Every day, we detect data leaks that others don’t.

CybelAngel

CybelAngel Remediation Services

In today’s risk landscape, every second counts

Time-to-take-down matters

Ever-increasing diversity in systems, devices and endpoints, new privacy and regulatory challenges, application delivery scale, shortage of skilled security professionals... Perfect **prevention** is not possible anymore in today’s cyberworld. Period.

While building new **detection** capabilities is more crucial than ever, coupling them with fast incident **response** mechanisms is paramount.

50%

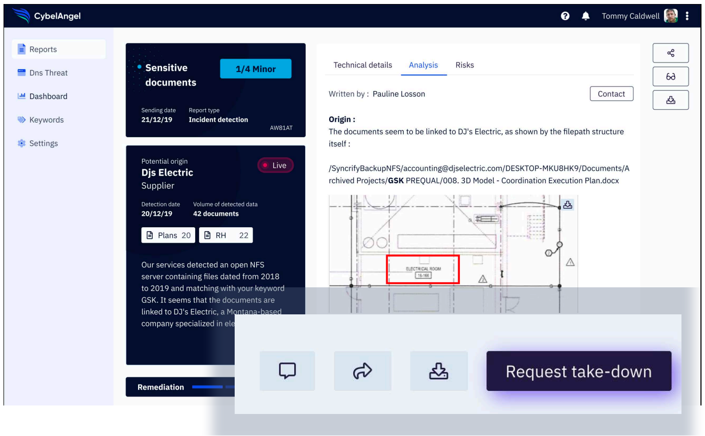
of legitimate cybersecurity threats are left unattended due to skill shortage.

CISCO, 2020

Incident detection and take-down, together

An integrated Data Exposure Management solution, CybelAngel bridges the gap between detection and remediation, bringing down the average time-to-take-down from **77* days to 11** days**. Activate Remediation Services on all incidents reported, or only a subset based on involved parties or severity levels. (source: *Ponemon, **CybelAngel)

Your CybelAngel analyst adopts a two-step, inclusive approach to threat take-down.



Written by : Pauline Losson

Origin :
The documents seem to be linked to DJ's Electric, as shown by the filepath structure itself :

/SyncrifyBackupNFS/accounting@djselectric.com/DESKTOP-MKU8HK9/Documents/Archived Projects/**GSK** PREQUAL/008. 3D Model - Coordination Execution Plan.docx

Our services detected an open NFS server containing files dated from 2018 to 2019 and matching with your keyword GSK. It seems that the documents are linked to DJ's Electric, a Montana-based company specialized in ele

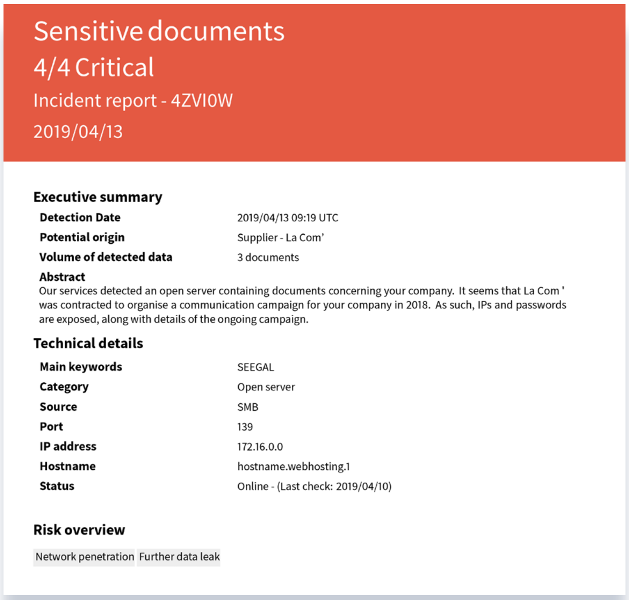
Request Remediation Services right from your platform

TAKE-DOWN

For incidents you want CybelAngel to remediate on your behalf, your analyst will swiftly **report** abuse to the hosting website or the owner of the device leaking data. Along with the take-down request, a formal **DMCA or EUCD** notice can be issued to the leak owner, as well as follow-up notices. In over 95% of cases, there is no need for your counsel’s involvement.

CLEAN-UP

Once the exposed data is offline, CybelAngel will **continue scanning** the various layers of the Internet and alert you should the device reappear. A set of recommendations will be submitted for your teams to mitigate further impact, which may include employee awareness campaigns, third-party education, or communication to your counsel's office.



Sensitive documents
4/4 Critical
Incident report - 4ZVI0W
2019/04/13

Executive summary

Detection Date	2019/04/13 09:19 UTC
Potential origin	Supplier - La Com'
Volume of detected data	3 documents

Abstract
Our services detected an open server containing documents concerning your company. It seems that La Com ' was contracted to organise a communication campaign for your company in 2018. As such, IPs and passwords are exposed, along with details of the ongoing campaign.

Technical details

Main keywords	SEEGAL
Category	Open server
Source	SMB
Port	139
IP address	172.16.0.0
Hostname	hostname.webhosting.1
Status	Online - (Last check: 2019/04/10)

Risk overview

Network penetration Further data leak

Actionable Incident Reports

Why CybelAngel Remediation Services?

Reduce time-to-take-down **by 85%**

Reduce SOC and CERT costs by up to **10%**

Focus your resources on the **20%** of most critical tasks

Adopt a **one-stop-shop**, integrated approach to Data Exposure Management

> "We are approaching "peak security product", as there are simply not enough skilled people to use the products. Seek out solution providers that offer a native service layer on top of the product offering."

Gartner, Top Security and Risk Management Trends, 2019

Leaks are **inevitable.** Damage is **optional.**

Request Remediation Services

New York | Paris

WWW.CYBELANGEL.COM