Castellum labs

Threat Advisory Report

#OpsShadowStrike

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

Executive Summary

- This document details about the OpsShadowStrike, a Hacktivist group which is actively involved in website defacing campaigns.

- OpsShadowStrike is a Hacktivist group which was formed on March 18, 2026. Over the time, they have built a reputation known for defacing websites with their slogans, DDoS Attacks & Data leaks.

Profile Summary ↘️

Name	OpsShadowStrike
Aliases:	NA
Motivation	Political
Infrastructure used	Biteblob.com (For hosting data leaks)
Associated Groups	NoHeartz, MalaysiaHacktivist, EagleCyberCrew, CyberActivistMalaysia, TheSweetNight
Campaigns	Eid Cyber Campaign
Last seen	April 28, 2026
Targeted Sectors	Educational Institution, Construction, Computer Games, Government, Transport, Agriculture & Food production, Energy, Political Parties
Targeted Countries	India, Israel, Ukraine, Vietnam, Australia, Bahrain, UAE, USA, UK
Attack Type	DDoS, Data leak
Exploited CVEs	CVE-2017-7921, CVE-2025-2945

Recent Activity Timeline:

APR 29, 2026

Data leak of Income Tax, Govt of India

- KYC (Know Your Customer) data of Income Tax, Government of India data was allegedly leaked by OpsShadowStrike in partnership with NoHeartz.
- The leaked data includes signatures, payslips, aadhaar card photos, etc.

APR 23, 2026

Hacking of SCADA System of Israel Water Management Company

- Modbus Protocol, HMI, SCADA Protocol of an Israeli Water Management Company called BERMAD CS Ltd, has been hacked in partnership with TheSweetNight.
- They have gained access to the panel where they can increase/decrease temperature control the flow of water, etc.

APR 13, 2026

DDoSing websites & Deface Campaigns

- Over this week, OpsShadowStrike, attacked a wide range of companies across different sectors & countries.
- The type of attack carried out was defacing websites & DDoS attacks and posting them on the Telegram Channel.

APR 12, 2026

Data breach of Lucrative Exim Consultants

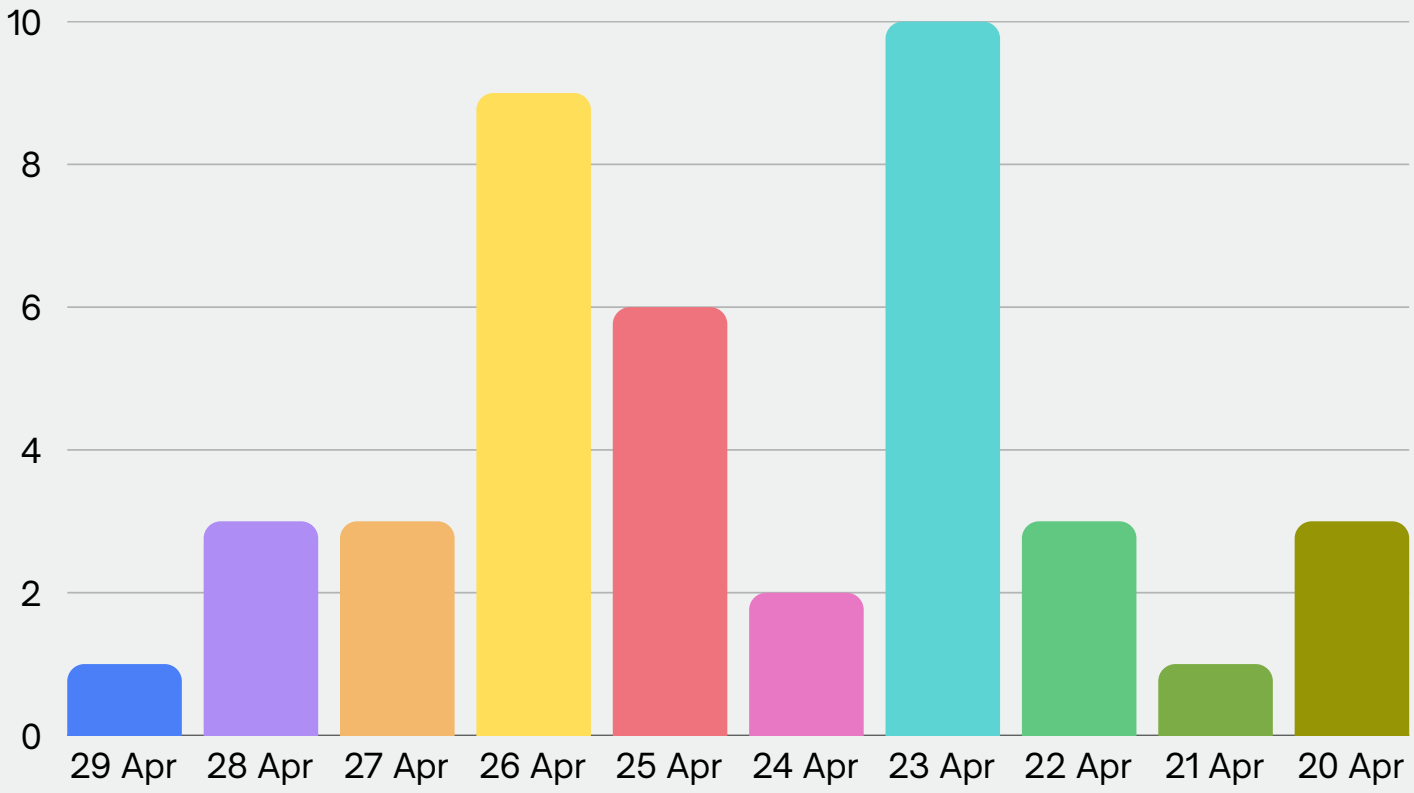
- Lucrative Exim Consultants, a outsourcing service company in India data was allegedly breached.
- The breached data includes 2GB+ Database, Postgresql admin access, complete source code, etc.

