LOGON
SOFTWARE & SERVICES

CATALOG

EXTERNAL ATTACK SURFACE MANAGEMENT SOLUTIONS

Secure Your External Assets in your public internet-facing assets,
both known and unknown

Our Website: www.logon-int.com

Your Trusted Cyber Security Partner in Asia

Since 1993, LOGON has provided security products, technical support, consulting and training services to organizations from all vertical industries in Asia.

Our cybersecurity software solutions and managed services help prevent malicious attacks and loss of sensitive information and building strong security practices.

30+ Years

Since 1993.
6 Local Offices.
Trained Certified Staffs.

1,000+ Trusts

Organizations from varies vertical industries in Asia

130+ Partners

Direct Global Partnership with Award winning Cybersecurity Vendors.

EASM

External Threat Intelligence Report

What to Expect in 2025

42%
rise in reported ransomware attacks

125%
increase in active ransomware groups YOY

68%
more exposed digital assets, compared to last year

20%
surge in open and unsecured databases

18%
expected Growth Rate of Global Threat Intelligence Market through 2029

70%
increase in the use of Telegram by cybercriminals

Protect against
External Cyber Threats
emerging beyond your managed IT perimeter

Source: CyberAngel 2025 External Threat Intelligence Report

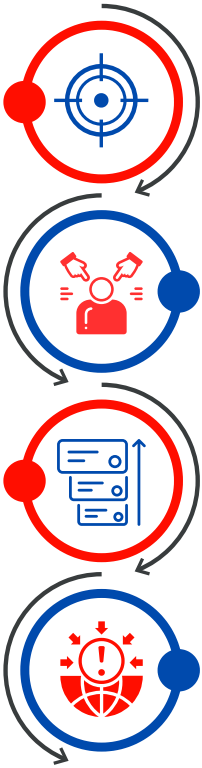
EASM

What We Offer

1. Asset Discovery & Monitoring

Asset Discovery is a core function of EASM.
Our EASM Solutions help organizations to identify, inventory, and continuously monitor their internet-facing assets.

We ensure you that even unknown, unmanaged, or forgotten assets—often referred to as "shadow IT"—are identified and brought under security management.



DISCOVERY
Asset found via pivoting and keyword matching

ATTRIBUTION
Asset determined to belong to your organization

PRIORITIZATION
Level of risk asset poses to organization is determined

REMEDIATION
Action taken to secure asset so it is no longer a threat

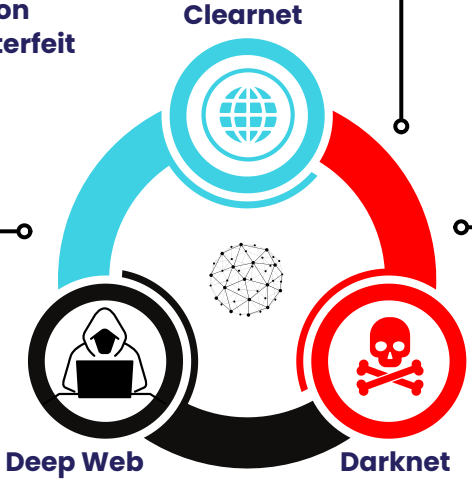
What We Offer

2. Digital Risk Protection

Digital risk protection works as a multi-layered approach to protecting an organization from online threats.
Our reliable DRP solutions include the following 3 components:

Threat Information Engine

- **Sensitive Data Exposure Monitoring**
- **Social Media Monitoring**
- **Domain Protection**
- **Fraud and Counterfeit Risks Monitoring**



