threatNIXD

Managed Detection and Response

www.castellumlabs.com

info@castellumlabs.com

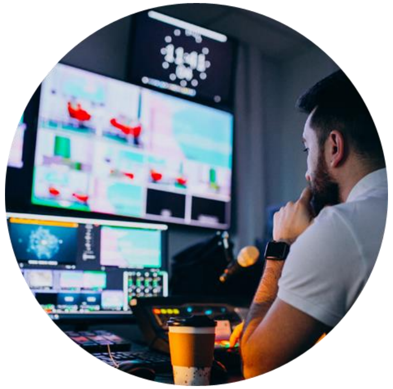
Our Platforms

Rajeev Shukla, Founder

- 25 years building IT products
- Leadership roles in Sun, CA, Quark and more
- Wide experience across US, India and Europe
- Founded Castellum Labs over three years back
- Commercially successful product/service portfolio

Portfolio

- Application Security & Governance
- Threat Intelligence & Threat Management
- SOC Monitoring (Managed Detection & Response)
- Cloud Security Solutioning and Cloud Security Operations



Foundation for Design

- Reporting is not Monitoring
- Data breaches don't hurt as much as ignorance
- Short-term service engagements deliver no real value
- Cybersecurity needs far more human intelligence than expected

watchOUT

Darkweb Monitoring

threatNiXD

Next Gen SOC Monitoring

appFORT

Continuous Application Security

threatNIXD

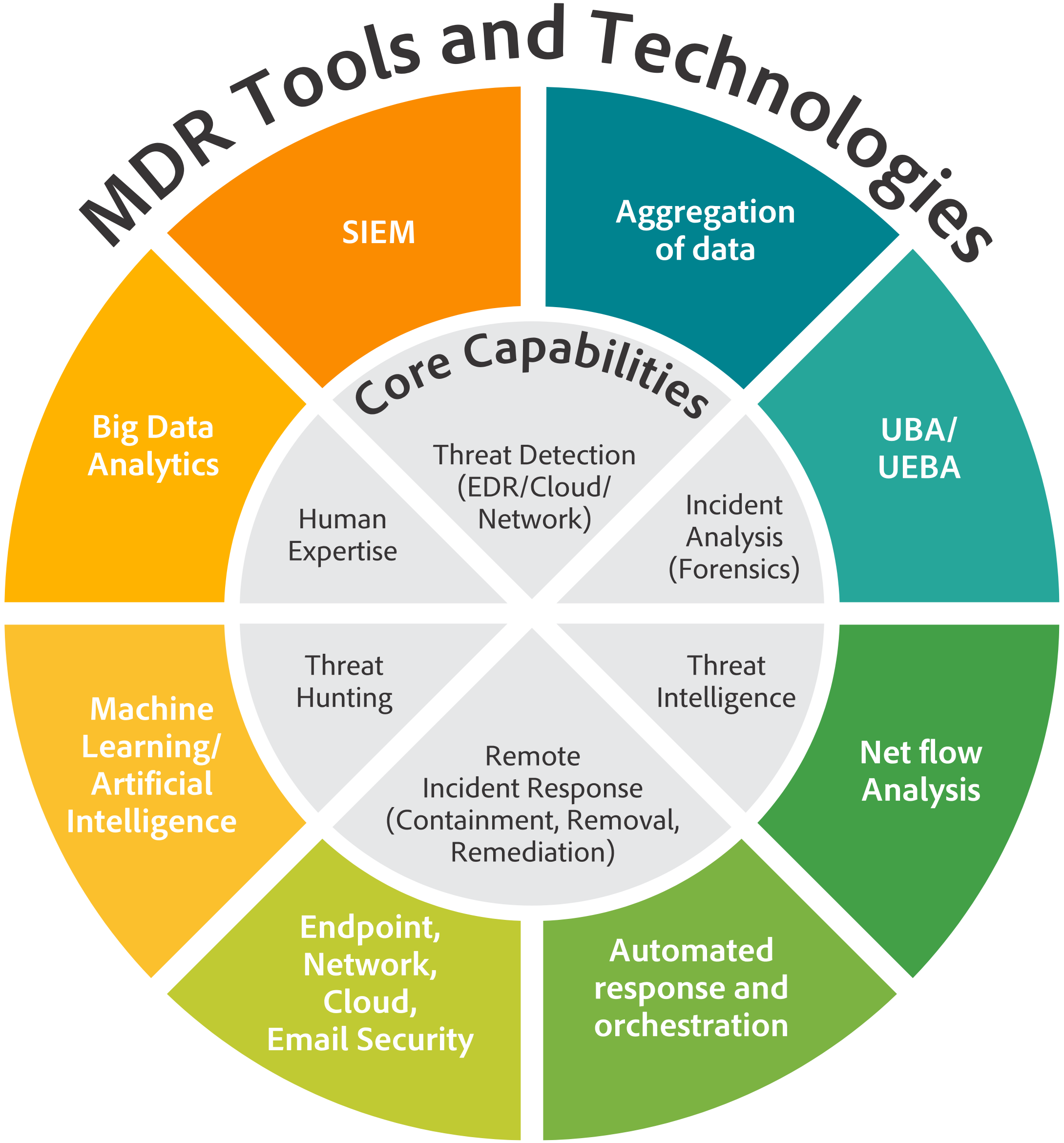
True Managed Detection & Response

www.getwatchout.com

Why Managed Detection and Response

Firewalls, intrusion detection systems, endpoint protection products, threat intelligence services, EDR, SIEM, UEBA, SOAR, IOA, IOC, UTM, IR, SOC, and many more technologies originated in response to emerging threats. Yet, as IDC says,

> "The perpetual shortage of cybersecurity professionals has led to a proliferation of incomplete or misconfigured security solutions. Even though cybersecurity budgets keep increasing, attackers still are often able to break through the patchwork of disparate systems to find their mark"


MDR Tools and Technologies
SIEM
Aggregation of data
UBA/ UEBA
Net flow Analysis
Automated response and orchestration
Endpoint, Network, Cloud, Email Security
Machine Learning/ Artificial Intelligence
Big Data Analytics
Core Capabilities
Threat Detection (EDR/Cloud/ Network)
Incident Analysis (Forensics)
Threat Intelligence
Remote Incident Response (Containment, Removal, Remediation)
Threat Hunting
Human Expertise

