

NETSCOUT®

Guardians of the Connected World

# Our Solutions

## Powered by the Visibility Without Borders Platform



### nGenius Enterprise Performance Management

Mission Critical Apps

Remote and Hybrid Workforce

UCaaS and Collaboration

Hybrid Multi-cloud Migration



### Taps and Packet Flow Switches

In Line Taps

Packet Flow Switches

High speed decryption appliances



### Omnis Network Security

Comprehensive Network Visibility

Cyber Threat Detection

Ecosystem Integration



### Arbor DDoS Protection

Pervasive Network Visibility

Adaptive DDoS Protection

Global Threat Intelligence

**The real-time network visibility platform for performance, security, and availability, at any scale.**



# Big Picture Challenges for Cybersecurity...



# Current State of Security Technology

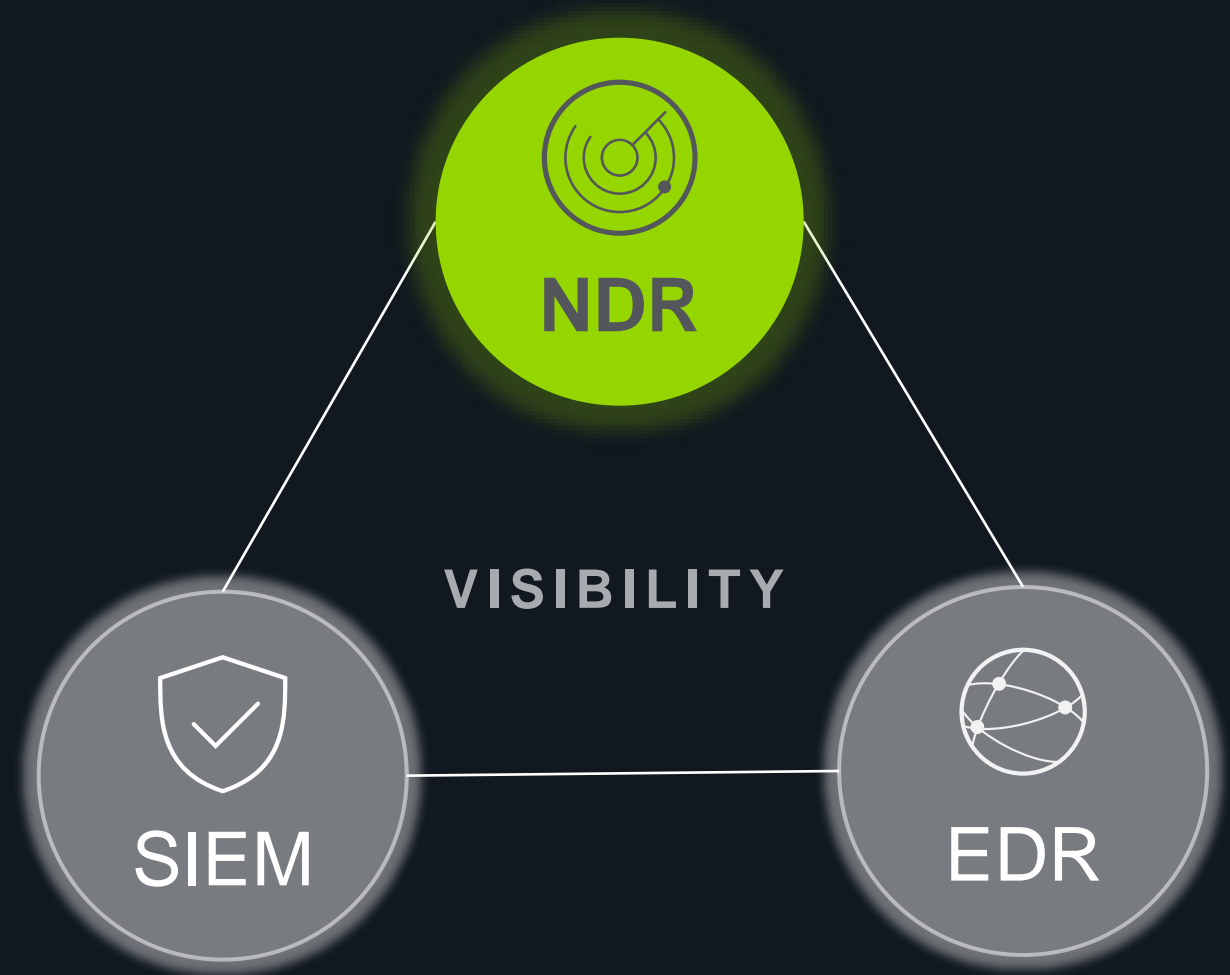
## Hackers Continue to Beat the “Good” Guys While Security Spend Skyrockets

- Security technology today is primarily focused on threat mitigation using tools like NGFW, IDS, NDR, SIEM, EDR etc. These technologies often focus on sophisticated detection algorithms on top of a poor and noisy data set.
- Despite all the spend driven by fear-factors, attacks continue to rise unabated and ransomware breaches are at all-time high. Hackers and malicious elements are always one step ahead.
- To address this, we need a **risk-focused approach** (rather than a threat-focused one) that can reduce the Mean Time to Restore to minutes instead of days or weeks.



# The SOC Visibility Triad (Gartner)

- *“You can’t protect yourself from what you can’t see”*
- Three main sources of SOC visibility: SIEM, EDR, NDR
- Each has its pros and cons, but security teams need all three to detect, investigate and remediate threats.



# Multiple Detection Methods (DM)

<input checked="" type="checkbox"/> Threat Intelligence	171
<input checked="" type="checkbox"/> Behavioral Analytics	16
<input checked="" type="checkbox"/> Attack Surface	0
<input checked="" type="checkbox"/> Compliance	7
<input checked="" type="checkbox"/> IDS	47
<input checked="" type="checkbox"/> Policy Violation	3
<input checked="" type="checkbox"/> File Detections	3

PLUS -MITRE ATT&CK –at source  
Configurable & Extensible



Behavior of an individual user or host, or a group of hosts or users, that deviates from the locally norm. MITRE ATT&CK mapping.