APR 6, 2026

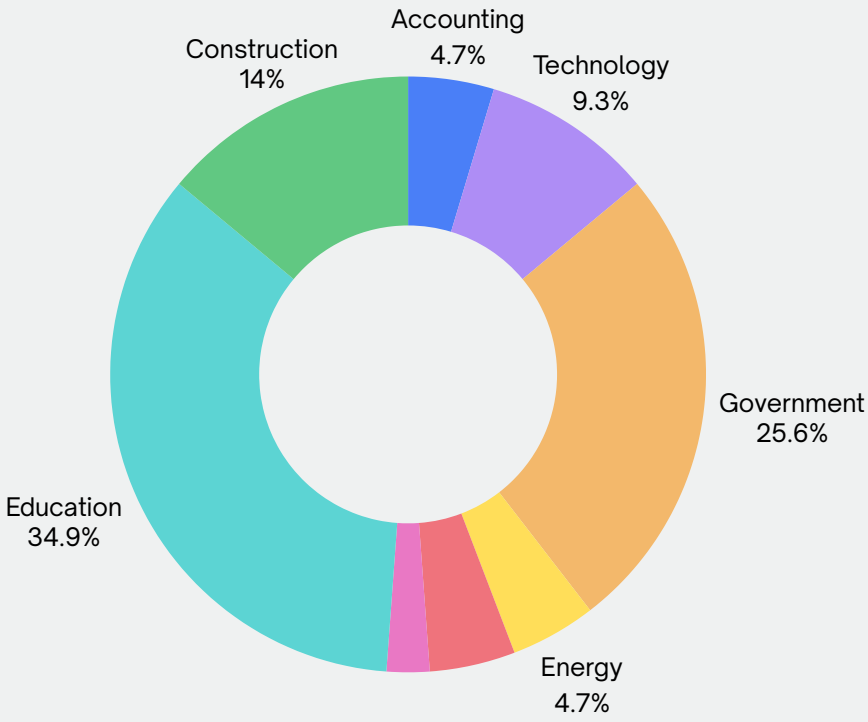
DDoSing websites & Deface Campaigns

- Over this week, OpsShadowStrike, attacked a wide range of companies across different sectors & countries.
- The type of attack carried out was defacing websites & DDoS attacks and posting them on the Telegram Channel.