Intelligence Operations

- **Proactive Infiltration and Monitoring Activities**

Counterintelligence

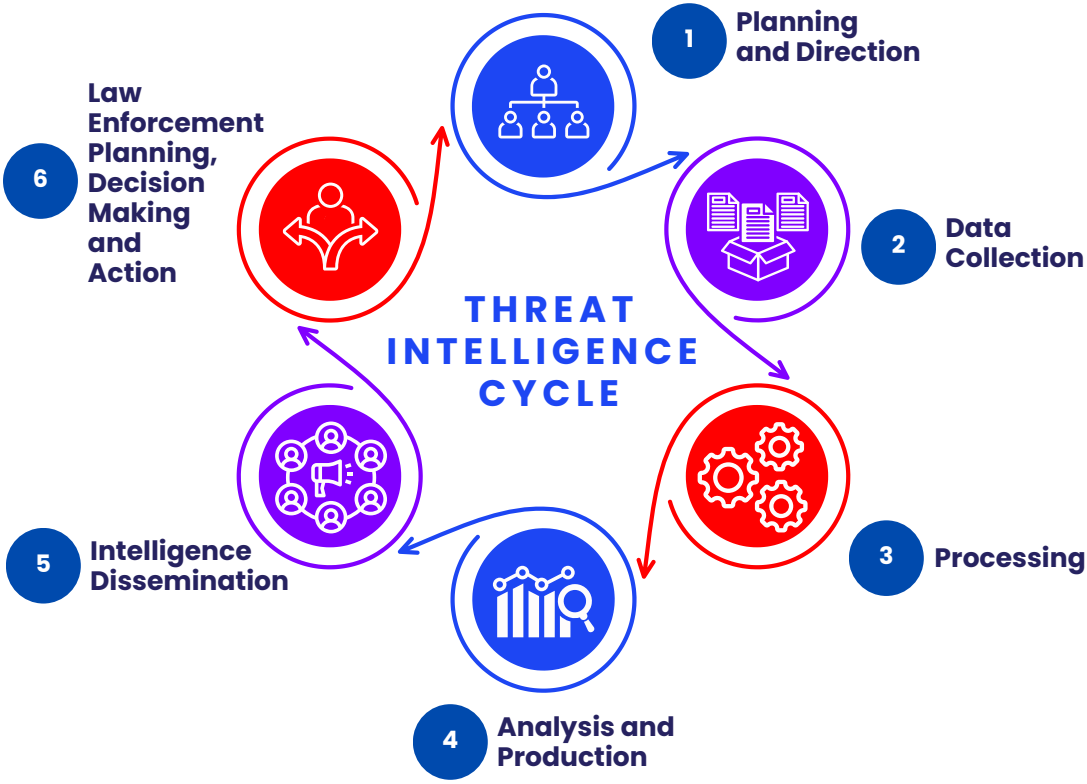
- **Third-Party Risk Monitoring**
- **Brand Protection**
- **Trademark Monitoring**
- **Takedown Services**

What We Offer

3. Cyber Threat Intelligence

Our CTI solutions provide organizations with valuable insights into emerging threats, enabling them to proactively protect their systems and data. These approaches include:

- **General Threat Landscape Monitoring**
- **Threat Intelligence Analysis**
- **Indicator of Compromise (IOC) Development**
- **Data Theft Detection**



EASM

EASM for Every Industry

Pharmacuetical / Life Sciences

- Continuously monitors cloud storage platforms (Box, Google Drive, Dropbox) for exposed folders
- Detects leaks using biotech-specific keywords and entity recognition
- Assesses exposure scope through geolocation data
- Facilitates rapid takedown and escalation to stakeholders

Financial Services

- Monitors for exposed documents and misconfigured servers
- Manages third-party risks effectively to protect customer data
- Monitors forums and messaging platforms for leaked content
- Automates vendor alerts and compliance responses

SaaS / Tech Platform

- Identifies non-production environments hosting sensitive data via behavioral analysis
- Analyzes behavioral patterns to flag sensitive data exposure
- Monitors breach markets for potential threats to your brand
- Provides alerts with severity scoring and remediation paths

Retail / Ecommerce

- Actively monitors dark web and messaging apps for brand abuse
- Detects cloned product pages and fake reviews by correlating with official SKUs
- Coordinates legal action and domain takedown with enforcement partners
- Provides reports on brand damage and reputational impact

Manufacturing / Industrial

- Secures operational technology and industrial control systems.
- Scans developer communities for exposed configurations.
- Identifies risks associated with sensitive operational data.
- Correlates leaked information with internal asset intelligence for risk mitigation.