Unexpected internal-to-external traffic patterns (**Attack Surface Events**)

Specific pattern or set of characteristics to identify known malicious activity or threats and files (**Suricata-based rules and signatures**)

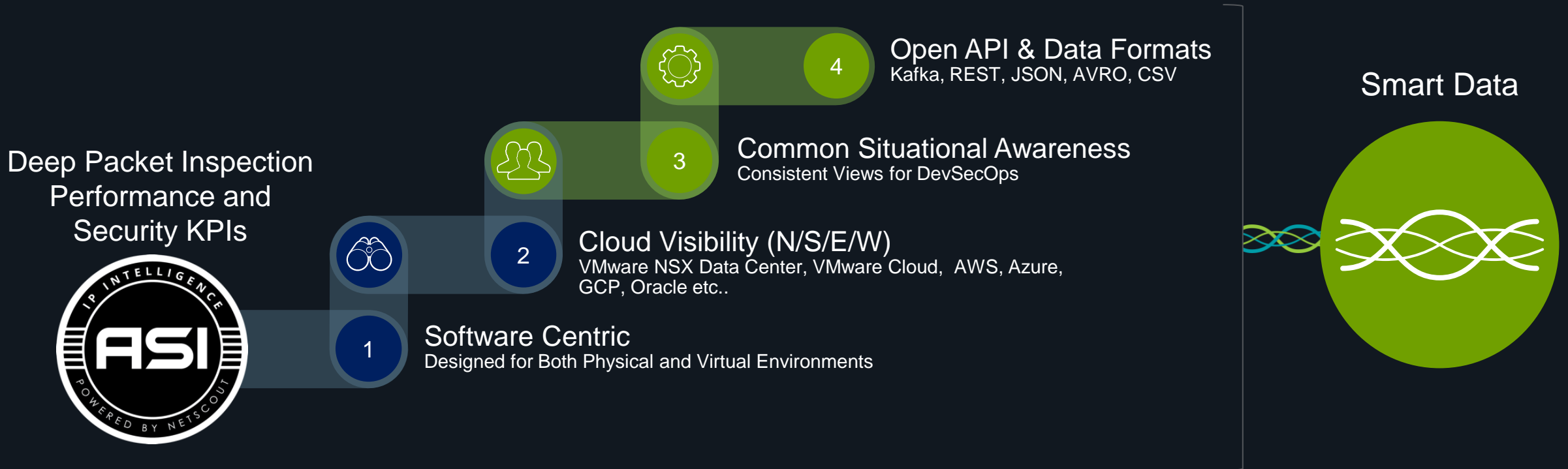
Use of configuration information to detect access violations, validation of compliance and network access policy configuration rules (**Uses Host Groups definitions**)

Specific pieces of evidence/IoCs (ex. known bad IP, URL, DNS) to indicate a security breach or malicious activity has occurred.



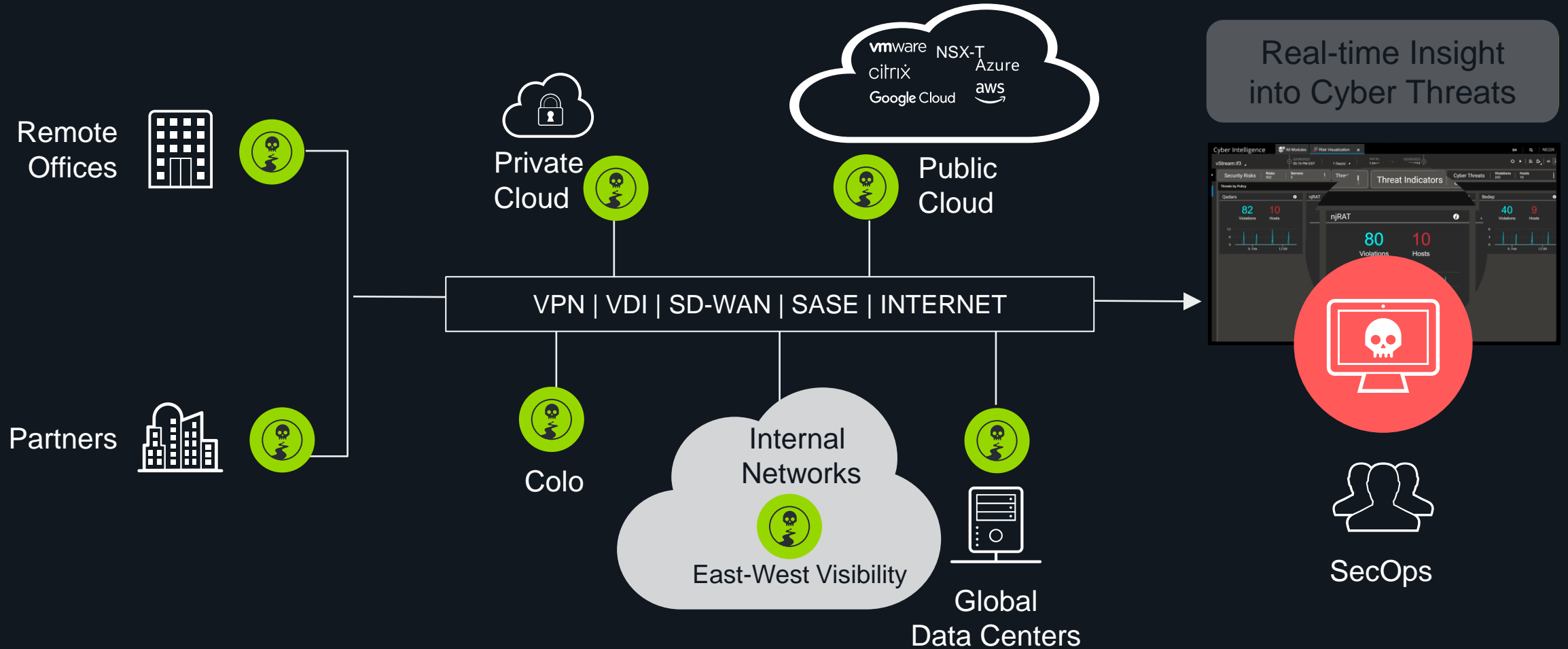
# What is Smart Data?

