CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 05 JULY – 11 JULY 2026

enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

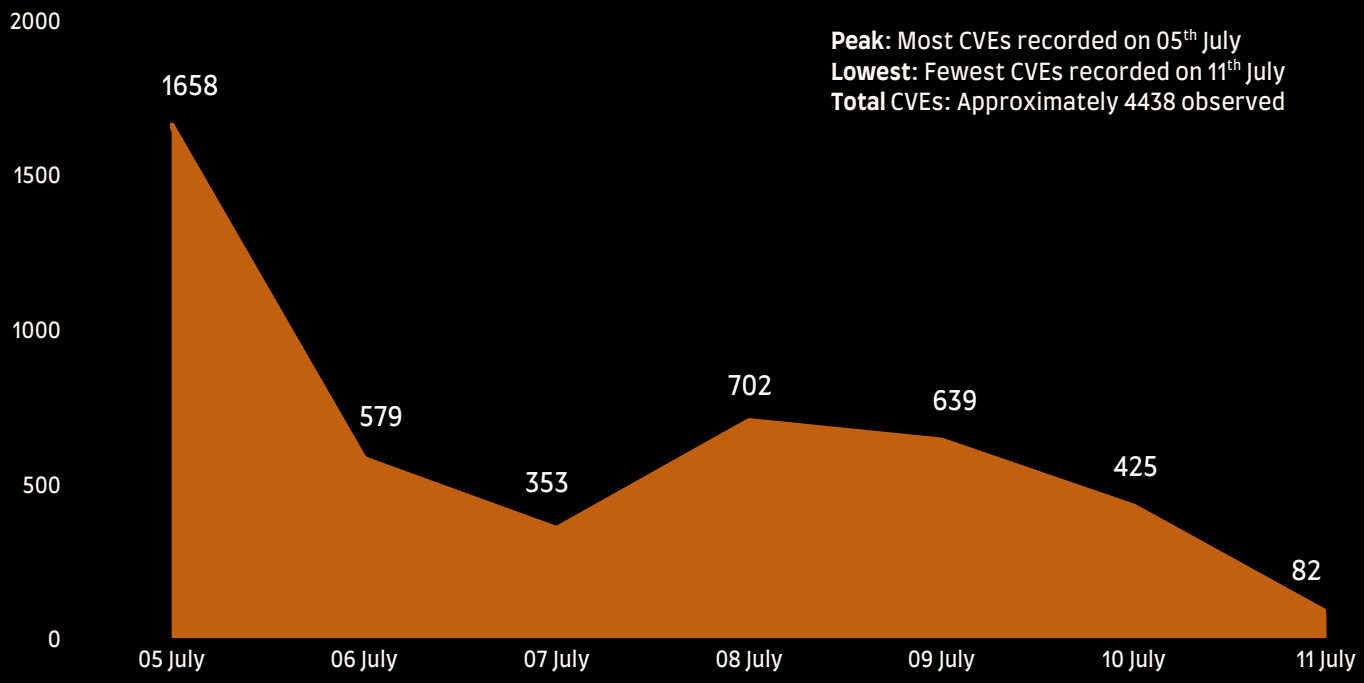
OSV

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Number of CVE this week



Top CVE this week

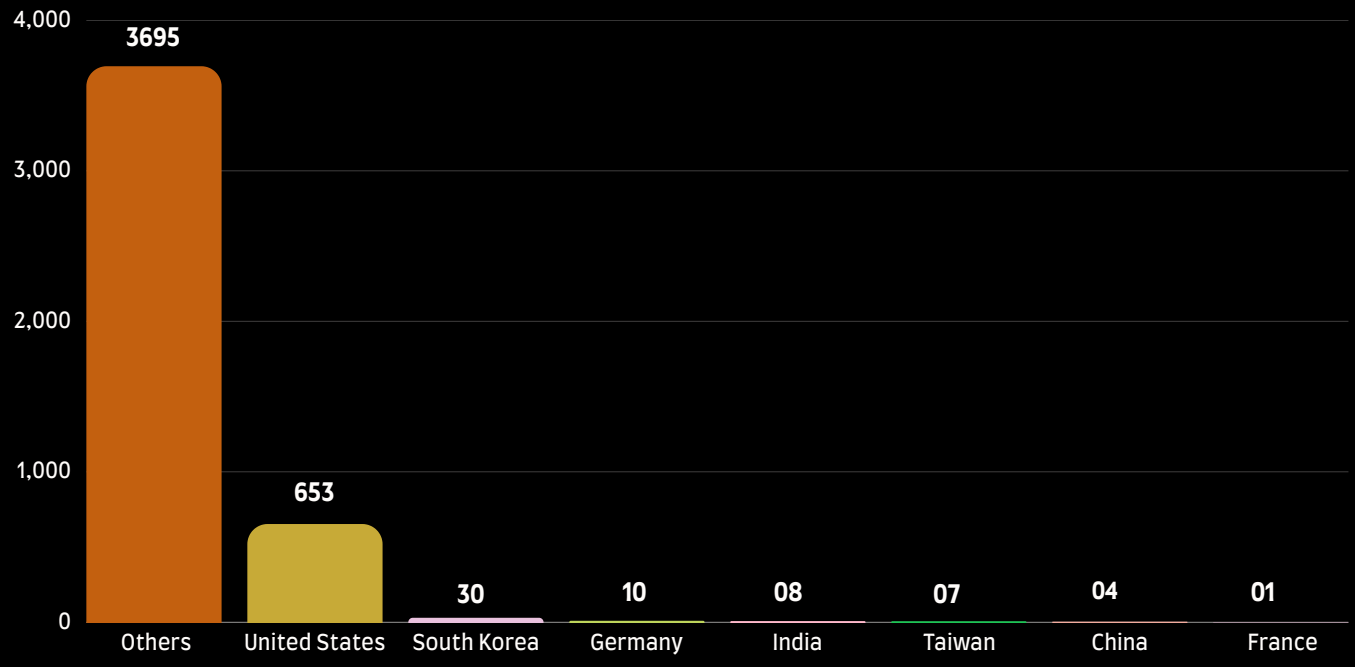
CVE ID	CVSS Score	Severity
CVE-2026-13768	10.0	Critical
CVE-2026-57572	10.0	Critical
