Castellum Labs

Castellum Labs

SOC Monitoring <> threatNiXD MDR <> Introduction

www.castellumlabs.com

About Us

Castellum Labs

New Age Cyber Security Company

- Services & Platforms at Cross Section of Intel, Monitoring & Simulations
- Based in Hyderabad, India with global customers
- Strong Handpicked Team of 70+ with (best of security talent globally)
- Started by people with decades of product & CySec exp
- Subscription Modeled & Globally Delivered CySec Services
- Value + Impact from Day One, No Installation & No Deployment

Rajeev Shukla, Founder

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

Current Customers in

- India
- Australia
- Middle East
- USA
- UK

Current Customer Segment

- SaaS Product Companies
- Financial and Banking
- E-Comm Player
- Telecom
- Retail

Served Customer in following Areas

- Application Security & Governance
- ISO 27K & GDPR readiness preparation
- Red Teaming. Active Defense Assessment
- Threat Intelligence and Threat Management
- SOC Monitoring (Managed Detection & Response)
- Cloud Security Designing and Cloud Security Governance

Castellum Cyber Security Services

Application Security

Managed AppSec Programs

SOC Monitoring

Managed Detection and Response

Intel & Hunt

Darkweb, Brand & Surface Monitoring

Cloud Security

Cloud Security Design & Governance

Enterprise Assessments

End-to-End Security Assessments

Vulnerability Management

Enterprise Vulnerability Orchestration

Threat Simulations

Red Teaming & Breach Simulations

Certifications

ISO 27K & GDPR Readiness

Threat Landscape, “Complex & Ever Evolving”

Almost all of the attacks use large automated infra

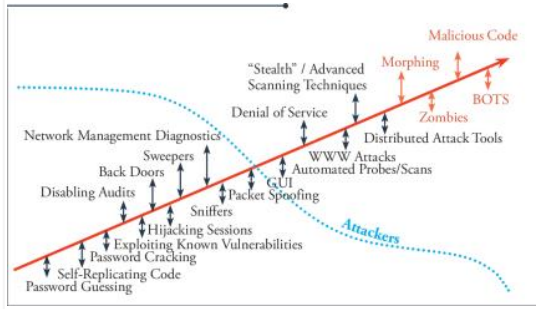
Large scale malicious traffic can be generated through automated infrastructure

Cyber criminals do not need to be hacking experts

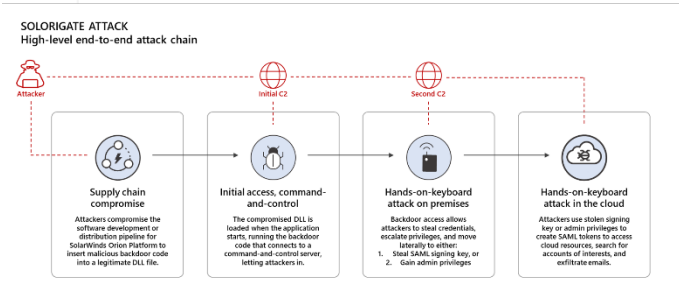
Ransomware as a service
Exploit code on darkweb
Hackers on rental hire

Time to exploit a vuln or a misconfigs reducing everyday

It takes mins and hours to get a vulnerability or gap to be exploited, not days/weeks

