CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 07 JUNE – 13 JUNE 2026

enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

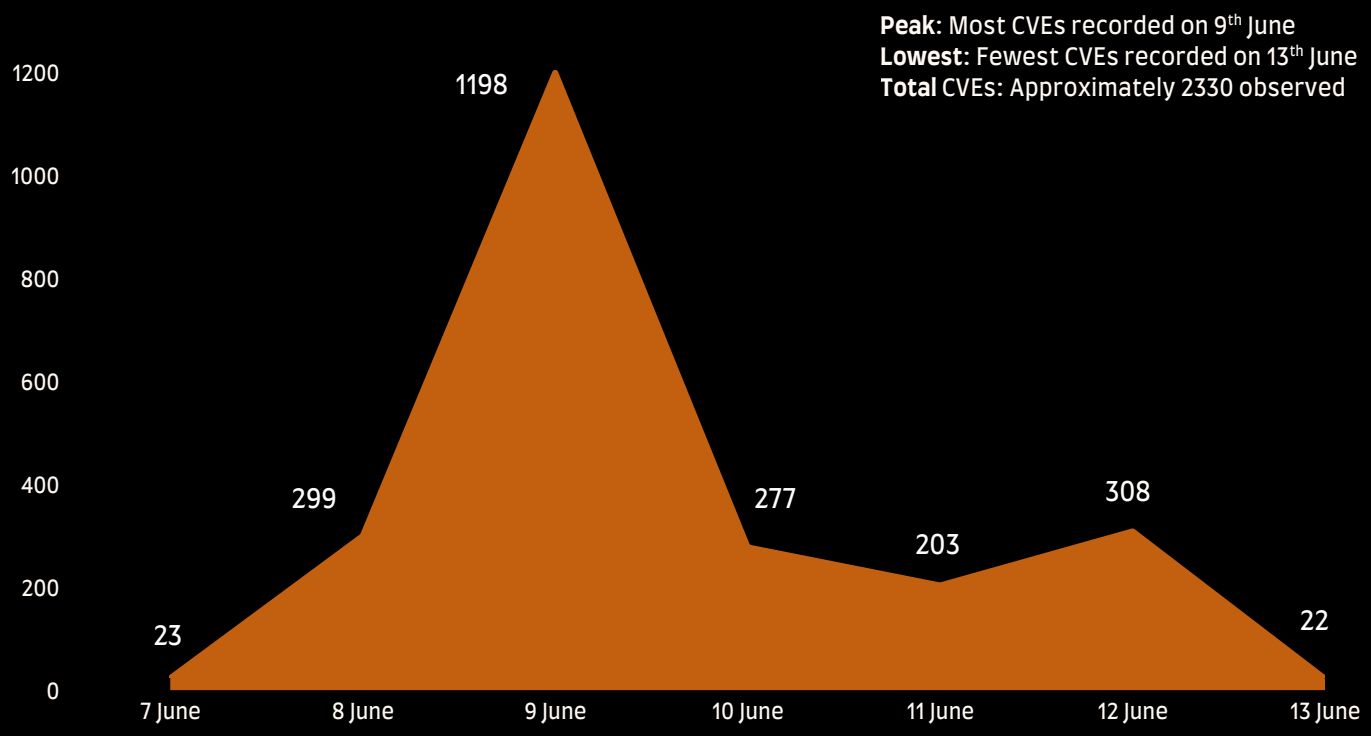
OSV

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

