

FORENSIC & RESPONSE

IR design, training 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



01

**Ransomware
Response
Service**



02

**Incident
Response
Process Design**



**Forensic / IR
Service**

03

**IR Workshops
& Attack
Training**

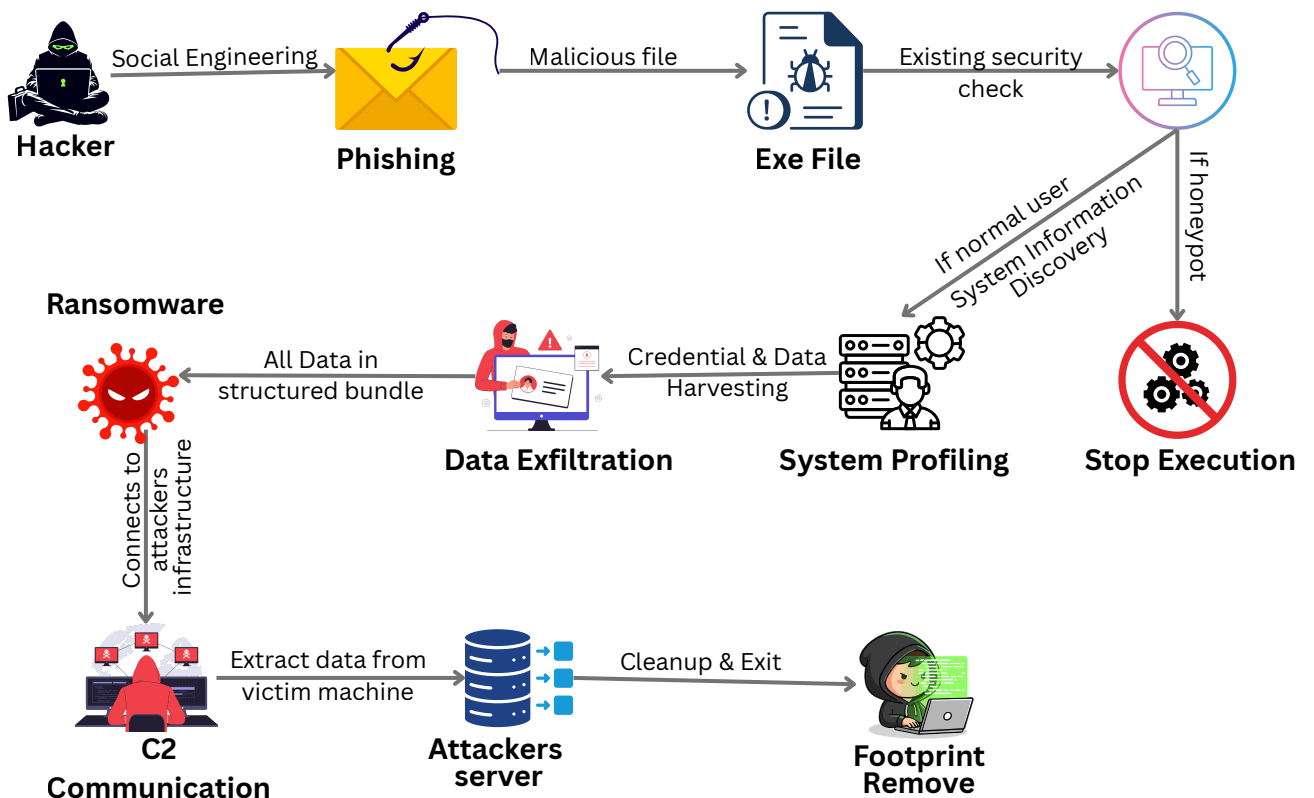
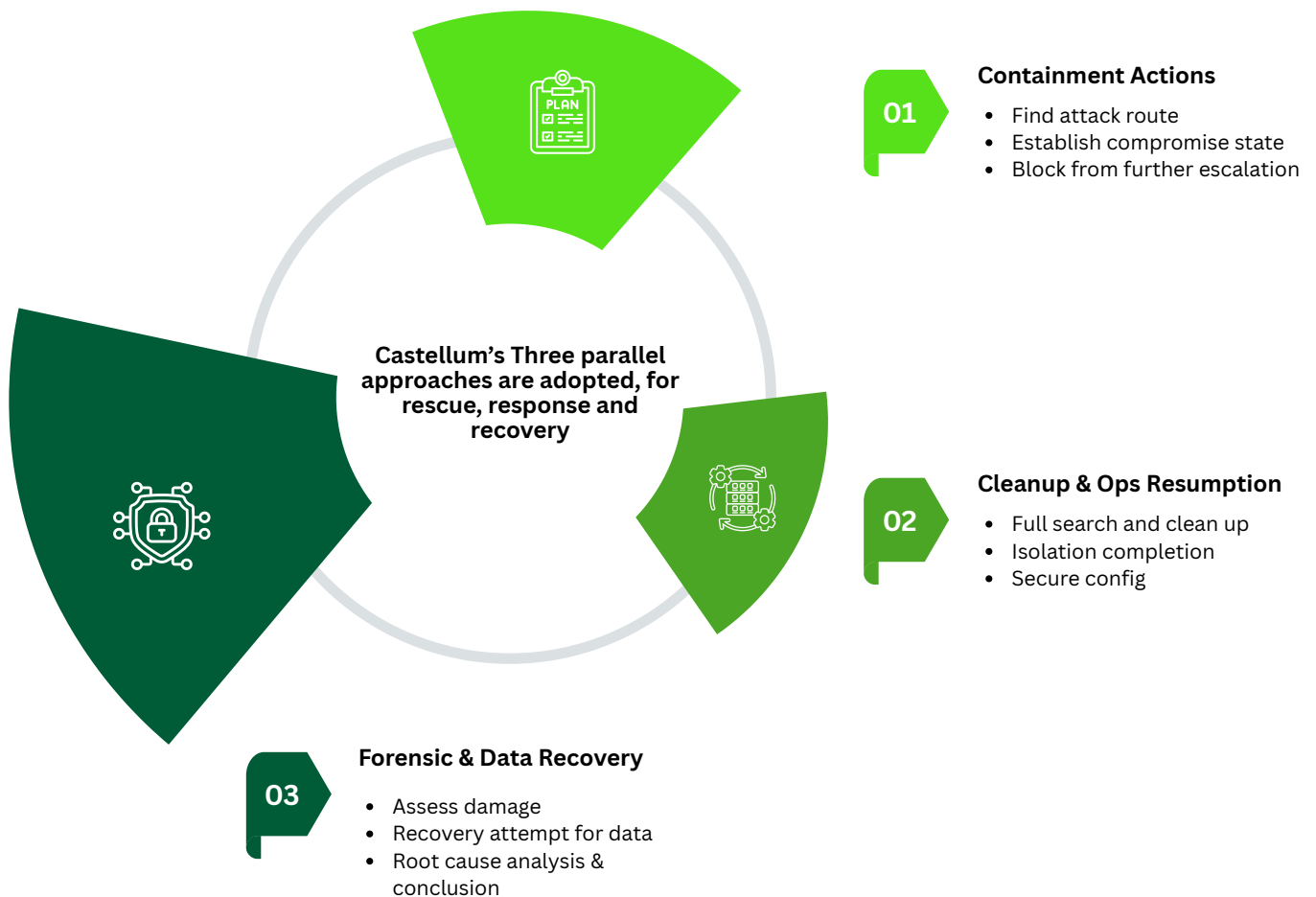