OpsShadowStrike activity over the time



Sectors Targeted by OpsShadowStrike by Count

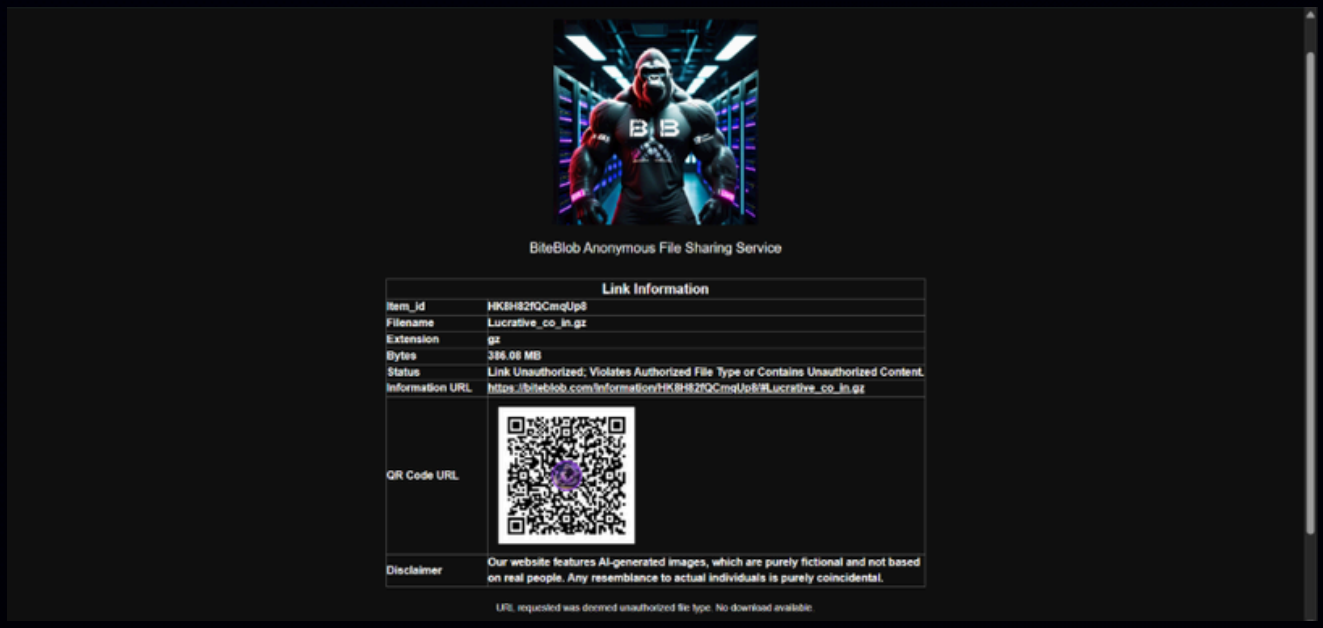


Countries Targeted by OpsShadowStrike

Notable Events

Summary

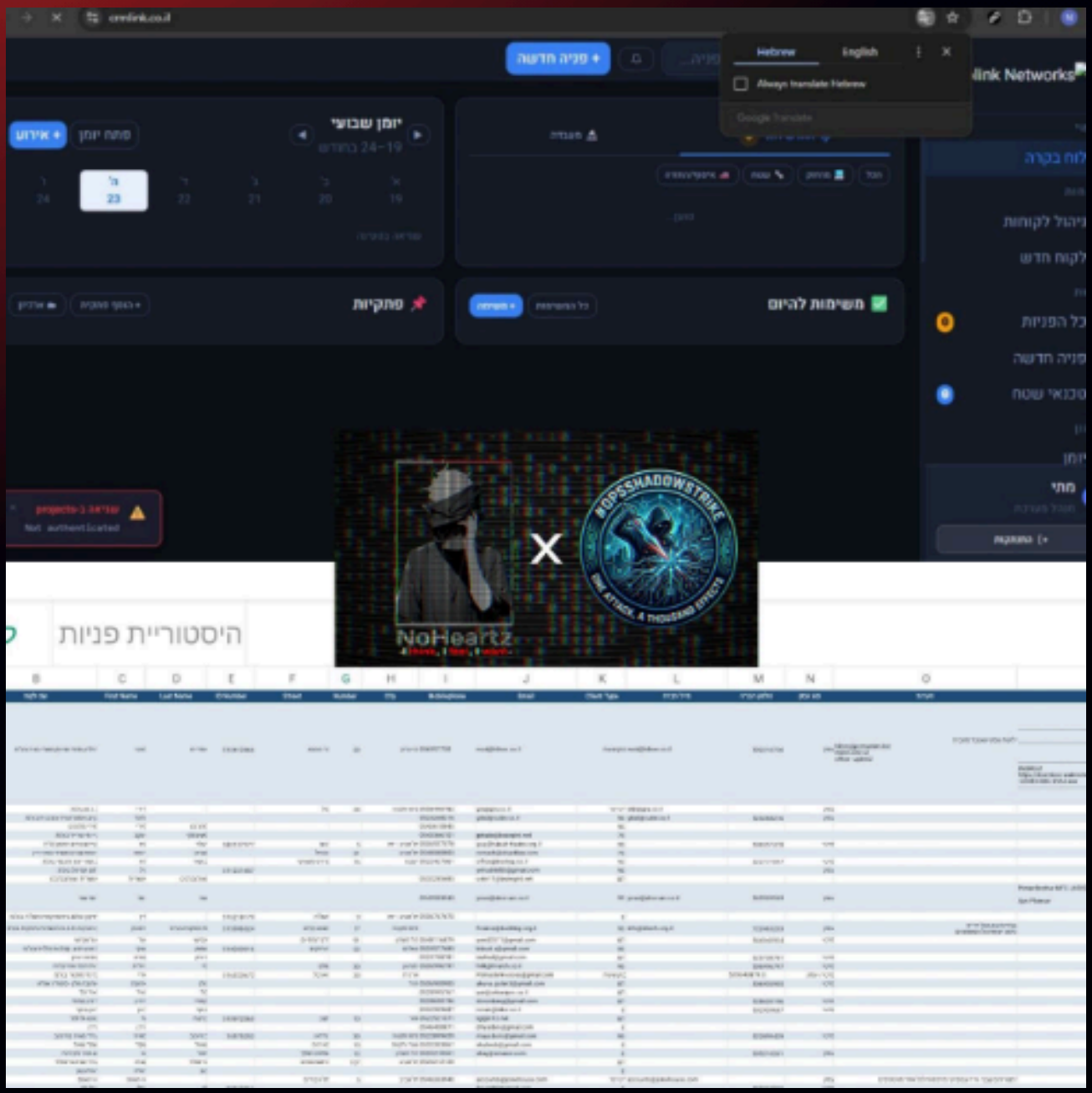
On April 12,2026 an Indian company called Lucrative Exim Consultants have been breached by OpsShadowStrike. It's an outsourcing services company. They have claimed to breached about 2GB+ Database, Source code. They've exploited the CVE-2025-2945 (RCE security vulnerability in pgAdmin 4) to carry out the attack.



Notable Events

On April 23,2026 an Israeli based Customer Relationship Management company was attacked by OpsShadowStrike in partnership with NoHeartz. The exposed admin panel suggests that the attackers may have gained privileged access to internal management systems, potentially increasing the risk of unauthorized data access or system manipulation. As of now, the exact scope of the intrusion and the size of any potentially compromised data remain unknown.