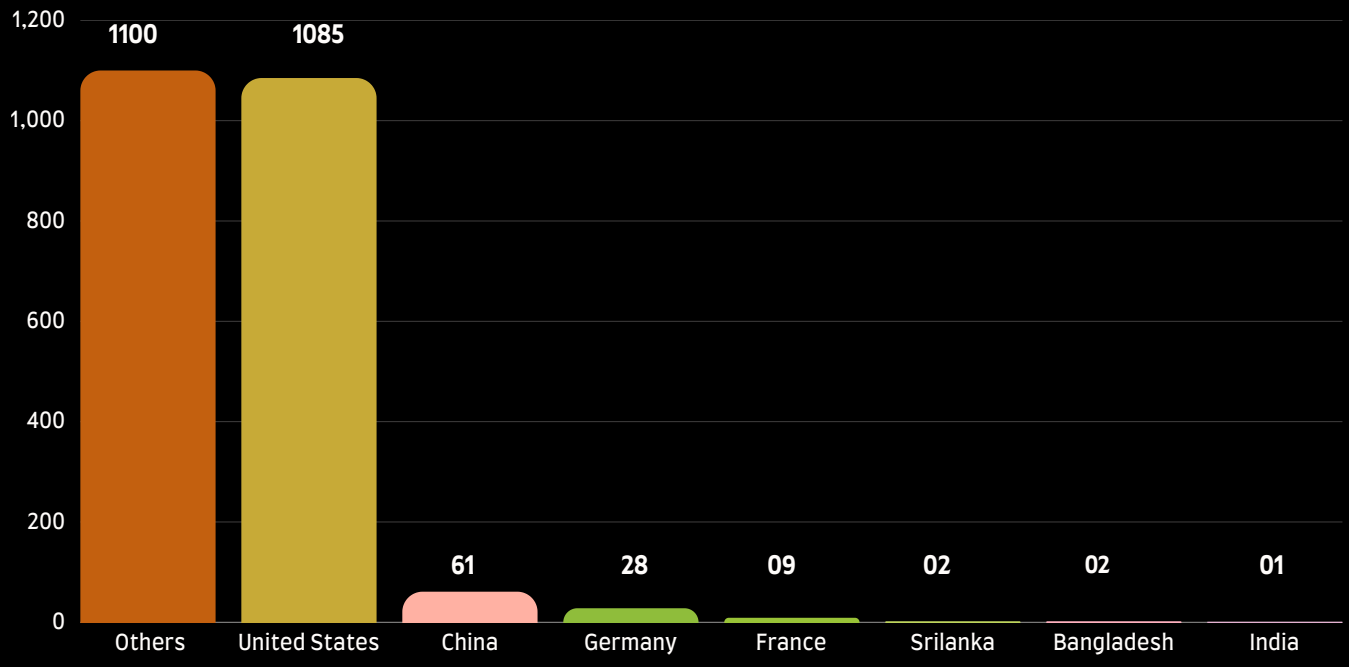
CVE ID	CVSS Score	Severity
CVE-2026-47938	10.0	Critical
CVE-2026-10520	10.0	Critical
CVE-2025-41115	10.0	Critical
CVE-2026-49261	10.0	Critical
CVE-2026-50086	10.0	Critical
CVE-2026-48558	10.0	Critical

