Castellum Labs

Secure What Matters.
Detect Before It Spreads.
Respond Before It Hurts You.

- Advance CySec
- Deep Tech Sec Platforms
- GSDC @ Hyderabad
- Customers Across Globe

www.castellumlabs.com | reach@castellumlabs.com | +91 7842046995

About Castellum Labs

⚡ Global Cyber Capability Center

Services delivered using advanced platforms from our GSDC in Hyderabad, India

👥 Handpicked Experts

Best-of-breed cyber security talent globally - deep product, services & tech experience

🌐 Global Customer Base

Active customers across India, US, Europe & Australia with subscription & contract models

🚀 Value + Impact from Day One

Immediate Impact Through Projects and Long-Term Strategic Engagements

🔒 Deep security genes

Cumulative experience of more than 200 years in leadership team on cyber security

📊 100+ Customers

Across Banking, Insurance, Manufacturing, Pharma, SaaS, Retail, Government & more

Leadership & Advisory Board

Rajeev Shukla

Founder & CEO (India)

Senior business leader with decades of MNC experience in data center, networking & cyber security. Ex-VP CA Technologies, Director Sun Microsystems, Ex-CTO Cygilant.

Rama

Advisor & Head – US Ops

30+ years across the entire spectrum of IT industry in US & India. Ex-Head IT Aryaka, Ex-PwC, Ex-IBM, Ex-VMware, Ex-Malwarebytes, Ex-Infosys, Ex-NetApp.

R

Rinky (Sukriti)

Head of Operations (India)

Seasoned operational leader with experience across Sales, HR, Operations & Legal. Foundational team member with a variety of roles across the organisation.

ADVISORY BOARD

Mr. Arvind Tawade

Former Group CTO – Reliance Capital

Top IT executive who built large complex digital infrastructure for Reliance Capital Group. Helping create next-generation growth for Castellum Labs across industry verticals.

