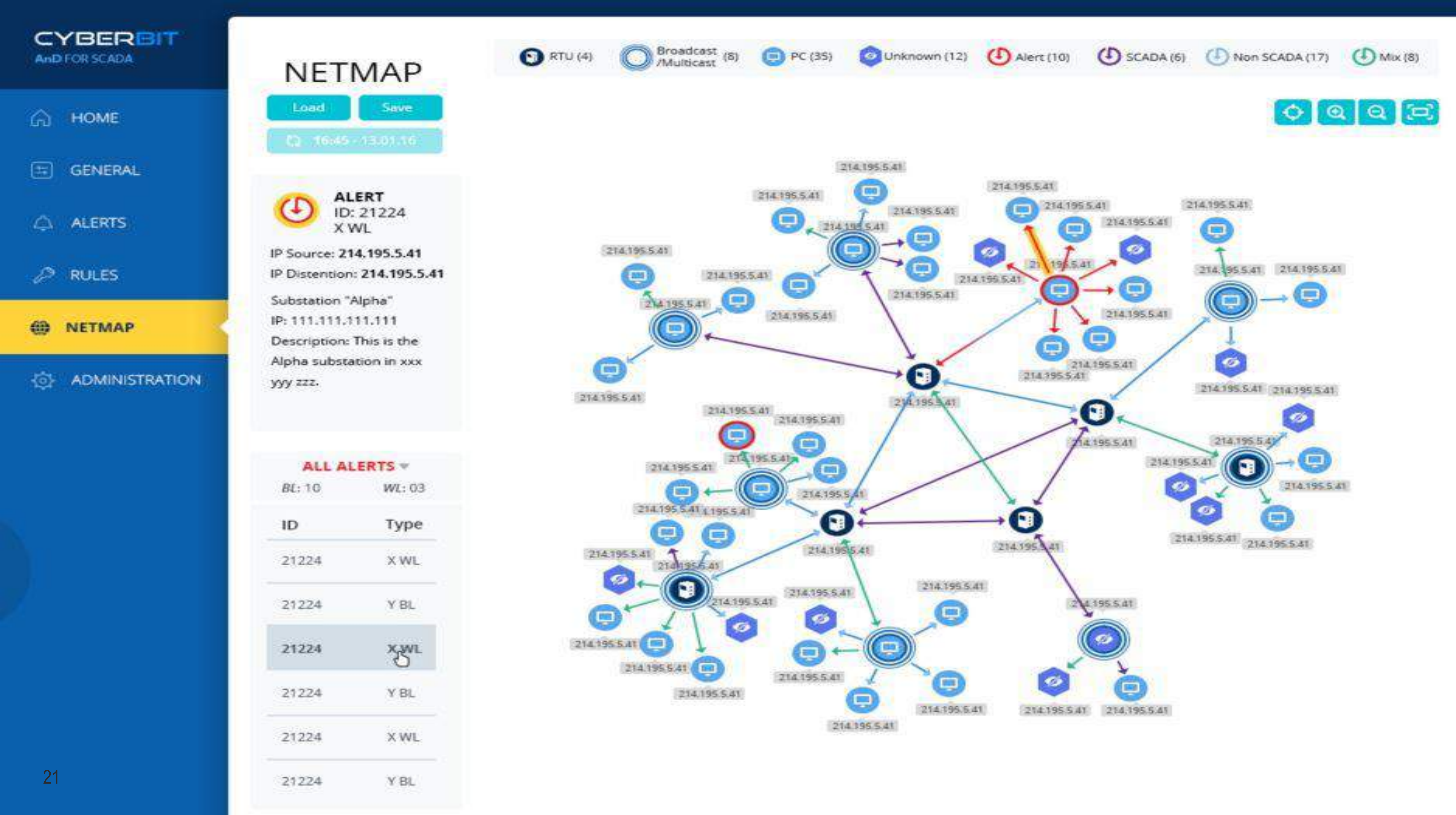
non-intrusive plug & play

CENTRALIZED BIG DATA STORAGE

Mapping and monitoring behaviors automatically

ALERTS, FORENSICS & MAPPING APPLICATION





NETMAP

ALERT
ID: 21224
X WL

IP Source: **214.195.5.41**

IP Distention: **214.195.5.41**

Substation "Alpha"