KEY HIGHLIGHTS

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

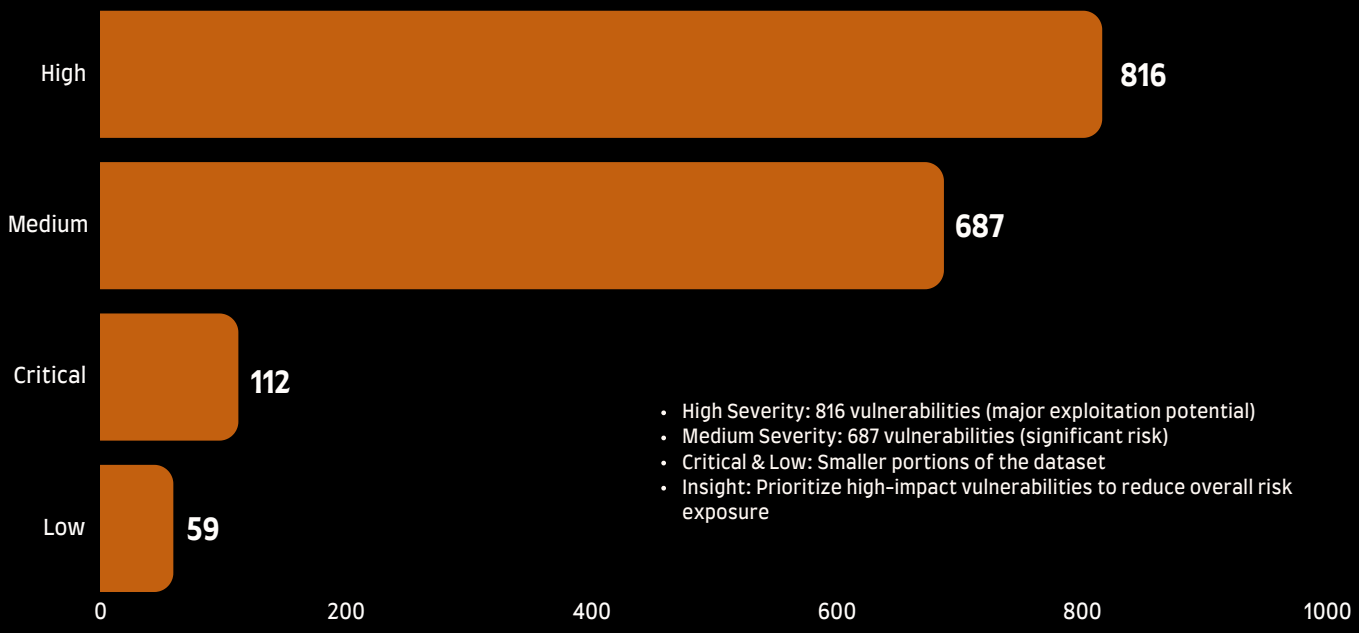
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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: 816 vulnerabilities (major exploitation potential)
- Medium Severity: 687 vulnerabilities (significant risk)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (88.8%) have fixes available, but 11.2% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-47938

Overview

A critical vulnerability has been identified in Adobe Campaign Classic that allows attackers to perform Server-Side Request Forgery (SSRF) attacks. Successful exploitation could lead to privilege escalation and compromise of affected systems without requiring user interaction.

Technical Details

The vulnerability is caused by improper handling of server-side requests, allowing attackers to force the application to send unauthorized requests to internal or external resources. A remote attacker can exploit this SSRF flaw to elevate privileges and potentially access sensitive services or data within the affected environment.

Vendor: **Adobe**
Affected Product: **Adobe Campaign Classic (ACC)**
Affected Versions: **Through 7.4.3 Build 9394**

- **Published Date:** 09-06-2026
- **Last Patch:** 09-06-2026
- **Vulnerability Type:** Server-Side Request Forgery (SSRF) / Privilege Escalation
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitaion Status

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

Reference: https://helpx.adobe.com/security/products/campaign/apsb26-66.html

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

CVE-2026-10520

Overview

A critical vulnerability has been identified in Ivanti Sentry that allows unauthenticated remote attackers to execute arbitrary operating system commands. Successful exploitation can result in root-level remote code execution, giving attackers complete control over the affected system.

Technical Details

The vulnerability is caused by improper neutralization of special characters in operating system commands, leading to an OS Command Injection flaw. A remote unauthenticated attacker can exploit this issue to execute arbitrary commands with root privileges on the underlying operating system.

Vendor: **Ivanti**
Affected Product: **Ivanti Sentry**
Affected Versions: **Before R10.5.2, R10.6.2, and R10.7.1**

- **Published Date:** 09-06-2026
- **Last Patch:** 09-06-2026
- **Vulnerability Type:** OS Command Injection / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** R10.5.2, R10.6.2, R10.7.1