CVE-2026-48282	10.0	Critical
CVE-2025-41115	10.0	Critical
CVE-2026-45480	10.0	Critical
CVE-2026-61447	10.0	Critical

KEY HIGHLIGHTS

This week's top five vulnerabilities reveal critical software and network weaknesses, with some already actively exploited, requiring urgent remediation.

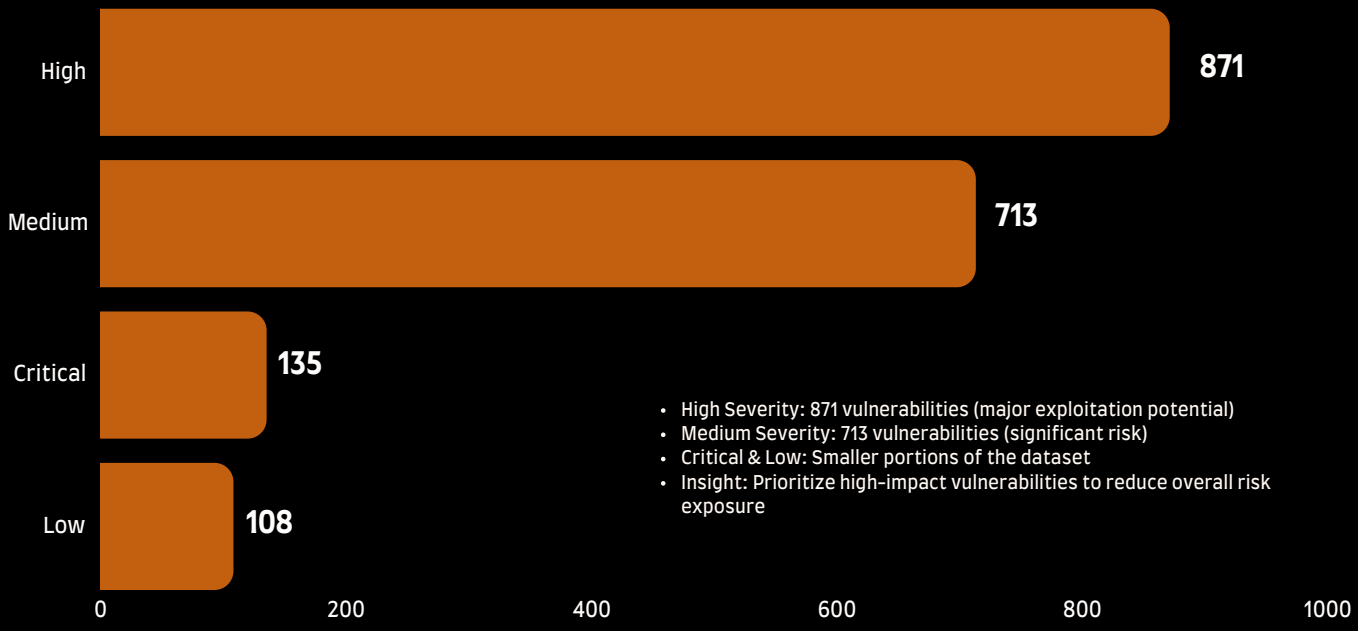
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

