CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 14 JUNE – 20 JUNE 2026

enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

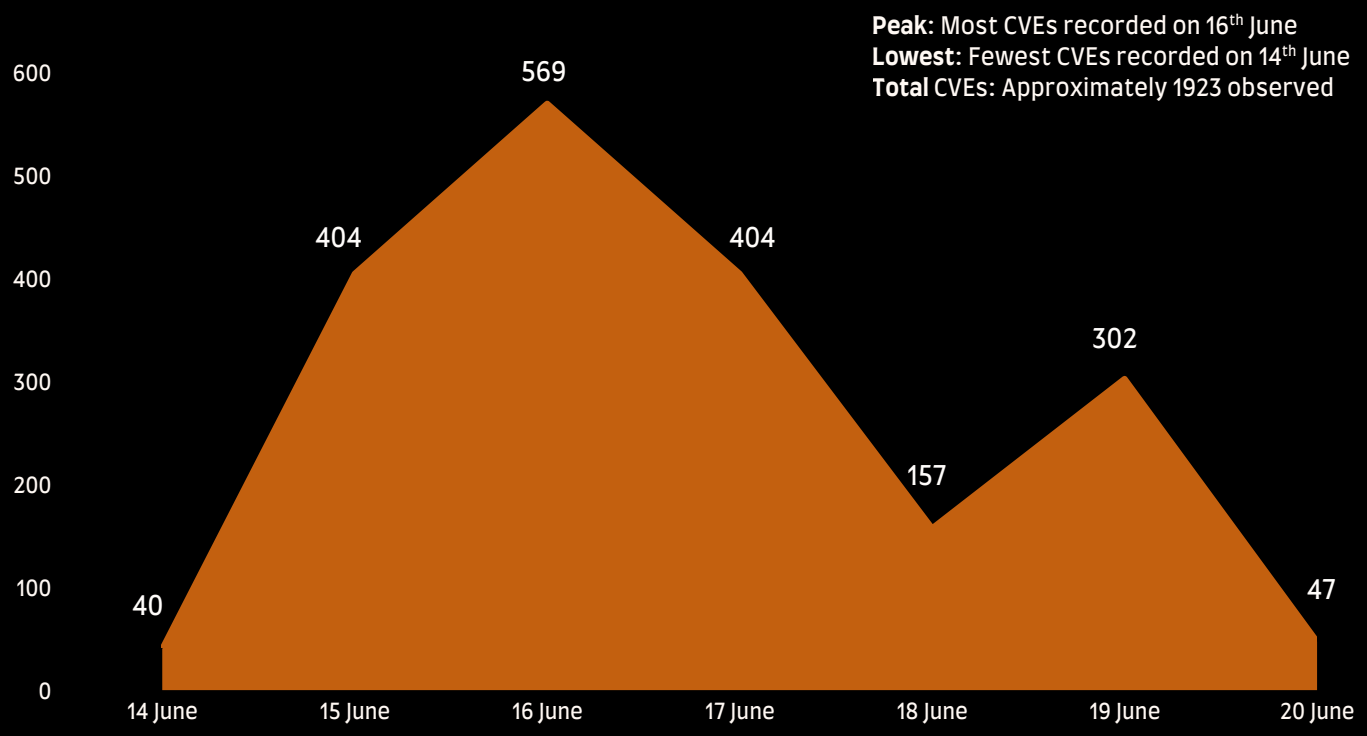
OSV

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