Why another MDR

Current MDR players focus only on large enterprise customers

- Cost and complexity of their technology platforms
- Multiple tools and solutions – integrated or acquired
- Vendors also need mature customers to be effective

Engagement and implementation is a challenge

- Legacy log and SIEM solutions exist in different stages of maturity
- In-house cybersecurity resources may not be up-to-date
- Getting to “go” is extremely time, money and people heavy

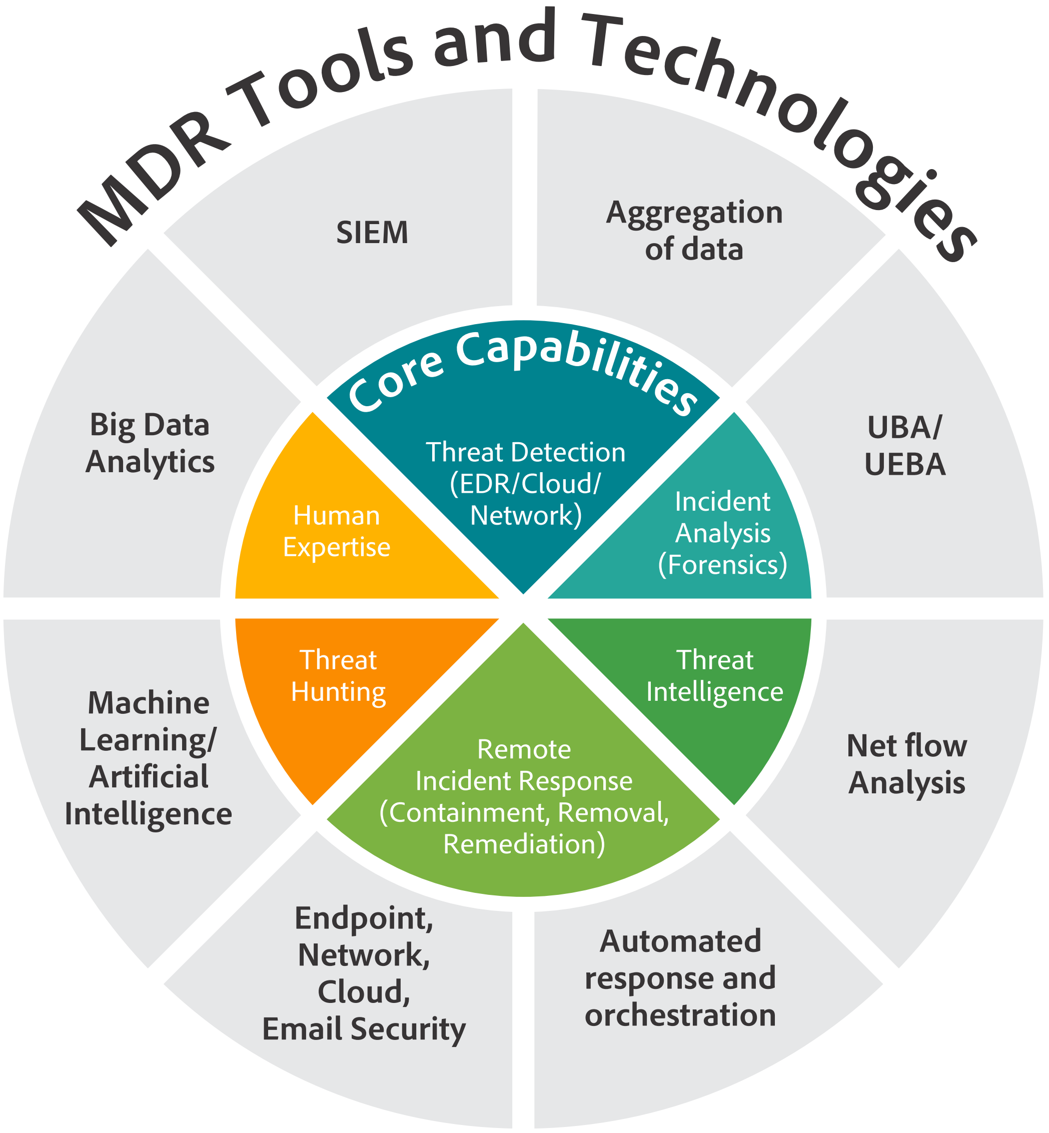
Closure of reported incidents is extremely poor

- Acknowledgement and coordination falls through org cracks
- Slow manual response by owners and product support vendors
- Inadequate or poor automated response capability

Where we Stand Out

Automation is essential to collate, manage and classify massive amount of data. Yet platforms that rely on automation alone are always playing catch up with threat actors who constantly devise means to avoid automatic detection. We don’t keep building obsolete castles with your money:

Human actors, external threat intelligence, threat hunting, manual threat detection, forensics and (what is generally poorly managed) Incident Response – manual and automated – these are our focus areas, since the tools and technologies are already built into our threatNiXD platform.



MDR Tools and Technologies
SIEM
Aggregation of data
UBA/ UEBA
Net flow Analysis
Automated response and orchestration
Endpoint, Network, Cloud, Email Security
Machine Learning/ Artificial Intelligence
Big Data Analytics
Core Capabilities
Threat Detection (EDR/Cloud/ Network)
Incident Analysis (Forensics)
Threat Intelligence
Remote Incident Response (Containment, Removal, Remediation)
Threat Hunting
Human Expertise

Not just another MDR

Contextual SOAR

Security orchestration, security automation and security response - the core elements of Security Orchestration and Response are at the heart of threatNiXD. And with our IoC analysts you get true **contextual** SOAR.

Integrated UEBA

Detect insider threats. Detect compromised accounts. Detect changes in permissions and creation of super users. Detect breach of protected data. Detect large data downloads. While not a complete UEBA solution, you get this as a basic capability.

Threat Intelligence

All the data in the world is useless without the intelligence to extract actionable signals from the noise. We have developed, and continuously refine and add to, a massive library of machine and human executed playbooks to sense, target and pick out risks, exploits and weaknesses.