Exploitation Status

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

Reference: https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US

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

CVE-2025-41115

Overview

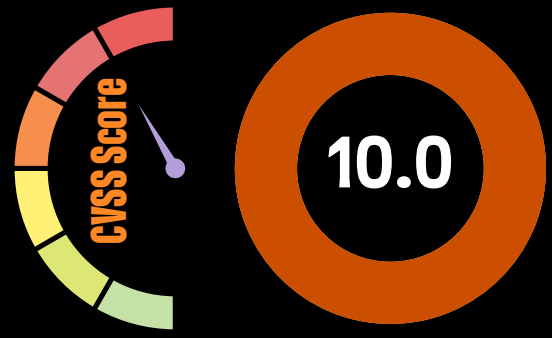
A critical vulnerability has been identified in Grafana Enterprise that could allow user impersonation and privilege escalation through improper handling of SCIM-provisioned user identities. A malicious or compromised SCIM client can manipulate the externalId field to override internal user IDs when SCIM provisioning is enabled.

Technical Details

The vulnerability exists in Grafana's SCIM provisioning feature, where numeric externalId values can conflict with internal user identifiers. A malicious SCIM client may exploit this behavior to impersonate other users or gain elevated privileges within affected Grafana deployments.

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

- **Published Date:** 21-11-2025
- **Last Patch:** 12-06-2026
- **Vulnerability Type:** Incorrect Privilege Assignment / Privilege Escalation
- **Fix Available:** Yes
- **Patched Version:** 12.2.1



Exploitation Status

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

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

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

CVE-2026-49261

Overview

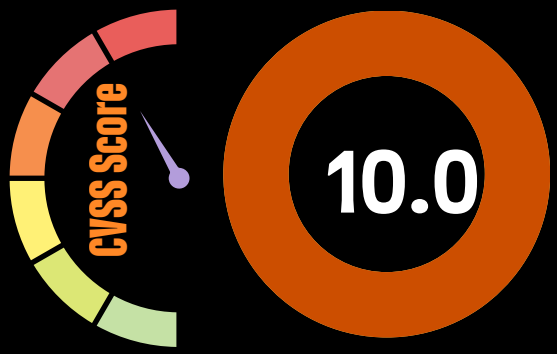
A critical vulnerability has been identified in MariaDB Server that allows execution of shell commands through unsafe handling of the wsrep_notify_cmd parameter. An attacker can exploit the flaw by embedding malicious commands in the name of a Galera cluster joiner node, potentially leading to remote code execution.

Technical Details

The vulnerability is caused by improper neutralization of special characters in the wsrep_notify_cmd functionality when processing joiner node names. If wsrep_notify_cmd is enabled, crafted node names can inject shell commands that are executed by the server, resulting in OS command execution.

Affected Product: **MariaDB Server**
Affected Versions: **10.6.1 to 10.6.26 , 10.11.1 to 10.11.17, 11.4.1 to 11.4.11, 11.8.1 to 11.8.7, 12.3.1**
Vendor: **MariaDB**

- **Published Date:** 11-06-2026
- **Last Patch:** 11-06-2026
- **Vulnerability Type:** OS Command Injection / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 10.6.27, 10.11.18, 11.4.12, 11.8.8, 12.3.2



Exploitation Status

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

Reference: github.com: https://github.com/MariaDB/server/security/advisories/GHSA-3p3m-4x7c-p4pw

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

CVE-2026-50086

Overview

A critical vulnerability has been identified in Aqara IAM/SSO Gateway that exposes cryptographic operations without authentication. An attacker can interact with AES encryption and decryption functions tied to the platform's signing key, potentially compromising sensitive authentication mechanisms.

Technical Details

The vulnerability exists because the Aqara IAM/SSO gateway exposes bidirectional AES encryption and decryption operations without requiring authentication. An attacker can abuse this AES oracle functionality to perform cryptographic attacks against the platform's signing key and authentication infrastructure.