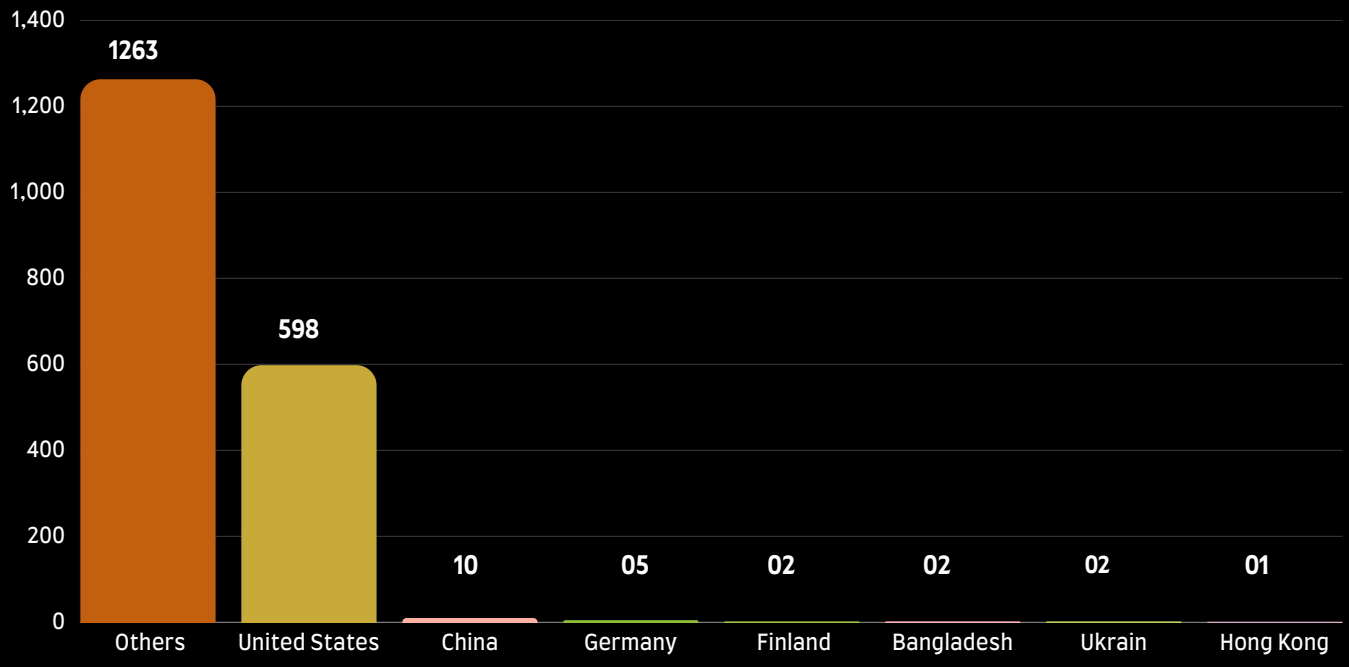
CVE ID	CVSS Score	Severity
CVE-2026-20127	10.0	Critical
CVE-2026-35292	10.0	Critical
CVE-2026-32169	10.0	Critical
CVE-2026-50242	10.0	Critical
CVE-2026-3490	10.0	Critical
CVE-2025-69129	10.0	Critical