Smart Visibility into Network, Applications, Dependencies, and Security



# Preferred NDR Deployment

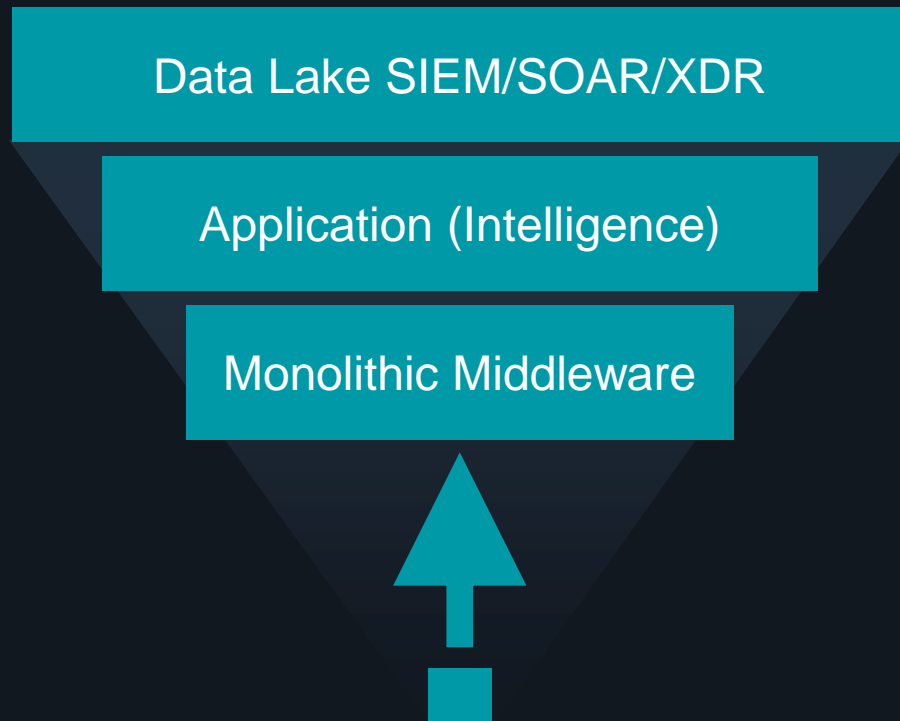
Wherever Workloads and Users are Located





# NDR Architecture Redefined

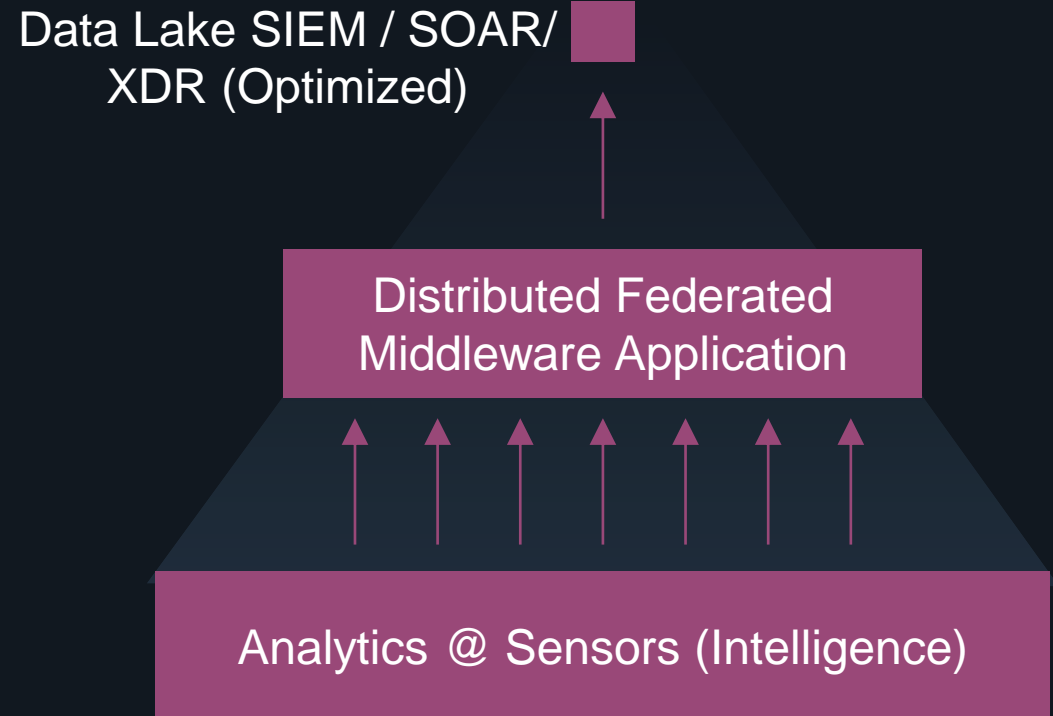
Industry Present Mode of Operation  
Centralized



Data Sources

- Intelligence in middleware/ higher layers (higher cost)
- Weak historical depth
- Point Products

NETSCOUT  
Disaggregated (Hierarchical)



- Intelligence in distributed sensors provides Visibility without Borders at less cost).
- Confidential, historical data kept local vs in public, multi-tenant, expensive cloud.
- Platform approach (starts with proprietary packet broker, decryption)



# IDS detections:

## Signature-based Detection

### String signatures:

The string signature engines support regular expression pattern matching and alarm functionality.

### Connection signatures:

They generate an alarm based on the conformity and validity of the network connections and protocols.

### DoS signatures:

They contain behavior descriptions that are considered characteristics of a DoS attack.

