CybelAngel

Managing Threats Beyond the Perimeter

Ensuring Comprehensive Protection of Your External Attack Surface

ISMG
INFORMATION SECURITY
MEDIA GROUP

Erwan Keraudy

Jeff Gore

CybelAngel CEO Keraudy, co-founded the company in 2013 with his brother Stevan, a renowned AI expert.

CybelAngel, the pioneer in outside-in threat detection, today offers the most comprehensive External Attack Surface Protection and Management (EASMX) solution available.

CybelAngel, founded in 2013, is on a mission to help businesses world-wide discover the unknown assets and exposures that reside beyond a company's security perimeter and act as access points, or 'doors and keys,' into company systems. Erwan Keraudy explains, "For comprehensive protection, organizations need full visibility across their external attack surface (EASM) to uncover unknown vulnerabilities such as exposed assets like devices and domains, as well as the threats and exposures such as look-alike domains, exposed credentials, dark web mentions and leaked data. CybelAngel's Xtended External Attack Surface Management (EASMX) is the only solution that can identify it all. It's not only the most thorough — a 10-year head start means no other solution can match its power or results."

Recently CybelAngel CEO, **Erwan Keraudy**, and CRO **Jeff Gore**, sat down with Mathew Schwartz, Executive Editor of DataBreachToday to discuss ways businesses can better protect their ever-growing external attack surface.

In this interview Keraudy and Gore discuss:

- How to illuminate unknown external attack surface threats.

""Thanks to our AI and analyst teams, we find assets and information leaking from open or unsecured sources… before they become breaches. Essentially we provide 'preemptive security' to find and remediate exposed attack surfaces, which is new in the world of cybersecurity. We are solving a huge problem here.""

– Erwan Keraudy

If Bad Guys Can Do It - We'll Do it Better and Faster!

Mathew Schwartz: Tell us about the history of your CybelAngel.

Erwan Keraudy: I co-founded CybelAngel with my brother, Stevan Keraudy, in 2013. I was working within financial services at the time and noticed that an investment portfolio took a radical decline within a single day due to a data breach. Stevan was designing artificial intelligence engines for one of the largest global IT services companies in the world, so naturally I asked him about the breach.

We assessed the market, the threats, and technology, and realized that attackers take advantage of both the external attack surface and data leaks to get to a company's most important information. We thought, if a hacker can access exposed data to use for ill will, why couldn't we do it faster for ethical use? **We'd find leaked data, assets, and shadow IT and take it down before threat actors even knew it was there!**

We knew we couldn't just catch-up to the bad guys' capability, we had to get ahead of them. To do this, we had the crazy idea of scanning the entire internet every 24 hours to find vulnerabilities. We wanted to be the 'Google' search for vulnerabilities.

The Protection Perimeter is Collapsing

Keraudy: In today's connected world there is no protection perimeter anymore. Firewalls and antivirus are no longer enough. With cloud migration, remote work cultures, and integrated supplier ecosystems, much of a company's information resides outside the firewall. While much of it is known and monitored, there is much more unknown exposure occurring everyday… and hackers fully understand that.

Closing the Doors and Hiding the Keys

Everyday we scan all open servers globally. Searching both the Internet and the Dark Web, we find tremendous amounts of leaked information, credentials, fake domains, and shadow IT assets – exposing confidential, business-critical, information. Built upon the most exhaustive and experienced machine-learning engine for finding exposures, CybelAngel's EASM solution finds all unknown external assets, or "*the Doors to the kingdom*," while our DRPS solution finds the credentials, or "*the Keys to the kingdom*."

"Thanks to our AI and analyst teams, we find information leaking from open or unsecured devices… before they become breaches. Essentially we provide 'Preemptive Security,' to find and remediate exposed attack surfaces, which is new in the world of cybersecurity. We are solving a huge problem here."

Challenges of Digital Transformation

Schwartz: In your conversations with organizations, and boards, do you see awareness of the challenges posed by overnight digital transformation? Do they get it?

Jeff Gore: Absolutely! New technologies add great flexibility to business operations, yet as the connected

ecosystem of employees, partners and suppliers, expands across the cloud, the proverbial security perimeter has evaporated and the smart CIOs and CISOs definitely understand that risk.

The challenge is in being able to derive definitive ROI without experiencing the loss... essentially placing a value on preventing a breach or ransome attack that never happens. However CISO's and board members do understand that you can't protect what you can't see and that having comprehensive threat protection requires full visibility of the external attack surface.

Communicating Risk to the Board

Schwartz: A lot of CISOs say that when they're communicating with the board and other senior executives, the conversation has to be about risk; the business case for what they're doing needs to be rendered in a business-acceptable way. How do they do that?

Keraudy: Board members, executive committee members, and the CEOs are generally not cyber experts. Yet they still understand risk. Getting back to the ROI challenge, while exact ROI is a challenge, board members most definitely know that a cyber attack can annihilate even the most sound five-year business plan.

In fact, Forrester Research recognized this in a recent report that looked at the 'composite' CybelAngel customer. The research found that on average, our customers decrease their risk by two major breaches per year, in addition to potentially saving on insurance premiums and analysts headcount. A CEO understands that.