KEY HIGHLIGHTS

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

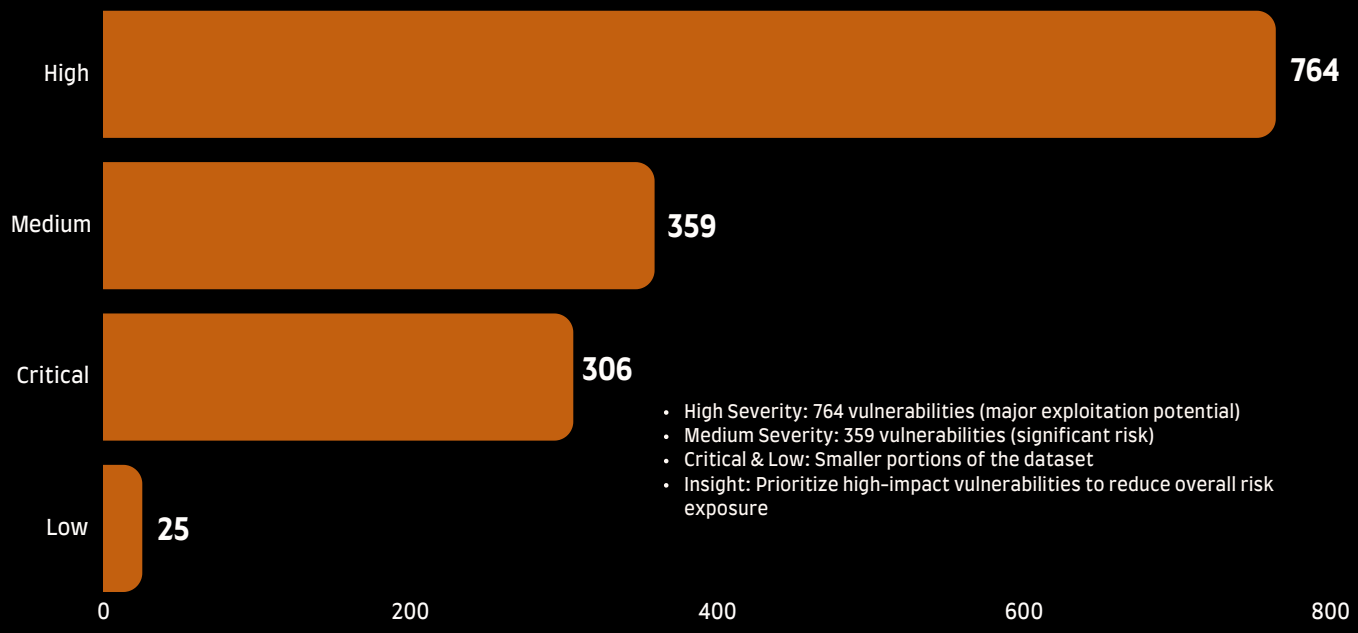
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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: 764 vulnerabilities (major exploitation potential)
- Medium Severity: 359 vulnerabilities (significant risk)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (75.9%) have fixes available, but 24.1% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-20127

Overview

A critical authentication bypass vulnerability has been identified in Cisco Catalyst SD-WAN Controller components. The flaw allows an unauthenticated remote attacker to bypass the peering authentication mechanism and gain administrative privileges on affected systems, potentially leading to unauthorized network configuration changes across the SD-WAN fabric.

Technical Details

The vulnerability exists because the peering authentication mechanism used by Cisco Catalyst SD-WAN components does not properly validate authentication during control-plane communications. An attacker can send specially crafted requests to bypass authentication controls and obtain access as an internal high-privileged user account. Successful exploitation enables access to NETCONF services, allowing manipulation of SD-WAN network configurations.

Vendor: **Cisco**
Affected Product: **Cisco Catalyst SD-WAN Manager**, **Cisco Catalyst SD-WAN Controller (vSmart)**
Affected Versions: **Multiple versions across releases 17.x, 18.x, 19.x, and 20.x**

- **Published Date:** 25-02-2026
- **Last Patch:** 16-06-2026
- **Vulnerability Type:** Authentication Bypass (CWE-287: Improper Authentication)
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitaion Status

- Exploite Status : Exploited In The Wild
- Threat Actors / Malware: None reported
- Exploit Availability: Active exploitation observed in the wild

Reference:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

CVE-2026-35292

Overview

A critical vulnerability has been identified in Oracle WebLogic Server that could allow an unauthenticated remote attacker to completely compromise affected servers. Successful exploitation can result in full takeover of the WebLogic Server instance and may impact additional connected products due to scope change.

Technical Details

The vulnerability affects the Console component of Oracle WebLogic Server. An unauthenticated attacker with network access via HTTP can exploit the flaw to compromise the server without requiring any user interaction or prior authentication. Successful exploitation may lead to complete system takeover, impacting the confidentiality, integrity, and availability of the affected environment.

Vendor: **Oracle Corporation**
Affected Product: **Oracle WebLogic Server**
Affected Versions: **14.1.2.0.0, 15.1.1.0.0**

- **Published Date:** 16-06-2026
- **Last Patch:** 16-06-2026
- **Vulnerability Type:** Unknown / Not Specified by Vendor
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitation Status

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

Reference: https://www.oracle.com/security-alerts/cspujun2026.html

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

CVE-2026-32169

Overview

A critical vulnerability has been identified in Microsoft Azure Cloud Shell that allows privilege escalation through a Server-Side Request Forgery (SSRF) flaw. An unauthenticated attacker may exploit the vulnerability over a network to gain elevated privileges within the affected cloud service environment.