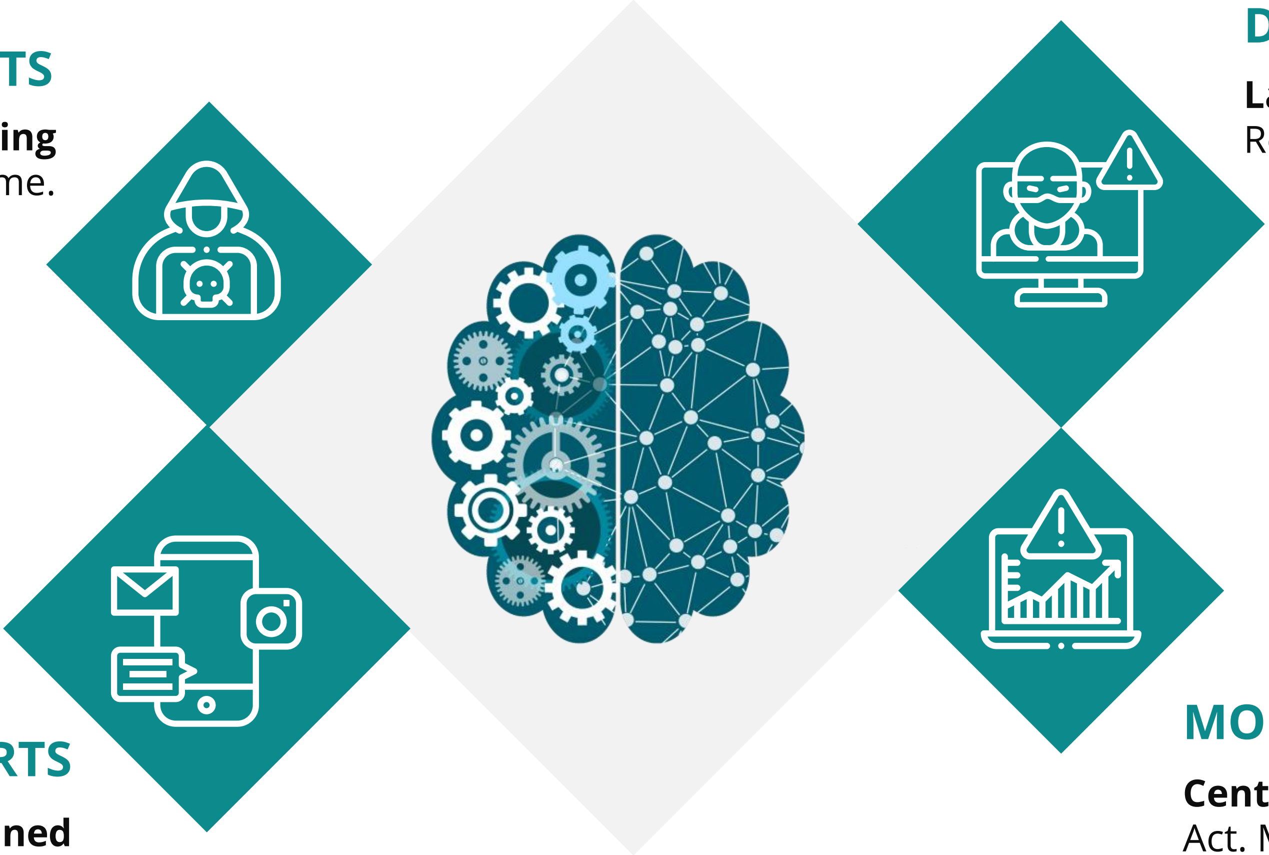
NBAD Alerts

Once a baseline is established the Network Behavior and Anomaly Detection built into threatNiXD tracks critical network characteristics like traffic volume, bandwidth use and protocol use. IoC analysts filter out false negatives for actionable alerts.

INCIDENT Management

We've seen real threat alerts getting lost due to different formats, channels and reports. threatNiXD is delivered in a single-pane-of-glass model that supports true management, control and governance of alerts.

Designed for Man and Machine



IOC ANALYSTS

Infuse Data with **Meaning**
Deep Correlation. Real Time.

DATA

Large Scale Data Collection
Redundant. Resilient. Secured.

ALERTS

False Negatives **Cleaned**
MITRE Mapped. Multi-channel.

MONITORING

Centralized Reporting
Act. Monitor. Manage. Govern.