Top Affected Vendors



Analysis of CVE-affected vendors reveals that a majority fall under the “Others” category, suggesting a highly distributed global impact across multiple countries.

Severity Breakdown



- High Severity: 871 vulnerabilities (major exploitation potential)
- Medium Severity: 713 vulnerabilities (significant risk)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (51%) have fixes available, but 49% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-13768

Overview

A critical vulnerability has been identified in Gardyn Home Firmware, Gardyn Studio Firmware, and Gardyn Cloud API due to the use of hard-coded privileged credentials. An attacker who obtains the exposed iothubowner key can retrieve device connection information, execute arbitrary commands on connected Gardyn devices, and potentially pivot to other systems on the victim's network.

Technical Details

The vulnerability exists because Gardyn devices expose a privileged iothubowner key that is embedded within the affected products. An attacker with access to this key can invoke IoT Hub Registry Manager functions to obtain connection information for all Gardyn Home Kit and Studio devices. The exposed credentials also allow arbitrary command execution on a targeted connected device and may enable lateral movement to other devices on the user's network.

Vendor: **Gardyn**
Affected Product: **Gardyn Home Firmware, Gardyn Studio Firmware, Gardyn Cloud API**
Affected Versions: **Gardyn Home Firmware: Before master.627 , Gardyn Studio Firmware: Before master.627**

- **Published Date:** 02-07-2026
- **Last Patch:** 06-07-2026
- **Vulnerability Type:** Use of Hard-coded Credentials (CWE-798)
- **Fix Available:** Yes
- **Patched Version:** Gardyn Home Firmware: master.627, Gardyn Studio Firmware: master.627

Exploitaion Status

- Exploite Status : No Known Exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public Technical Advisory Available

Reference: https://www.cisa.gov/news-events/ics-advisories/icsa-26-183-03

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

CVE-2026-57572

Overview

A critical vulnerability has been identified in Crawl4AI that allows unauthenticated remote code execution through Chromium launch-argument injection. An attacker can supply malicious browser launch arguments to the Docker API, resulting in arbitrary command execution as the container's runtime user.

Technical Details

The vulnerability exists because the Crawl4AI Docker API server accepts user-controlled browser_config.extra_args values and passes them directly to Chromium's launch arguments without proper validation. By injecting malicious Chromium switches along with the --no-zygote option, an attacker can force Chromium to execute an attacker-controlled command. Since the Docker API is unauthenticated by default, a single crafted request can achieve arbitrary command execution as the container's runtime user.

Vendor: **unclecode**
Affected Product: **Crawl4AI**
Affected Versions: **Before 0.9.0**

- **Published Date:** 06-07-2026
- **Last Patch:** 06-07-2026
- **Vulnerability Type:** Argument Injection (CWE-88) / Code Injection (CWE-94)
- **Fix Available:** Yes
- **Patched Version:** 0.9.0

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public technical advisory and patch available

Reference: github.com: https://github.com/unclecode/crawl4ai/security/advisories/GHSA-r253-r9jw-qg44

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

CVE-2026-48282

Overview

A critical vulnerability has been identified in Adobe ColdFusion that allows arbitrary code execution through a Path Traversal vulnerability. An attacker can exploit improper pathname validation to access restricted files and execute arbitrary code in the context of the current user without requiring user interaction.