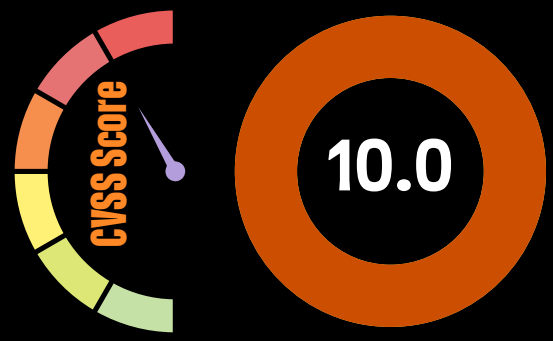
Technical Details

The vulnerability is caused by a Server-Side Request Forgery (SSRF) weakness in Azure Cloud Shell. By exploiting the SSRF condition, an attacker can induce the service to make unintended requests on their behalf, potentially leading to privilege escalation and unauthorized access to sensitive cloud resources.

Microsoft

Affected Product: **Azure Cloud Shell**
Affected Versions: **Cloud Service (Version Information Not Specified)**
Vendor: **Microsoft**

- **Published Date:** 19-03-2026
- **Last Patch:** 19-06-2026
- **Vulnerability Type:** Server-Side Request Forgery (SSRF) / Elevation of Privilege
- **Fix Available:** Yes
- **Patched Version:** Not Available



Exploitation Status

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

Reference: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32169

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

CVE-2026-50242

Overview

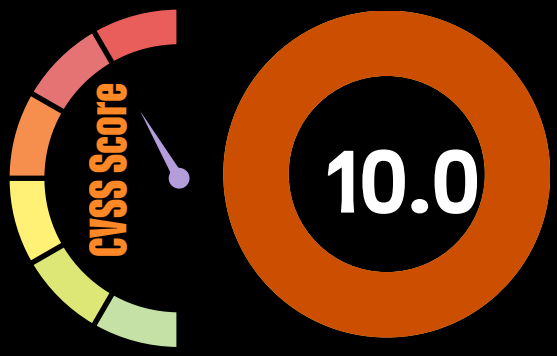
A critical authentication bypass vulnerability has been identified in JetBrains Hub that could allow an attacker to gain administrative access to the affected system. The flaw may enable unauthorized access through direct database interaction, potentially leading to full administrative control.

Technical Details

The vulnerability stems from improper authentication controls that allow authentication bypass through direct database access. An attacker who can exploit this weakness may bypass normal authentication mechanisms and obtain administrative privileges within the JetBrains Hub environment.

Affected Product: **JetBrains Hub**
Affected Versions: **Before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120,**
Vendor: **JetBrains**

- **Published Date:** 19-06-2026
- **Last Patch:** 19-06-2026
- **Vulnerability Type:** Missing Authentication for Critical Function (CWE-306) / Authentication Bypass
- **Fix Available:** Yes
- **Patched Version:** 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, and 2024.2.148429 or later



Exploitation Status

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

Reference: https://www.jetbrains.com/privacy-security/issues-fixed/

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

CVE-2026-3490

Overview

A critical vulnerability has been identified in picklescan that allows attackers to bypass the application's security blocklist and execute arbitrary code. By abusing the pkgutil.resolve_name function, an attacker can indirectly invoke dangerous functions that are intended to be blocked, potentially leading to full system compromise.

Technical Details

The vulnerability exists because picklescan fails to block the pkgutil.resolve_name function. An attacker can leverage indirect REDUCE calls to resolve and execute dangerous functions that would normally be restricted by the blocklist, such as system command execution or code execution functions. This effectively bypasses the entire security mechanism and can result in remote code execution.