04

**Forensic
Services
On-Demand**



Ransomware Response & Recovery



Ransomware Response & Recovery

- 01
- 02
- 03
- 04

Network Investigation



Directory Analysis



Device Forensic



Log Correlation



- 05
- 06
- 07
- 08

Darkweb Searcher



Data Extraction



Ransomware Negotiation



Ransomware Decryption

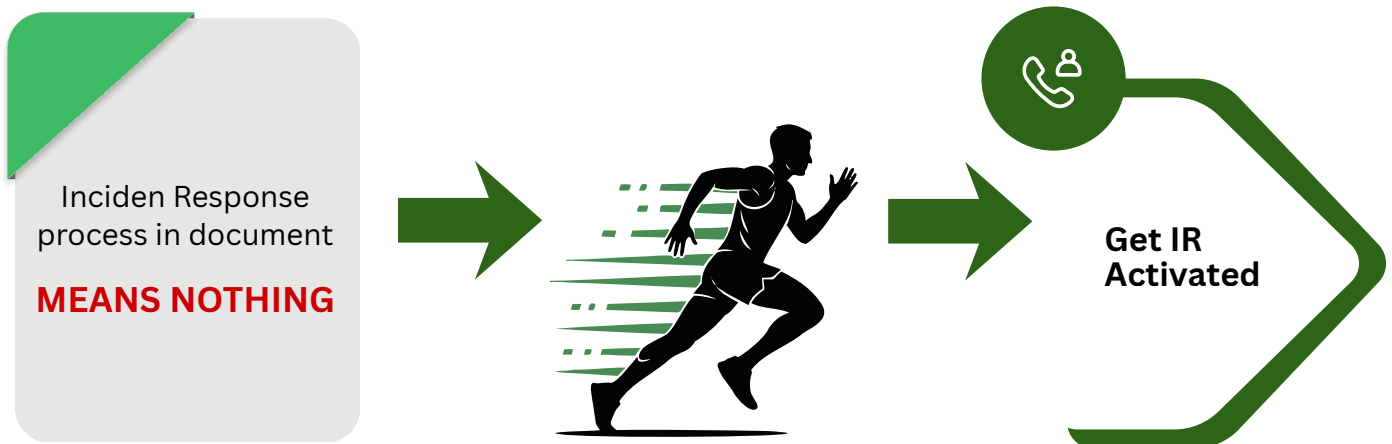


Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques
Active Scanning (0.00)	Acquire Access (0.00)	Content Injection (0.00)	Cloud Administration Command (0.00)	Account Manipulation (0.00)	Abuse Elevation Control Mechanism (0.00)	Abuse Elevation Control Mechanism (0.00)	Adversary-in-the-Middle (0.00)	Account Discovery (0.00)	Exploitation of Remote Services (0.00)	Adversary-in-the-Middle (0.00)	Application Layer Protocol (0.00)
Gather Victim Host Information (0.00)	Acquire Infrastructure (0.00)	Drive-by Compromise (0.00)	Command and Scripting Interpreter (0.00)	BITS Jobs (0.00)	Access Token Manipulation (0.00)	Access Token Manipulation (0.00)	Brute Force (0.00)	Application Window Discovery (0.00)	Internal Spearphishing (0.00)	Archive Collected Data (0.00)	Communication Through Removable Media (0.00)
Gather Victim Identity Information (0.00)	Compromise Accounts (0.00)	Exploit Public-Facing Application (0.00)	Container Administration Command (0.00)	Boot or Logon Autostart Execution (0.00)	Account Manipulation (0.00)	BITS Jobs (0.00)	Credentials from Password Stores (0.00)	Browser Information Discovery (0.00)	Lateral Tool Transfer (0.00)	Audio Capture (0.00)	Data Transfer Size Limits (0.00)
Gather Victim Network Information (0.00)	Compromise Infrastructure (0.00)	External Remote Services (0.00)	Deploy Container (0.00)	Boot or Logon Initialization Scripts (0.00)	Boot or Logon Autostart Execution (0.00)	Build Image on Host (0.00)	Exploitation for Credential Access (0.00)	Cloud Infrastructure Discovery (0.00)	Remote Service Session Hijacking (0.00)	Automated Collection (0.00)	Exfiltration Over Alternative Protocol (0.00)
Gather Victim Org Information (0.00)	Develop Capabilities (0.00)	Hardware Additions (0.00)	Exploitation for Client Execution (0.00)	Browser Extensions (0.00)	Boot or Logon Initialization Scripts (0.00)	Debugger Evasion (0.00)	Forced Authentication (0.00)	Cloud Service Dashboard (0.00)	Remote Services (0.00)	Data Encoding (0.00)	Exfiltration Over C2 Channel (0.00)
Phishing for Information (0.00)	Establish Accounts (0.00)	Phishing (0.00)	Inter-Process Communication (0.00)	Compromise Client Software Binary (0.00)	Boot or Logon Initialization Scripts (0.00)	Deobfuscate/Decode Files or Information (0.00)	Forge Web Credentials (0.00)	Cloud Storage Object Discovery (0.00)	Replication Through Removable Media (0.00)	Clipboard Data (0.00)	Exfiltration Over Other Network Medium (0.00)
Search Closed Sources (0.00)	Obtain Capabilities (0.00)	Supply Chain Compromise (0.00)	Native API (0.00)	Create Account (0.00)	Create or Modify System Process (0.00)	Direct Volume Access (0.00)	Input Capture (0.00)	Container and Resource Discovery (0.00)	Software Deployment Tools (0.00)	Data from Cloud Storage (0.00)	Exfiltration Over Physical Medium (0.00)
Search Open Technical Databases (0.00)	Stage Capabilities (0.00)	Trusted Relationship (0.00)	Scheduled Task/Job (0.00)	Create or Modify System Process (0.00)	Domain Policy Modification (0.00)	Domain Policy Modification (0.00)	Modify Authentication Process (0.00)	Debugger Evasion (0.00)	Taint Shared Content (0.00)	Data from Configuration Repository (0.00)	Fallback Channels (0.00)