Link: https://crmlink.co.il/

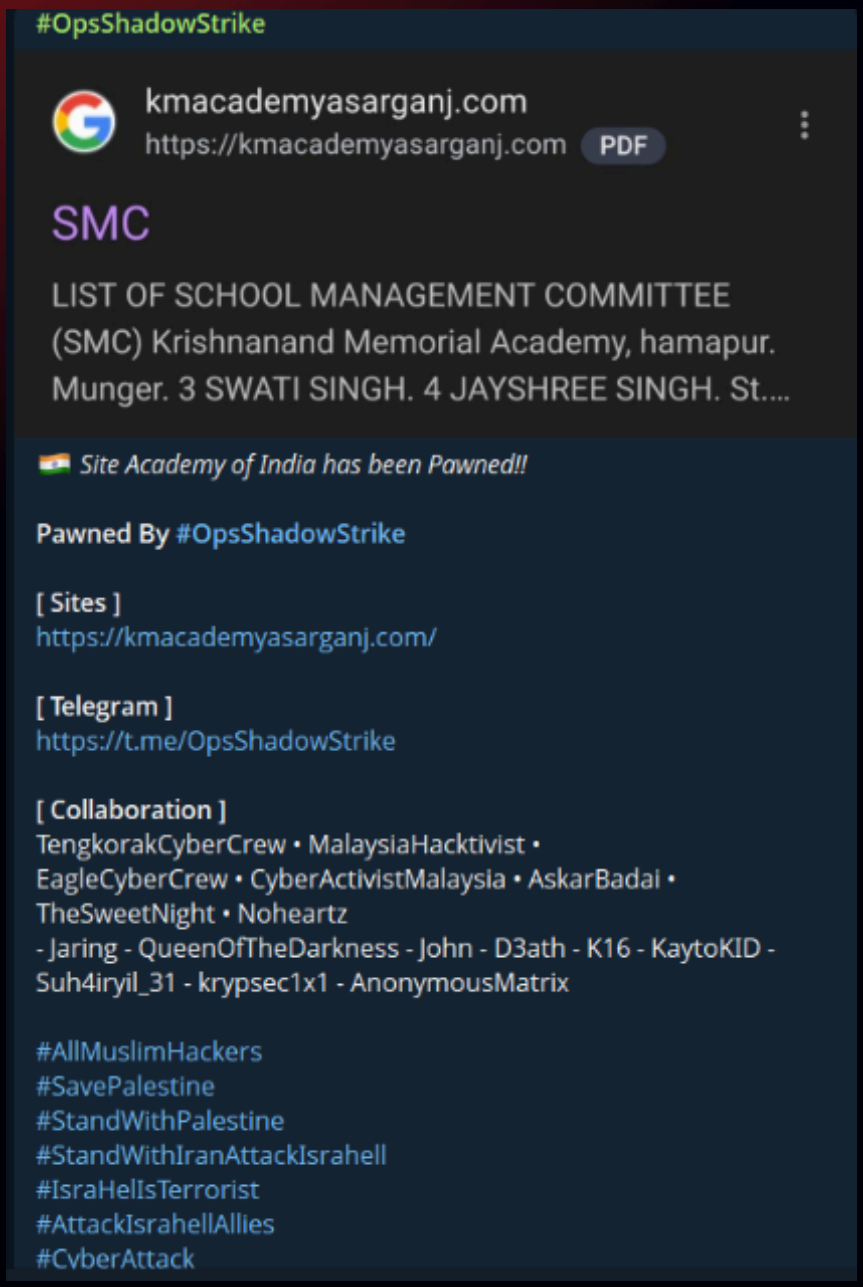


Notable Events

Summary

On April 20, 2026, an Indian school was defaced by OpsShadowStrike and posted on their telegram Channel. No data leak has been claimed by them. The attackers altered the website's content, indicating unauthorized access to the web platform and potential weaknesses in the site's security posture. At the time of reporting, no claims of data exfiltration or leakage had been made by the threat actors. The incident appears to be limited to website defacement, which is often used by attackers to demonstrate access, spread messaging, or establish notoriety. However, a deeper forensic investigation would be required to determine whether any backend systems or sensitive information were accessed during the intrusion.

Website: https://kmacademyasarganj.com/



Indicators of Compromise (IOCs):

TYPE	IOC Value	Description
URL	https://t.me/OpsShadowStrike	Primary Communication Channel
URL	https://t.me/+yVEtHRzCY_szZmVl	Communication channel about DDoS Attacks

External References:

- https://socradar.io/blog/telegram-activity-timeline-iran-israel-us-war/
- https://x.com/DailyDarkWeb/status/2034610317695549887

Abbreviations:

Abbreviation Name	Full form
DDOS	Distributed Denial of Service Attack
RCE	Remote Code Execution

RECOMMENDATIONS

1. ENFORCE STRONG AUTHENTICATION

Weak or reused credentials remain one of the most common initial access vectors in website compromises and defacement campaigns. Threat actors frequently rely on credential stuffing, password spraying, and brute-force attacks to gain administrative access. Organizations should enforce strong authentication hygiene across all privileged accounts.