Technical Details

The vulnerability exists because Adobe ColdFusion improperly restricts file path handling, allowing directory traversal outside the intended directory structure. A remote attacker can craft malicious requests to access restricted resources and ultimately achieve arbitrary code execution with the privileges of the current user. Exploitation does not require user interaction and the vulnerability has a scope change, potentially impacting resources beyond the vulnerable component.

Affected Product: **Adobe ColdFusion**
Affected Versions: **2023.20 and earlier (including 2025.9)**
Vendor: **Adobe**

- **Published Date:** 30-06-2026
- **Last Patch:** 08-07-2026
- **Vulnerability Type :** Path Traversal (CWE-22) / Arbitrary Code Execution / Remote Code Execution (RCE)
- **Fix Available:** Yes
- **Patched Version:** Adobe ColdFusion 2023 Update 21 and 2025 Update 10

Exploitation Status

- Exploite Status : PoC Available
- Threat Actors / Malware: None reported
- Exploit Availability: Public vendor advisory available

Reference: https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html

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

CVE-2025-41115

Overview

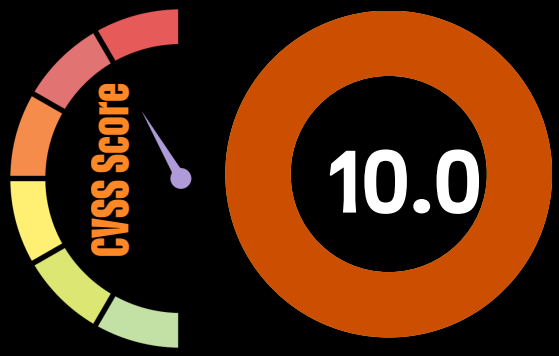
A critical vulnerability has been identified in Grafana Enterprise that allows privilege escalation through improper handling of SCIM user provisioning. A malicious or compromised SCIM client can manipulate user identity information to impersonate existing users and obtain elevated privileges.

Technical Details

The vulnerability exists because Grafana Enterprise improperly handles the externalId field during SCIM provisioning. A malicious or compromised SCIM client can provision a user with a numeric externalId, allowing internal user IDs to be overridden. This can result in user impersonation and privilege escalation. The vulnerability is exploitable only when SCIM provisioning is enabled with both the enableSCIM feature flag and the user_sync_enabled configuration option enabled.

Affected Product: **Grafana Enterprise**
Affected Versions: **12.0.0 before 12.2.1**
Vendor: **Grafana Labs**

- Published Date: **21-11-2025**
- Last Patch: **13-07-2026**
- Vulnerability Type: **Incorrect Privilege Assignment / Privilege Escalation / User Impersonation**
- Fix Available: **Yes**
- Patched Version: **12.2.1 or later**



Exploitation Status

- Exploite Status: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public technical advisory available

Reference: https://grafana.com/security/security-advisories/cve-2025-41115

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

CVE-2026-45480

Overview

A critical vulnerability has been identified in Microsoft Azure Active Directory (Azure AD) that allows privilege escalation due to improper authentication. An unauthenticated attacker could exploit this flaw over the network to gain elevated privileges within the Azure Active Directory service.

Technical Details

The vulnerability is caused by improper authentication within Azure Active Directory. An unauthorized attacker can exploit the authentication weakness over the network to elevate privileges without requiring user interaction. Since Azure Active Directory is a Microsoft-hosted cloud service, customers are not required to install updates, as remediation is handled by Microsoft.