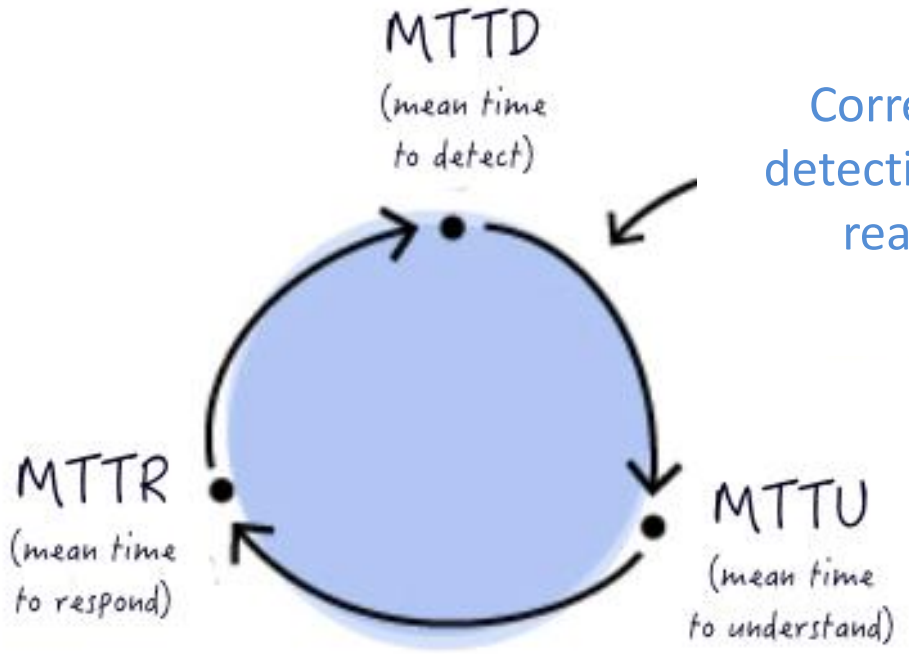


Ever Evolving
Cyber Attack Models



Detection & Response is “The Need”

Despite security products, tools and solutions bought and implemented by enterprises, customers still face breaches.