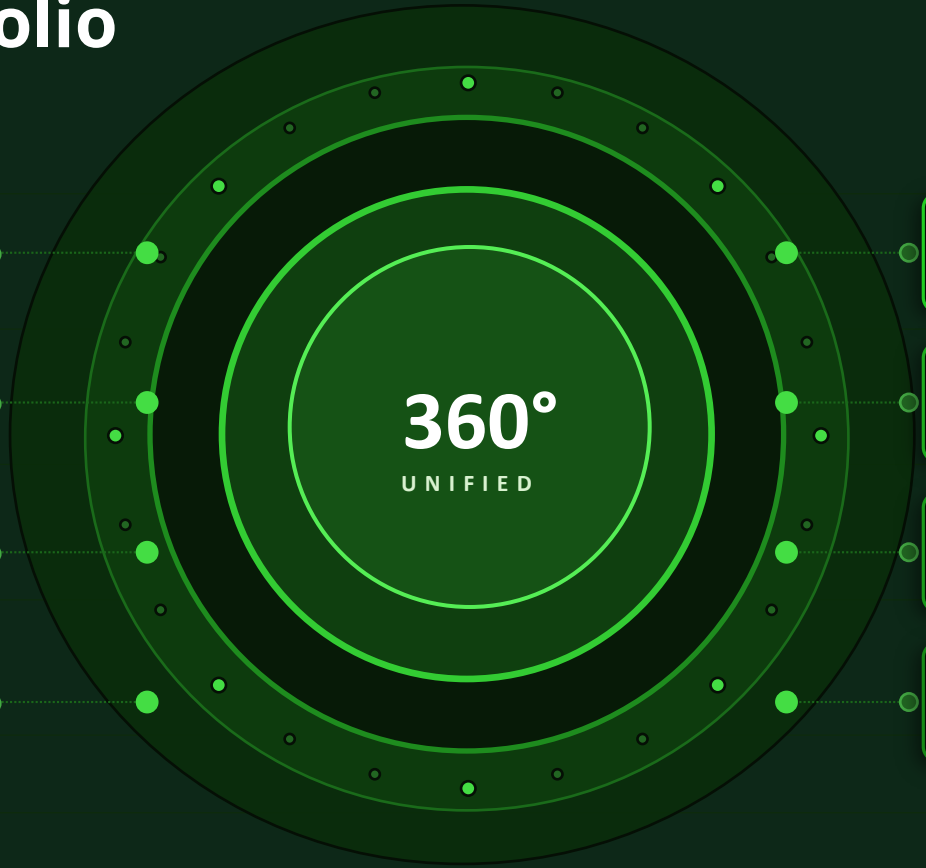
Dr. Akash Bharadwaj

Professor & Head Cyber, UPES Dehradun

Senior cyber security professional with deep research and academic focus. Leads Centre of Excellence in UPES, Dehradun and creates collaborative research opportunities for Castellum Labs.

Some of Our Enterprise Customers

CySec Portfolio



SOC / MDR
24×7 Threat Monitoring

AppSec & VAPT
Vulnerability Assessment

IR & Forensics
Incident Response

AI Security
AI-Driven Threat Defense

Darkweb & TI
Deep Threat Intelligence

Cloud Security
Multi-Cloud Protection

Phishing Simulation
Security Awareness Training

Managed DevSecOps
Secure Dev Lifecycle

Global Footprint

140+	3	12+	24×7
Customers	Continents	Sectors	Delivery

SECTORS SERVED

- Banking
- Insurance
- SaaS / IT Services
- E-Commerce / Retail
- Telecom
- Construction

GLOBAL OFFICES

- USA
- MUMBAI
- HYDERABAD
- LUCKNOW

CUSTOMER GEOGRAPHIES

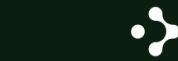
INDIA
Mumbai · Bengaluru · Hyderabad · Delhi · Indore · Chennai · Kolkata · Bhopal · Pune

USA
Customers across major US tech & financial hubs

EUROPE
UK & European enterprise customers

REST OF WORLD
Australia · Middle East · Other global regions

AI SECURITY



"Your organization is using AI in more ways than you can imagine"

Employees

Your Employees are using Chat GPT for almost every task

What are they placing in those promts ?

Tools

Tool in your company have embedded AI

Is that generated code secure enough to be considered ?

DevOps

Developers are generating code ten times the speed

Can your security pipeline handle that speed ?

AI Apps

Your application use LLMs from dozen of sources

Are those LLMs biased and will create challenges for you ?

Infra

Digital Infra in your company is managed by AI

How would you gain visibility into dynamic infrastructure ?

Pervasive AI Exposures

- Data Poisoning
- AI Tool and Plugin Abuse
- Roleplay Based Jailbreaks
- Membership Interference Attacks

AI THREAT EXPOSURE

- Prompt Injection
- Jailbreaking
- Shadow AI
- Model Theft and Extraction

"Billions Of Dollars Will Be Lost Because Of Insecure AI Adoption & Engineering "

Castellum's Secure AI Frameworks

AI Security Testing

Assess AI applications, LLM systems, RAG pipelines, agents, prompts, outputs, and tool integrations against real-world AI attack scenarios.

AI Supply Chain Security

Validate model origin, training data integrity, fine tuning data, embedding stores, AI dependencies, third-party vendors, release integrity, and version control

Enterprise AI Governance

Define AI policies, ownership, risk classification, approval workflows, employee usage controls, audit readiness, and governance maturity.

Secure AI Architecture

Design secure AI systems with model isolation, API controls, data protection, guardrails, monitoring, logging, access control, and incident response readiness.

Castellum's AI Security

1 **AI Security Testing**

2 **Enterprise AI Governance**

3 **AI Supply Chain Security**

4 **AI Security Architecture**

AI Security Testing

Assess AI applications, LLM systems, RAG pipelines, agents, APIs, and prompts for prompt injection, jailbreaks, data leakage, insecure output handling, excessive agency, and model abuse.

Enterprise AI Governance

Establish AI governance across inventory, risk classification, ownership, policy, approval process, workforce AI usage, data protection, audit readiness, and maturity roadmap.

AI Supply Chain Security

Evaluate model origin, training data integrity, fine tuning data, embeddings, AI dependencies, third-party vendors, MCP tools, release integrity, and LLM version control.

AI Security Architecture

Design secure AI systems with model isolation, data flow controls, API security, access control, guardrails, logging, monitoring, and incident response readiness.