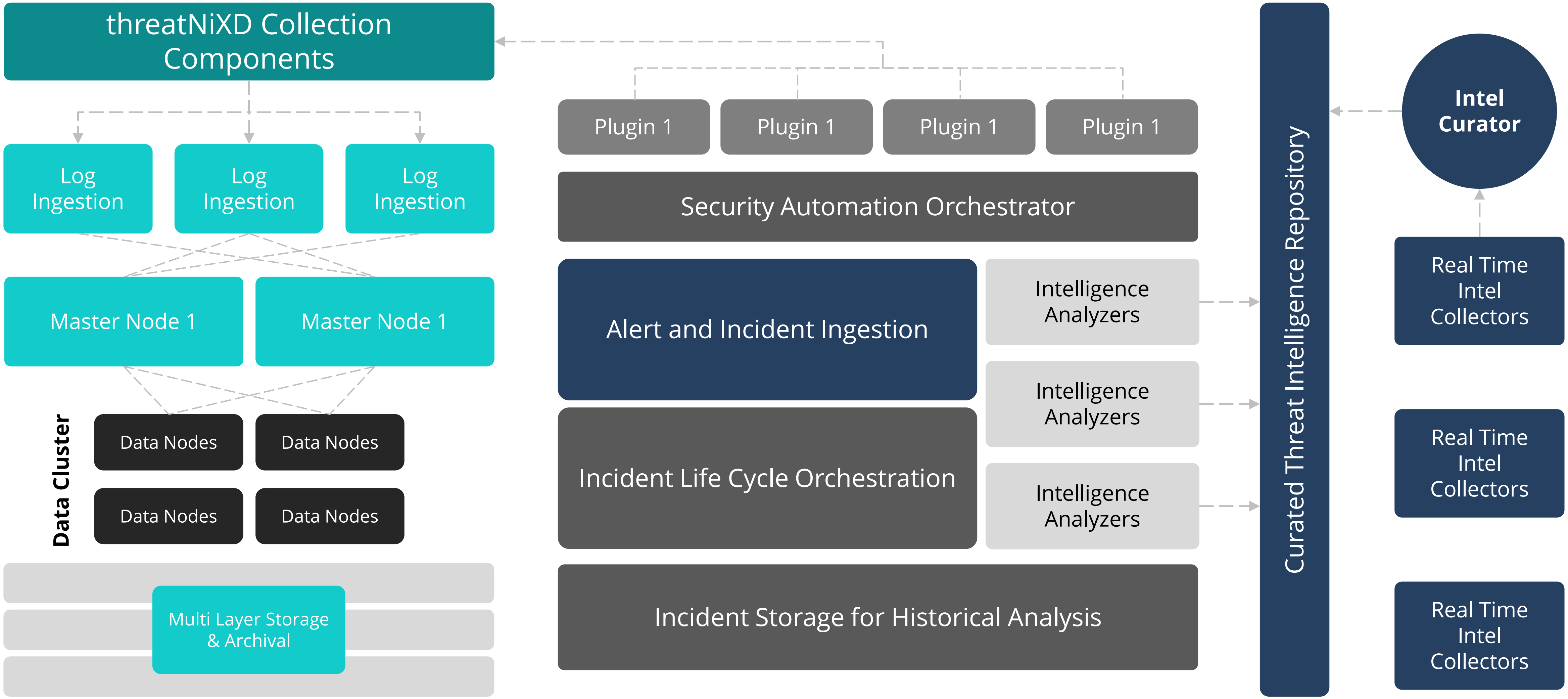
threatNIXD

Introducing the threatNiXD Platform

Representative Source List

Sample Event Sources	Type of Event/Logs
DNS Resolution (Route 53)	Query Logs
Load Balancing Infra (ELB/ALB/CLB)	Access Logs
Base Computing Resource (EC2)	OS logs (Host & Malware Logs)
VPC (Network Level Events)	Flow logs
Queue Systems (Redis)	Metrics
Databases (Oracle DB, Mongo DB, MySQL)	Database Audit Logs / Query, Error, Slow query, general logs
Container Management (Kubernetes)	Container Logs and Container Management System Log
Analytics Infra (Dynamo DB)	Metrics
Storage and Content (S3 Bucket)	Bucket Level Operations
Endpoint Protection Logs	IDS/IPS/AV/DLP Events and Alerts
Windows / Linux / *NIX	Syslogs, Win Event Logs
Application Logs	Custom Logs of Applications in Enterprise
Certificate Infra Logs	Certificate Authority Logs from Enterprise

Data Flow and Analysis



threatNiXD Collection Components

Log Ingestion

Log Ingestion

Log Ingestion

Master Node 1

Master Node 1

Data Cluster

Data Nodes

Data Nodes

Data Nodes

Data Nodes

Multi Layer Storage & Archival

Plugin 1

Plugin 1

Plugin 1

Plugin 1

Security Automation Orchestrator

Alert and Incident Ingestion

Incident Life Cycle Orchestration

Intelligence Analyzers

Intelligence Analyzers

Intelligence Analyzers

Incident Storage for Historical Analysis

Curated Threat Intelligence Repository

Intel Curator

Real Time Intel Collectors

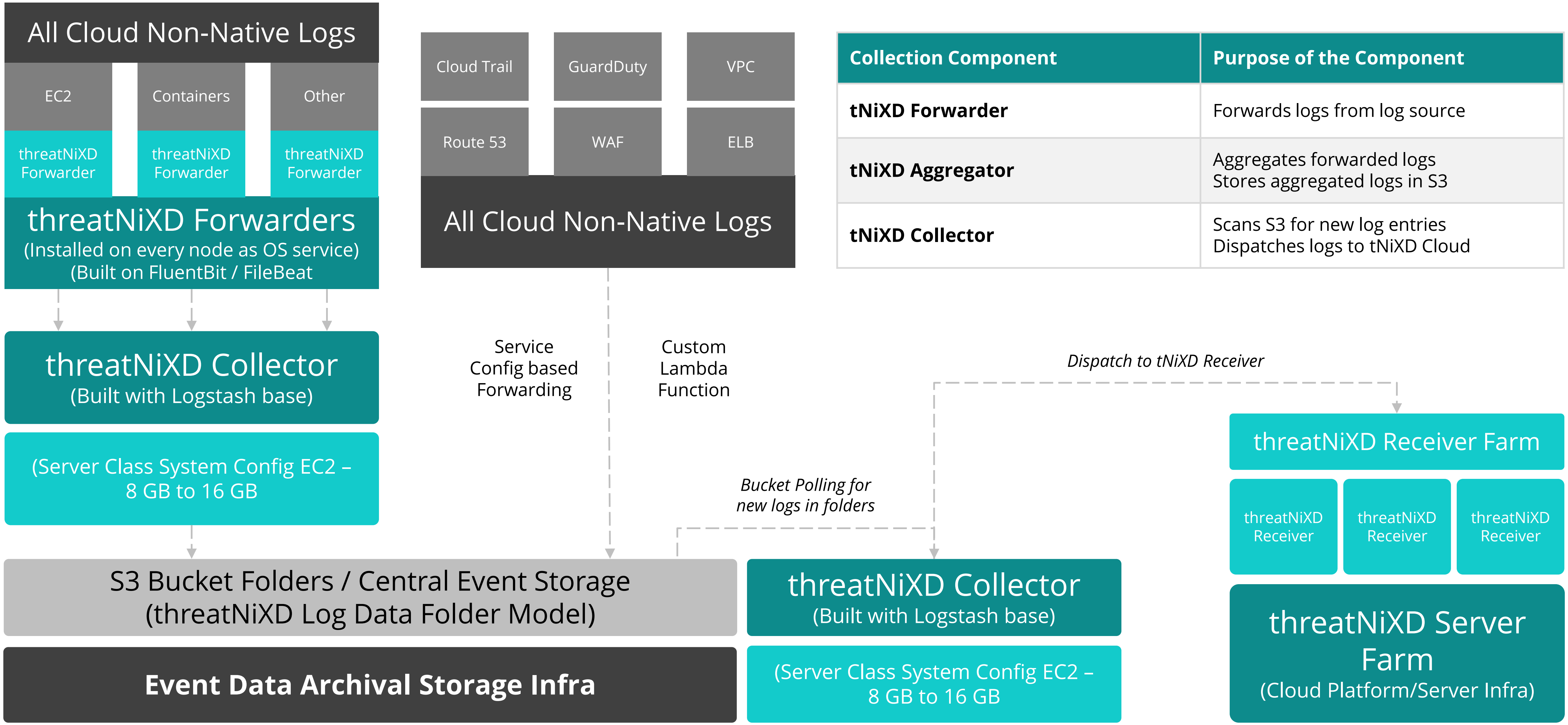
Real Time Intel Collectors

Real Time Intel Collectors

Collection & Real Time Correlation | **Incident Orchestration & Automation** | **Threat Intelligence & Hunting**

threatNiXD Solution Model

Collection Component	Purpose of the Component
tNiXD Forwarder	Forwards logs from log source
tNiXD Aggregator	Aggregates forwarded logs Stores aggregated logs in S3
tNiXD Collector	Scans S3 for new log entries Dispatches logs to tNiXD Cloud