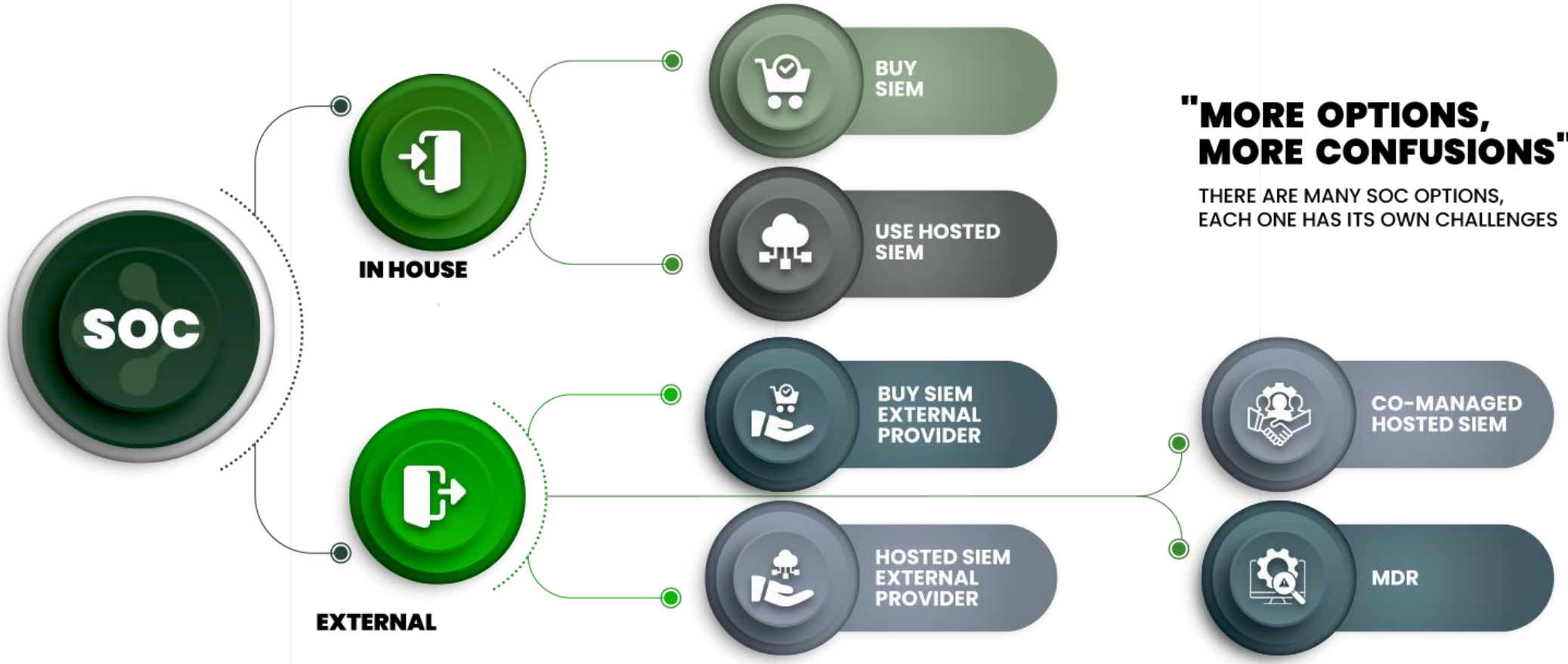


Correlate logs, so that detection and response in real time, happens

- Different alerts & console by diff tool can’t detect an attack in its tracks
- You need to consolidate logs, events and data and correlate it to detect attacks
- You need a real time action on detected scenarios of attacks or threats
- SOC products (SIEM) consolidate your log into single repo & correlate them

www.castellumlabs.com

Many SOC Options. Many Confusions !



"MORE OPTIONS, MORE CONFUSIONS"

THERE ARE MANY SOC OPTIONS,
EACH ONE HAS ITS OWN CHALLENGES

www.castellumlabs.com

MDR, A Good Option

No SIEM Licenses Required
No Tech Implementation/Adoption
No Data Infrastructure Complexities
No SOC Monitoring Team Needed
No 24x7 Shift Overheads
Reduced Capex and Opex

"Why MDR is a great option of 24x7 SOC monitoring"

Definitive SLAs for Monitoring
Best of Breed Incident Response Process
Expand Monitoring in Phased Plan
All Security Reports Consolidation
No Struggle with Talent Hunt
Free Your Time for Strategic Focus

www.castellumlabs.com

threatNiXD MDR

“threatNiXD MDR is managed detection & response using integrated platform ”

www.castellumlabs.com

Where we stand out

Most MDR players

- become alert forwarders
- depend only on tools to do magic
- automation by MDR players is trivial