USE:

- Minimum 14–16 character passwords to increase resistance against brute-force attacks
- Unique passwords for every administrative account to prevent lateral compromise
- Enterprise-approved password managers to securely generate and store credentials
- Immediate removal or disabling of default credentials such as admin/admin or root/root

BEST PRACTICE:

Password rotation for privileged accounts should be risk-based rather than periodic. Rotation should be enforced immediately upon suspected compromise, privilege changes, or employee offboarding.

2. ENABLE MFA EVERYWHERE

Multi-factor authentication (MFA) significantly reduces the risk of unauthorized access, even if credentials are exposed through phishing, credential leaks, or brute-force attacks. Critical administrative interfaces should require MFA as a mandatory control layer.

Protect:

- CMS administrative panels
- Hosting control panels (cPanel, Plesk)
- SSH administrative access
- VPN gateways
- Cloud management dashboards

MFA serves as a strong mitigation against password-only compromise attempts.

Recommended methods:

- Authenticator applications (TOTP-based)
- Hardware security keys (preferred for privileged accounts)
- Push-based MFA with strong device trust controls

Avoid:

- **SMS-based MFA where possible due to SIM-swapping and interception risks.**

3. RESTRICT ADMINISTRATIVE PANEL ACCESS

Publicly exposed administrative interfaces provide attackers with direct access to authentication portals and increase attack surface visibility. Administrative access should be restricted to authorized networks and personnel only.

Use:

- **IP allowlisting for known administrator locations**
- **VPN-restricted administrative access**
- **Reverse proxy access control mechanisms**
- **Geographic access restrictions where operationally feasible**

Reducing public exposure of management interfaces significantly lowers the risk of brute-force and reconnaissance activity.

4. RATE-LIMIT AND BLOCK BRUTE FORCE ATTEMPTS

- Brute-force attacks remain a frequent technique for compromising CMS panels, SSH services, and exposed authentication portals.

- Rate-limiting and automated blocking mechanisms should be deployed to reduce repeated login attempts.

Deploy protections for:

- CMS login endpoints
- XML-RPC interfaces
- SSH services
- FTP authentication portals

Implement:

- **Account lockout policies after repeated failures**
- **Progressive authentication delays**
- **CAPTCHA challenges after failed attempts**
- **Automated IP banning using tools such as Fail2Ban**

These controls help disrupt automated attack campaigns and reduce authentication abuse.

6. PATCH CMS, PLUGINS, AND THEMES

- Outdated CMS software and plugins remain one of the leading causes of website compromise and defacement.

- Threat actors actively scan for vulnerable versions of widely used content management systems.

PRIORITIZE PATCHING:

- **WordPress core installations**
- **Joomla components and extensions**
- **Drupal modules**
- **Web server software and dependencies**

Unused plugins, themes, and modules should be removed entirely to eliminate unnecessary attack surfaces.

7. IMPLEMENT FILE INTEGRITY MONITORING

- File Integrity Monitoring (FIM) is a critical defensive control for detecting unauthorized changes to website files, configurations, and application components. In web defacement and web shell deployment incidents, attackers typically modify core files, inject malicious scripts, or alter templates to establish persistence or alter website content.

- FIM provides visibility into these modifications by continuously monitoring file states and generating alerts when changes occur.

- Early detection of unauthorized file modifications can significantly reduce attacker dwell time and improve incident response speed.

USE:

- Wazuh – provides real-time file integrity monitoring, log analysis, and alert correlation through centralized dashboards

- Tripwire – detects unauthorized file changes using baseline comparison and policy enforcement

MONITOR:

- Core website index files (index.php, index.html)
- Theme and template files
- Upload directories
- Configuration files (wp-config.php, .env, server configs)
- Plugin and module directories

BEST PRACTICE:

- **Establish file baselines after every legitimate update and configure alerts for high-risk file modifications.**

- **Real-time alerting on unauthorized changes enables rapid containment before broader compromise occurs.**

8. HARDEN FILE PERMISSIONS

Improper file permissions can expose critical website files to unauthorized modification, privilege escalation, or malicious code execution. Attackers often exploit weak file permissions to alter content, inject malware, or deploy web shells.

