STELLAR CYBER®

Making Security Operations Simpler

Snehal Contractor

Vice President

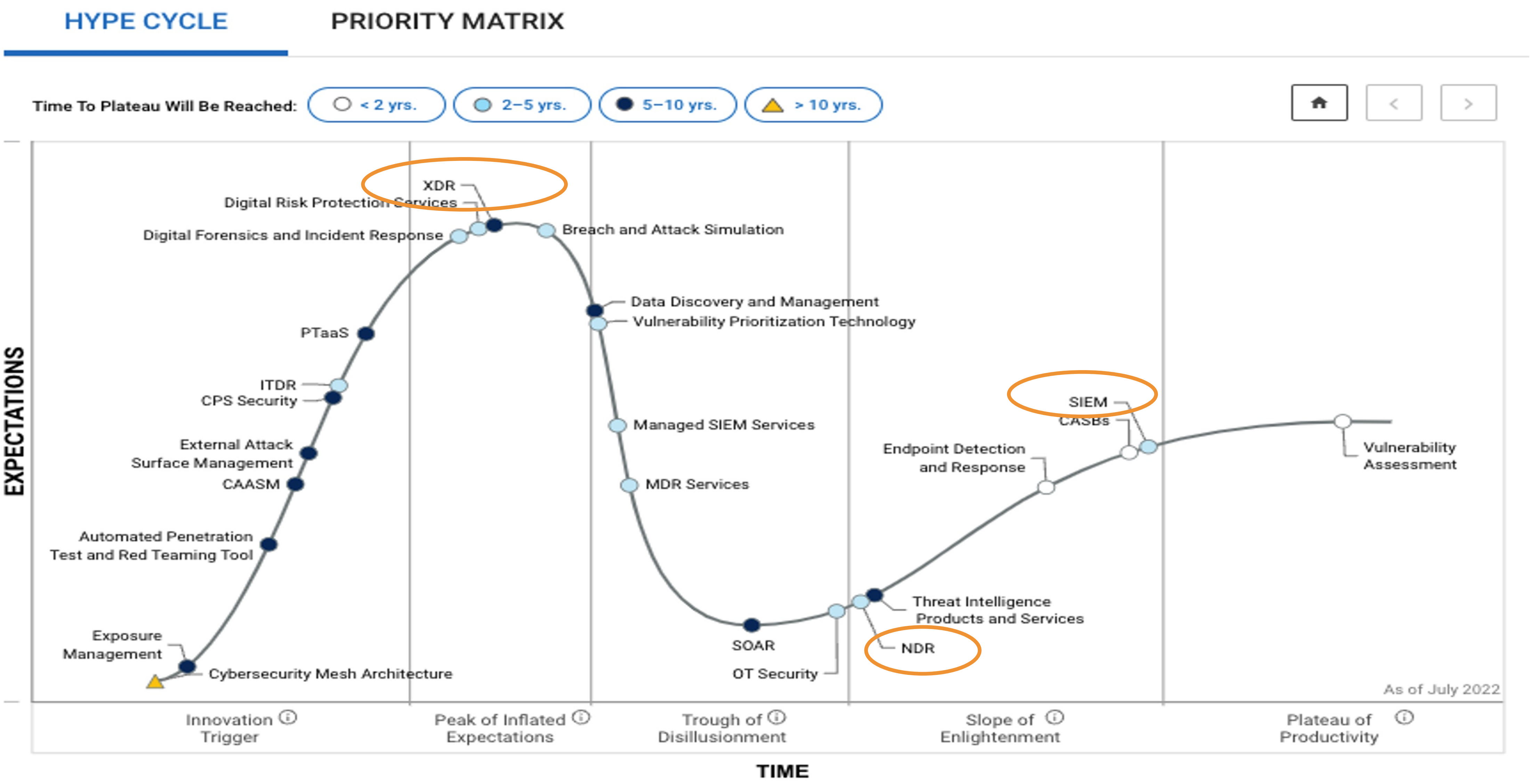
Global Sales Engineering

snehal@stellarcyber.ai

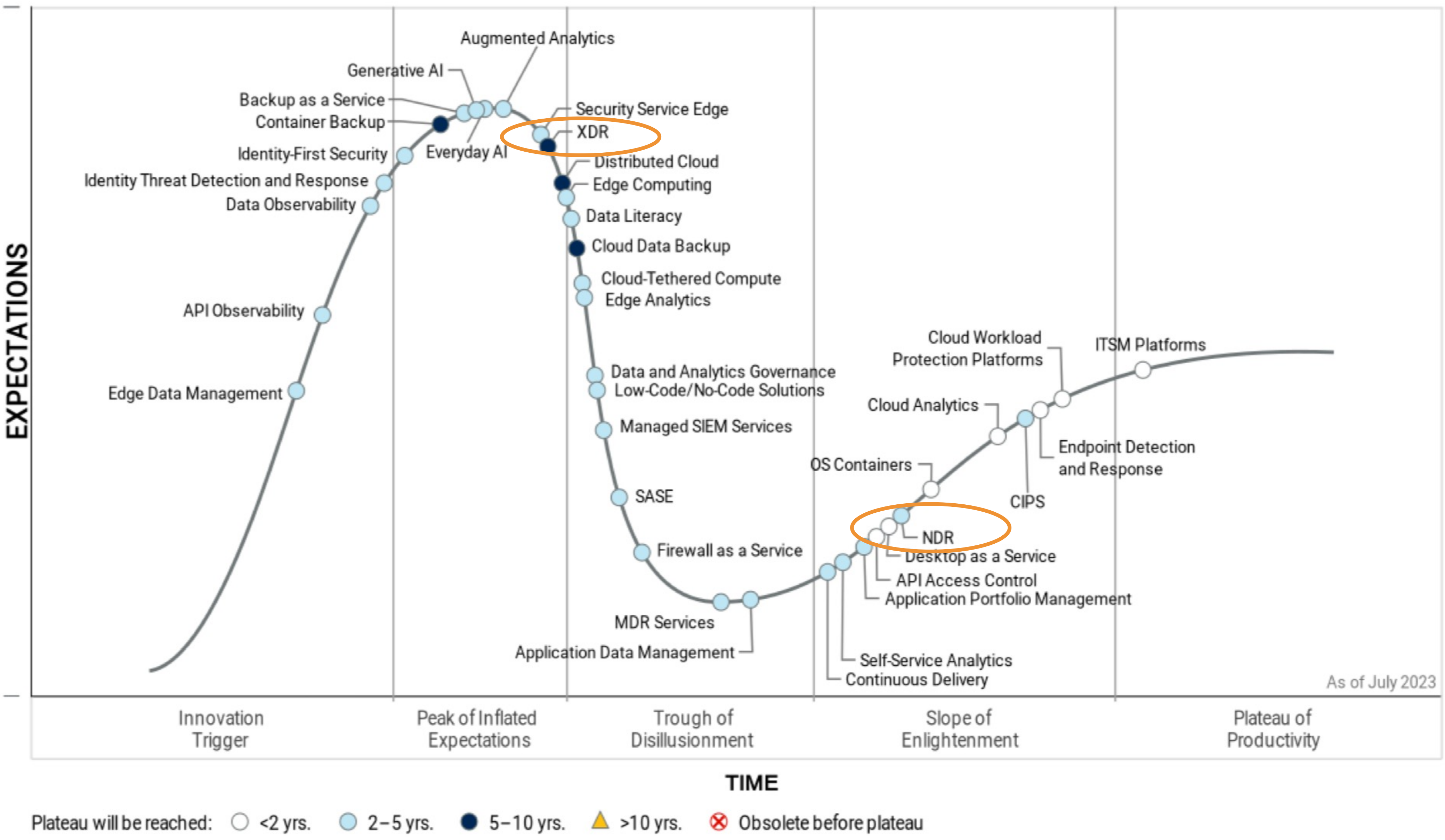
+1 847 760 7700

August 2023

Gartner Technology Hyper Cycle - 2022



Gartner Technology Hyper Cycle - 2023



STELLAR CYBER®

Gartner® Open vs. Closed vs. Anchored XDR

Open XDR

- Best of breed components
- Minimizes partner lock-in
- Requires significant integration
- Does not require any rip and replace of current security tools
- Example vendors: Exabeam Fusion XDR, ReliaQuest
  Stellar Cyber Open XDR

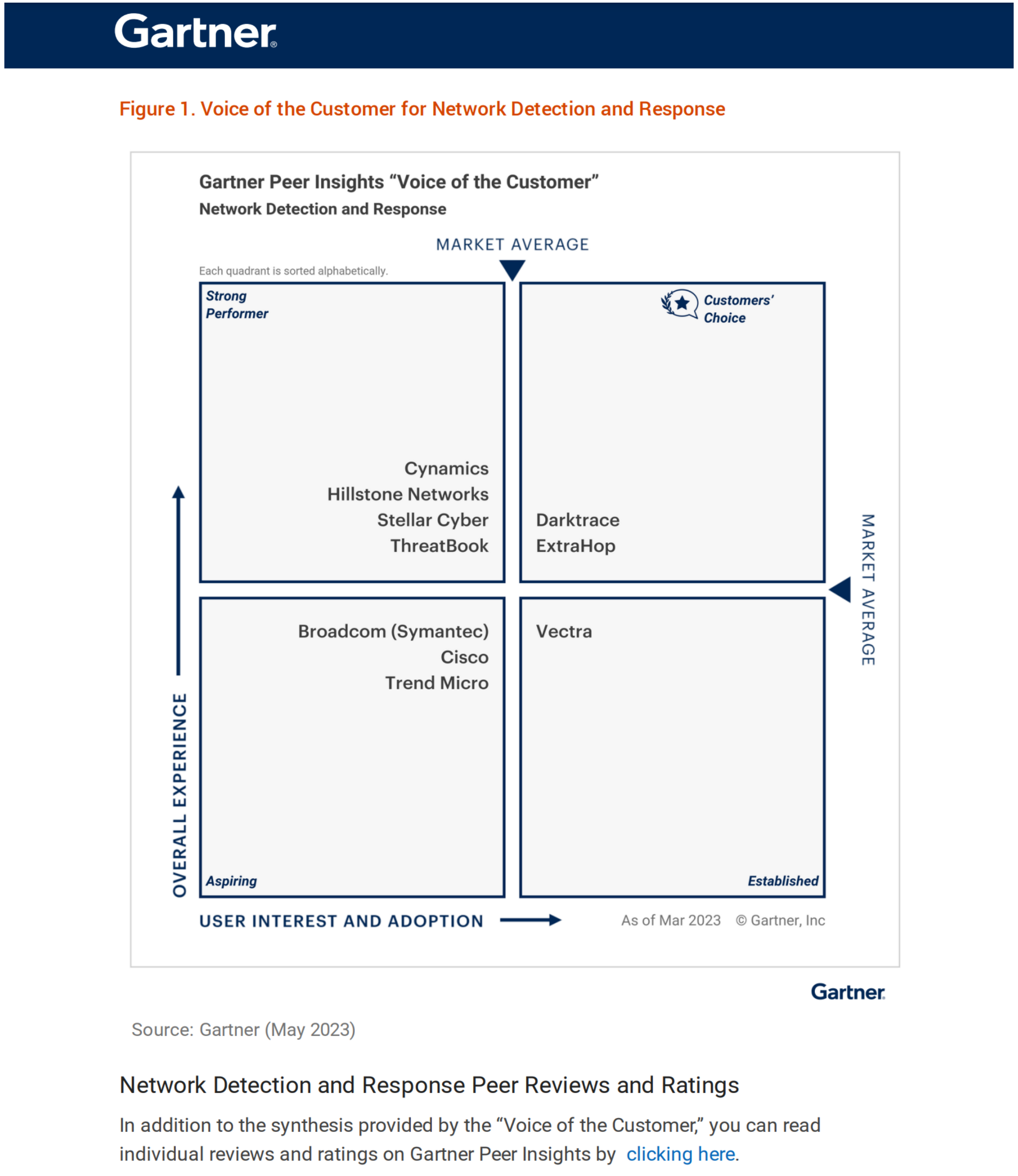
Native/Closed XDR

- Integrate security **tools from a single vendor**
- Example vendors: Microsoft 365 Defender, Palo Alto Networks, Cisco XDR

Anchored XDR

- Halfway point between open and closed XDR
- Relies on integrations with third parties for telemetry, with a **heavy reliance on EDR**
- Works well for service offering leaders with modest security investment footprints or vast numbers of technical partners

STELLAR CYBER®



Gartner

Figure 1. Voice of the Customer for Network Detection and Response

Gartner Peer Insights "Voice of the Customer"
Network Detection and Response

MARKET AVERAGE

Each quadrant is sorted alphabetically.