Integrated Incident Response

Effective Response Automation

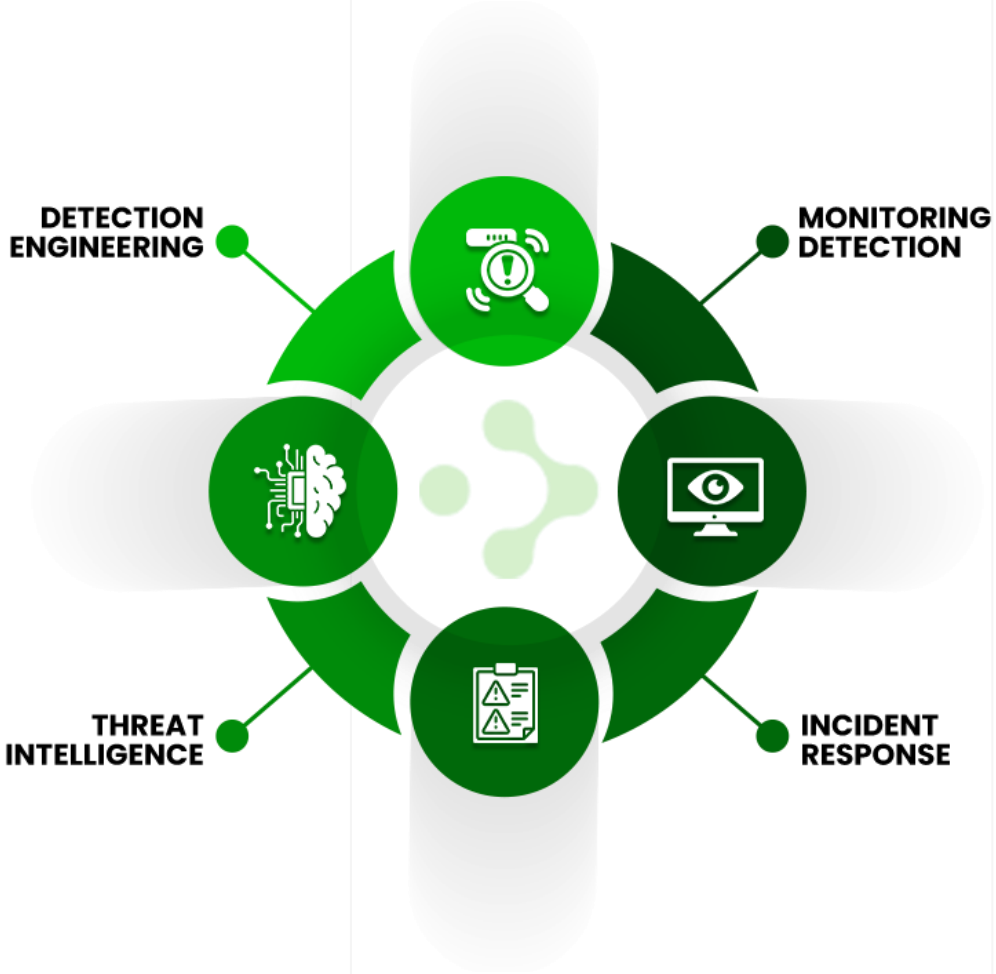
Darkweb and Deepweb Intelligence

Human Actors & Intelligence

Hunting Model for Monitoring

Forensic Modeled Analytics

Not Just Another MDR



"Detection needs engineering, not just event correlation, tNiXD does that"

"MDR success depends on real time monitoring & detection abilities"

"An integrated & embedded intelligence is built in threatNiXD platform"

"Incident response is designed to be complete and comprehensive"