DARKWEB MONITORING

& DEEP THREAT INTELLIGENCE

CASTELLUM LABS

The Threat Landscape – 2024–25

8,000+	120+	16+	$30B+
Ransomware Attacks / Year	Countries Affected	Sectors Impacted	Total Financial Loss

⚠ **Almost ALL ransomware attacks have roots in the Dark Web - early detection = prevention**

HOW DARK WEB ENABLES RANSOMWARE

1. Malware Coded on TOR
2. Buyer Downloads from Dark Web
3. Ransomware Spreads
4. Victim Machines Infected
5. Ransom via Crypto

External Threat Exposure – What Attacks You

🔗 Lookalike phishing domain

📱 Fraudulent mobile app

🔑 Stolen credentials on Telegram/Darkweb

🟣 Data sold on Dark Web marketplace

Threat Sources Against You

🌐 Website using your logo for fake promo

🛒 Products listed on fake e-commerce

📞 Fake contact number on Google search

💻 Coder leaked code & secrets on GitHub

Our Threat Intelligence Services

Darkweb Intelligence 24×7

Real-time dark web surveillance across underground forums, breach sites & Telegram

Brand Monitoring

Continuous monitoring for impersonation, fake apps, fraudulent listings & social media abuse

Attack Surface Management

Discover and monitor exposed digital attack surface across web, cloud, DNS & network

Phish Exposure | **Cred Exposure** | **Stealer Log Exposure** | **Git Exposure**

Fake Exposure | **Leak Exposure** | **Rep Exposure** | **Dark Exposure**

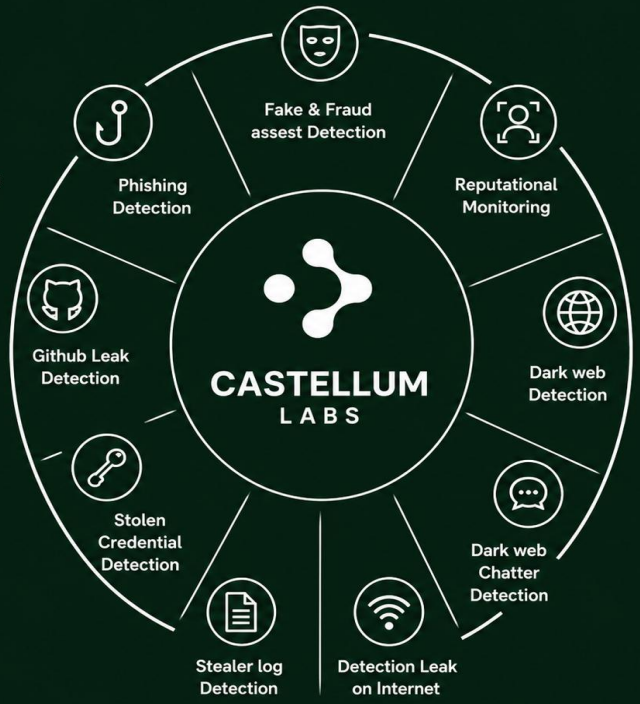
Advance Intelligence

“Take Advance Threat Intelligence To The Center Of Your Defence”