Strong Performer

Cynamics
Hillstone Networks
Stellar Cyber
ThreatBook

Customers' Choice

Darktrace
ExtraHop

Aspiring

Broadcom (Symantec)
Cisco
Trend Micro

Established

Vectra

OVERALL EXPERIENCE

USER INTEREST AND ADOPTION

MARKET AVERAGE

As of Mar 2023 © Gartner, Inc

Gartner

Source: Gartner (May 2023)

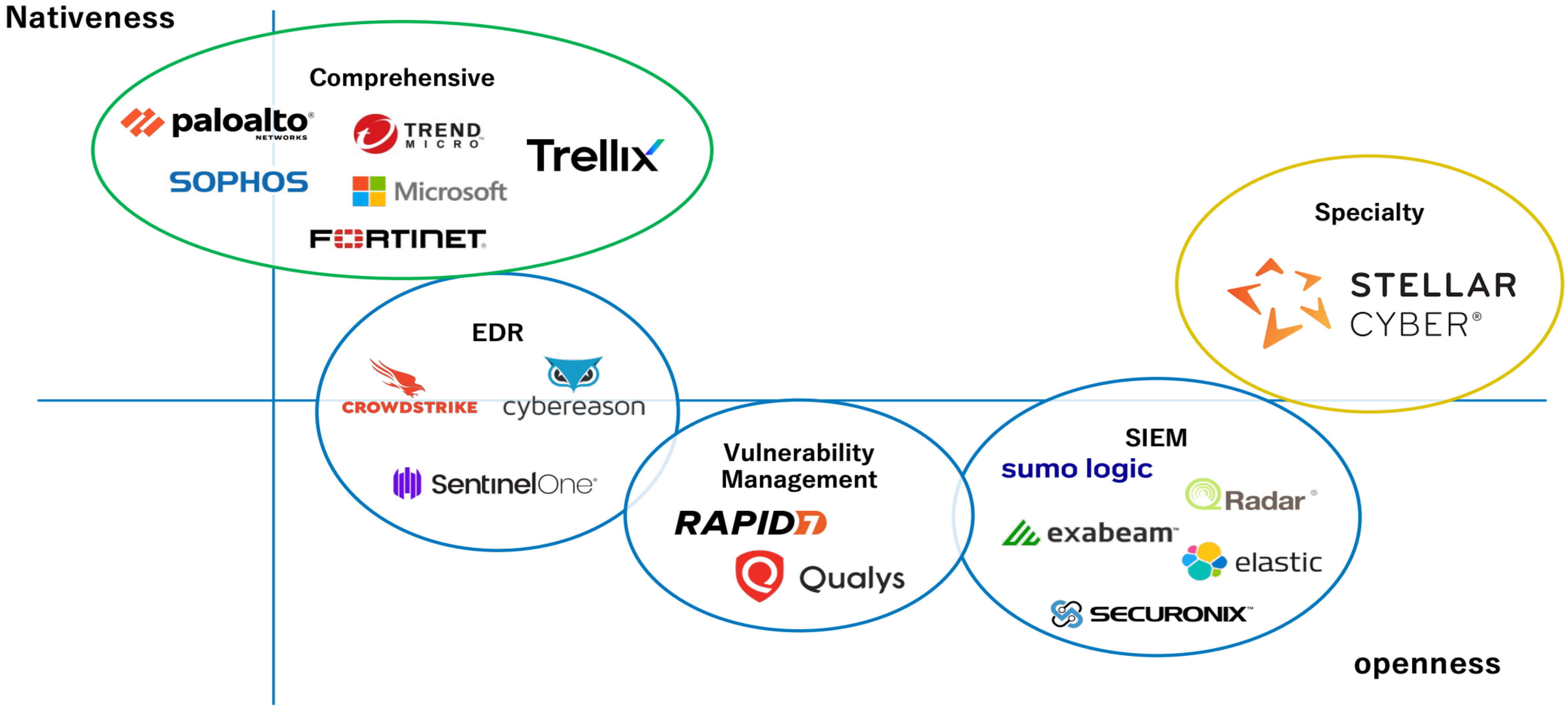
Network Detection and Response Peer Reviews and Ratings

In addition to the synthesis provided by the "Voice of the Customer," you can read individual reviews and ratings on Gartner Peer Insights by clicking here.

Gartner

STELLAR
CYBER®

XDR Players



Nativeness

Comprehensive

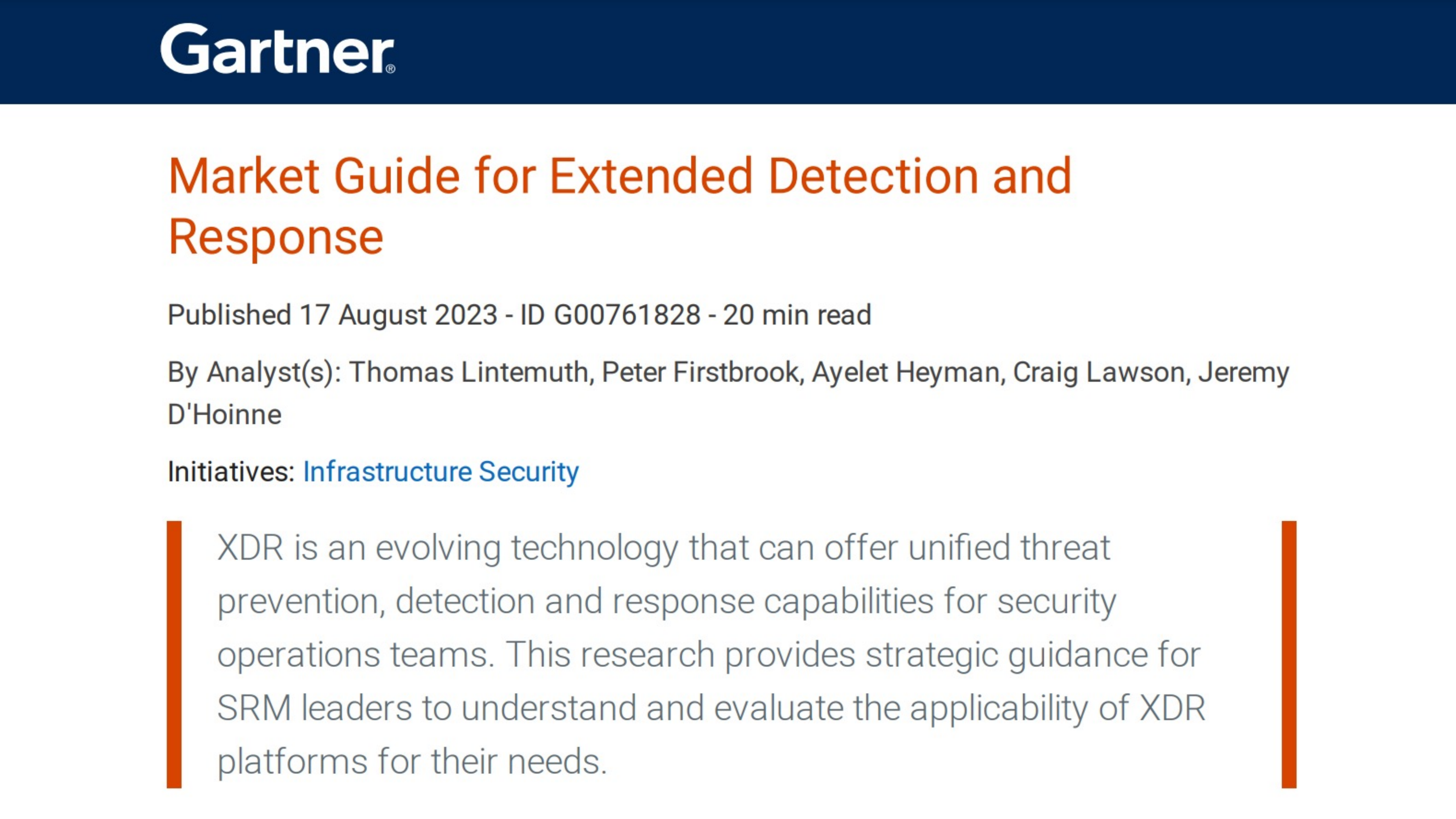
EDR

Vulnerability Management

SIEM

Specialty

openness



Gartner

Market Guide for Extended Detection and Response

Published 17 August 2023 - ID G00761828 - 20 min read

By Analyst(s): Thomas Lintemuth, Peter Firstbrook, Ayelet Heyman, Craig Lawson, Jeremy D'Hoinne