Organizations should implement strict file permission policies based on the principle of least privilege, ensuring users and services have only the minimum required access.

SECURE DEFAULTS:

- Files: 644 (owner read/write, group read, public read)
- Directories: 755 (owner full access, group/public read-execute)
- Sensitive configuration files: 600 (owner read/write only)

Critical controls:

- Restrict write permissions on configuration files
- Prevent unnecessary write access to web root directories
- Ensure application files are owned by appropriate system users
- Separate web server and administrative user privileges

Critical web directories should not be writable by the web server unless operationally required.

Regular permission audits should be conducted to identify insecure configurations and privilege drift.

9. DISABLE DANGEROUS UPLOAD EXECUTION

- File upload functionality is one of the most commonly abused attack vectors in website compromises. Attackers frequently exploit insecure upload mechanisms to deploy web shells, malware payloads, or persistence tools.

- By default, uploaded content should be treated as untrusted and should never be executable.

- Organizations should implement strict controls around upload handling and execution restrictions.

Implement:

- **Disable PHP execution within upload directories**
- **Restrict executable file extensions (.php, .phtml, .jsp, .asp)**
- **Enforce strict MIME-type validation**
- **Validate file signatures (magic bytes)**
- **Scan uploads for malware before storage**
- **Rename uploaded files to prevent execution by predictable names**

Additional controls:

- Store uploads outside the web root where possible
- Restrict direct public access to uploaded files
- Use sandboxing for processing uploaded content

These controls significantly reduce the risk of attackers weaponizing upload functionality for code execution and persistence.

10. CENTRALIZE LOGGING AND ALERTING

- Comprehensive logging is essential for visibility into attacker behavior, compromise attempts, and post-compromise actions. Without centralized logging, detecting suspicious activity becomes significantly more difficult.

- Security logs should be collected, centralized, and monitored continuously for anomalies and indicators of compromise.

- Centralized logging supports both detection and forensic investigations.

MONITOR:

- Failed authentication attempts
- Successful administrative logins
- File modifications
- New privileged account creation
- Plugin/module installation activity
- Administrative setting changes
- Unexpected outbound connections

USE:

- **Elastic Stack** – centralized log collection, search, and analytics for threat hunting and alerting
- **Splunk** – advanced log analysis, correlation, and incident investigation

Best Practice

- Configure automated alerts for high-risk events such as multiple failed logins, privilege escalation, or unauthorized file modifications.
- Timely alerting improves detection efficiency and reduces incident response time.

11. DISABLE UNUSED SERVICES

- Unused or legacy services increase the attack surface and may expose unnecessary vulnerabilities. Attackers often scan for exposed services such as FTP, legacy APIs, or outdated management interfaces.
- Reducing the number of exposed services lowers the number of potential entry points.
- Organizations should review all running services and disable those not required for operations.

TURN OFF:

- FTP services
- Unused administrative interfaces
- Legacy APIs
- Deprecated remote management services
- Unused database management interfaces
- Deprecated remote management services

REPLACE:

- FTP WITH OPENSSH SFTP FOR ENCRYPTED FILE TRANSFER

Additional hardening:

- Restrict management interfaces to internal networks
- Disable anonymous access mechanisms
- Remove outdated service versions

Reducing exposed services directly decreases attack surface exposure and limits attacker opportunities.

12. MAINTAIN BACKUP AND RECOVERY READINESS

- Reliable backup and recovery capabilities are essential for restoring operations after web defacement, ransomware, destructive malware, or operational failures.
- Attackers increasingly target backup systems to prevent recovery, making backup protection equally important.
- Organizations should implement resilient backup strategies to ensure business continuity.