All Cloud Non-Native Logs

EC2

Containers

Other

threatNiXD Forwarder

threatNiXD Forwarder

threatNiXD Forwarder

threatNiXD Forwarders
(Installed on every node as OS service)
(Built on FluentBit / FileBeat

threatNiXD Collector
(Built with Logstash base)

(Server Class System Config EC2 –
8 GB to 16 GB

Cloud Trail

GuardDuty

VPC

Route 53

WAF

ELB

All Cloud Non-Native Logs

Service
Config based
Forwarding

Custom
Lambda
Function

Dispatch to tNiXD Receiver

*Bucket Polling for
new logs in folders*

threatNiXD Receiver Farm

threatNiXD Receiver

threatNiXD Receiver

threatNiXD Receiver

S3 Bucket Folders / Central Event Storage
(threatNiXD Log Data Folder Model)

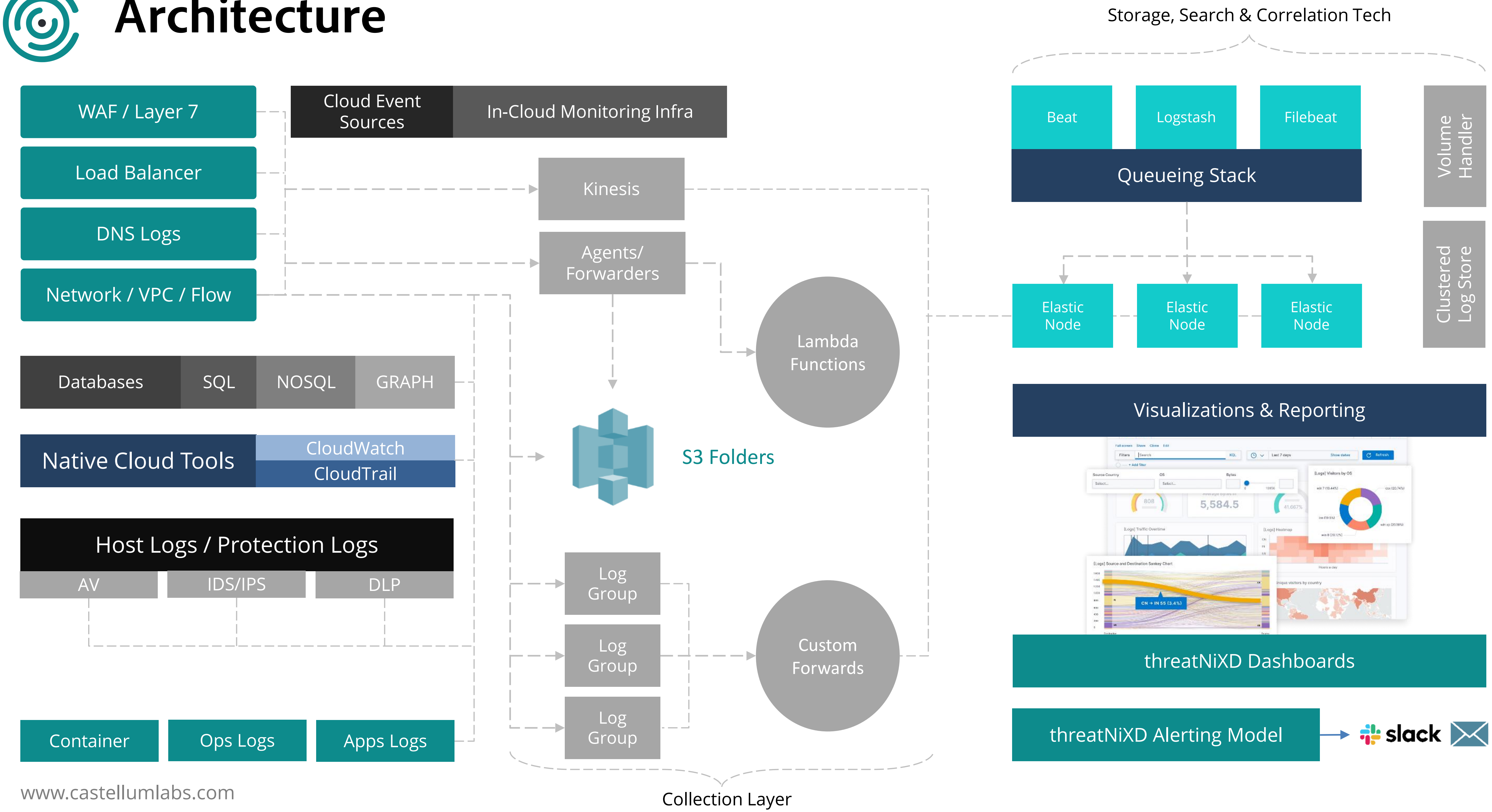
Event Data Archival Storage Infra

threatNiXD Collector
(Built with Logstash base)

(Server Class System Config EC2 –
8 GB to 16 GB

threatNiXD Server
Farm
(Cloud Platform/Server Infra)

