Castellum Labs

SERVICE DESCRIPTION

FORENSIC & RESPONSE

IR design, traning and forensic

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995

Weak IR Wreaks Havoc

> *Last year companies worldwide lost huge money to ransomware*

$30+ BILLION LOSS

8000+
ATTACKS OCCURED

120+
AFFECTED COUNTRIES

16+
SECTORS AFFECTED

Financial Impact
Increased losses from business disruption, recovery, and remediation.

Security Impact
Persistent threats due to incomplete investigation and containment.

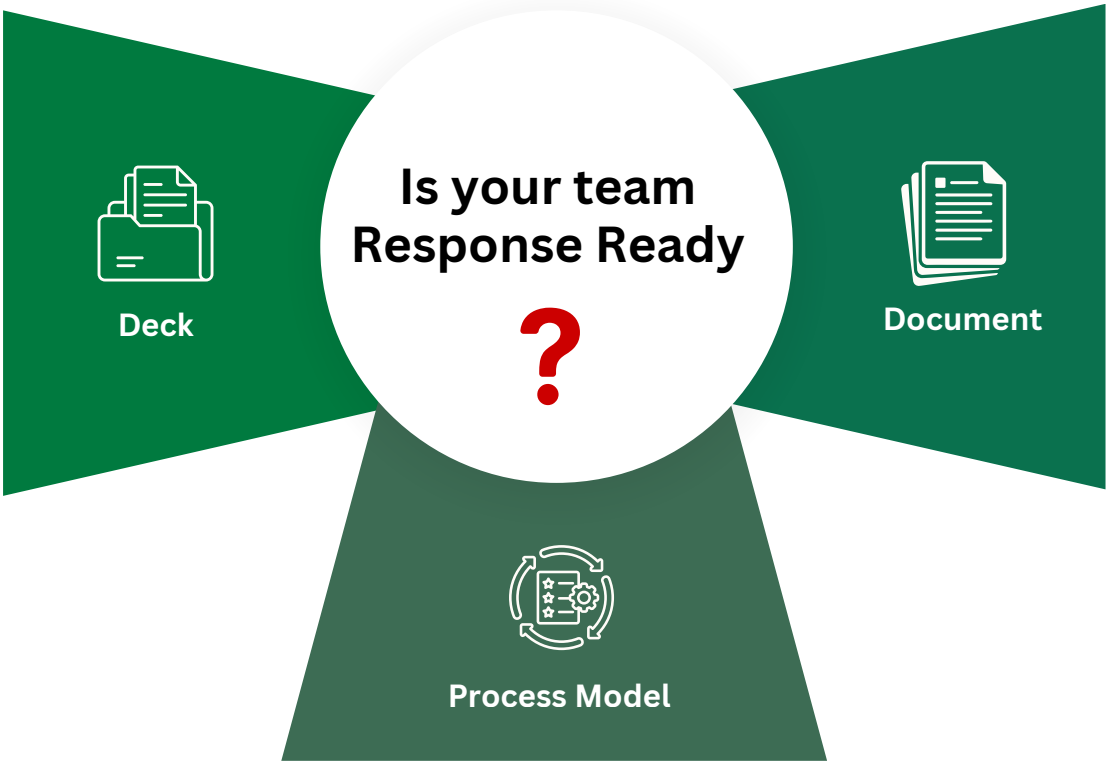
Operational Impact
Downtime and delays caused by ineffective response processes.

Compliance & Legal Impact
Regulatory penalties and legal risks from improper incident handling.

Business Continuity Impact
Service disruptions affecting critical business operations.

Reputational Impact
Loss of customer trust and damage to brand reputation.