We hunt for threat sources in wild of Interact, social media & dark web

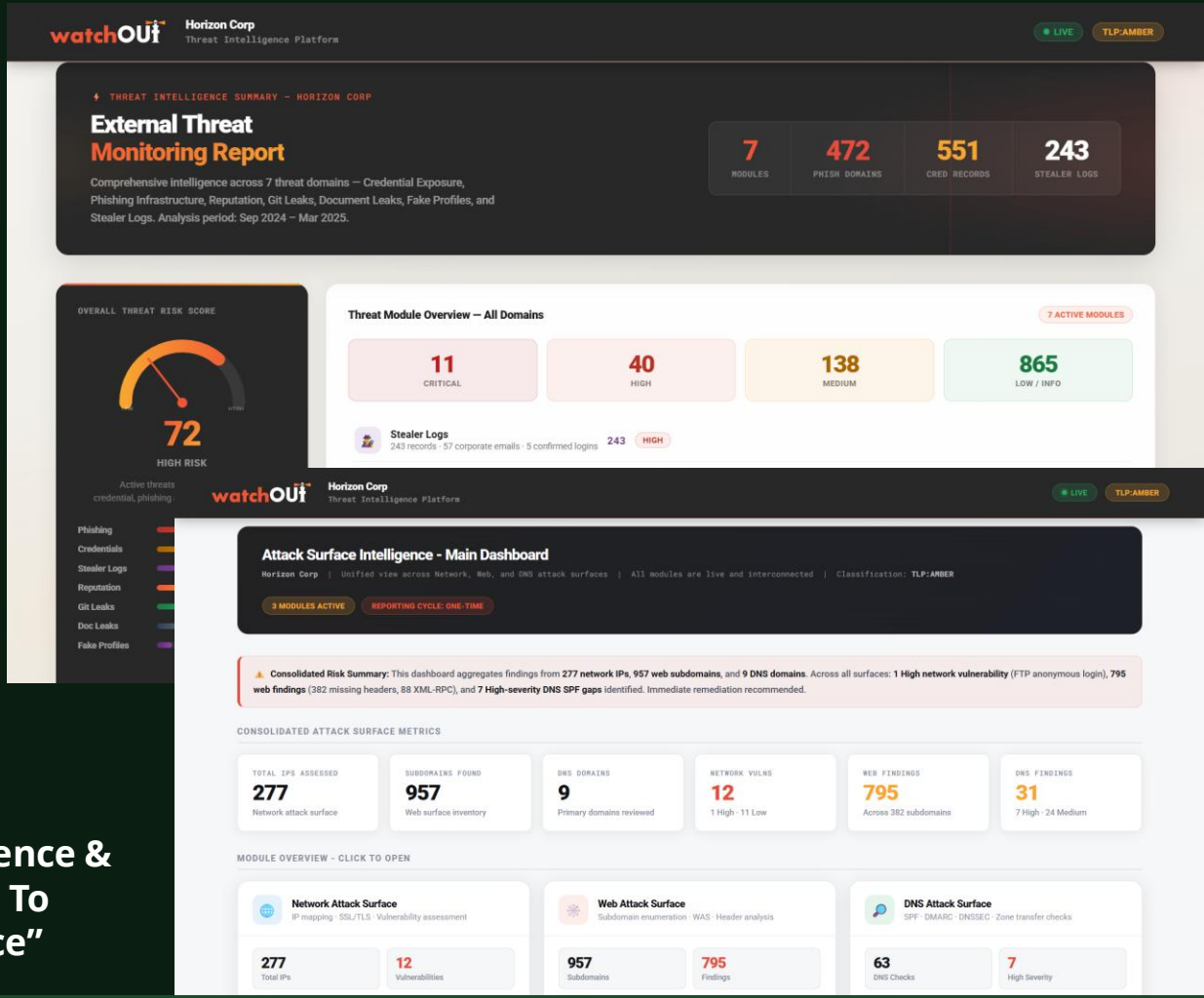
We analyse find and convert then into actionable intle

We don’t give you data, We provide with defence intel



Intel Technology

"watchOUT, An Advance Intelligence & Dark Web Platform Designed To Discover Directed Intelligence"



Powered By watchOUT

SIGNAL COLLECTION

- Dark Web Sources
- Web Monitoring
- Threat Intel Feeds

ANALYSIS & CURATION

- Base Curation
- Advanced Correlation
- Darkweb Correlation
- Expert Analyst Team

CURATED INTEL OUTPUT

- Intel Reports
- Intel Bundles
- STIX/TAXII
- Web Dashboard

watchOUT PLATFORM MODULES

phishWATCH | credWATCH | leakWATCH | gitWATCH | darkWATCH | fakeWATCH | repWATCH

Real-time Monitoring | Intelligent Filtering | Contextual Analysis | Unified Dashboard

RANSOMWARE RESPONSE

& FORENSIC SERVICES

CASTELLUM LABS

Many Ways To Damages

#1

Exposed Assets Of Companies

Inadvertently left out assets causing breaches.

#2

Insider Malicious Activities

Careless & Disgruntled employees causing damages.