MAINTAIN:

- Daily automated backups
- Offsite backup storage
- Immutable backup copies
- Versioned backups for rollback capability

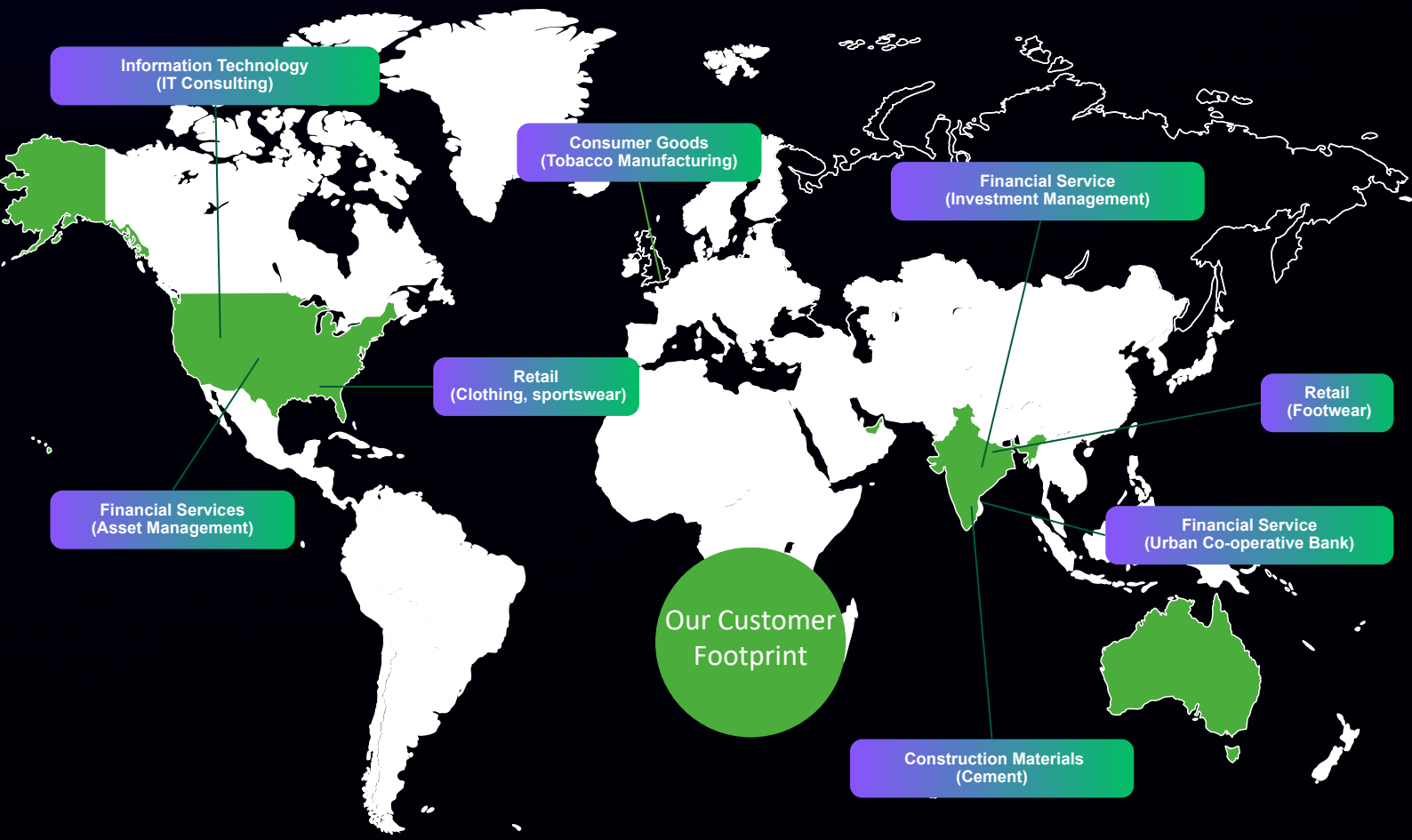
BEST PRACTICES:

- Encrypt backup data at rest and in transit
- Isolate backup systems from production environments
- Test restoration procedures regularly
- Maintain documented recovery workflows
- Regular backup restoration testing ensures operational readiness and reduces downtime during recovery efforts.
- A mature backup strategy significantly improves resilience against destructive attacks and operational disruption.

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