Initiatives: Infrastructure Security

XDR is an evolving technology that can offer unified threat prevention, detection and response capabilities for security operations teams. This research provides strategic guidance for SRM leaders to understand and evaluate the applicability of XDR platforms for their needs.

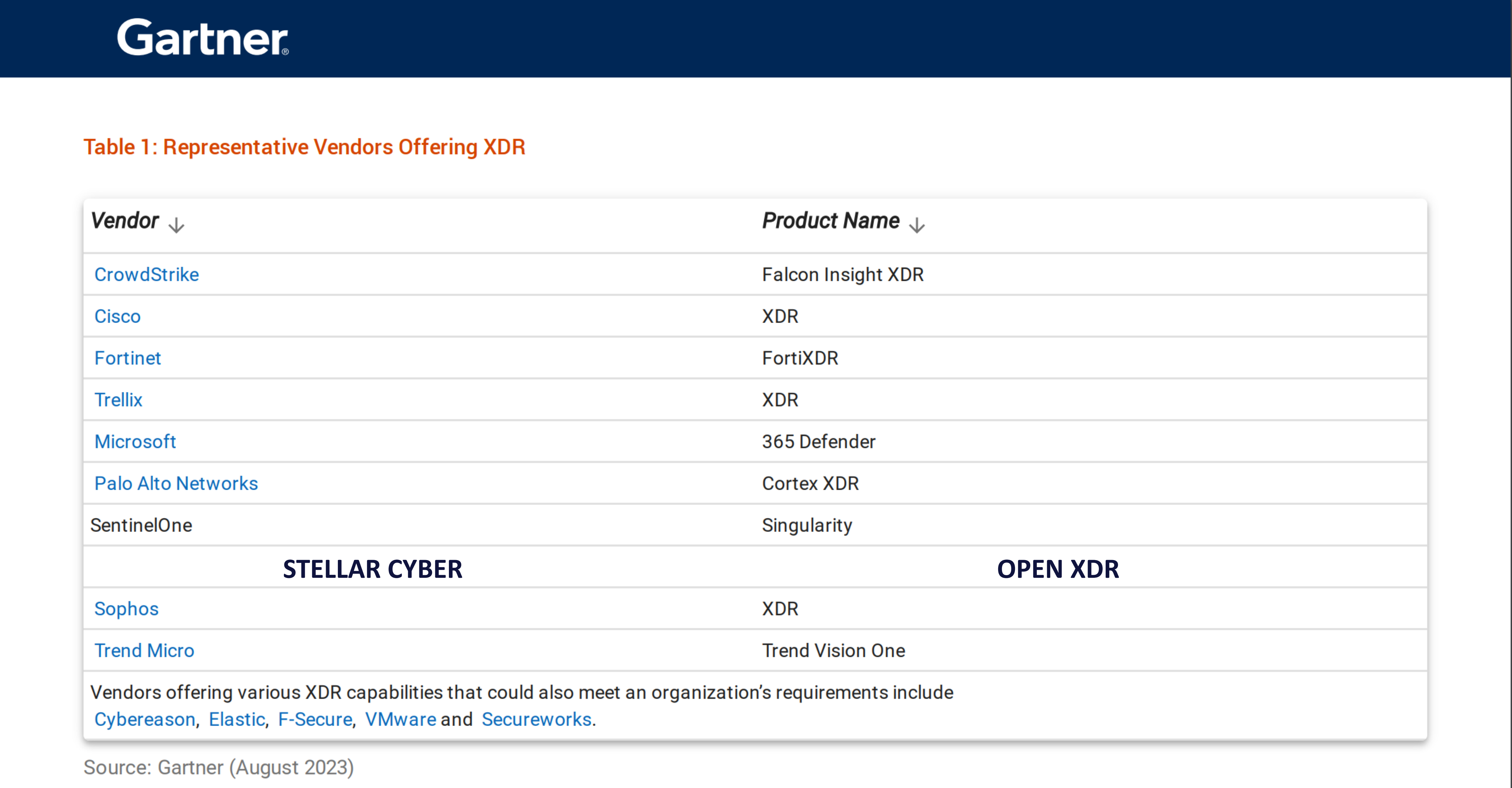


Table 1: Representative Vendors Offering XDR

Vendor ↓	Product Name ↓
CrowdStrike	Falcon Insight XDR
Cisco	XDR
Fortinet	FortiXDR
Trellix	XDR
Microsoft	365 Defender
Palo Alto Networks	Cortex XDR
SentinelOne	Singularity
STELLAR CYBER	**OPEN XDR**
Sophos	XDR
Trend Micro	Trend Vision One
Vendors offering various XDR capabilities that could also meet an organization's requirements include Cybereason, Elastic, F-Secure, VMware and Secureworks.	

Source: Gartner (August 2023)

Gartner Market Guide for XDR - Summary

- Stellar Cyber: named as one of top XDR vendors
- Stellar Cyber vision of Open XDR and Gartner's findings are well-aligned
- HUGE validation for Stellar Cyber technology, model and GTM
  - Only Open XDR
  - Only pure play XDR
  - Only single platform, single license model
  - Only XDR vendor to offer SIEM, NDR and integrate with all leading EDRs
  - NDR is a key requirement for XDR
  - No SIEM vendor made the list!
  - "Mid market" is the current sweet spot for XDR
  - Customers are encouraged to leverage their current investment in tools (Open)
  - "Bring Your Own EDR" is seen as an effective way to deliver EDR capability
  - Only Stellar Cyber gives customers true flexibility to control their security tech stack

Addressing Industry Challenges

The Case for Open XDR

Infrastructure Security
Network Firewall
Network Monitoring
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Protection & Anti-Virus
Endpoint Detection & Response
Messaging Security
Application Security
WAF & Application Security
Vulnerability Assessment
Web Security
IoT Security
Transaction Security
Security Operations & Incident Response
SIEM
Security Incident Response
Risk & Compliance
Threat Intelligence
Specialized Threat Analysis & Protection
Mobile Security
Identity & Access Management
Cloud Security

Source: Momentum Partners.