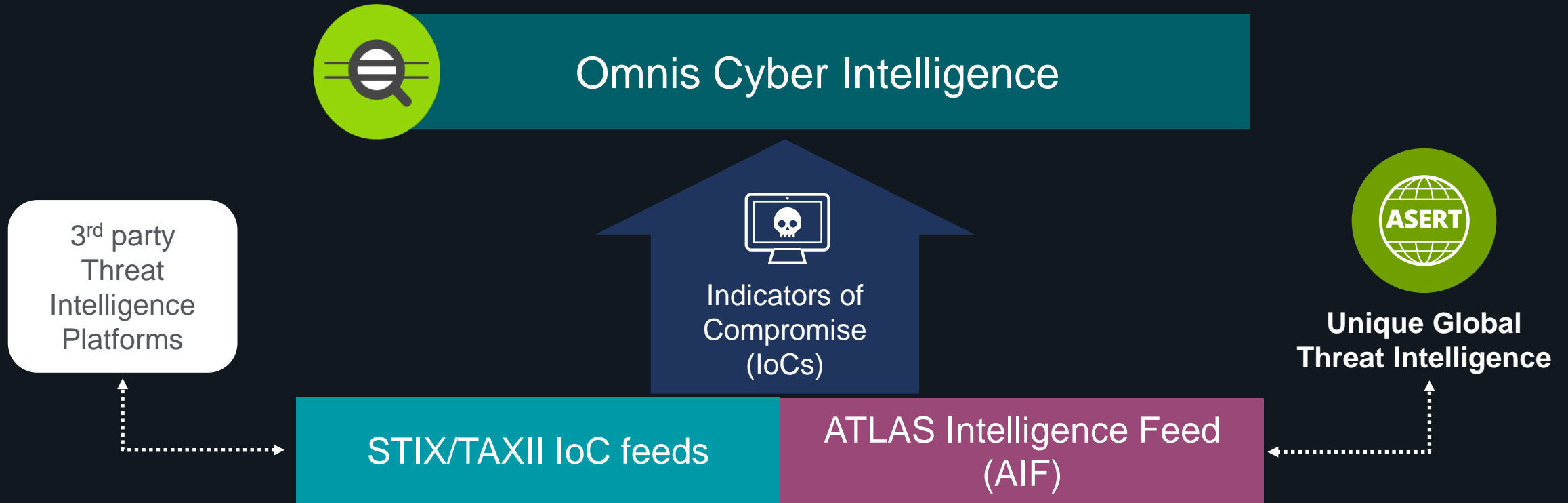
### Exploit signatures:

They typically identify a traffic pattern that is unique to a specific exploit; therefore, each exploit variant may require an individual signature. Attackers may be able to bypass detection by slightly modifying the attack payload. One often must produce an exploit signature for each attack tool variant.

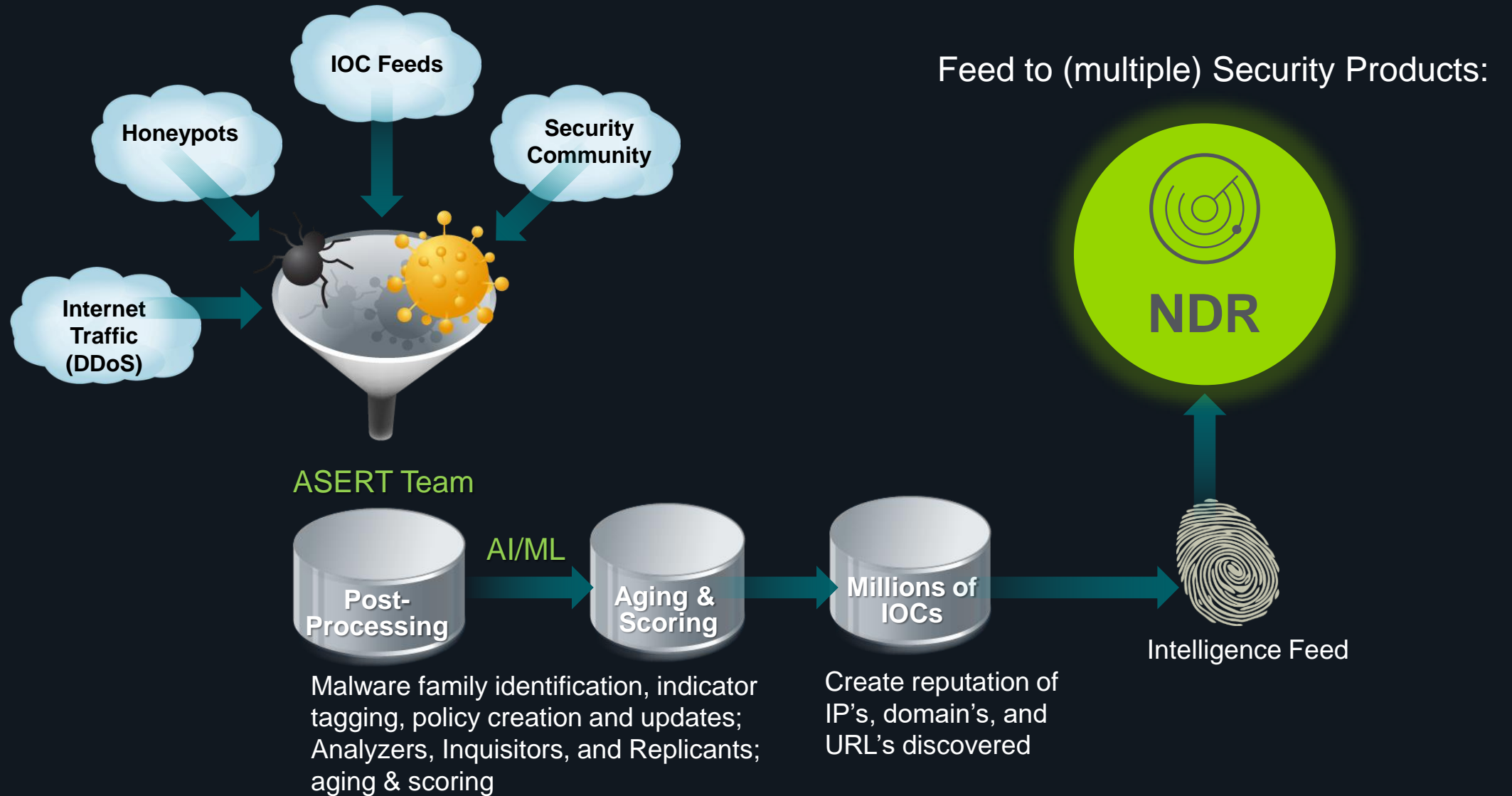


# Cyber Threats – IoC support

Signature Matching with IoC feeds



# A highly curated intelligence feed



# Detecting Initial Phase of an Attack

The screenshot displays a security dashboard with several key components:

- Detection Details:** Lists alerts such as "Internal Insecure Fi...", "Outgoing file detect...", "ET DROP Spamhaus...", "OS Command Inject...", and "CP / DB other Proto...".
- Violation Details:** Shows a rule for "Outgoing file detected" with a severity score of 8, priority 3, and status "Open".
- Initiator Bytes:** A bar chart showing initiator bytes over time, with a peak at 16:00.
- Cyber Intelligence:** A central dashboard with a "Security Events Center" tab, a world map, and a table of events.
- Detected Files:** A table listing files with columns for File Name, SHA256 CheckSum, File Direction, File Size (B), File Stored, and Alert SID.
- Inbound/Outbound Connections:** Tables showing network traffic volumes for various hosts and host groups.

Date Time	Event type	Description
05/31/2023 02:00:00 PM CDT	Geolocation	4.79.42.20 has an inbound connection from outside enter...
05/31/2023 02:00:00 PM CDT	Geolocation	4.79.42.70 has an inbound connection from outside enter...
05/31/2023 03:00:00 PM CDT	Geolocation	4.79.42.70 has an outbound connection to outside enterpr...
05/31/2023 03:00:00 PM CDT	Geolocation	4.79.42.20 has an inbound connection from outside enter...
05/31/2023 03:00:00 PM CDT	Geolocation	4.79.42.70 has an inbound connection from outside enter...
05/31/2023 04:00:00 PM CDT	Application	4.79.42.70 has an outbound connection to outside enterpr...

Host	Host Group	In Volume (MB)	Out Volume (MB)
4.79.42.20	DMZ-external-IPS	21.07	387.49
4.79.42.70	DMZ-external-IPS	7.15	1.18
4.79.42.71	DMZ-external-IPS	0	0

Host	Host Group	In Volume (MB)	Out Volume (MB)
4.79.42.70	DMZ-external-IPS	2.52	1.27
4.79.42.41	DMZ-external-IPS	0.06	0.85
4.79.42.3	DMZ-external-IPS	0.32	0.37
4.79.42.20	DMZ-external-IPS	0	0

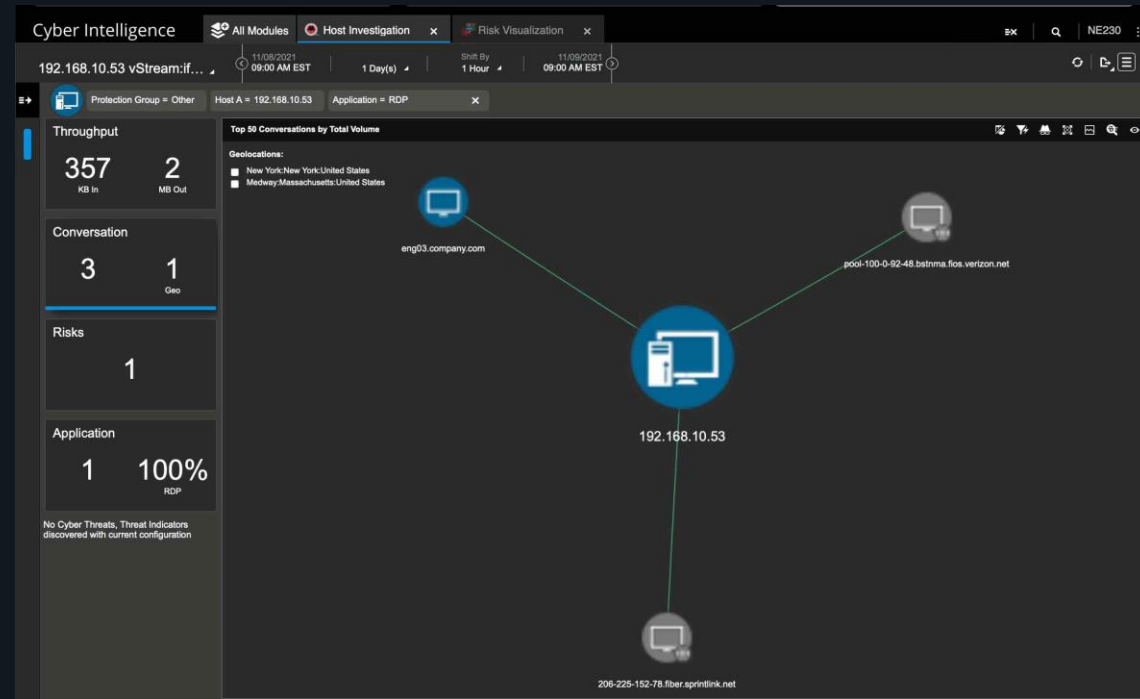
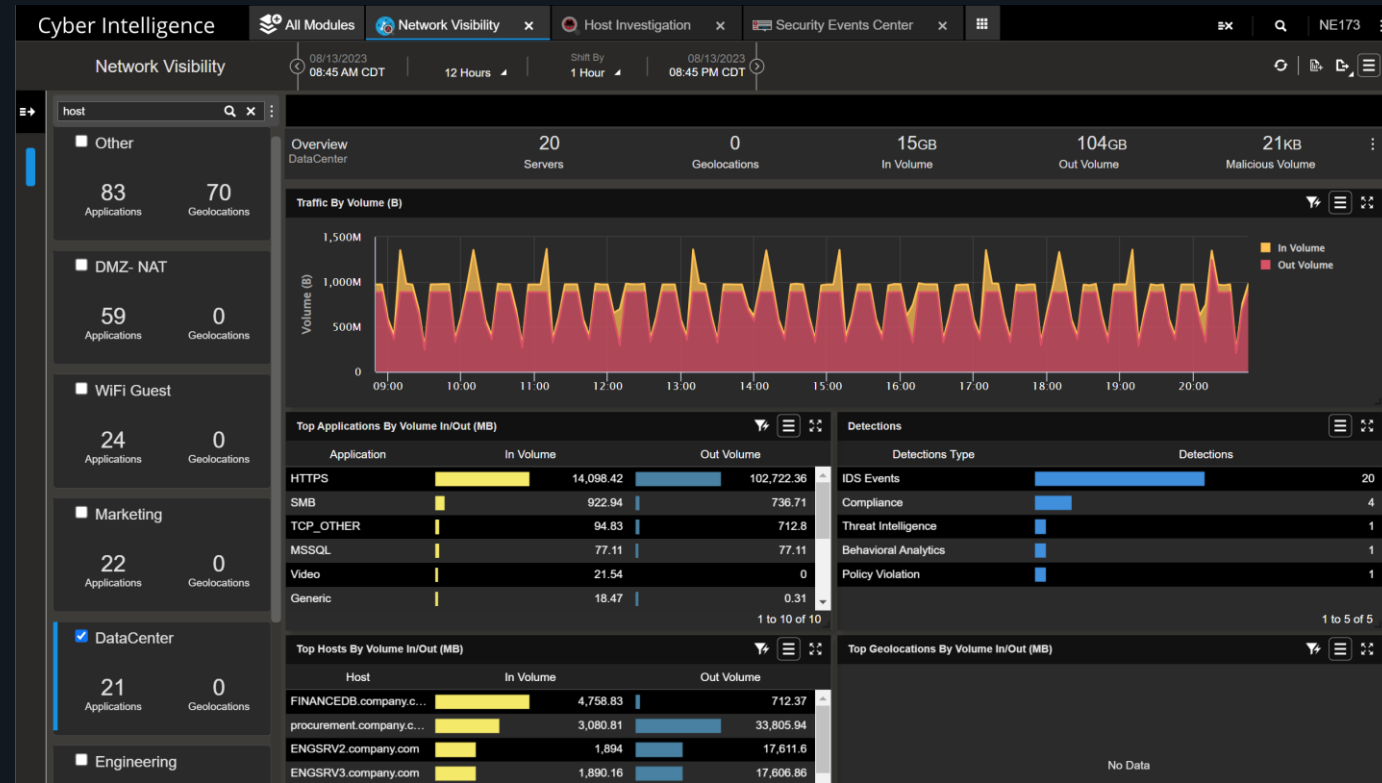
File Name	SHA256 CheckSum	File Direction	File Size (B)	File Stored	Alert SID
/update/check.html	e28f9a743e0cd3f4d60...	Incoming	20	True	1000010
/roots/dstrootcax3.p7c	a2ce3a0fa7d2a833d1...	Incoming	893	True	1000010
/plain/clientip	40a58618cb697f749c...	Incoming	13	True	1000010
/libhttp::request_uri_no...	2c3618fae136a65e5c...	Incoming	167702	False	1000010
/json	5f8a1a1c5a8dbe5d09...	Incoming	317	True	1000010