#3

Ransomware Attack

Barrage of Ransomware Attacks everyday globally.

#4

Business Mail Compromise

Business mails compromised leaking data and IP.

Is Your Company Ready To Recover From An Attack ?

Castellum's Advance Ransomware Recovery

Stage 1

Containment Actions

- Find attack route
- Establish breach state
- Block further damage

Stage 2

Data Recovery

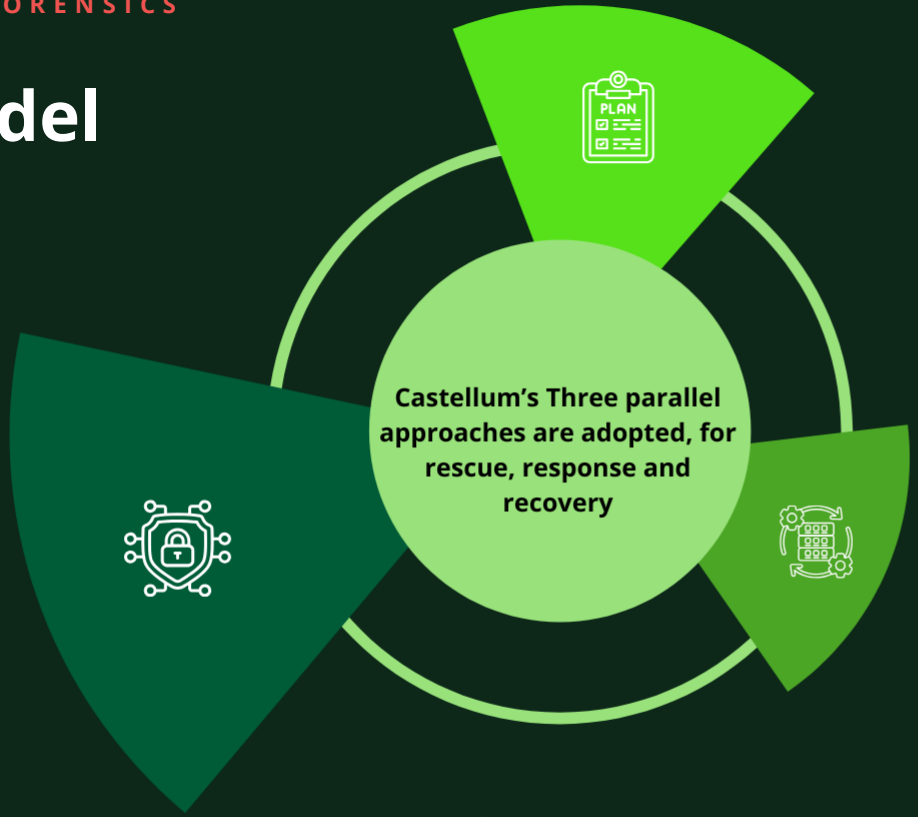
- Assess damage
- Data recovery attempt
- Root cause analysis

Stage 3

Cleanup & Ops Resumption

- Search and clean up
- Isolation completion
- Secure configurations

Model



01 Containment Actions

- Find attack route
- Establish compromise state
- Block from further escalation

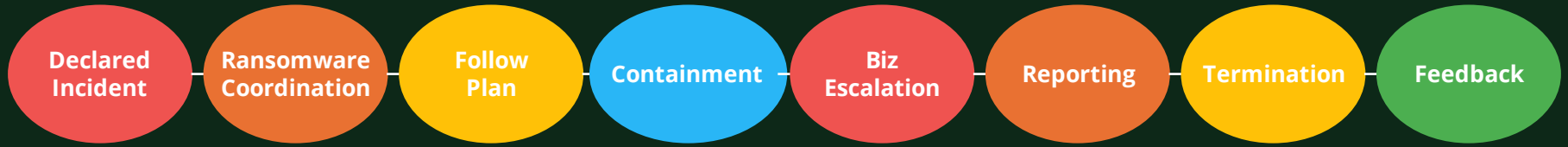
02 Cleanup & Ops Resumption

- Full search and clean up
- Isolation completion
- Secure config

03 Forensic & Data Recovery

- Assess damage
- Recovery attempt for data
- Root cause analysis & conclusion

Customized Incident Response Design



Coordinate & Assess

- Coordinate with triaging committee
- Assess severity of ransomware attack
- Gather IR team from system, network & cloud