Security Stack

Security Operations Stack

The Security Tool and Vendor landscape is growing out of control.

How does an organization defend itself **efficiently** and **on-budget** given this complexity?

Too many Tools and Vendors creates **complexity**.

↑ Tools

↑ Vendors

↑↑ Data

↑↑ Alerts

↑↑ Licenses

↑↑ DevOps

STELLAR CYBER®

Stellar Cyber Open XDR

Simplifies the Complexity of Security Operations

Simply Connect all your existing tools into the Stellar Cyber Open XDR Platform

Automatically Identify and **Correlate** threats using intelligent data analysis

Automate Response and take decisive action fast directly from Stellar

Open XDR Business Value

Focus on the Things That Matter – Capture all of the data from disparate tools in our platform, correlate & enrich it, giving your analysts the ability to respond efficiently and control incidents.

On-board Any Technology – Open means ingest everything in the environment.

Tool Consolidation – Keep what you need, replace what you don’t = Lower cost/Greater Margins!

Reduce Manual Work – By correlating the threat data across the entire attack surface; Take educated, appropriate actions via our automated SOAR Playbooks.

Reduce SOC Burnout – Complexity of disparate tools combined with false positives leads to Analyst burnout.

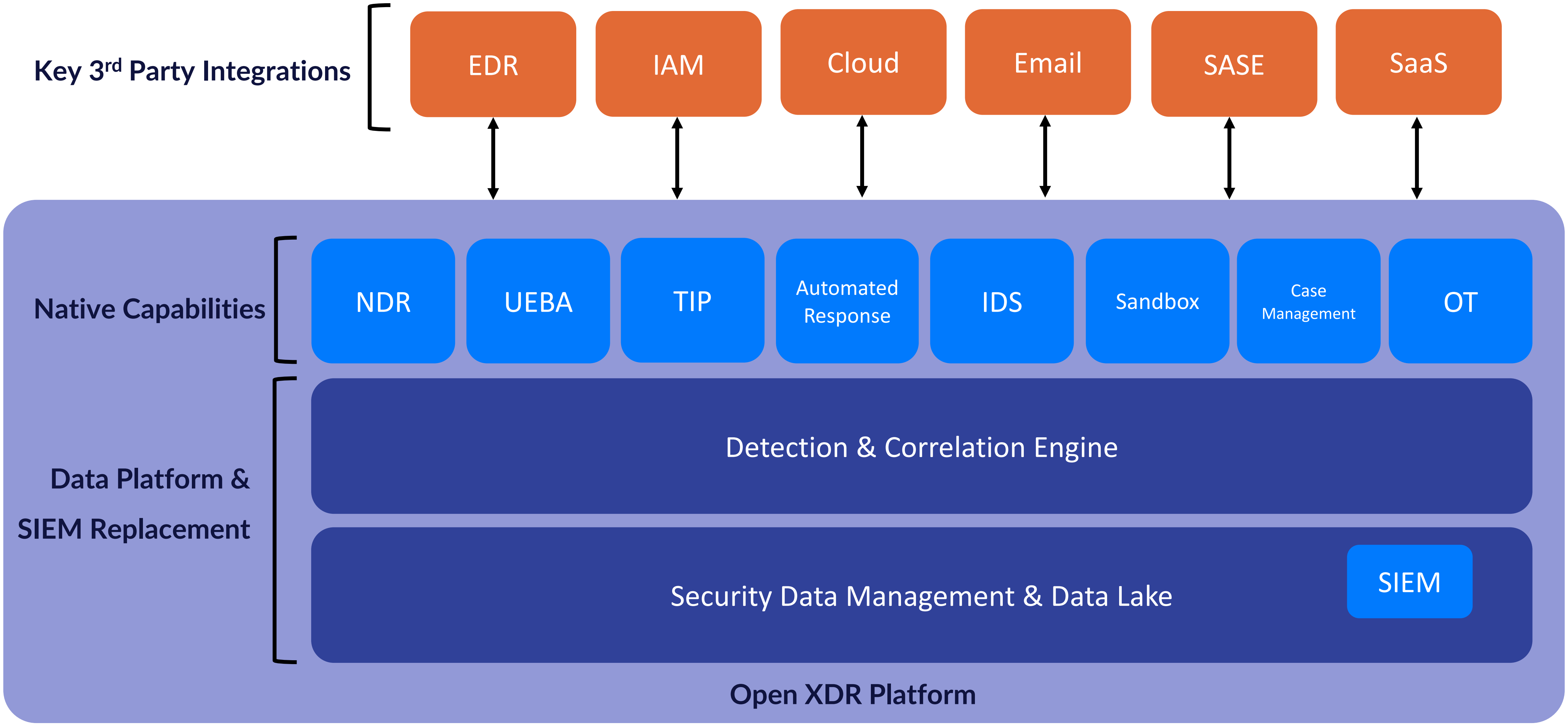
Stellar Cyber View on the Central Security Operations Question

WHICH OF THESE PAIN POINTS RESONATE WITH SECOPS TEAMS?

- Not all *relevant* security data is consolidated into a single location for complete visibility
- *Rule* creation and maintenance is tedious and produces low accuracy
- Manually correlating events is a physically and time- intensive process
- Manually coordinated response across security tools increases attack dwell time