**A NDR solution needs to detect more than 50% of previously unknown outbound threats and 95% of otherwise undetected reconnaissance:**

- Define Protection Groups to highlight activity in high-risk areas
- Detect scanning and brute force access attempts
- Alert on activity associated with known vulnerabilities



# Attack Surface Discovery



## A NDR needs the ability to identify vulnerabilities in the infrastructure:

- Discovery of unauthorized servers, firewall rules and access; use of vulnerable protocols
- Detect successful reconnaissance attempts, e.g., TCP connections to open ports
- Identify breaches of security controls, e.g., use of external DNS services
- Poor SSL hygiene, e.g., weak cipher suites and certificates



# Contact-Tracing For Incidents



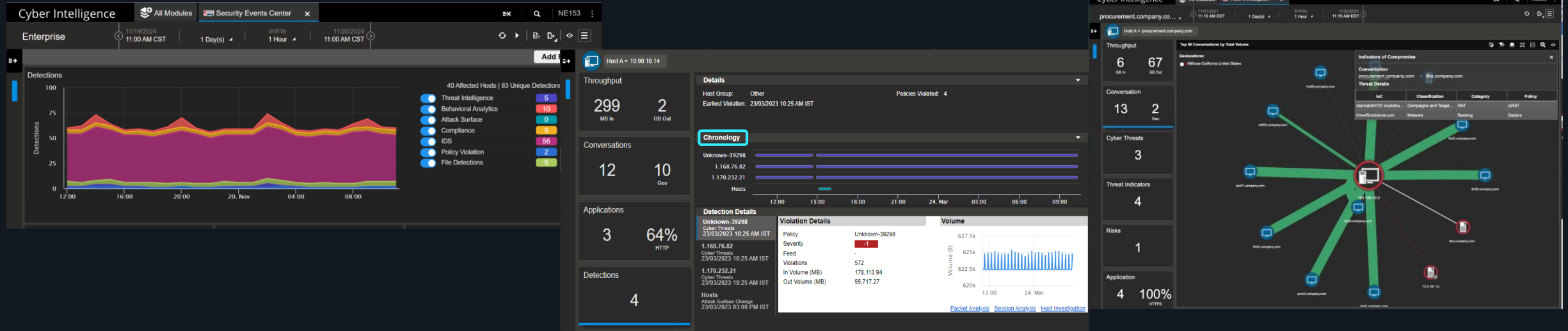
A NDR needs to enable incidence response teams to reduce Mean Time To Knowledge to minutes:

- Collect evidence
- Identify the entry points and attack vectors used by the threat actor
- Determine if lateral movement or data exfiltration occurred
- Focus resources on incident boundary by establishing the extent of a breach or anomaly





# Back In Time Investigation



51	1:58:45.798.297.834 PM EDT	0.000.015.395	54	FINANCEDB.company.com	eng02.company.com	TCP: S=51670 D=43479 LEN=0 SEQ=171501477 ACK=34662	ACK
52	1:58:45.798.461.881 PM EDT	0.000.164.047	95	FINANCEDB.company.com	eng02.company.com	FTP: Response 200 Active data connection established.	ACK/PSH
53	1:58:45.798.463.075 PM EDT	0.000.001.194	95	FINANCEDB.company.com	eng02.company.com	TCP: S=21 D=60570 LEN=41 SEQ=3696153880 ACK=394866	ACK/PSH
54	1:58:45.799.123.236 PM EDT	0.000.660.161	79	eng02.company.com	FINANCEDB.company.com	FTP: Request RETR finance_export.csv	ACK/PSH
55	1:58:45.799.963.454 PM EDT	0.000.840.218	108	FINANCEDB.company.com	eng02.company.com	FTP: Response 125 Data connection already open. Transfer sta	ACK/PSH