Scope & Collect

- Scope the investigation for IR closure
- Collect IR documents, system, network & cloud data
- Define containment actions & communicate to team

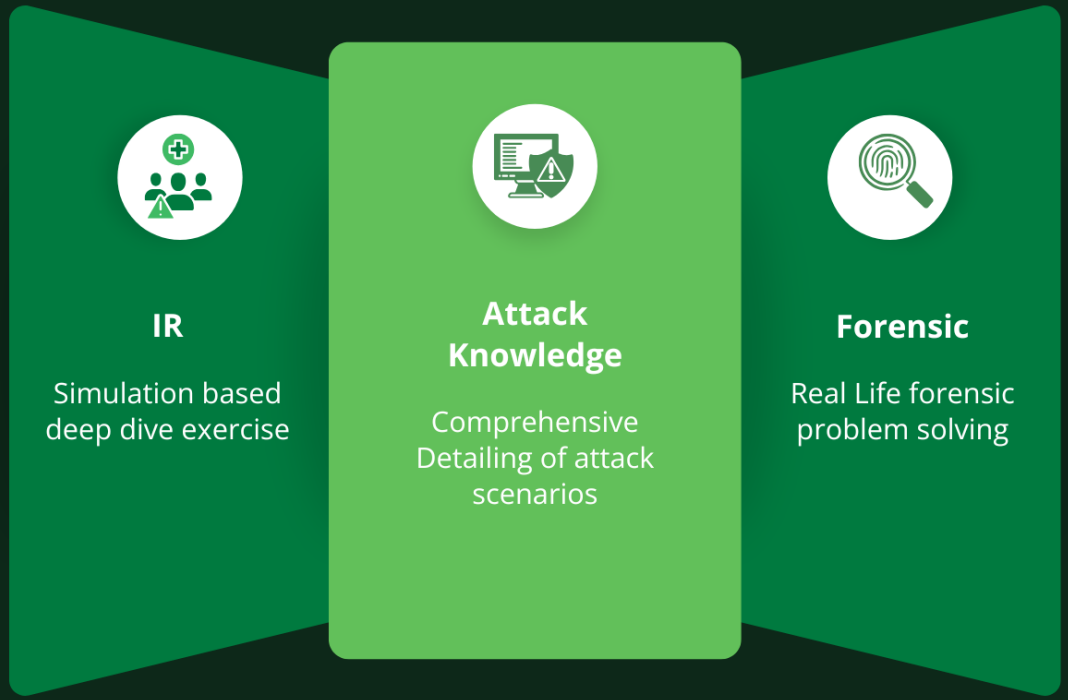
Communicate & Report

- Communicate to biz with incident summary
- Support PR and legal actions as needed
- Prepare incident reports and evidence packages

Close & Learn

- Communicate closure to all stakeholders
- Issue incident closure statement
- Post-incident meeting for learnings and corrections

Advance Attacks, IR & Forensic Trainings



Convenient Modes Of Sessions

Stage 1

Simulation Based

Simulate real-world cyberattacks to improve employee threat awareness.

Stage 2

Table-Top Exercise

Role-Play driven workshops for real world experience of attacks/IR .

Stage 3

Instructor Led Training

Structured classroom sessions-based training on attacks, IR & Forensics.

PHISHING SIMULATION

& EMPLOYEE AWARENESS PROGRAMS

CASTELLUM LABS

Employee Risky Behavior – The Biggest Threat

1/3
of all data breaches in 2025 involved phishing

1/25
branded emails is a phishing email

76%
of organizations targeted by phishing attacks

83%
of companies reported risky employee behaviors

Employees are the first line of attack & last line of defence - they must be assessed!!

