ASSET DISCOVERY AND MONITORING

Prevent attacks against vulnerable shadow assets

Is your digital infrastructure fully protected against hackers? Unsanctioned assets, decommissioned services and partners' vulnerable products extend your attack surface outside of your purview. These shadow assets may remain invisible to you, but not to your attackers; 30% of successful cyber-attacks target vulnerable shadow assets (Gartner).

Traditional vulnerability management solutions are incapable to guarantee the safety of shadow assets at scale. Hence organizations worldwide rely on CybelAngel to prevent harmful attacks by detecting and securing vulnerable shadow assets before they are breached.

LOWER YOUR EXPOSURE WITH CYBELANGEL

- **Discover Shadow Assets** set up by employees, third and fourth-parties.

- **Focus On Highly Vulnerable Machines** with a risk-driven approach, not an inventory approach.

- **Protect In The Long Run** by putting newly discovered IPs under surveillance.

KEY TECH BENEFITS

4.3B IPV4 scanning with in-depth, risk-driven matching.

>7 CVEs only. Focus on highly critical vulnerabilities to secure the most exposed assets.

<2h Set-up time. No additional FTE, no probe or sensor required.

KEY BUSINESS BENEFITS

0% Zero false positives. Avoid losing time and money sorting feeds of false alerts.

0 Additional FTE required on your side. Investigation is led by your CybelAngel analyst.

4 Quick return on investment, with average 4-week payback.

VULNERABLE SHADOW ASSETS INCLUDE

- **Connected File Servers**: IPv4+ connected storage, NAS drives, FTP servers, RSync backups, etc.

- **Databases**: ElasticSearch, Cassandra, Redis, CouchDB, RethinkDB, etc.

- **Industrial Systems:** telemetry systems, hardware machines, heating systems, etc.

- **DevOps Tools**: infrastructure control servers, container management softwares, etc.

- **Remote Desktop Services**: RDP, vnc, Team viewer, etc.

- **IoT**: medical imagery equipment, etc.

> CybelAngel is the only solution that detects a potential crisis before it effectively becomes one.
>
> Thierry Auger, Deputy CIO and CISO, Lagardère International

GET NOTIFIED WHEN

Internet-facing RDPs are providing information to attackers in recon phase.

Misconfigured Industrial protocols are leaving your buildings vulnerable to hacking.

Shadow web servers are exposing you to ransomware attacks.

No Probe Required

Zero False Positives

Dedicated Analyst
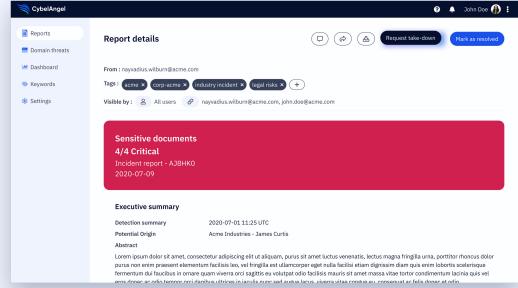
Fully Actionable

Severity Indicator
Focus your efforts on the most critical incidents first.

Details of the exposed asset
Authentify service or device.

Incident Origin
Pinpoint incident response.

Risk assessment
Anticipate potential attackers' next move.

Integrate CybelAngel In Your Toolstack

KEY FEATURES

- Fully documented RESTful API. Build a robust and scalable asset discovery workflow.

- Real-time synchronization. Retrieve, manage, resolve all Incidents Reports.

- Custom connectors on-demand. Map Incidents detected in CybelAngel to events in your SOAR, ITSM or SIEM platforms.

KEY BENEFITS

- Scale your digital risk protection by integrating realtime, zero false-positive asset discovery and monitoring capacities with your existing toolstack.

- Streamline your incident response by building simplified workflows.

- Enrich your threat intelligence strategy by correlating CybelAngel incidents with alerts from other digital risk protection solutions.

Book Your Free Trial Now   CYBELANGEL.COM

Paris | New York | London