Architecture



Storage, Search & Correlation Tech

WAF / Layer 7

Load Balancer

DNS Logs

Network / VPC / Flow

Cloud Event Sources

In-Cloud Monitoring Infra

Kinesis

Agents/ Forwarders

Lambda Functions

S3 Folders

Databases

SQL

NOSQL

GRAPH

Native Cloud Tools

CloudWatch

CloudTrail

Host Logs / Protection Logs

AV

IDS/IPS

DLP

Log Group

Log Group

Log Group

Custom Forwards

Container

Ops Logs

Apps Logs

Collection Layer

Beat

Logstash

Filebeat

Queueing Stack

Volume Handler

Elastic Node

Elastic Node

Elastic Node

Clustered Log Store

Visualizations & Reporting

5,584.5

threatNiXD Dashboards

threatNiXD Alerting Model

slack

www.castellumlabs.com

Reports, Dashboards, Incident Closure

Representative List of Reports

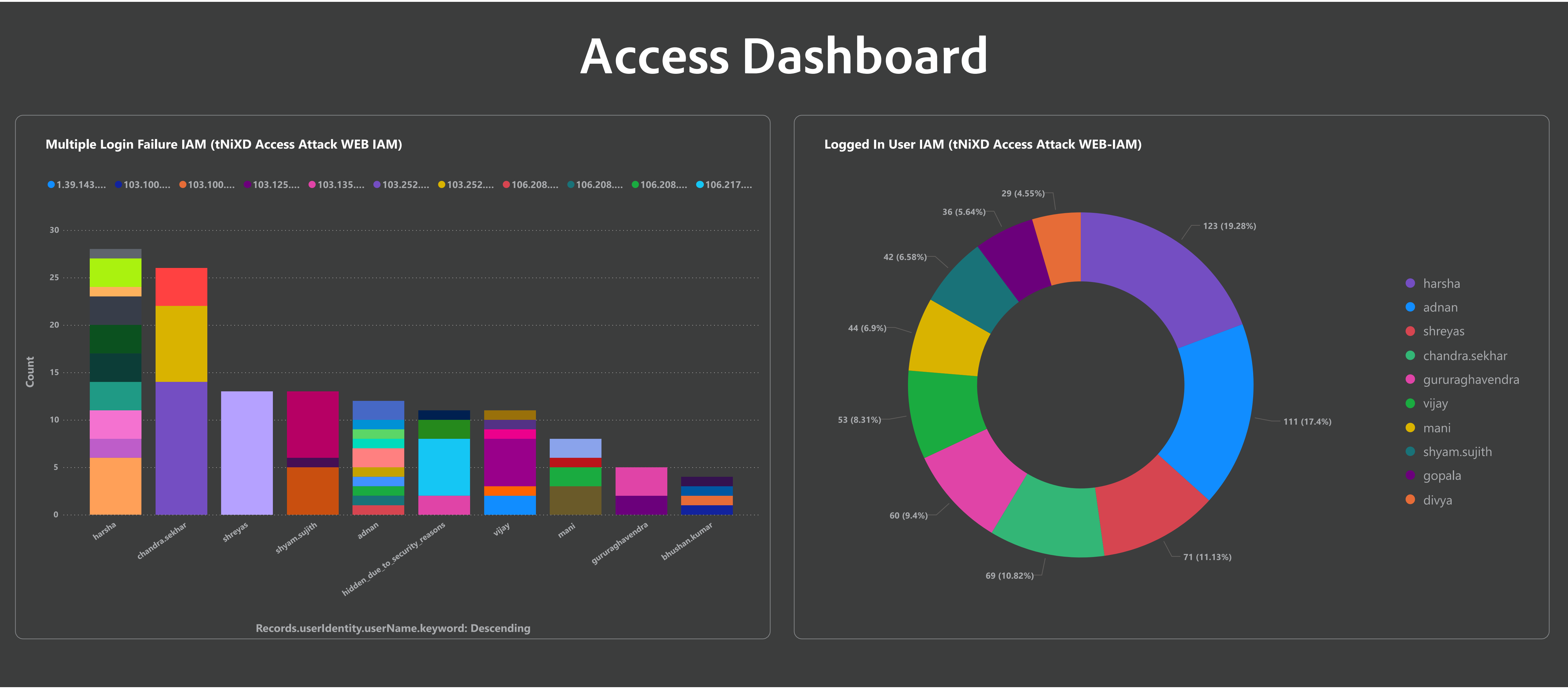
Main Dashboards	Alerts
Network Attack Dashboard	Network Alerts
Access Monitoring	Access Alerts
Host/Endpoint Dashboard	Log Failure Alerts
Operational Activity	Critical Ops Alerts
DNS Dashboard	Malware Alerts
Web Dashboard	Web & API Alerts
Threat Category Alert Monitoring	**Alert Data Navigation**