PHISHERS TODAY ARE SUPER SOPHISTICATED

Multi-Channel
Phishing via email, SMS, WhatsApp, voice calls & social media simultaneously

Reconnaissance-Based
Attackers research targets, org structure, and social graph before launching attacks

Super-Targeted
Hyper-personalized spear phishing using OSINT and dark web credentials

Castellum's Managed Employee Awareness

Employee Profiling | Designed Phishing | Dispatch Calendaring | Response Tracking | Deep Insights & Analysis | Custom Prompts | Awareness Content | Behavior Shift Tracking

Assess Employees

Identify susceptibility using targeted phishing simulations across employee groups and org layers.

Prompt Risky Behavior

Real-time caution prompts and immediate feedback when risky behaviors are exhibited.

Train on Threats

Awareness content, cyber threat web sessions and multi-channel awareness delivered continuously.

Reassess & Track Shift

Behavioral shift tracking across cycles to measure improvement and identify persistent risk.

Deep Tech

“PhishBLAZE, An Advance Platform for turning your employees in a human firewall”

Advanced Phishing Methodology

Stage 1

Target Profiling

- Behavior profiling
- Situational context
- Develop target model
- Audience groups
- Organizational context

Stage 2

Phishing Operations

- Phishing design
- Dispatch controls
- Infra development
- Response collections
- Deep behavior analysis

Stage 3

Awareness & Training

- Mail prompts
- Mail, SMS, WhatsApp
- Web sessions
- Behavior assessment
- Self paced learning

Stage 4

Behavior Shift Tracking

- Behavioral Tracking
- Cycle management
- Track deviations
- Course corrections
- Special programs

SOC MONITORING

SIEM, MDR & SOLUTIONS

CASTELLUM LABS

Detection & Response – The Need & Why MDR

WHY DETECTION & RESPONSE IS CRITICAL

⚠ Security products and tools alone do not prevent breaches

⚠ Different alerts from different consoles can't detect an attack in its tracks

⚠ Logs, events and data must be consolidated and correlated for detection

⚠ Real-time action is needed on detected threat scenarios

⚠ SIEM/SOC consolidates logs into a single repository and correlates them

WHY MDR IS A GREAT OPTION

- No SIEM Licenses Required
- No SOC Monitoring Team Needed
- Reduced Capex and Opex
- Best-of-Breed IR Process
- Consolidated Security Reports
- No Tech Complexity
- No 24×7 Shift Overheads
- Definitive SLAs for Monitoring
- Phased Monitoring Expansion
- No Struggle with Talent Hunt

Castellum's MDR – Overview & Differentiators

A managed detection & response service using an integrated platform Combining human intelligence, hunting, forensic analytics and automation.

Human Actors & Intelligence

SOC team with detection, response, forensic and intelligence skills - not just automation.

Hunting Model for Monitoring

Proactive threat hunting model ensures threats are found before they cause damage.

Dark & Deep Web Intelligence

Integrated darkweb and deepweb intelligence built into the tNiXD platform natively.

Forensic Modelled Analytics

Detection algorithms designed using forensic methodology for deeper investigation.

Integrated Incident Response

Complete and comprehensive IR - from detection to closure, coordinated response model.

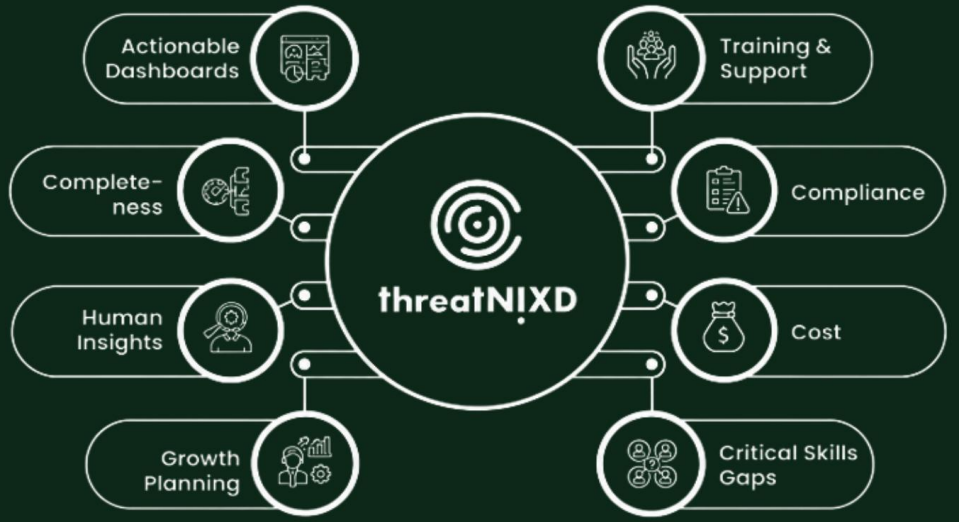
Effective Response Automation

Response automations reduce dwell time and eliminate manual steps in critical actions.