Picklescan

Affected Product: **picklescan**
Affected Versions: **Before 1.0.4**
Vendor: **picklescan**

- **Published Date:** 17-06-2026
- **Last Patch:** 17-06-2026
- **Vulnerability Type:** Permissive List of Allowed Inputs (CWE-183) / Remote Code Execution (RCE)
- **Fix Available:** Yes
- **Patched Version:** 1.0.4

Exploitation Status

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

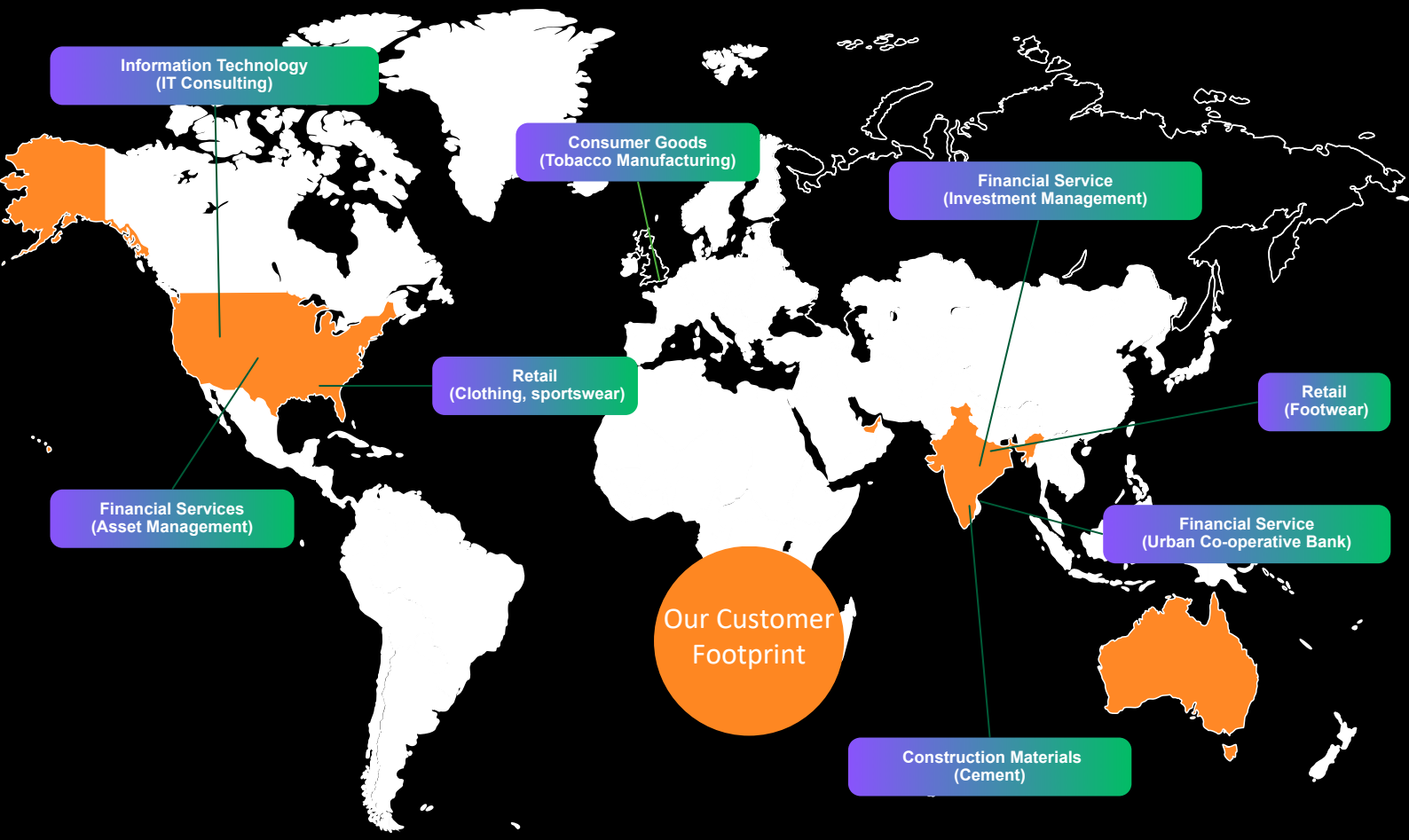
Reference: https://github.com/mmaitre314/picklescan/security/advisories/GHSA-vvpj-8cmc-gx39

+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