Additionally, C-level executives and board members see the value in CybelAngel's ability to conduct thorough 'Due Diligence' on cyber exposure. Because our keyword search methodology is built upon algorithms with a rich, almost decade-long history of machine learning experience in finding vulnerabilities - it's the strongest on the market. Searching with key terms means that we can find the threats, leaks and shadow assets of potential business partners or acquisitions.

If you're the CEO working on a secret billion-dollar acquisition, having insight into the information leaks of the companies that you are about to either partner with, or potentially purchase is incredibly valuable. When we bring this information to a CEO, they get it!

And, because our findings go deep and can get to a granular level, we not only protect a company's technology, we protect their strategic intellectual property from getting into the wrong hands too.

Managing Alerts

Schwartz: You mentioned alerts. Alert fatigue in the cybersecurity industry is a real problem. What can organizations do to drive down the number of alerts that they're facing? And how can they get a better handle on the constantly changing systems and configurations?

Gore: Our customers use Cybelangel because the advanced AI algorithms find critical exposed assets,

"CybelAngel takes an outside-in approach. We uncover exposed assets and can track back to the point of origin. This search methodology provides CISOs with a comprehensive view of active suppliers with exposed vulnerabilities, without even knowing who the suppliers are"

– Jeff Gore

and our EASM capabilities make visible open doors they didn't know existed outside their firewalls. Our analysts then prioritize and categorize the findings to give our customers both a comprehensive view into unknown assets that need to be inventoried, as well as a critical perspective on the most serious issues in need of remediation. It's really a win/win, being thorough for inventorying unknown assets, yet targeted in honing in on the most critical issues for action or remediation.

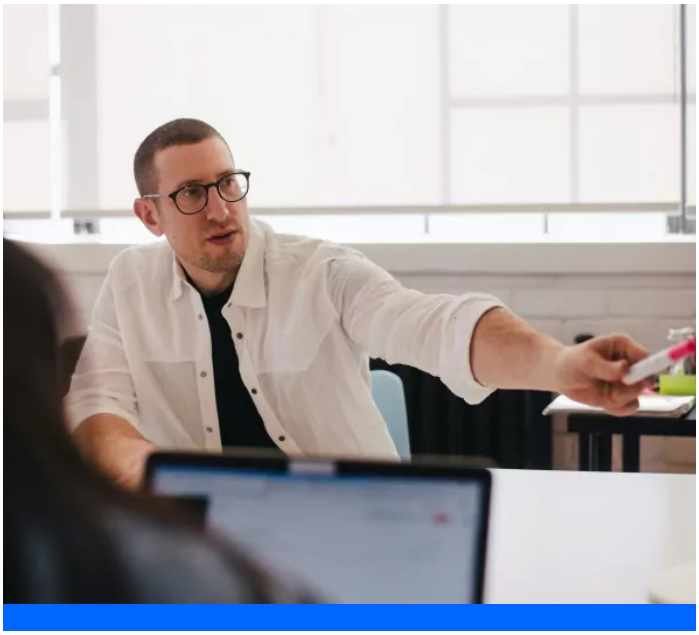
Keraudy: To add on, CISOs have way too many issues on their plate to spend time cleaning up noise. **CybelAngel sends ZERO false positives. It's a bold statement that I am completely comfortable making, because it's true**. I want my clients to use their time focused on only the most critical issues. Every time a CISO's team is working on cleaning up noise, it's not spent on what matters most. CybelAngel's motto is to help our clients, our CISOs, to focus on activities that add value and protect their organizations.

'Seeing Beyond the Perimeter'

Schwartz: One of the biggest concerns today is the risk associated with the connected interdependencies across third parties, highlighted by many high profile vulnerabilities and attacks over recent years. How does the industry get a better handle on this?

Keraudy: If you ask any CISO in the world to give you the list of all their suppliers, it's technically impossible. **Finding exposed assets beyond a company's perimeter is not only our tagline, it is what CybelAngel does better than any other provider today, hands down**. Remember, when my brother and I founded CybelAngel, Stevan was already a serious contender in building AI and ML solutions, for that reason, the CybelAngel technology and search engine has almost a decade's head start over any other similar solution.

Gore: By scanning the internet using keywords, CybelAngel takes an outside-in approach. We uncover exposed assets and can track back to the point of origin. This search methodology provides CISOs with a comprehensive view of active suppliers with exposed vulnerabilities, without even knowing who the suppliers are — we look for vulnerabilities first then make the connection back to our client companies — most other solutions need the connection first. It's really efficient, and the names of the suppliers/partners/integrations are not even required. Bottom line, CybelAngel provides the visibility to let CISOs "See Beyond Perimeters."



CybelAngel

See Beyond with Xtended External Attack Surface Protection

At CybelAngel, we protect business from cyber attack, revenue disruption, and other inherent risks associated with digital transformation by making the internet safer for managing operations, storing data, and conducting transactions by giving organizations full visibility and control of their external security profile.

More information is available at **cybelangel.com**

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io