Our MDR Features

- Unique collection architecture to reduce noise
- Comprehensive collection: events, data & logs
- Large variety of devices, servers, apps, DBs supported
- Real-time multi-level correlation engine
- MITRE-mapped threat alert library (continuously updated)
- Fully integrated threat intelligence
- Dark web intelligence embedded in platform
- Critical alert dispatch to multiple channels
- 24×7 eye-on-glass monitoring by layered SOC team
- UEBA – User & Entity Behavior Analytics
- Network behavior analytics and diagnostics
- Advanced threat hunting model
- Coordinated response model with task tracking
- Multi-level SLAs and response automations
- Log retention for audit and compliance

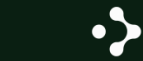
Next Gen SOC Tech



“threatNiXD, Advance detection & response platform for AI First digital Infrastructures ”

MANAGED
DEVSECOPS

CASTELLUM LABS



DevSecOps – Broad Meaning & Why It Matters

PLAN	CODE	BUILD	TEST	RELEASE	DEPLOY	OPERATE	MONITOR

Design Controls
Security controls embedded at the planning stage before code is written

Automate Scans/Tests
SCA, SAST, DAST, IAST scans triggered automatically at each CI/CD stage

Decision Tree
Security-gated release decisions: automated pass/fail based on defined policies

Policy Frame
AppSec owner-defined security policies drive what scans run and what gates release

WHY DEVSECOPS MOSTLY FAILS

- Very Noisy Scans
- No Realtime Decisions
- Security Control Conflict
- Missing Feedback Loop

Castellum's DevSecOps Model

Stage 1

Security Controls Framework Design

Design a custom security controls framework based on the customer's CI/CD infrastructure, DevOps maturity, release model and security objectives — aligned to software and developer context.

Stage 2

Tool Integration & Optimization

Integrate or optimize vulnerability tools across the CI/CD chain for optimal coverage. Includes event-based automated triggering, enriched output, deduplication of vulnerabilities, and reporting model.

Stage 3

Operational Streamlining

Streamline the DevSecOps operational model, conduct test releases for vulnerability handling, run workshops for developers, AppSec owners and executives. Design the DevSecOps roadmap.

CI/CD PIPELINE CONTROL STAGES

Pre-Commit	On Commit	Branch Merges	Artifact Creation	Pipeline Executions	Quality Releases	Pre-Prod Testing	Prod Release	Post-Prod Sanity	Prod Monitoring

Solution Features

On-Premise Setup	Cloud Native	Unified Views	Multi-Model Deployment
SCA / SAST / DAST / IAST	26 Vulnerability Categories	Automated Security Controls	Quality Comprehensive Scans
10 Quality Parameters	Across Release Controls	Integrate Any Scanner	Dynamic Real-Time Notification
Individual Vulnerability Results	Any DevOps Model / Infrastructure	Extensible Solution Stack	Leads to Full DevSecOps

SECURITY & QUALITY TECHNOLOGY

SCA Software Composition Analysis - open source & dependency vulnerabilities

SAST Static Application Security Testing - code-level vulnerability scanning

DAST Dynamic Application Security Testing - runtime & API vulnerability detection

IAST Interactive Application Security Testing - instrumented runtime analysis

Castellum Labs

REQUEST DEMO

INQUIRE NOW

Get Started Today

🌐 www.castellumlabs.com

✉ reach@castellumlabs.com

📞 +91 7842046995

📍 **Office #403, Fourth Floor,** Magna Park View Towers, Urdu University Rd
Sri Shyam Nagar, Telecom Nagar, Gachibowli
Hyderabad, Telangana 500032