Search Open Websites/Domains (0.00)	Valid Accounts (0.00)	Valid Accounts (0.00)	Serverless Execution (0.00)	Event Triggered Execution (0.00)	Execution Guardrails (0.00)	Execution Guardrails (0.00)	Multi-Factor Authentication Interception (0.00)	Device Driver Discovery (0.00)	Use Alternate Authentication Material (0.00)	Data from Information Repositories (0.00)	Ingress Tool Transfer (0.00)
Search Victim-Owned Websites (0.00)	Shared Modules (0.00)	Software Deployment Tools (0.00)	System Services (0.00)	Hijack Execution Flow (0.00)	Exploitation for Privilege Escalation (0.00)	File and Directory Permissions Modification (0.00)	Multi-Factor Authentication Request Generation (0.00)	Domain Trust Discovery (0.00)	File and Directory Discovery (0.00)	Data from Local System (0.00)	Multi-Stage Channels (0.00)
	User Execution (0.00)	System Services (0.00)	Windows Management Instrumentation (0.00)	Implant Internal Image (0.00)	Hijack Execution Flow (0.00)	Hijack Execution Flow (0.00)	Network Sniffing (0.00)	File and Directory Discovery (0.00)	Group Policy Discovery (0.00)	Data from Network Shared Drive (0.00)	Non-Application Layer Protocol (0.00)
				Modify Authentication Process (0.00)	Process Injection (0.00)	Impair Defenses (0.00)	OS Credential Dumping (0.00)	Log Enumeration (0.00)	Network Service Discovery (0.00)	Data from Removable Media (0.00)	Non-Standard Port (0.00)
				Office Application Startup (0.00)	Scheduled Task/Job (0.00)	Impersonation (0.00)	Steal Application Access Token (0.00)	Network Share Discovery (0.00)	Network Sniffing (0.00)	Data Staged (0.00)	Protocol Tunneling (0.00)
				Power Settings (0.00)	Valid Accounts (0.00)	Indicator Removal (0.00)	Steal or Forge Authentication Certificates (0.00)	Password Policy Discovery (0.00)	Peripheral Groups Discovery (0.00)	Email Collection (0.00)	Prony (0.00)
				Pre-OS Boot (0.00)	Valid Accounts (0.00)	Indirect Command Execution (0.00)	Steal or Forge Kerberos Tickets (0.00)	Permission Groups Discovery (0.00)	Process Discovery (0.00)	Input Capture (0.00)	Remote Access Software (0.00)
				Scheduled Task/Job (0.00)	Valid Accounts (0.00)	Masquerading (0.00)	Steal Web Session Cookie (0.00)	Query Registry (0.00)	Remote System Discovery (0.00)	Screen Capture (0.00)	Traffic Signaling (0.00)
				Server Software Component (0.00)	Valid Accounts (0.00)	Modify Authentication Process (0.00)	Unsecured Credentials (0.00)	Software Discovery (0.00)	System Information Discovery (0.00)	Video Capture (0.00)	Web Service (0.00)
				Traffic Signaling (0.00)	Valid Accounts (0.00)	Modify Cloud Compute Infrastructure (0.00)		System Location Discovery (0.00)	System Network Configuration Discovery (0.00)		
				Valid Accounts (0.00)	Valid Accounts (0.00)	Modify Registry (0.00)		System Network Connections Discovery (0.00)			
				Valid Accounts (0.00)	Valid Accounts (0.00)	Modify System Image (0.00)					
				Valid Accounts (0.00)	Valid Accounts (0.00)	Network Boundary Bridging (0.00)					
				Valid Accounts (0.00)	Valid Accounts (0.00)	Obfuscate Files or Information (0.00)					
				Valid Accounts (0.00)	Valid Accounts (0.00)	Plist File Modification (0.00)					
				Valid Accounts (0.00)	Valid Accounts (0.00)	Pre-OS Boot (0.00)					