IP: 111.111.111.111

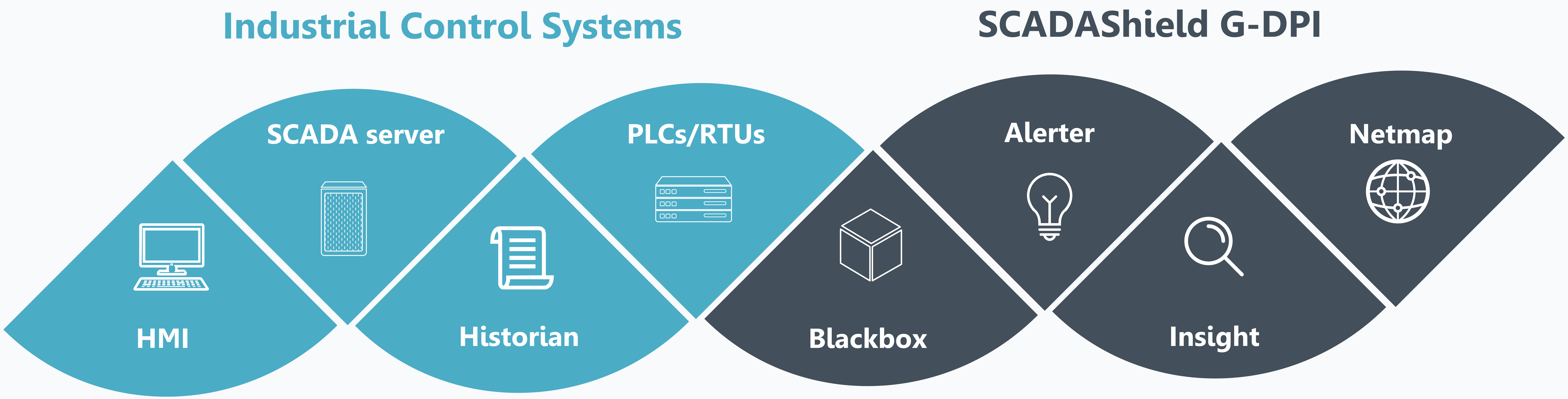
Description: This is the Alpha substation in xxx yyy zzz.

ALL ALERTS ▾

BL: 10 *WL*: 03

ID	Type
21224	X WL
21224	Y BL
21224	X WL
21224	Y BL
21224	X WL
21224	Y BL

The New Operational Toolbox



- Alarm handling
- Meter readings
- Remote configuration

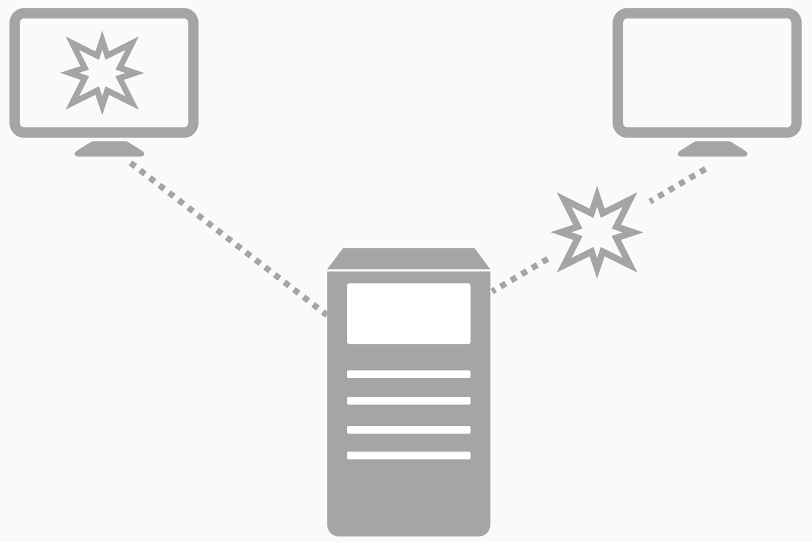
- Real network map
- Malfunction prediction
- “Keep alive” monitoring
- Alarm investigation and analysis
- Network forensics