Affected Product: **Microsoft Azure Active Directory**
Affected Versions: **Microsoft-managed cloud service**
Vendor: **Microsoft**

- **Published Date:** 19-06-2026
- **Last Patch:** 08-07-2026
- **Vulnerability Type:** Improper Authentication (CWE-287) / Elevation of Privilege
- **Fix Available:** Yes
- **Patched Version:** Not Applicable (service-side update by Microsoft)

Exploitation Status

- Exploite Status: No Known Exploited
- Threat Actors / Malware: None reported
- Exploit Availability: Technical advisories available

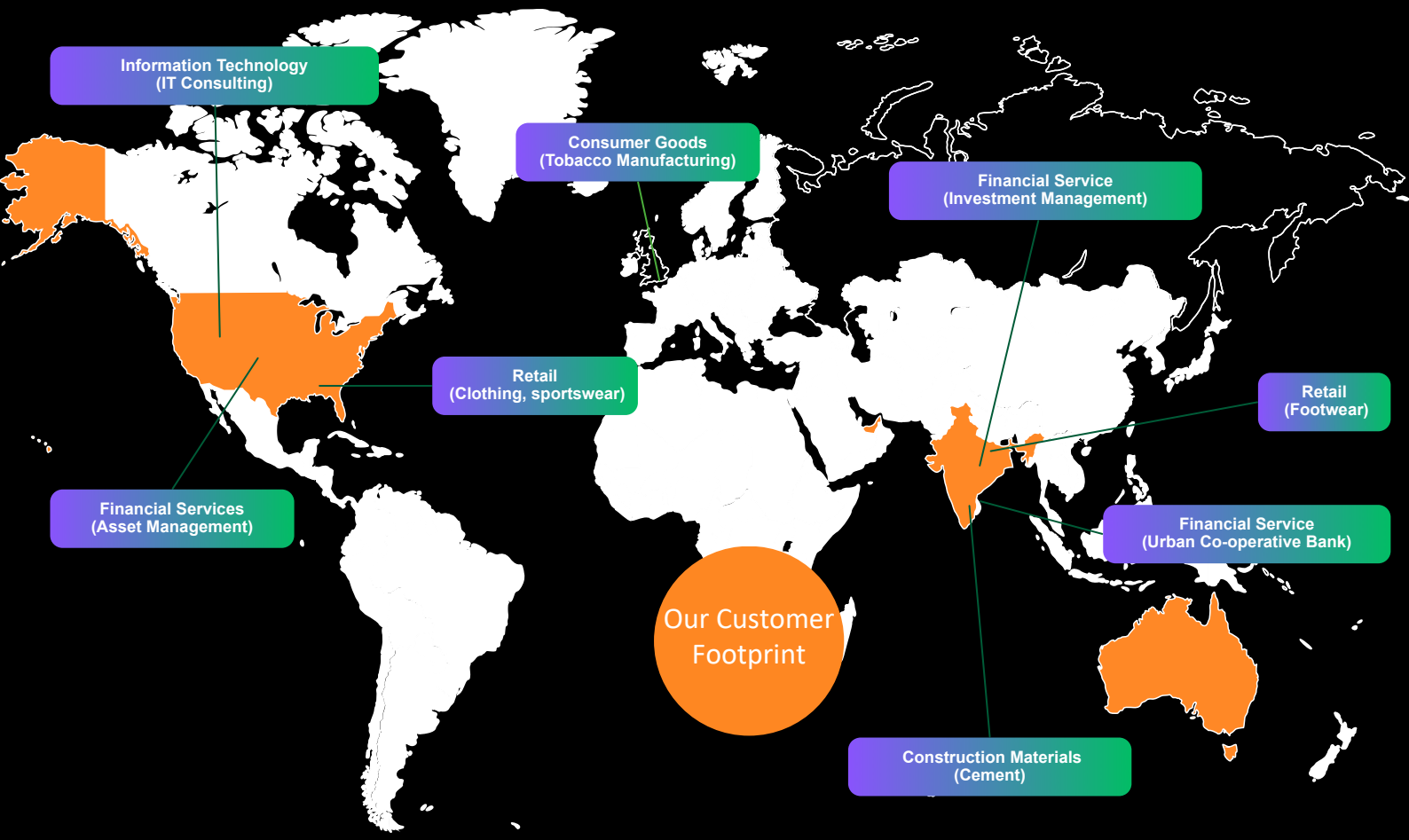
Reference: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45480

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

About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (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