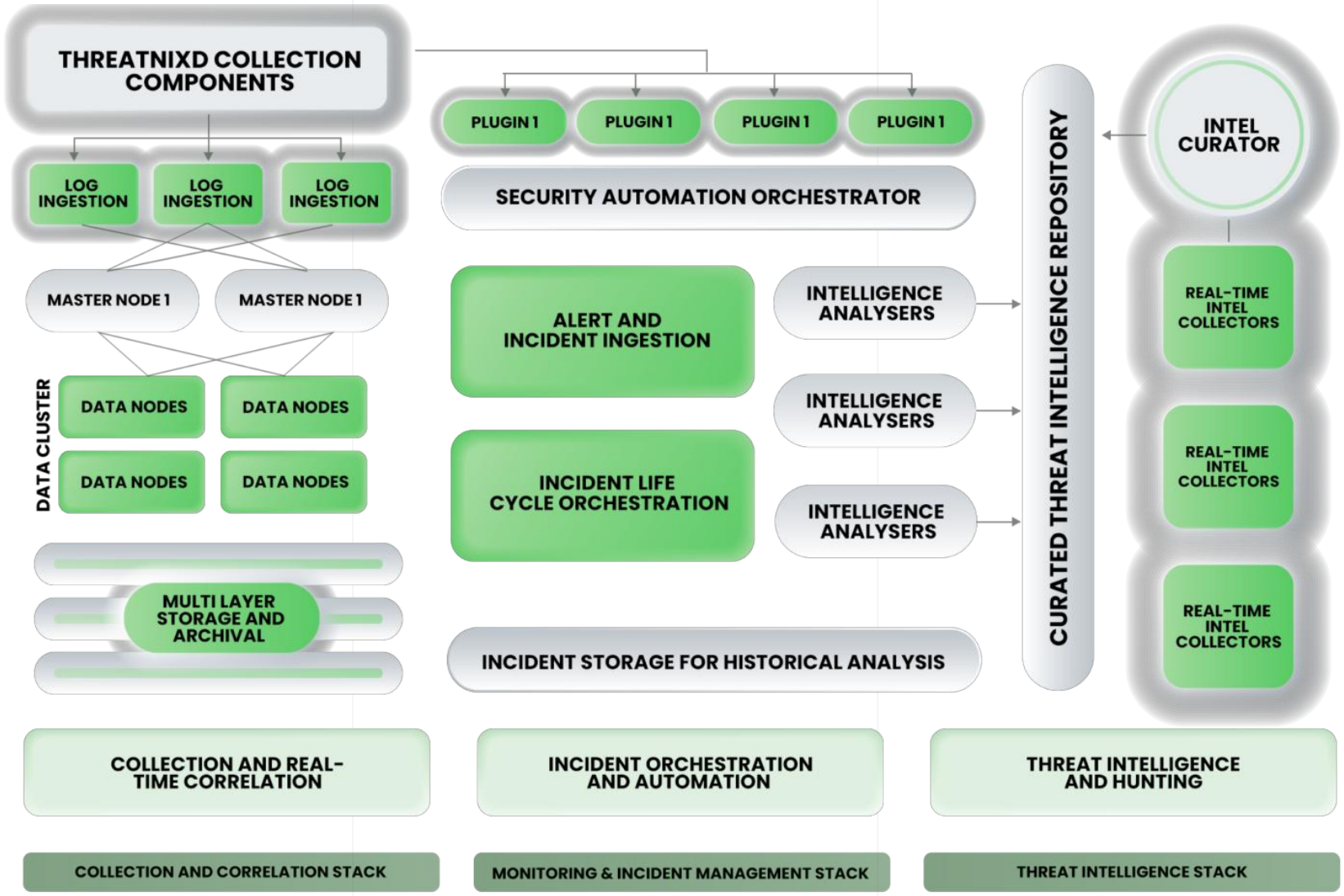
Feature Grid of threatNiXD MDR

Feature Grid of threatNiXD MDR (Monitoring as a Service)
Unique collection architecture to reduce noise collection
Comprhensive collection capability for all kind of events, data & logs
Large variety of device, server, application, database, stacks, solution collected
Real time multi level correlation capability for threat/attack scenarios detection
Continuously updated threat alert library mapped to MITRE
Built-in fully integrated threat intel with real time application
Darkweb intelligence integrated into the platform
Critical alert dispatch to multiple channels
24x7 eye on the glass monitoring by layered SOC team
SOC team with composite skill set of detection, response, forensic, intelligence
Dashboards for real time outlier and pattern monitoring
Fully coordinated response model built into service
Incident and task tracking and closure follow ups

Feature Grid of threatNiXD MDR (Monitoring as a Service)
Definitive multi-level SLAs covering entire incident lifecycle
Response automations built into the technology stack
Centralized security reporting delivered by tNiXD MDR
Simplified log retention/consolidation for audit & compliance
Automted provisioning for additional devices collection
Standard daily, weekly and monthly security reports
User and entity behavior analysis
Network behavior and diagnostics
Advance threat hunting on recurring basis
Extended retention models for prolonged live data
Advance report sets with deep security analytics
Advance threat hunting on recurring basis
Advance threat hunting on recurring basis