Weak IR Wreaks Havoc



01 What was the last time your IT saw a real Ransomware attack.

02 Get your process to wake up
Get it activated

03 Redesign IR for activation
Get your team Ransomware Ready

Forensic / IR Service

01

Ransomware Response Service

02

Incident Response Process Design

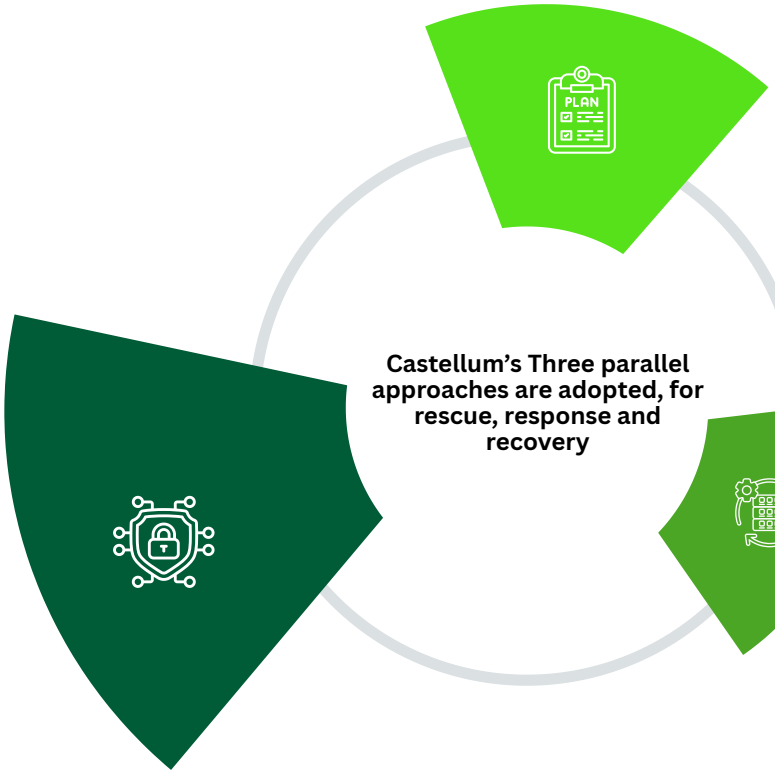
03

IR Workshops & Attack Training

04

Forensic Services On-Demand

Ransomware Response & Recovery



01

Containment Actions

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

02

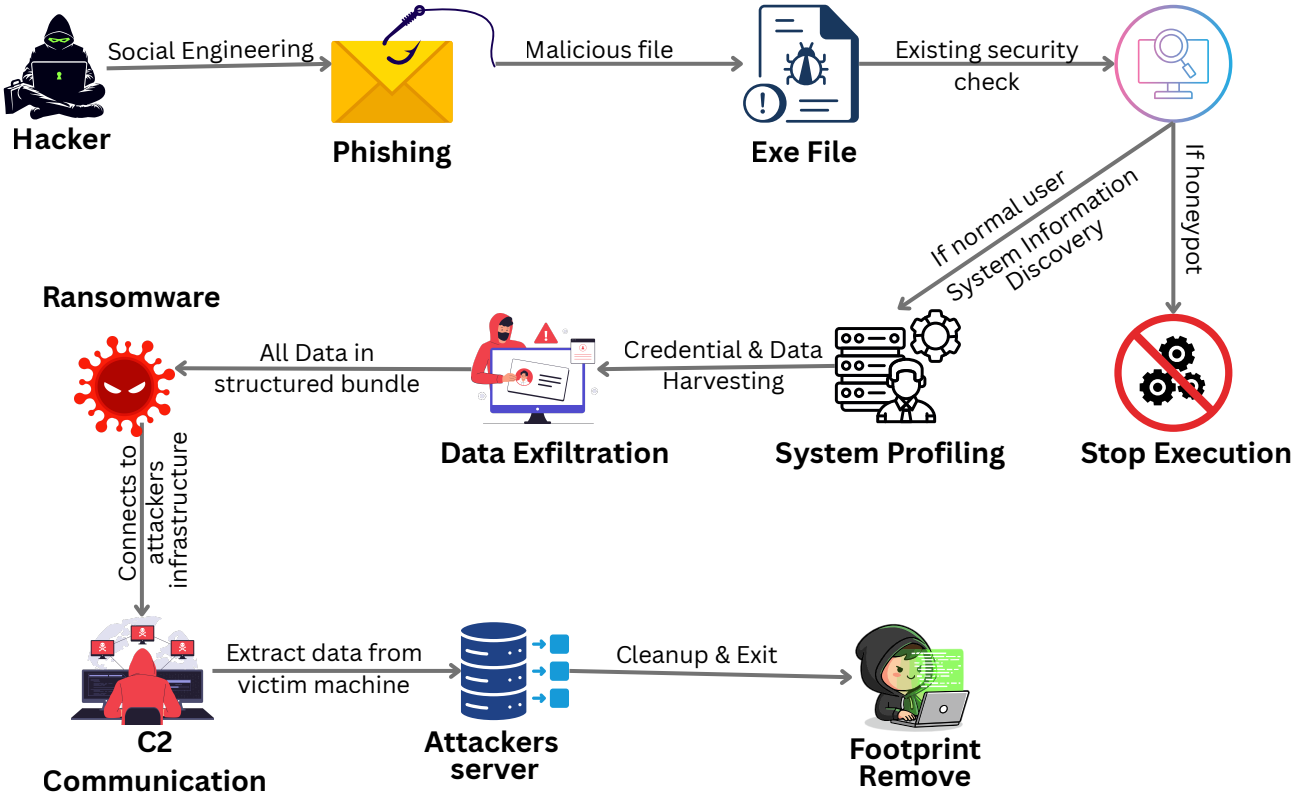
Cleanup & Ops Resumption

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

03

Forensic & Data Recovery

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



Ransomware Response & Recovery

01 Network Investigation

02 Directory Analysis

03 Device Forensic