Attack Scenario DB

- Initial Access
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration

MITRE F/W Scenarios

threatNiXD Dashboard



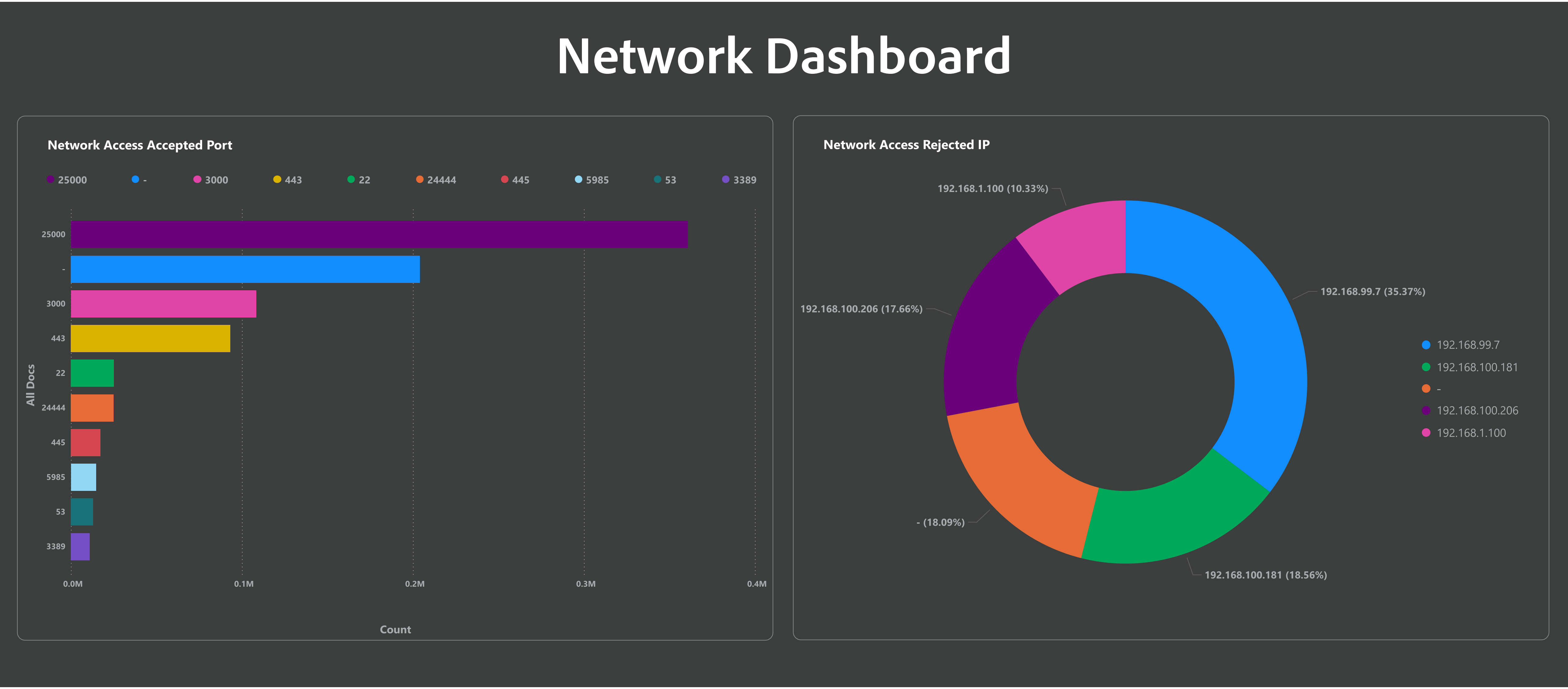
Access Dashboard

Multiple Login Failure IAM (tNiXD Access Attack WEB IAM)

Records.userIdentity.userName.keyword: Descending

Logged In User IAM (tNiXD Access Attack WEB-IAM)