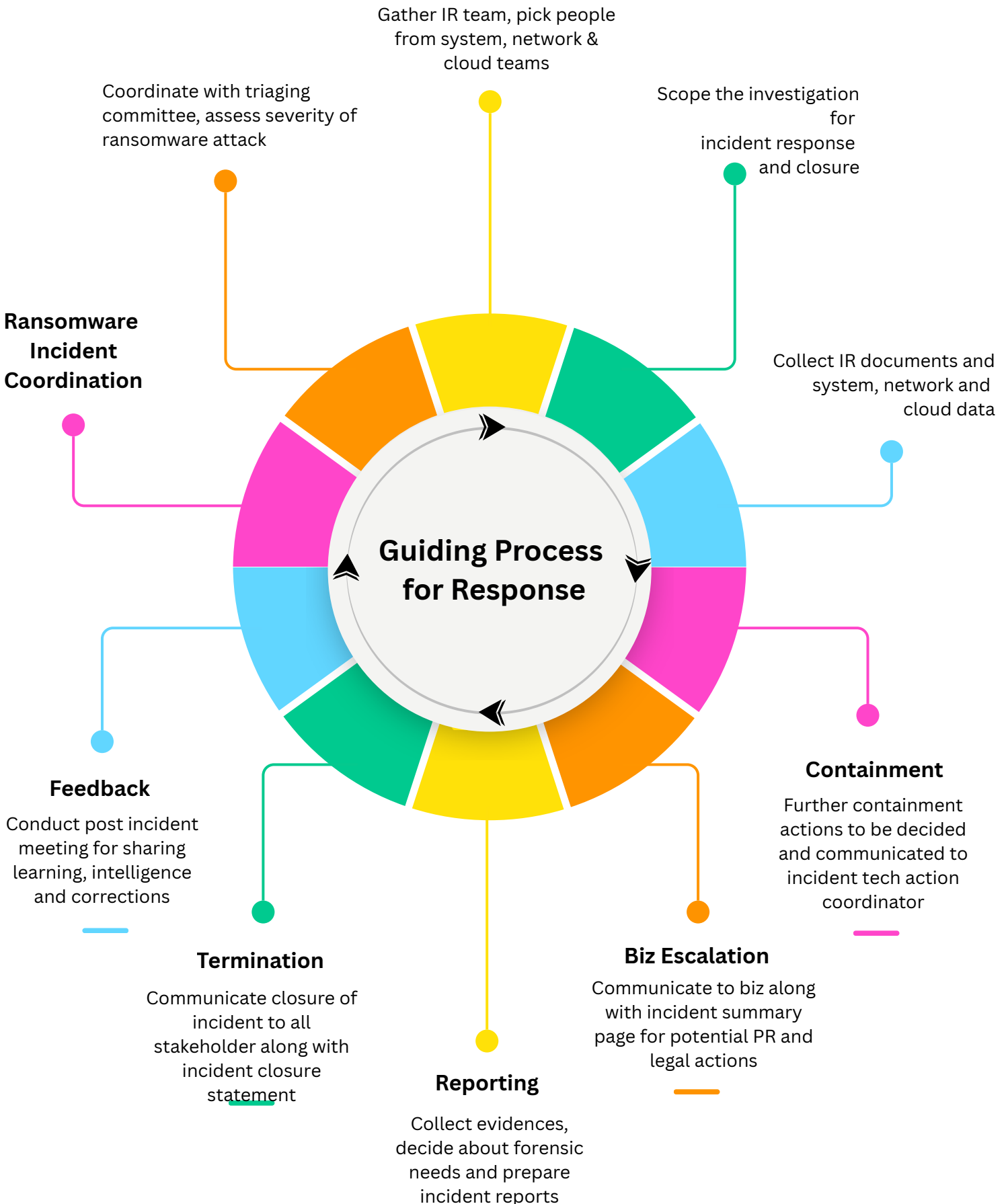
Activated your IR



Most Incident Response process is passive



Activated your IR



IR & Attack Simulation

Process Speed

Measure how fast workflows are compared to competitors' benchmarks.



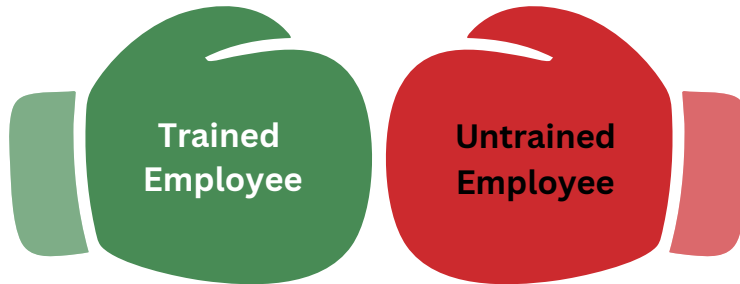
Service Quality

Review customer satisfaction and support effectiveness across all touchpoints.



Team Skills

Assess staff expertise and ability to complete tasks efficiently.



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.