## Mean Time To Knowledge needs to be reduced from weeks or months to minutes:

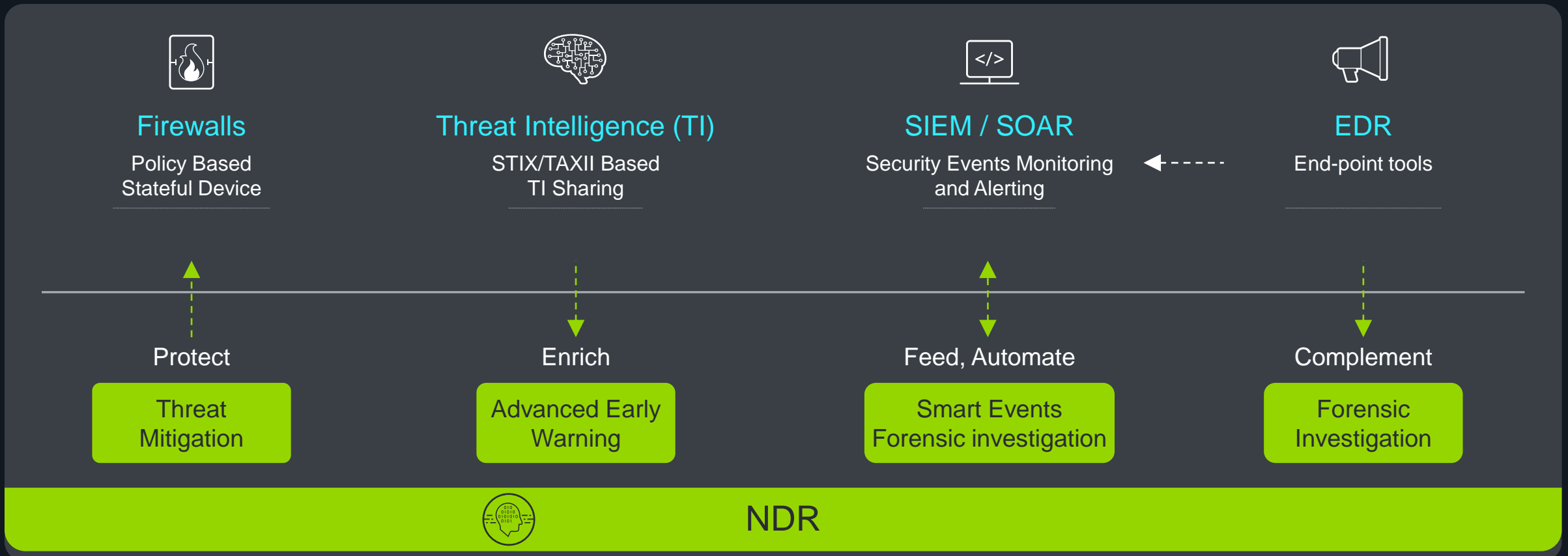
- Quickly browse backwards through massive amounts of network traffic
- View breaches and anomalies as they happened
- Avoid re-creating problems or waiting for repeat incidents to troubleshoot them
- Apply newly available IoCs *IP addresses* retrospectively