www.castellumlabs.com

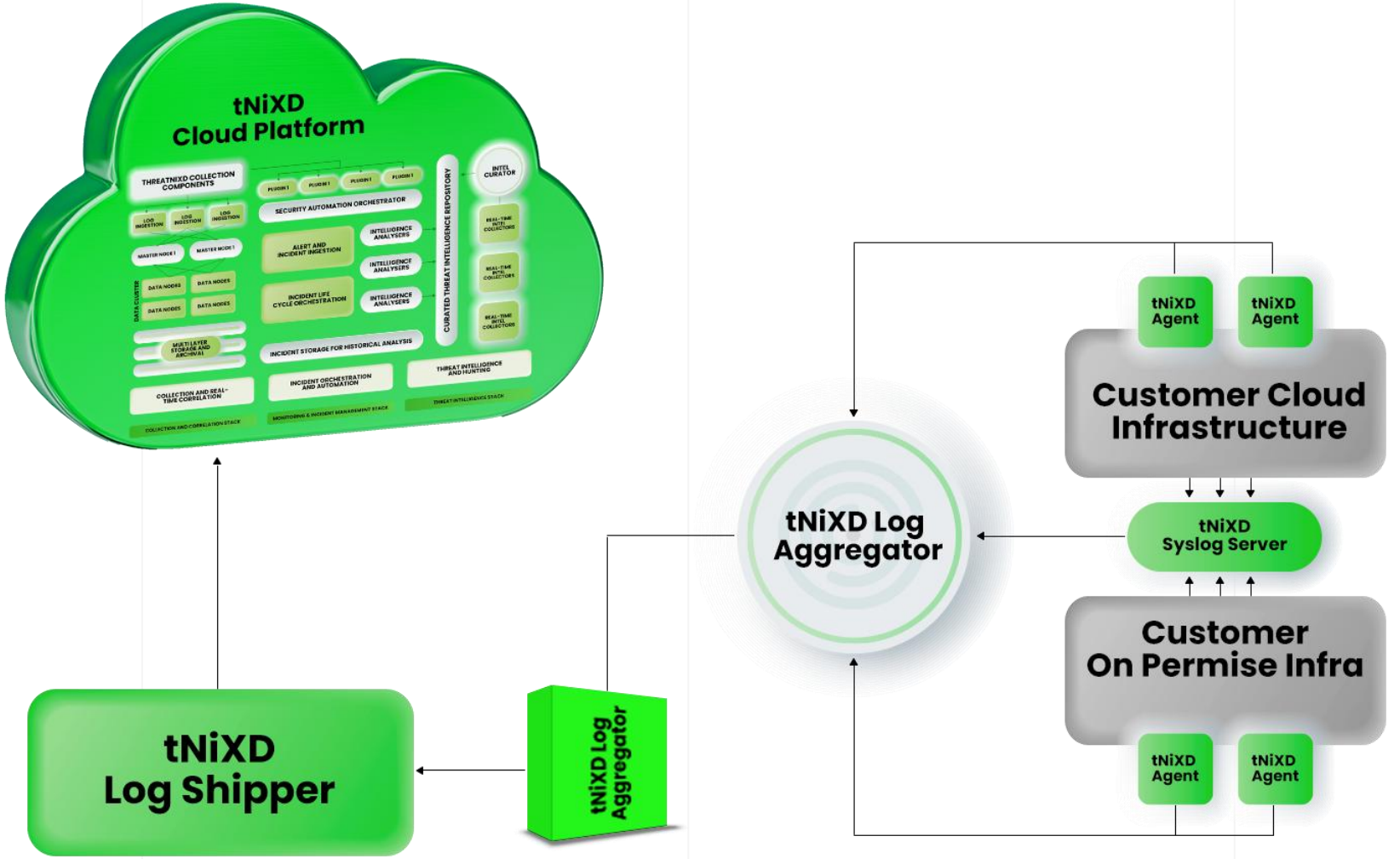
threatNiXD Cloud Technology



Multi Cloud Hosted
Highly Available Architecture
Scalable Log & Event Ingestions
Real Time Correlation Algorithms
Multi-Channel Notifications Systems
Advance Visualization & Dashboarding
Advance Data Protections
Data Isolations and Protections
Data Localizations Enforcements
Built-In Automation Capabilities
Fail Over Architecture
Deep Intelligence Stack
Seamlessly Integrated Stacks
Integration with Ticketing Systems
Advance Data Encryptions
Adaptable Change Management