Cyberbit Range

The “flight simulator” for cybersecurity staff

Addressing the Challenge

A complete organizational-training ecosystem

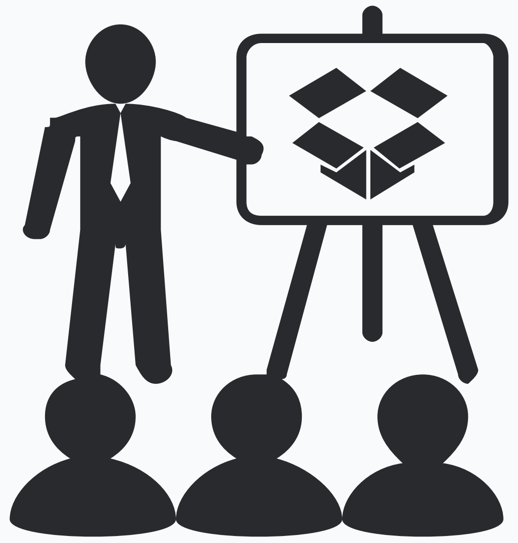


Real-life simulation

- Threats
- Traffic
- Real-life components and tools
- IT and OT networks

Team & individual training

- Collaborative training
- Assess and address team capabilities
- Learn and enforce best practices



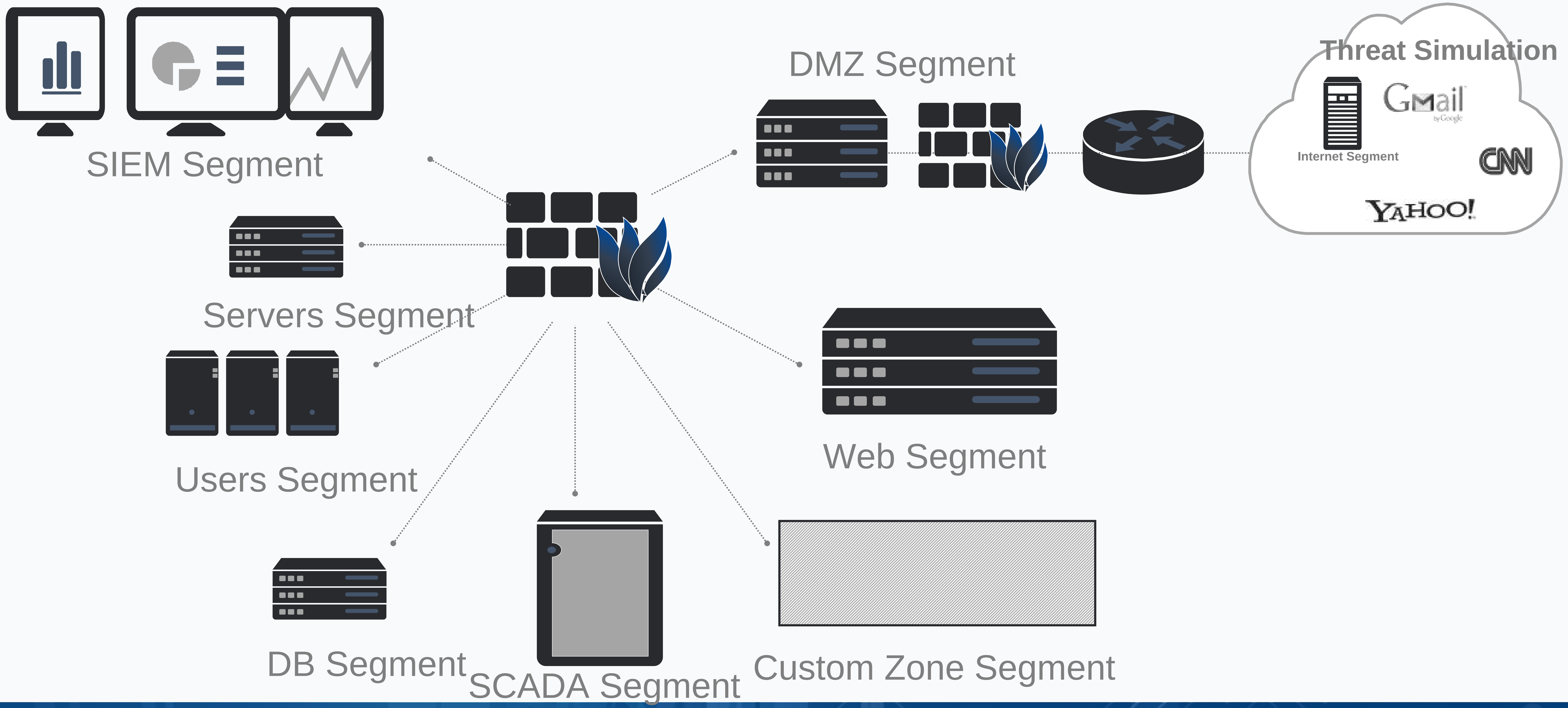
Extensive Training Tools

- Training programs
- Recording & debrief
- Knowledge base

Powerful Scenario Builder

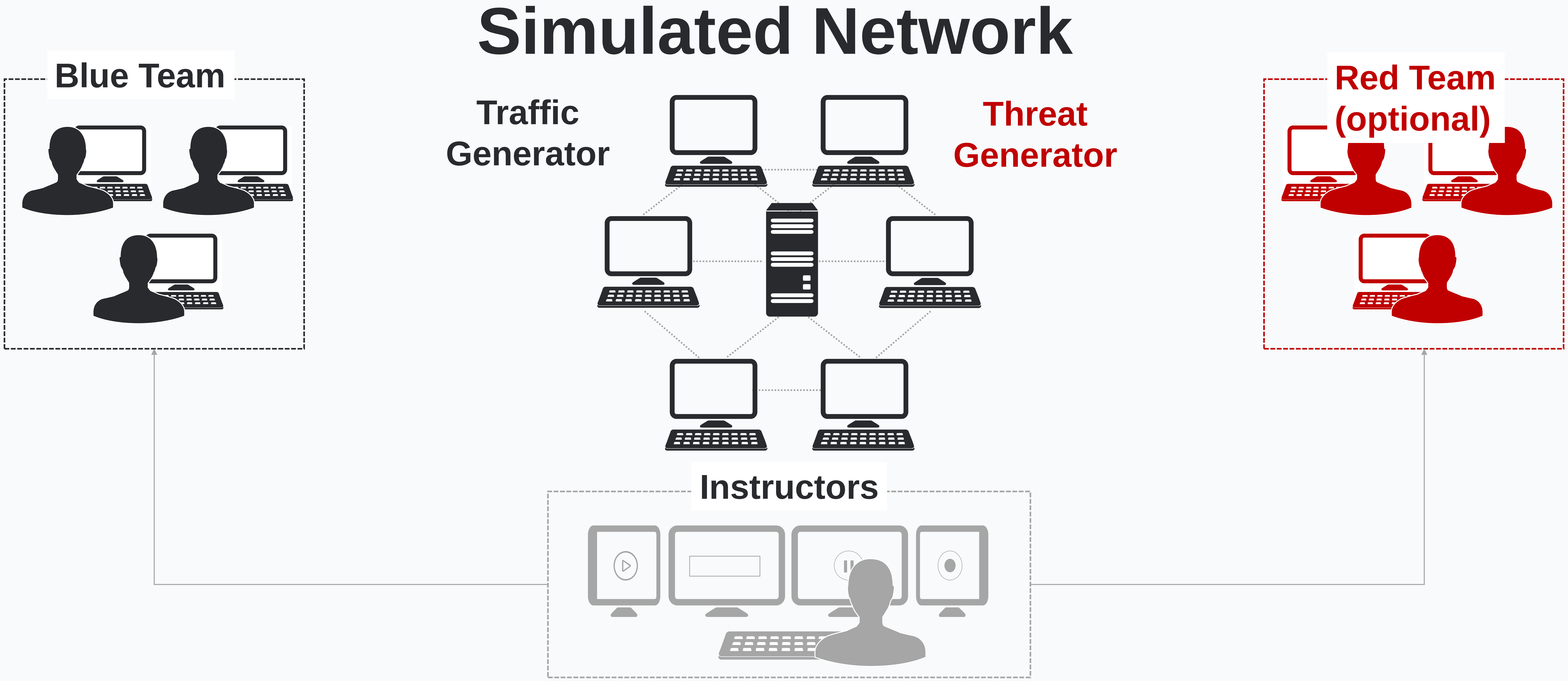
- Custom networks
- Custom attacks
- Custom traffic