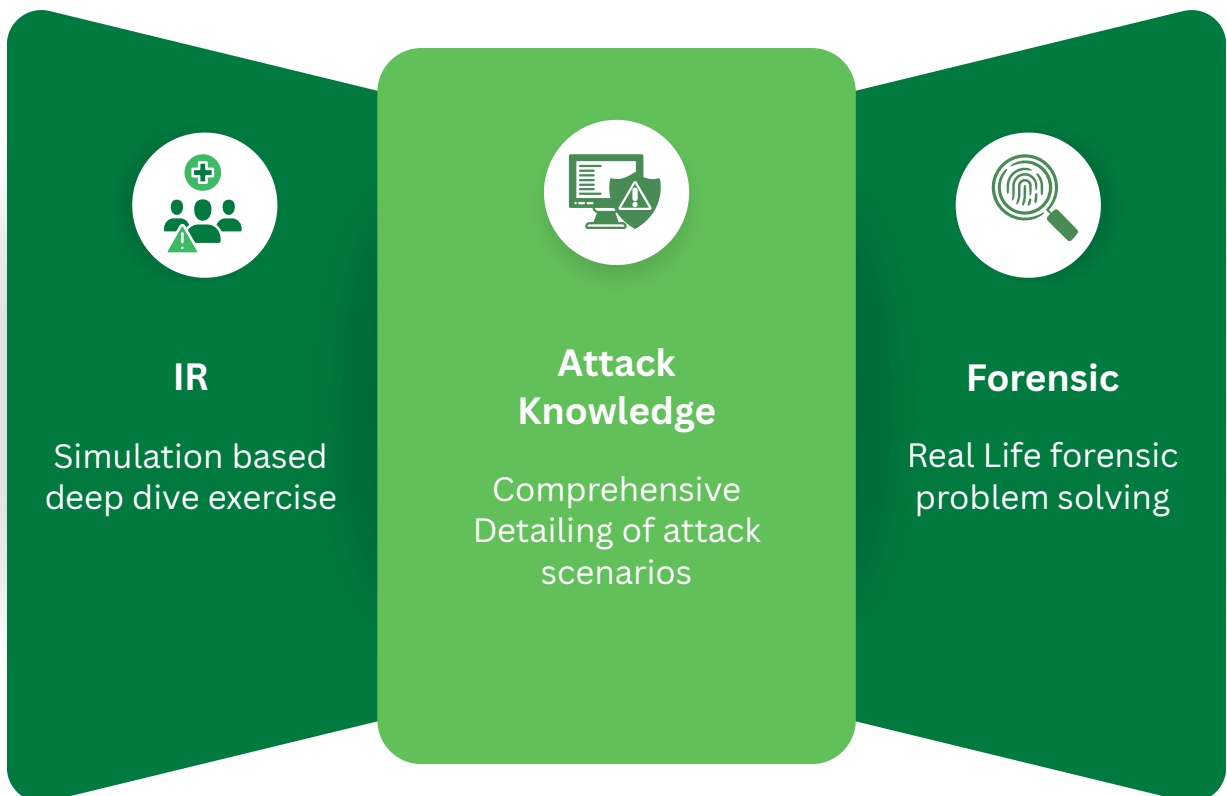
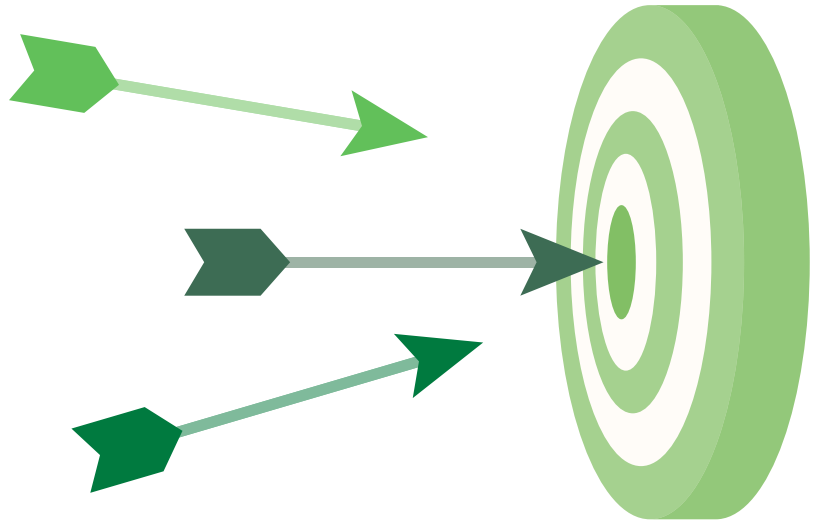