www.castellumlabs.com

Clean Meaningful Collection

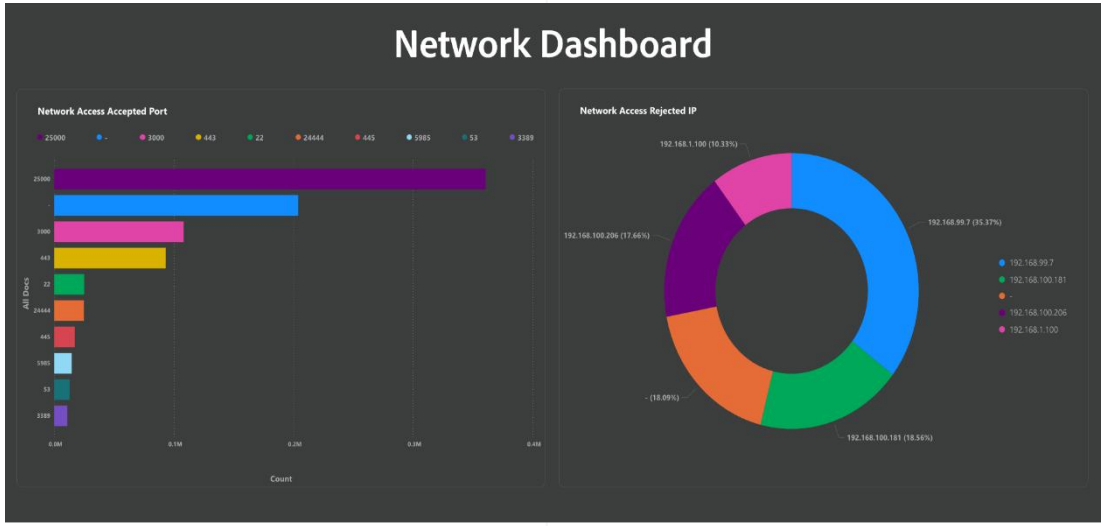


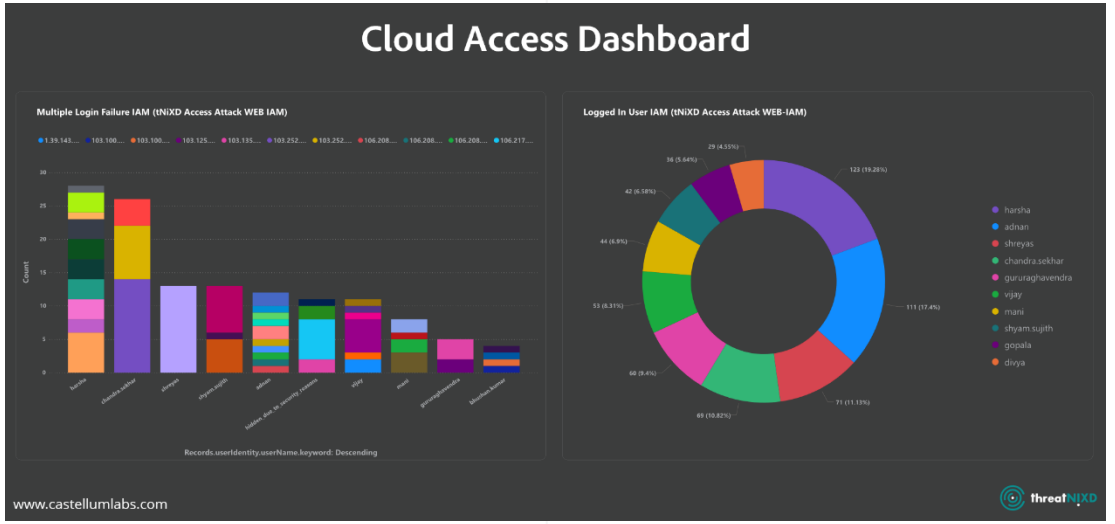
www.castellumlabs.com

threatNiXD MDR Reports & Dashboards

"tNiXD consolidates all of your reporting and dashboards requirements into a single place"

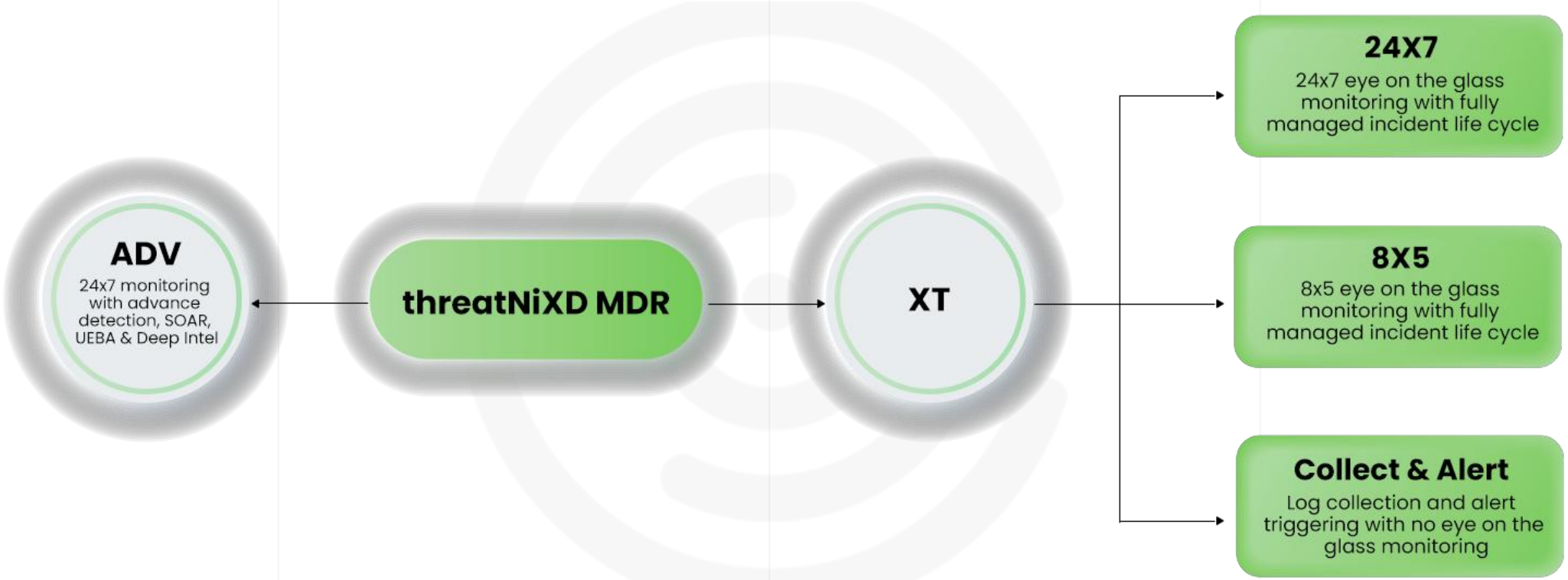
1. Multi level monitoring dashboards
2. Operational activity dashboards
3. Security alerts dashboards
4. Attack scenario dashboards
5. Analyzed reports