Affected Product: **Aqara IAM/SSO Gateway**
Affected Versions: **Affected from 2026-04-20 before 0**
Vendor: **Aqara**

- **Published Date:** 12-06-2026
- **Last Patch:** 12-06-2026
- **Vulnerability Type:** Missing Authentication for Critical Function / Use of a Broken or Risky Cryptographic Algorithm
- **Fix Available:** Not Available
- **Patched Version:** Not Available

Exploitation Status

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

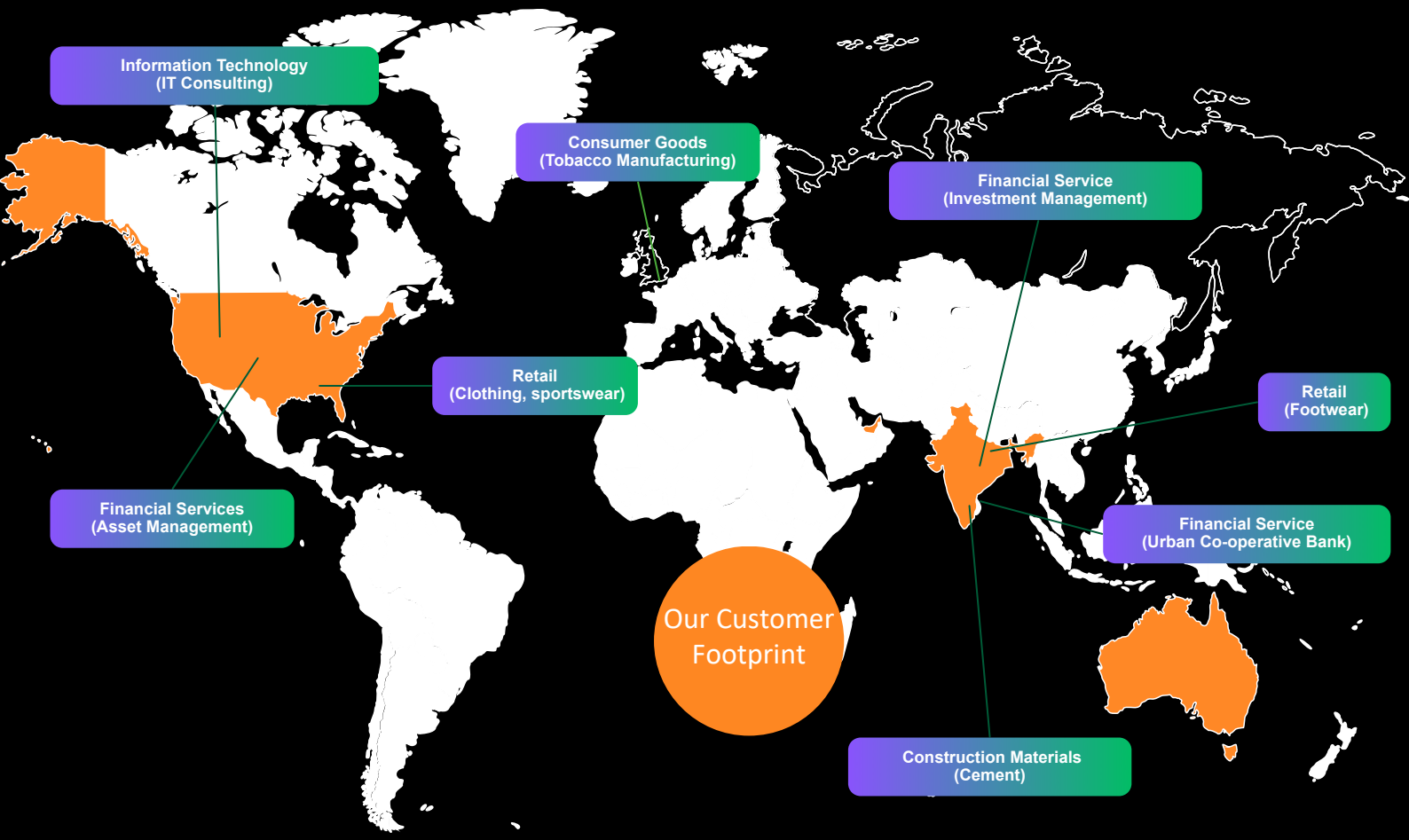
Reference: https://github.com/xn0tsa/theres-no-place-like-home

+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