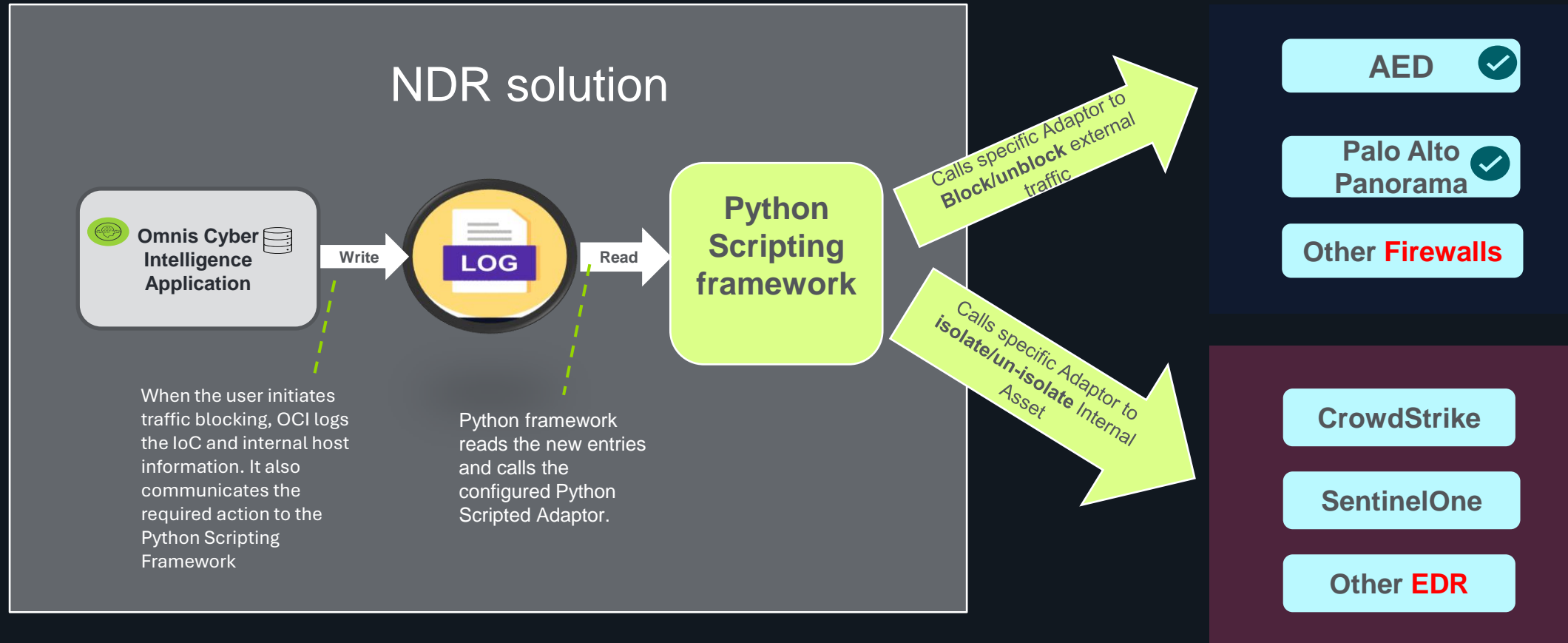
# NDR in the Security Ecosystem

Fully Integrated with Security Stack to Maximize ROI



# Open Architecture for 3<sup>rd</sup> Party Integration

An Open Integration Architecture to integrate with any Firewall (block Traffic) or EDR (quarantine Assets), by calling their exposed API interface.



# SIEM integration

Global Time Range: Last 60 minutes | Event Type: All | Severity: All | Attacker: All | Target: All

**Event Type and Affected hosts**

IDS Analytics	8
Behavioral Analytics	3
Policy Violation	2

**Attackers by Country**

**Targets**

Not Applicable	10.200.6.15
192.168.27.140	172.20.136.223
192.168.26.91	192.168.11
192.168.25.201	
192.168.23.215	
192.168.23.108	
192.168.21.17	192.168.1101

**Severity**

8	1
7	2
6	
5	3

**Event Investigation - Select Event Type**

**Attackers**

Select Attacker to be denied in Arbor Edge Defense

192.168.175.116	31.41.244.124
	78.46.218.253
	172.20.136.168
192.168.1101	

**Arbor Edge Defense**

Click on icon to set deny rule in Arbor Edge Defense for selected attacker

**Arbor Edge Defense - Denied Hosts rules**

Waiting for Input...

Select single target event in the Event Investigation panel then select Icon

- Click on icon to launch Host Investigation
- Click on icon to launch Behavioral Analytics
- Click on icon to launch Dashboard

**Current Event Count**

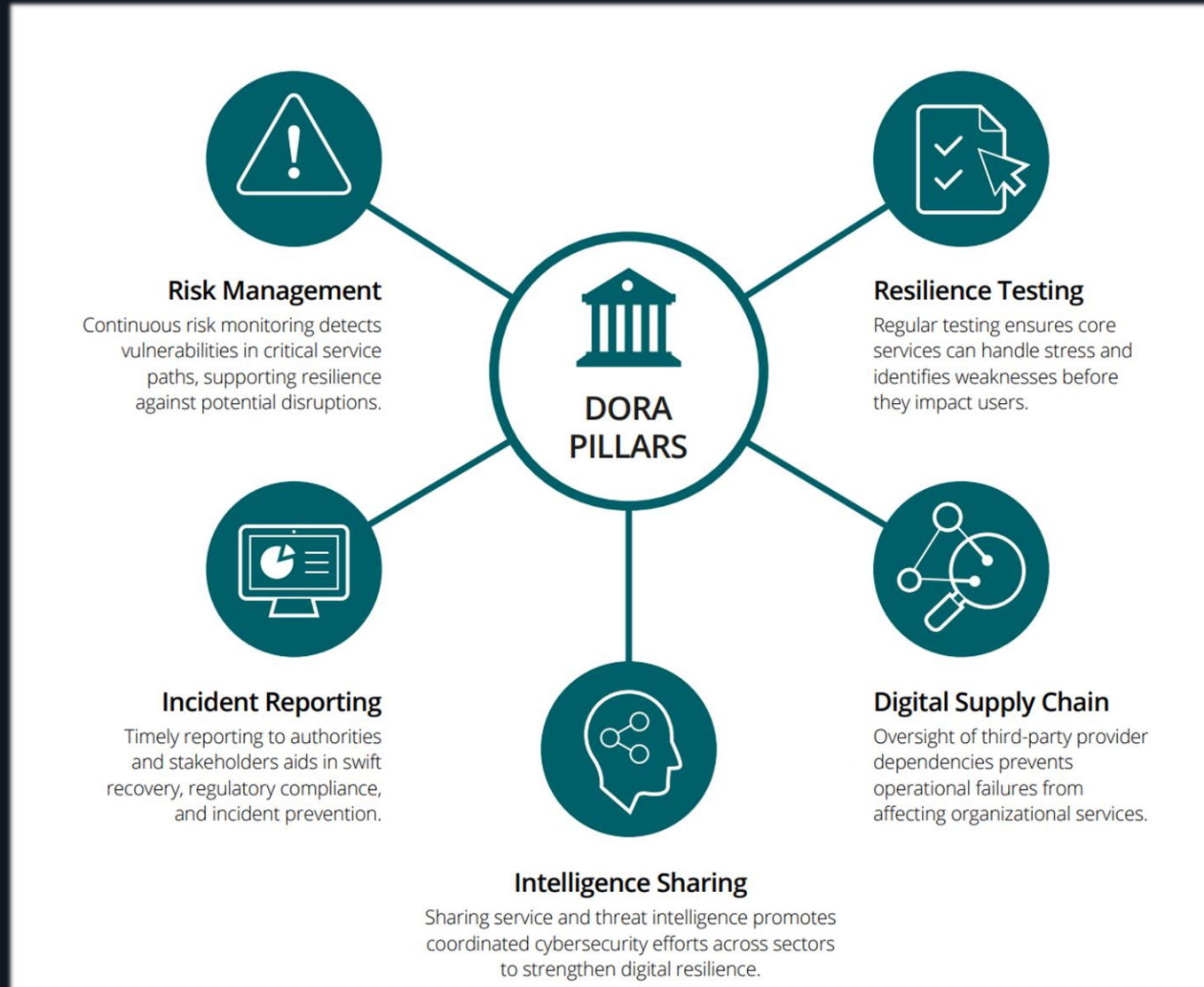
0

Trend comparison with Event count 24 hours ago



# Continuous risk monitoring for Compliance and Performance Standards

DORA – NIS-2



NETSCOUT®

Guardians of the Connected World