STELLAR CYBER®

OPEN XDR PLATFORM CORE PRINCIPLES



Key 3rd Party Integrations

EDR

IAM

Cloud

Email

SASE

SaaS

Native Capabilities

NDR

UEBA

TIP

Automated Response

IDS

Sandbox

Case Management

OT

Data Platform & SIEM Replacement

Detection & Correlation Engine

Security Data Management & Data Lake

SIEM

Open XDR Platform

STELLAR CYBER®

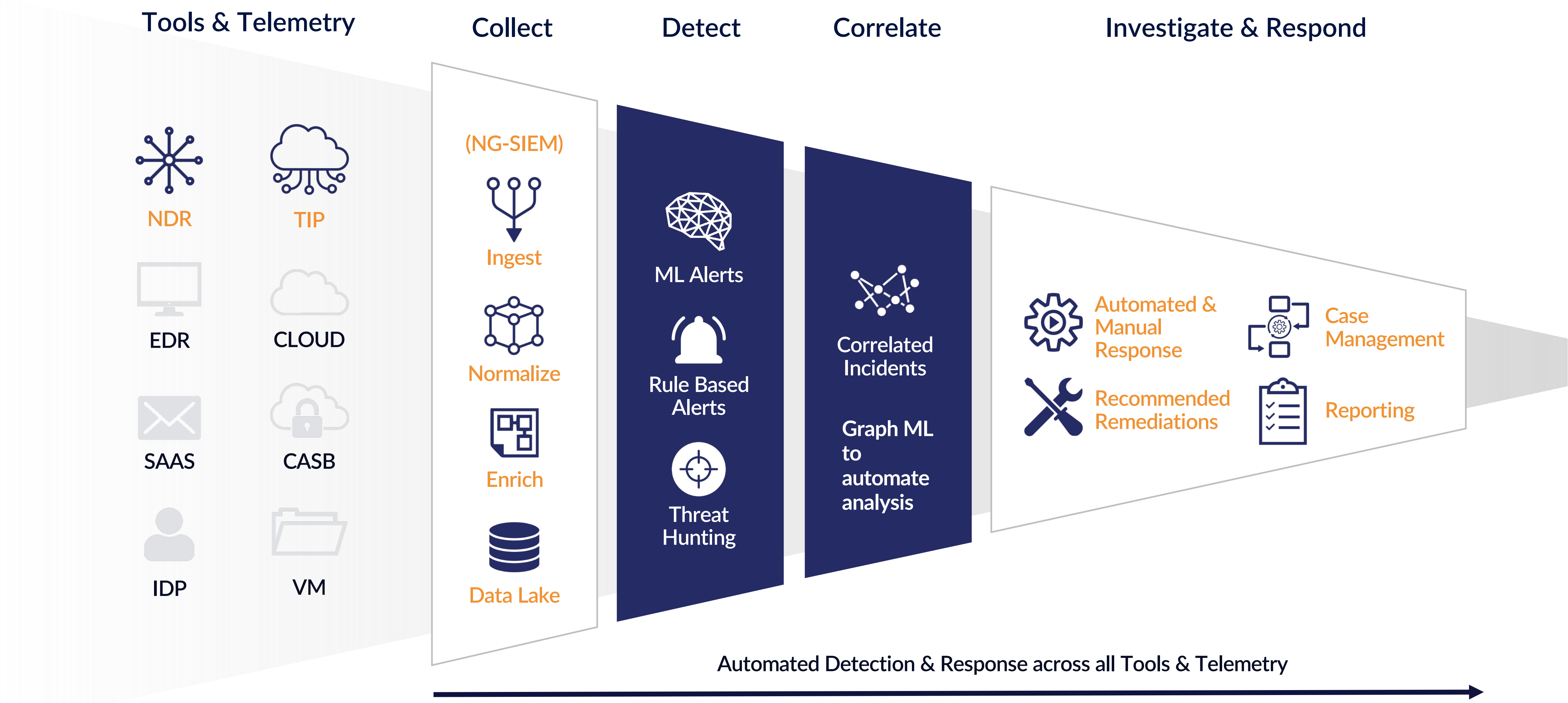
Data Coverage/Integration

- Network:
  - NDR: **Network Sensor**: DPI, **Security Sensor** : sandbox, IDS
  - Firewall logs: Cisco, Palo Alto, Checkpoint, Barracuda, etc
  - Netflow
- Syslog: **Log Forwarder**: nearly 500 parsers, (add based on customer requests)
- API Connectors:
  - Vulnerability Scanner: Tenable, Rapid7, Qualys etc
  - Cloud data: AWS Cloud Trail, Guard Duty, Cloud Watch, Azure EventHub, GCP Audit, OCI Cloud Guard etc
  - SaaS: Office 365, Gsuite, SalesForce, Box, etc
  - Identity provider: Azure AD, Windows AD, Okta, Duo Security, OneLogin,etc
- Endpoint
  - All major EDR: CrowdStrike, SentinelOne, CarbonBlack, Cylance, Cybereason, MS Defender, Cisco AMP etc
  - **Server sensor**: Windows, Linux
  - Antivirus: Windows Defender, Sophos, Trend Micro etc
- TI provider:
  - Proofpoint Emerging Threat Pro, DHS, AT&T AlienVault OTX, PhishTank, OpenPhish, abuse.ch, Anomali ThreatStream* etc
  - Any STIX/TAXI feeds

STELLAR CYBER®

SINGLE PLATFORM AND SINGLE LICENSE FOR SECURITY OPERATIONS

■ Native Components to Stellar Cyber's Open XDR Platform



Tools & Telemetry

NDR
TIP
EDR
CLOUD
SAAS
CASB
IDP
VM

Collect

(NG-SIEM)
Ingest
Normalize
Enrich
Data Lake

Detect

ML Alerts
Rule Based Alerts
Threat Hunting

Correlate

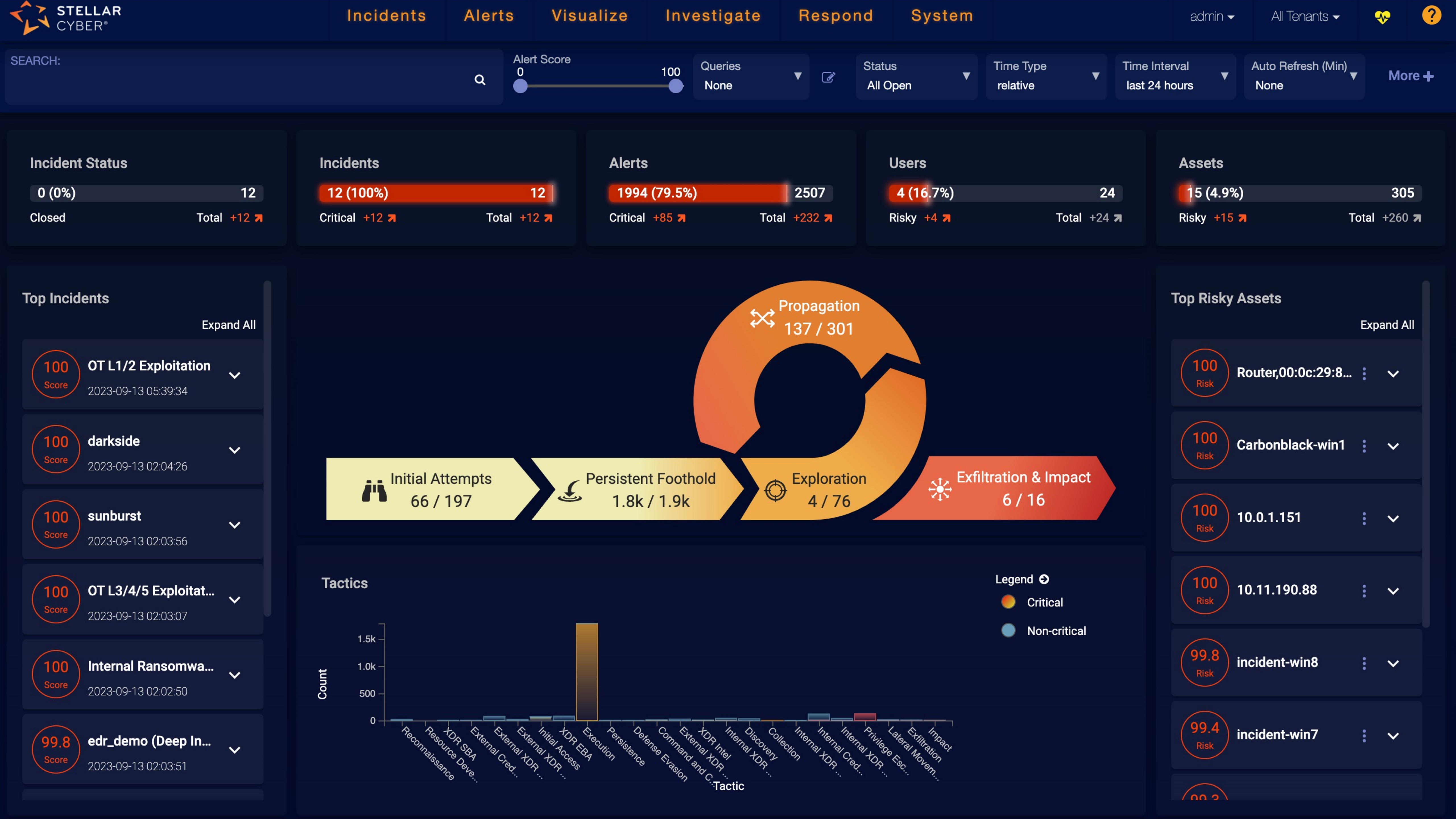
Correlated Incidents
Graph ML to automate analysis