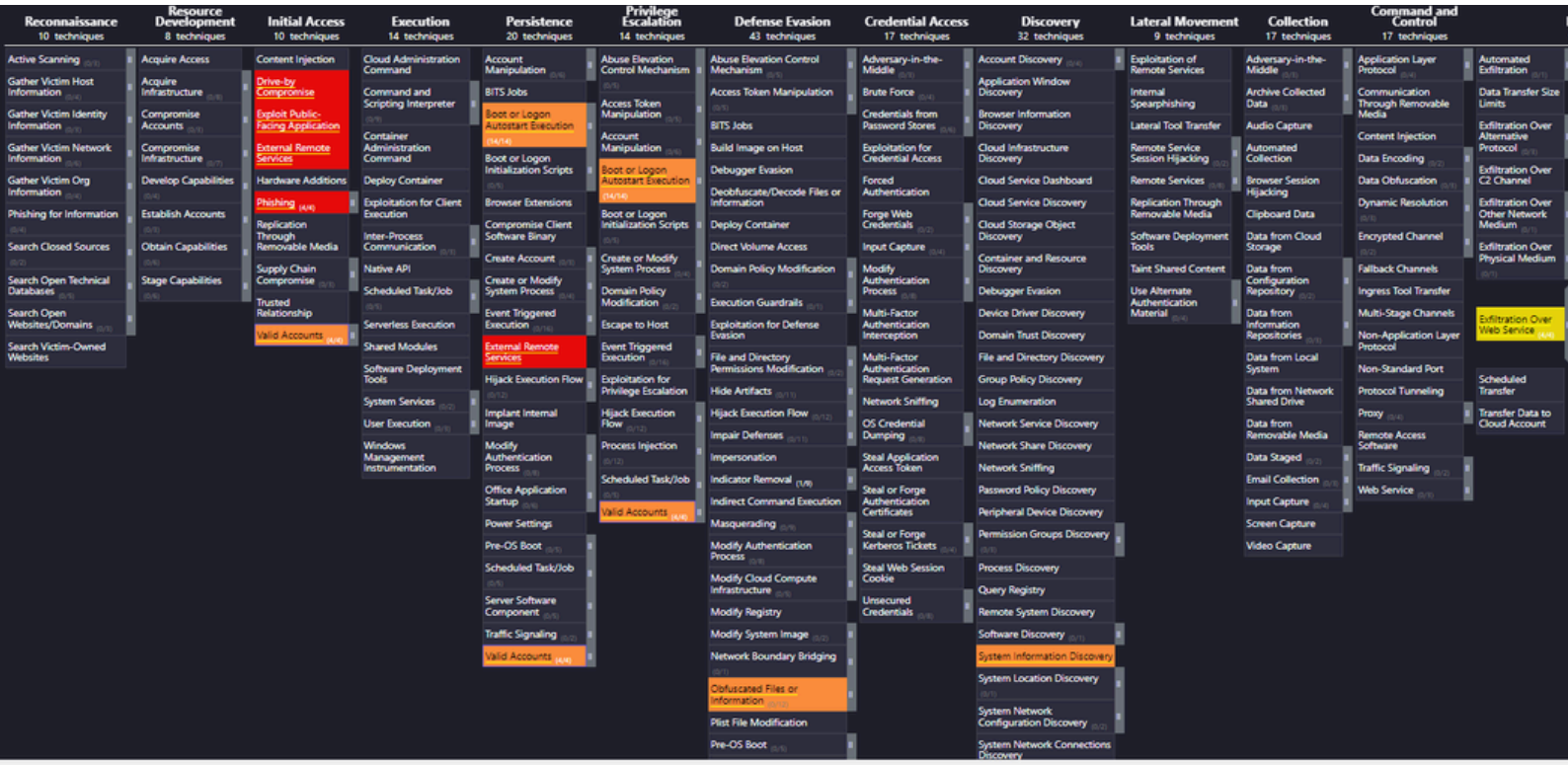
04 Log Correlation

05 Darkweb Searcher

06 Data Extraction

07 Ransomware Negotiation

08 Ransomware Decryption



Activated your IR

Most Incident Response process is passive

Inciden Response process in document

MEANS NOTHING

Get IR Activated

Activated your IR

Gather IR team, pick people from system, network & cloud teams

Coordinate with triaging committee, assess severity of ransomware attack

Scope the investigation for incident response and closure

Ransomware Incident Coordination

Collect IR documents and system, network and cloud data

Feedback

Conduct post incident meeting for sharing learning, intelligence and corrections

Containment

Further containment actions to be decided and communicated to incident tech action coordinator

Termination

Communicate closure of incident to all stakeholder along with incident closure statement

Biz Escalation

Communicate to biz along with incident summary page for potential PR and legal actions

Reporting

Collect evidences, decide about forensic needs and prepare incident reports

IR & Attack Simulation

Process Speed

Measure how fast workflows are compared to competitors' benchmarks.

Service Quality

Review customer satisfaction and support effectiveness across all touchpoints.

Team Skills

Assess staff expertise and ability to complete tasks efficiently.

Trained Employee

Untrained Employee

Engagement Channels

Analyze variety and efficiency of customer communication methods.

Automation Tools

Evaluate automation tools used to improve workflow productivity.

Feedback Systems

Examine how customer insights are collected and applied effectively.