Simulated Network – Default Package



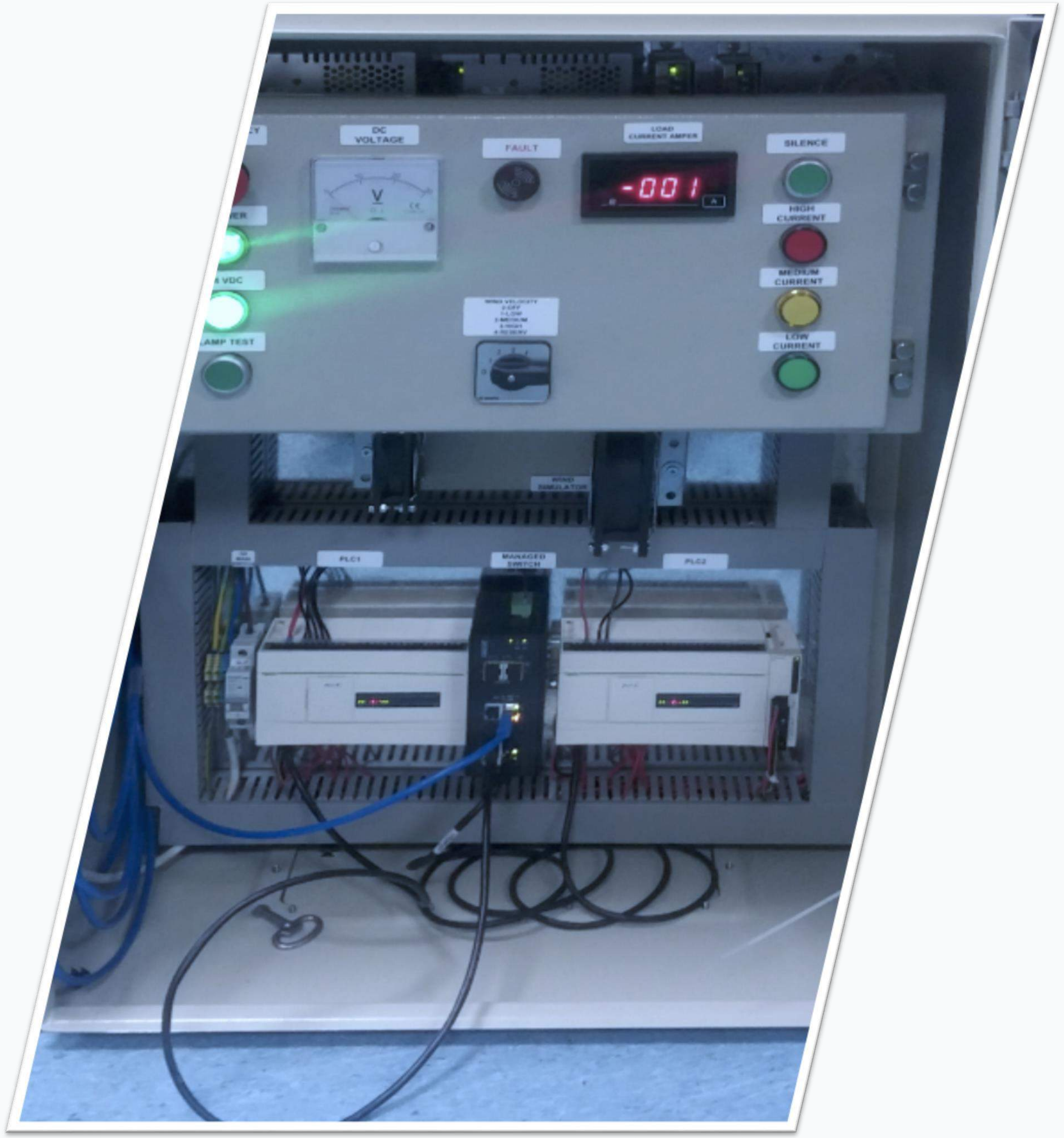
DETECT ANALYZE RESPOND

The Training Environment



Operational Network (OT) Module

- Physical OT hardware
- Integration with the simulated IT and SCADA environment
- Variety of SCADA scenarios and threat vectors



Thank you!

Adam Aizenberg
EMEA Director
Adam.Aizenberg@Cyberbit.net