Investigate & Respond

Automated & Manual Response
Case Management
Recommended Remediations
Reporting

Automated Detection & Response across all Tools & Telemetry

STELLAR CYBER®



SEARCH:

Alert Score 0 – 100

Queries: None

Status: All Open

Time Type: relative

Time Interval: last 24 hours

Auto Refresh (Min): None

Incident Status
0 (0%) — 12
Closed — Total +12

Incidents
12 (100%) — 12
Critical +12 — Total +12

Alerts
1994 (79.5%) — 2507
Critical +85 — Total +232

Users
4 (16.7%) — 24
Risky +4 — Total +24

Assets
15 (4.9%) — 305
Risky +15 — Total +260

Top Incidents

Expand All

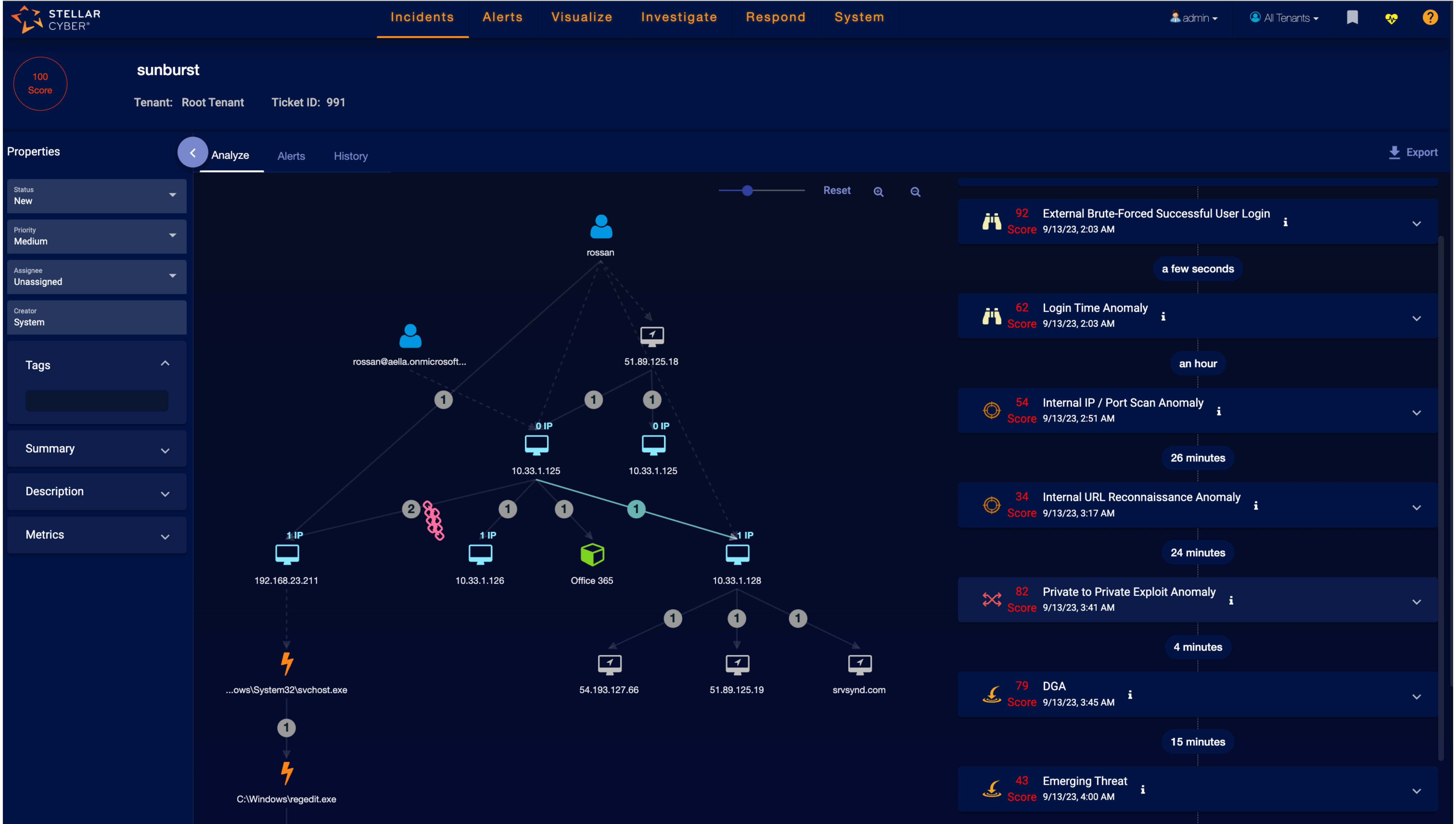
Score	Incident	Time
100	OT L1/2 Exploitation	2023-09-13 05:39:34
100	darkside	2023-09-13 02:04:26
100	sunburst	2023-09-13 02:03:56
100	OT L3/4/5 Exploitat...	2023-09-13 02:03:07
100	Internal Ransomwa...	2023-09-13 02:02:50
99.8	edr_demo (Deep In...	2023-09-13 02:03:51

Tactics

Top Risky Assets

Expand All

Risk	Asset
100	Router,00:0c:29:8...
100	Carbonblack-win1
100	10.0.1.151
100	10.11.190.88
99.8	incident-win8
99.4	incident-win7
99.3	