Dashboards

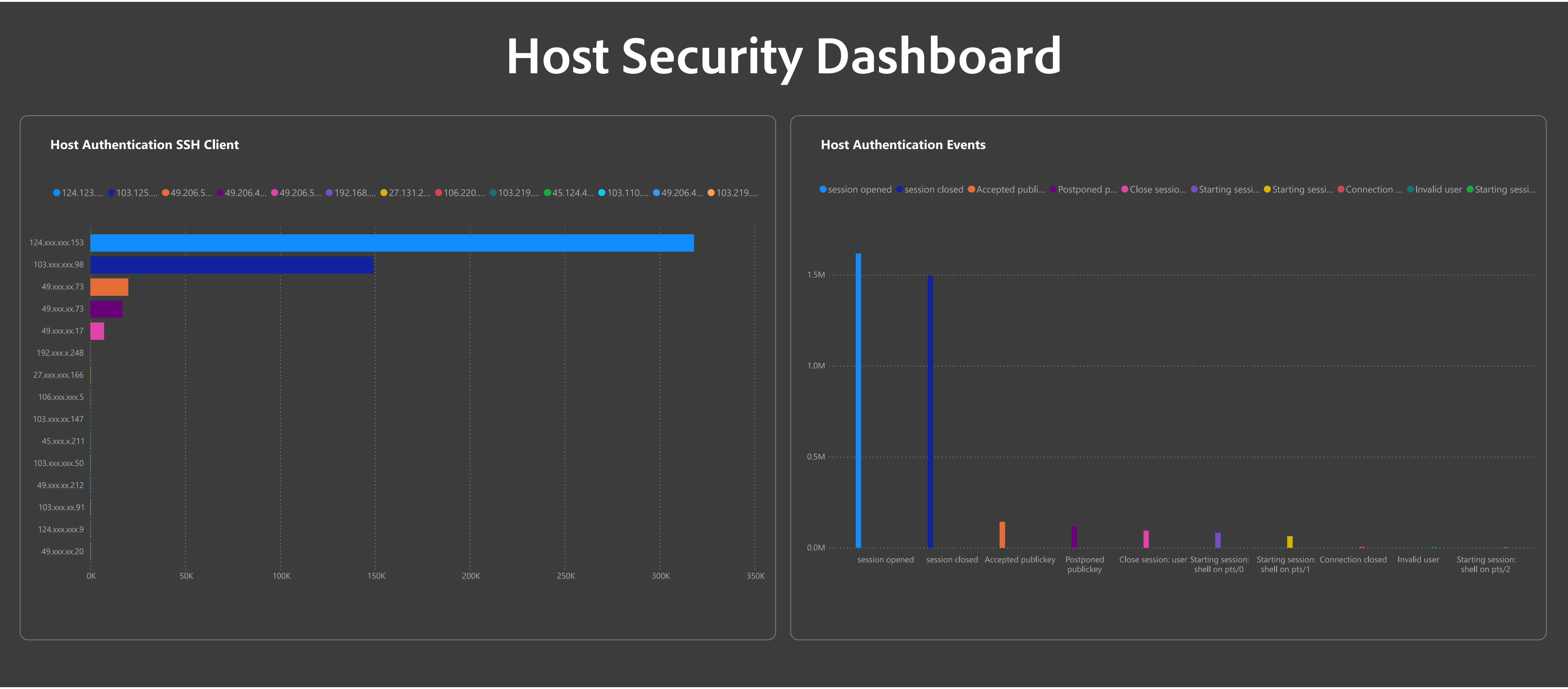


Network Dashboard

Network Access Accepted Port

Network Access Rejected IP

Dashboards



Host Security Dashboard

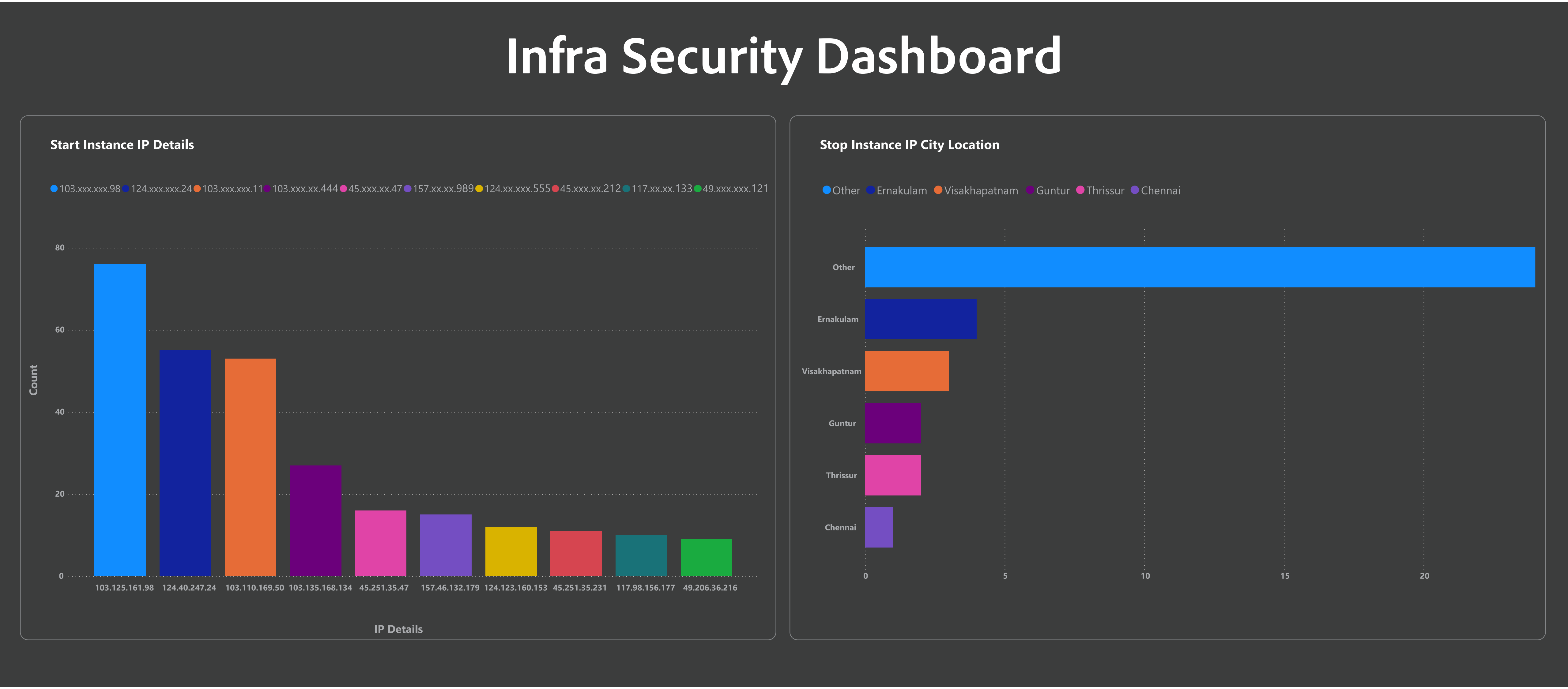
Host Authentication SSH Client

Host Authentication Events

● session opened ● session closed ● Accepted publi... ● Postponed p... ● Close sessio... ● Starting sessi... ● Starting sessi... ● Connection ... ● Invalid user ● Starting sessi...
1.5M
1.0M
0.5M
0.0M
session opened
session closed
Accepted publickey
Postponed publickey
Close session: user
Starting session: shell on pts/0
Starting session: shell on pts/1
Connection closed
Invalid user
Starting session: shell on pts/2

www.castellumlabs.com

Dashboards



Infra Security Dashboard

Start Instance IP Details

● 103.xxx.xxx.98 ● 124.xxx.xxx.24 ● 103.xxx.xxx.11 ● 103.xxx.xx.444 ● 45.xxx.xx.47 ● 157.xx.xx.989 ● 124.xx.xxx.555 ● 45.xxx.xx.212 ● 117.xx.xx.133 ● 49.xxx.xxx.121
Count
80
60
40
20
0
103.125.161.98
124.40.247.24
103.110.169.50
103.135.168.134
45.251.35.47
157.46.132.179
124.123.160.153
45.251.35.231
117.98.156.177
49.206.36.216
IP Details

Stop Instance IP City Location

● Other ● Ernakulam ● Visakhapatnam ● Guntur ● Thrissur ● Chennai
Other
Ernakulam
Visakhapatnam
Guntur
Thrissur
Chennai
0
5
10
15
20

In Conclusion

MDR on threatNiXD

threatNIXD

ACTIONABLE DASHBOARDS
Single-pane-of-glass reports and dashboards with insights and advice for rapid action

COMPLETENESS
All facets of Incident Identification, Reporting and Management

HUMAN INSIGHTS
Not mere automation – experts sniff out potential issues that machines take time to be programmed to detect

GROWTH PLANNING
Start with the package that works, and scale as your needs grow

TRAINING & SUPPORT
We train your response management personnel regularly

COMPLIANCE
Deliver evidence for regulations and compliances

COST
Complete value for your money

CRITICAL SKILLS GAPS
We fill critical and had-to-get (and afford) cybersecurity skills

Only MDR With

Centralized, simplified retention of **historical log data**

Advanced correlation and detection **capabilities**

Default network behavior and anomaly **detection capabilities**

Integrated threat intel data for real time **detections**

Custom SLAs and response times **contracts**

Built-in user and entity behavior **analysis capabilities**

Centralized, simplified retention of **historical log data**

Real time threat hunting models **constantly updated**

Uniform, consolidated security **dashboards**

Consolidation of all event data in single **repository**

Integrated incident life cycle **management**

MDR Options

	threatNiXD Secure	threatNiXD Secure +	threatNiXD Preempt	threatNiXD NxtGen
Pricing Model	Per Device Per Month Pricing	Per Device Per Month Pricing	Per Device Monthly Pricing	Per Device Monthly Pricing
Usage Model	Subscription Model	Subscription Model	Subscription Model	Subscription Model
Payment Plans	Half Yearly, Yearly	Quarterly, Half Yearly, Yearly	Monthly, Quarterly, Half Yearly, Yearly	Monthly, Quarterly, Half Yearly, Yearly
Service Element	**Service Availability**	**Service Availability**	**Service Availability**	**Service Availability**
24x7 Monitoring				
Shift Coverage	No	Yes	Yes	Yes
Alert Based Coverage	Yes	Yes	Yes	Yes
Eye on the Glass Coverage	No	No	Yes	Yes
Customer threatNiXD Portal				
Incident Tracking	No	Yes	Yes	Yes
Incident Reporting	No	Yes	Yes	Yes
Other Reports	No	Yes	Yes	Yes
Asset Management	No	No	Yes	Yes
Default Monitoring Coverage (Alert Based)				
Attack Monitoring	Yes	Yes	Yes	Yes
AAA Monitoring	Yes	Yes	Yes	Yes
Malware Monitoring	Yes	Yes	Yes	Yes
Compromise Monitoring	Yes	Yes	Yes	Yes
Network Behavior Monitoring	Yes	Yes	Yes	Yes
Suspicious Behavior Monitoring	No	No	Yes	Yes
Anomalies Monitoring	No	No	No	Yes

threatNIXD

Contact Us.

+91 86399 53505

inquiry@castellumlabs.com

www.castellumlabs.com