Most of the IT Staff have never seen attack for real



IR & Attack Simulation

- 01 Simulation Based
- 02 Table Top Exercise
- 03 Instructor Led Training



Forensic Service / Experts on Demand



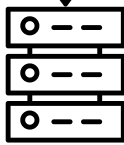
Forensic Experts
with real life
work

Team Viewer
Compromised

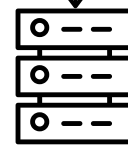


Internal laptop
Employee laptop

(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
initiated

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

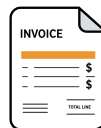


₹5 Crores Loss to our customer
Impact on Clients/Venders

- Unknown



Fake mails to Clients/Venders for bank details change
- They did



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



02



Zero business disruption
during investigation

01

\$

03

24/7 monitoring during
critical phases



04



Professional coordination
across all providers.



Containment within 7 days



Counter measure within 11 Days



Zero business disruption



5 million dollar saved



About Castellum Labs

Based in Hyderabad, India with global customer base across India, US, Europe

Started by people with decades of product, services & deep tech experience

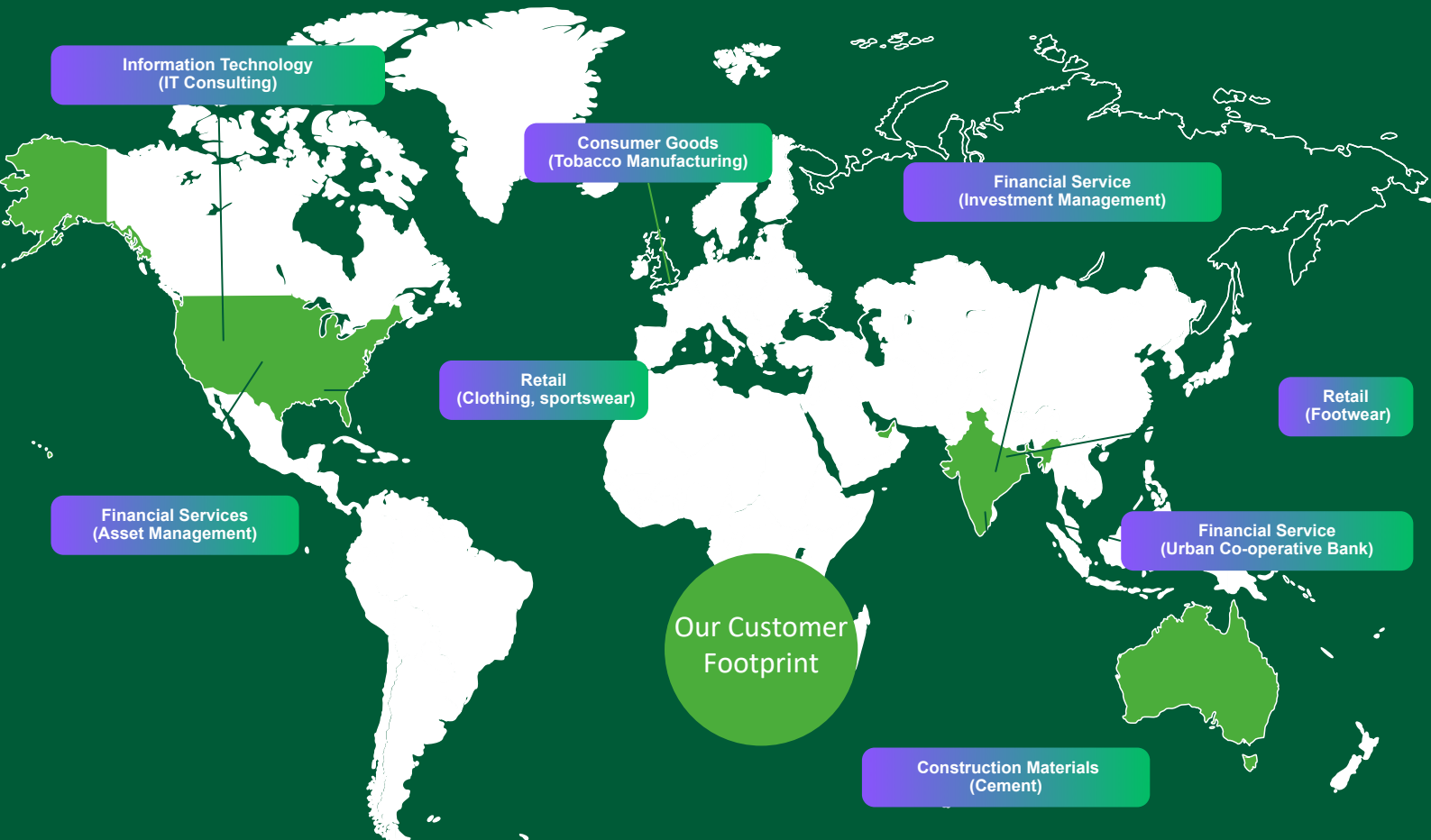
Value + Impact from Day One, No Installation & No Deployment