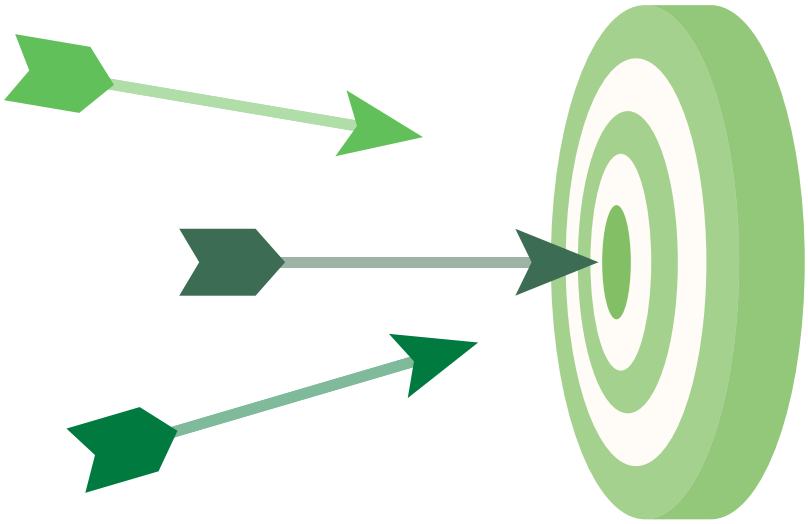
Most of the IT Staff have never seen attack for real

IR & Attack Simulation

01 Simulation Based

02 Table Top Exercise

03 Instructor Led Training



IR

Simulation based deep dive exercise

Attack Knowledge

Comprehensive Detailing of attack scenarios

Forensic

Real Life forensic problem solving

Forensic Service / Experts on Demand

Forensic Experts with real life work

Team Viewer Compromised

Internal laptop Employee laptop

(Either a direct access or through a phishing)

RDP Access Known Credentials

RDP Access Known Credentials

Large no of special privilege logons → System audit policy changes → New processes, “C”/”R” created (for copy / encryption) → Csrss.exe executed from unusual location → External connection made for extraction

Data Copied & Encrypted (Local on server) (.play encryption)

Shutdowns & Server Controls

Data Extracted (Taken to C2C) (Taken to Darkweb)

Ransomware Tools/Tech inititated

Forensic Service / Experts on Demand

Senior DFIR experts provide specialized guidance, investigation strategy, evidence interpretation, and incident decision support.

Our forensic experts visit your location to collect, preserve, analyze, and support evidence handling directly within your environment.

Secure remote support for quick forensic triage, evidence review, log analysis, and investigation guidance without physical presence.

Case Study, Mail Breach & Financial Loss

01 A Customer in manufacture got duped.

02 His mail infrastructure was breached by hackers.

03 Phisher/Hackers impersonate company officials.

04 The Company lost large sum of money.

$ 500K +

LOSS

Phishing mails with Spoofed Domain

Employee Clicks Malicious Link

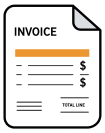
Account Takeover by bad Actors

Fake mails to Clients/Venders for bank details change

– They did

₹5 Crores Loss to our customer
Impact on Clients/Venders

- Unknown



Fake Invoice to Account

– They Approved

Sent Fake Invoice/Emails to Account Section/Clients/Venders

Case Study, Castellum Labs Response for Breach

01

Phase 1 - Containment

- Establish Compromise
- Detect Root Cause
- Close Doors

02

Phase 2 – Fix Sec Gaps

- Correct DNS Sec Configs
- O365 Sec Configuration
- Spoofing Protection

03

Phase 3 – RCA & Closure

- Submit forensic conclusion
- RCA to management
- Closures

Full containment. response & recovery

Zero business disruption during investigation

24/7 monitoring during critical phases

Professional coordination across all providers.