Contact Us Today to discuss your industry requirement!

EASM

Use Cases for EASM

DevOps Credentials Leaked to GitHub

Incident

A DevOps engineer mistakenly exposed AWS IAM admin credentials in a public GitHub repo, leading to a crypto mining bot launching 24 EC2 instances and causing a **$12,300 loss within 24 hours** before being detected by a billing alert.

Implementation:

- Detected the AWS key within 30 minutes of being posted
- Enriched alert with repository link, timestamp, author, & potential impact
- Correlated the leaked key to your organization's GitHub activity using domain and email intelligence
- Enabled immediate IAM key revocation and rotation before the blast radius expanded

Forgotten Subdomain Points to Test VPN Login

Incident

The inactive subdomain vpn-emea.clientname.com, linked to a decommissioned VPN and using default OpenVPN credentials without 2FA, was **indexed by Shodan and exploited within 72 hours**, leading to a successful credential stuffing attack on a Jira test account.

Implementation:

- Detected forgotten subdomain as part of continuous external asset mapping
- Flagged the endpoint as high-risk due to exposed login panel + lack of 2FA
- Enriched alert with associated certificates and SSL fingerprints
- Provided remediation recommendations to decommission and update DNS records

Jenkins Server Exposed to Internet

Incident

A new Jenkins instance with a public IP and no authentication was exploited by attackers, who installed a **malicious plugin and exfiltrated sensitive API keys from the secrets.xml file** after discovering the server on Censys.io.

Implementation:

- Detected the Jenkins instance via external service exposure scanning
- Identified it as vulnerable due to version fingerprinting and lack of authentication
- Prioritized alert based on critical asset correlation (e.g., matching org domain, Git commit references)
- Suggested access control fixes and helped initiate emergency patch workflows

Expired Domain Hijacked for Phishing

Incident

After the domain **retailgroupindia.com expired post-brand transition**, an attacker re-registered it, cloned the vendor portal, and sent phishing emails to suppliers, **compromising over 30 accounts** and resulting in fraudulent invoices before detection.

Implementation:

- Detected domain expiration and flagged it in real-time as a high-risk asset
- Notified your team when the domain was re-registered by a third party
- Detected that the new DNS pointed to a phishing infrastructure with reused SSL certs from previous scams
- Offered takedown support via brand protection workflows and legal escalation paths

Misconfigured Azure Blob Exposes PII

Incident

A marketing agency partner exposed customer onboarding files in a publicly accessible Azure Blob container, allowing a journalist to discover and publish an exposé on the leaked data, which included **sensitive information like Aadhaar IDs and mobile numbers.**

Implementation:

- Detected exposed Azure blob using cloud scanning against third-party asset surfaces
- Identified PII based on content classification: IDs, personal forms, and location metadata
- Alert included direct links, hosting region, and Azure blob URI
- Enabled rapid contact with the third-party agency and remediation via access controls and DMCA notice

Executive Impersonation on LinkedIn

Incident

A threat actor impersonated your CFO with a fake profile, connected with over 40 HR and Finance employees, and successfully **tricked a junior controller into wiring €270,000 to a fraudulent M&A escrow account**.

Implementation:

- Detected fake profile using AI-based identity monitoring & fuzzy image matching
- Correlated LinkedIn activity patterns with anomalous impersonation attempts across other execs
- Flagged urgent alert to brand protection team and initiated takedown request to LinkedIn Trust & Safety team
- Create internal awareness campaign around executive impersonation risks

LOGON
SOFTWARE & SERVICES

Trust LOGON as
Your Cyber Security Partner in Asia

Contact us to discuss your requirements.
We are here to help.

Email Address
Sales Inquiry: sales@logon-int.com
Support Inquiry: support@logon-int.com

Phone Number
APAC: +852 2512 8491
India: +91 70220 22744 / +91 63668 26133

Website
www.logon-int.com