All Services delivered from Global Security Delivery Center (GSDC)

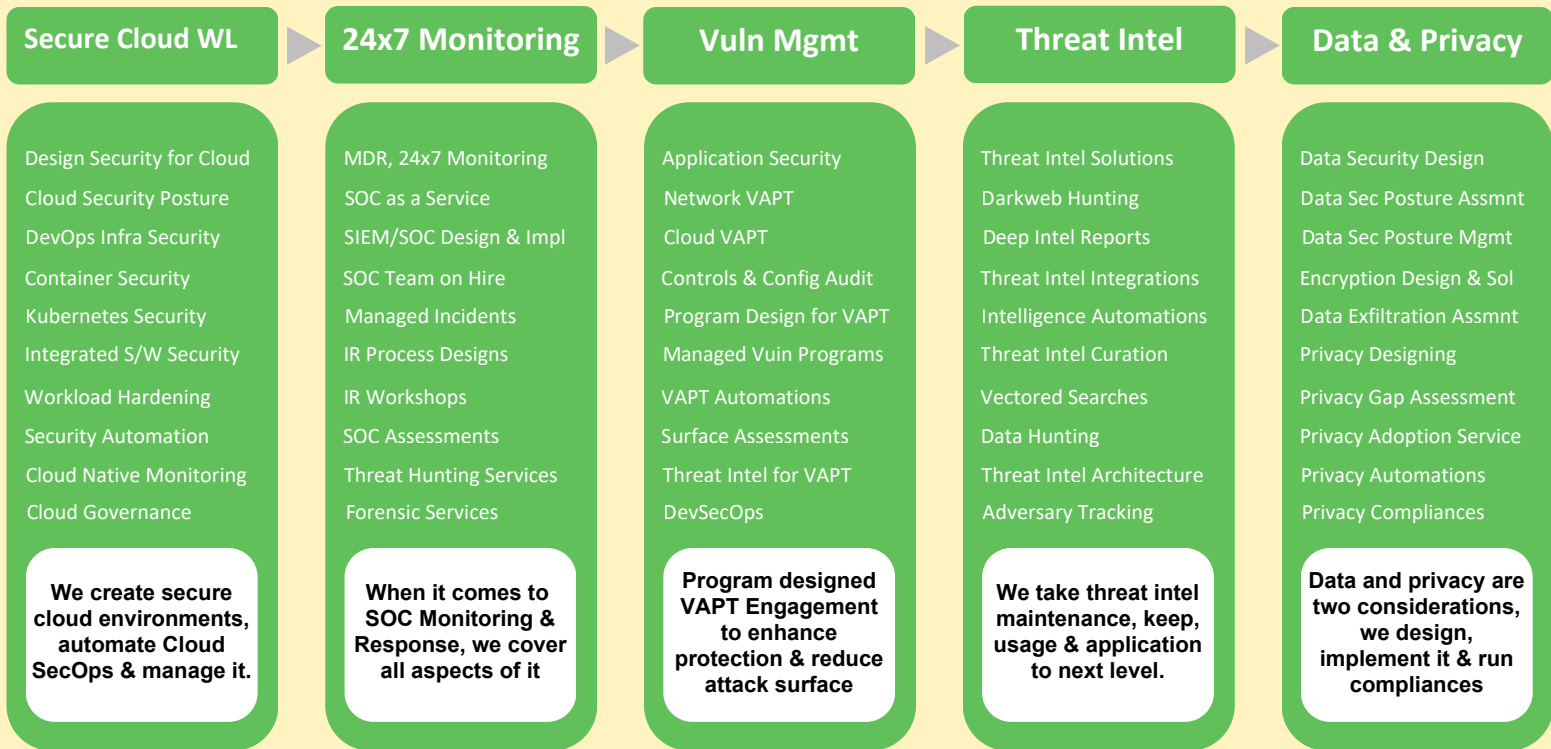
Strong handpicked team of (best of security talent globally)

Subscription & annual contract modeled services delivered globally

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio



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