Containment within 7 days

Counter measure within 11 Days

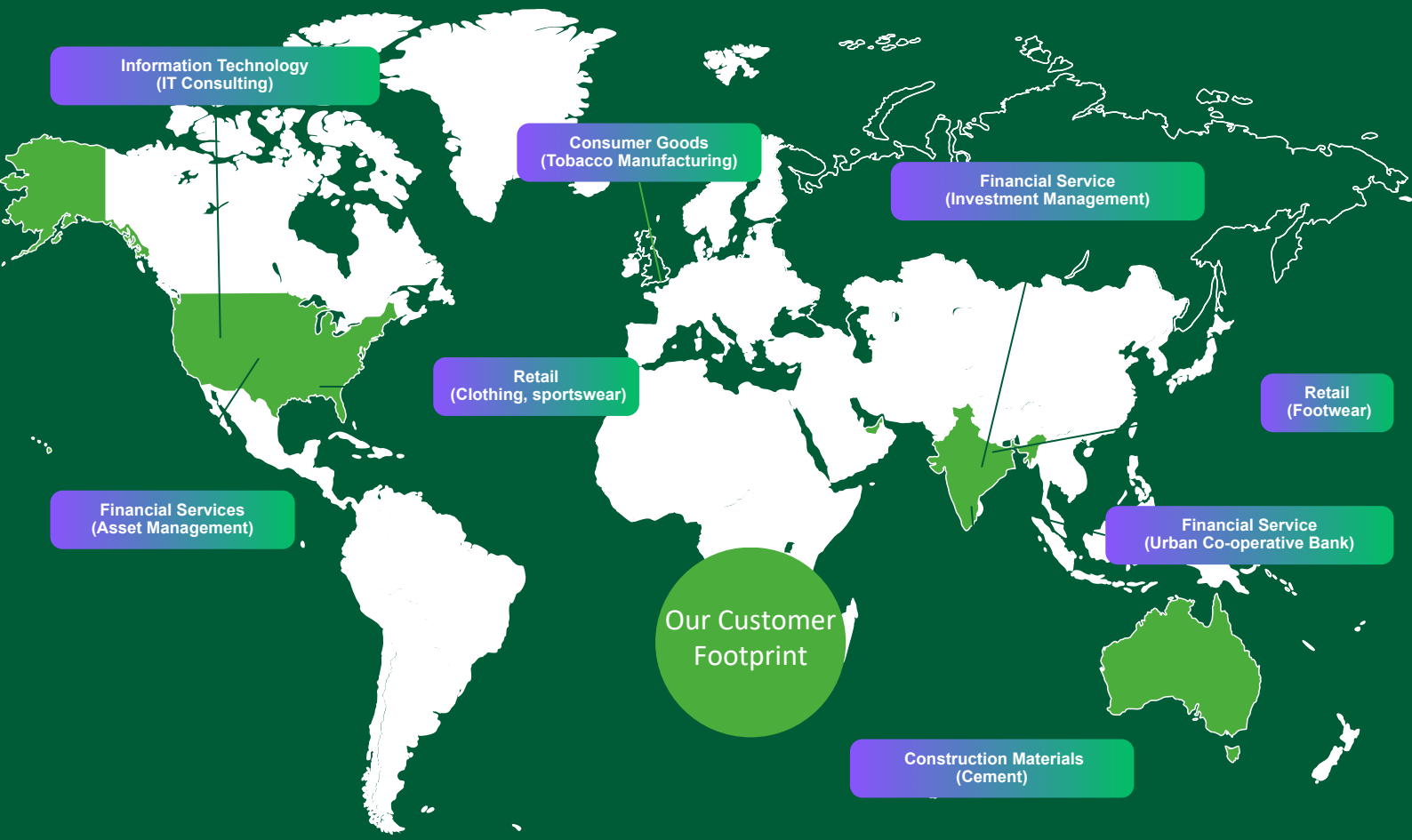
Zero business disruption

5 miilion dollar saved

About Castellum Labs

- All Services delivered from Global Security Delivery Center (GSDC)
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong handpicked team of (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio

Secure Cloud WL

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

We create secure cloud environments, automate Cloud SecOps & manage it.

24x7 Monitoring

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

When it comes to SOC Monitoring & Response, we cover all aspects of it

Vuln Mgmt

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuin Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

Program designed VAPT Engagement to enhance protection & reduce attack surface

Threat Intel

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

We take threat intel maintenance, keep, usage & application to next level.

Data & Privacy

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

Data and privacy are two considerations, we design, implement it & run compliances

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995