100 Score

sunburst

Tenant: Root Tenant   Ticket ID: 991

Properties

Status: New

Priority: Medium

Assignee: Unassigned

Creator: System

Tags

Summary

Description

Metrics

92 Score — External Brute-Forced Successful User Login — 9/13/23, 2:03 AM

a few seconds

62 Score — Login Time Anomaly — 9/13/23, 2:03 AM

an hour

54 Score — Internal IP / Port Scan Anomaly — 9/13/23, 2:51 AM

26 minutes

34 Score — Internal URL Reconnaissance Anomaly — 9/13/23, 3:17 AM

24 minutes

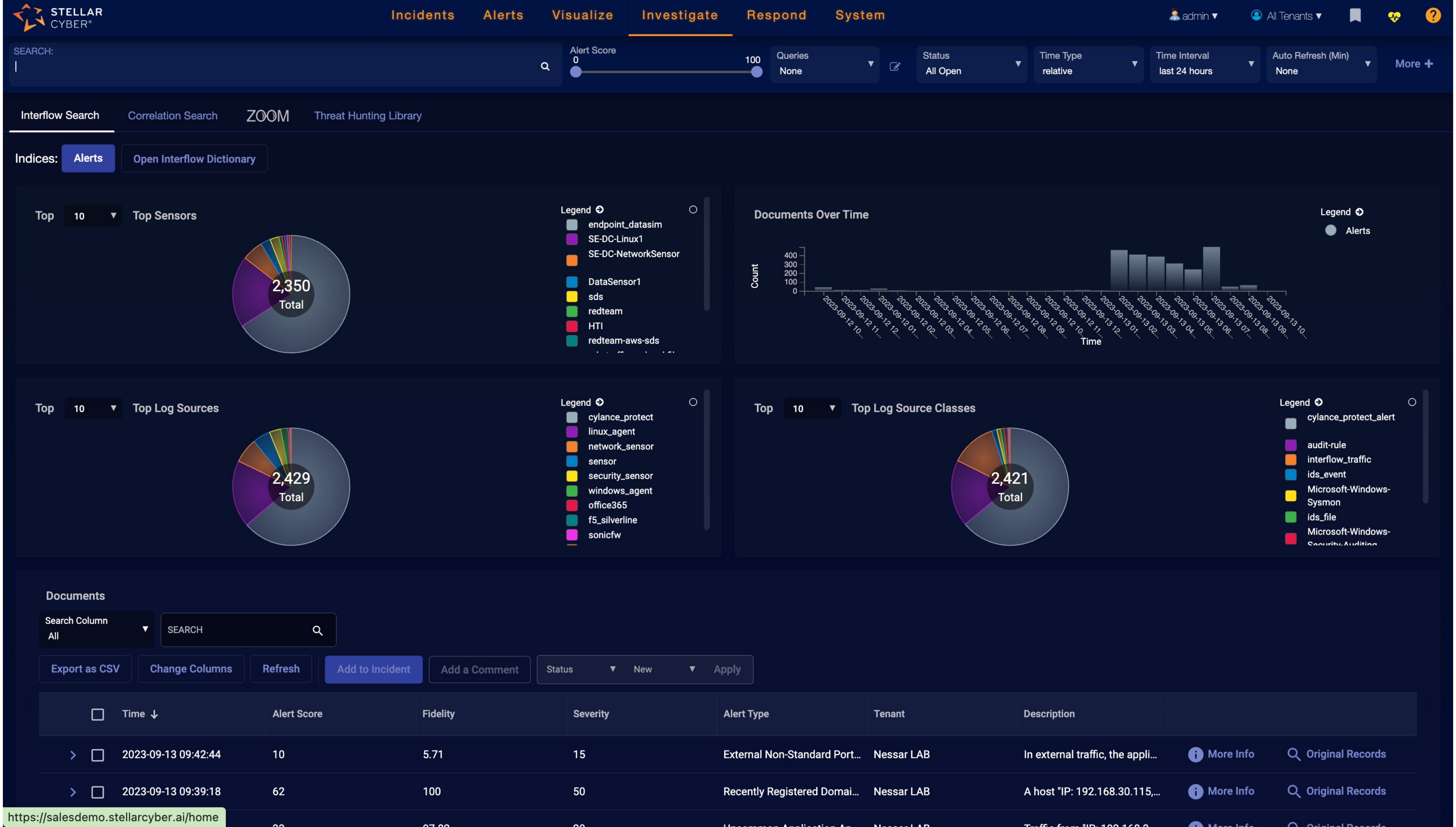
82 Score — Private to Private Exploit Anomaly — 9/13/23, 3:41 AM

4 minutes

79 Score — DGA — 9/13/23, 3:45 AM

15 minutes

43 Score — Emerging Threat — 9/13/23, 4:00 AM



SEARCH:

Alert Score: 0 – 100

Queries: None

Status: All Open

Time Type: relative

Time Interval: last 24 hours

Auto Refresh (Min): None

Indices: Alerts

Top 10 Top Sensors

2,350 Total

Legend
- endpoint_datasim
- SE-DC-Linux1
- SE-DC-NetworkSensor
- DataSensor1
- sds
- redteam
- HTI
- redteam-aws-sds

Documents Over Time

Legend
- Alerts

Top 10 Top Log Sources

2,429 Total

Legend
- cylance_protect
- linux_agent
- network_sensor
- sensor
- security_sensor
- windows_agent
- office365
- f5_silverline
- sonicfw

Top 10 Top Log Source Classes

2,421 Total

Legend
- cylance_protect_alert
- audit-rule
- interflow_traffic
- ids_event
- Microsoft-Windows-Sysmon
- ids_file
- Microsoft-Windows-Security-Auditing

Documents

Search Column: All

SEARCH

Status ▾ New ▾

	Time ↓	Alert Score	Fidelity	Severity	Alert Type	Tenant	Description		
› □	2023-09-13 09:42:44	10	5.71	15	External Non-Standard Port...	Nessar LAB	In external traffic, the appli...	More Info	Original Records
› □	2023-09-13 09:39:18	62	100	50	Recently Registered Domai...	Nessar LAB	A host "IP: 192.168.30.115,...	More Info	Original Records

https://salesdemo.stellarcyber.ai/home

Stellar Cyber Open XDR – Unique Advantages

- ✓ **Single License:** ALL functionality included; single license per service provider
- ✓ **Single Platform:** Unified and automated detections and correlation
- ✓ **Open Platform:** Deep Integrations, Retain current investments with 500+ existing integrations
- ✓ **Optimal for Service Providers:** Multi-Tier, Multi-Tenant; no MSSP or per-tenant fees
- ✓ **Flexible Deployment:** Public/Private cloud (PaaS agnostic), on-prem or SaaS
- ✓ **Continuous Content Update**
  - TIP & Security Research team continuously pushes threat detections to the platform
- ✓ **Modernized Security Operations:** Easy to deploy, easy to use
  - Designed for self-service: Create tenants, deploy sensors, launch connectors with a single click
  - Custom, hi-touch onboarding and enablement to optimize deployment, knowledge transfer, efficiency, and GTM value for security architect, sales and customer success teams

STELLAR
CYBER®

Thank You

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Call to Action >>