www.castellumlabs.com

threatNiXD MDR Options



www.castellumlabs.com

threatNiXD Options for Every Budget

If you have reasonable budget and want good quality SOC monitoring	If are budget constrained & still want active monitoring	If you have almost no budget but want to be audit compliant	You are not budget constrained & expect high quality detection
threatNiXD MDR XT 24x7	**threatNiXD MDR XT 8x5**	**threatNiXD MDR XT Collect n Alert**	**threatNiXD MDR ADV**
"Great coverage, full incident life cycle management, SLA bound and 24x7 eye on the glass monitoring"	"Great coverage, full incident life cycle management, SLA bound and 8X5 eye on the glass monitoring"	"We configure all your logs for collection & then we send alerts to you on mail or teams/slack channel"	"24x7 eye on the glass monitoring with advance features such as Response Automation, UEBA, Deep Intelligence & Custom Collection"

threatNiXD MDR SLAs

		Mins/Time	Conditional Terms
Alerts	Critical alert forwarding/notifications	0	These SLAs are applicable to the base model of tNiXD MDR engagement
	SOC analysts action on alert (High)	120	
	SOC analysts action on alert (Medium and Low)	180	
	Case conversion of an alert, if applicable	240	
Incidents	Incident identification (All critical alerts are not incidents)	60	
	Incident first reporting/notification	90	
	Incident remediation/action plan	120	
	Incident closure and documentation	240	
Breach	Breach notification	120	
	Breach specific regulatory actions tracking	180	
	Breach specific documentations	300	
	Breach closure actions	360	
Reports	Daily reports	Everyday 0900 AM	
	Weekly Reports	Monday 1200 PM	
	Monthly reports	Last day of month, 1200 PM	
	On demand reports	12 Hours	

www.castellumlabs.com

Keep in Touch.

+91 9700970397 enquiry@castellumlabs.com www.castellumlabs.com

Provisioning of threatNiXD

Phase	Phase Steps
tNiXD Provisioning	tNiXD Cloud Provisioning
	Collection Configuration
	Reporting Optimizations/Configs
tNiXD Customer Readiness	Customer Walkthrough & Training
	Process Validation
tNiXD Monitoring Start	24x7 Alert Monitoring
	Daily/Weekly/Monthly Reporting

www.castellumlabs.com

Sample Infra for Collection

Data Center / Enterprise Network Infra		Device Count	Totals	Final Device Counts
Data Center Servers	Windows	50	172	172
	Linux	50		
	Other Unix	40		
	Other OS	32		
Network	Firewall	4	22	22
	Routers	6		
	Switches	10		
	Gateways/Proxies	2		
Mail/DNS/Content	Mail Server	1	6	6
	Dev Repository Servers	1		
	LDAP/AD/DNS	2		
	FTP/Content Serfver	2		
Endpoints	Laptops (Win)	0	0	0
	Laptops (Linux)	0		
	Desktop (Win)	0		
	Desktop (Linux)	0		
		Total Device Count	**200**	**200**

www.castellumlabs.com