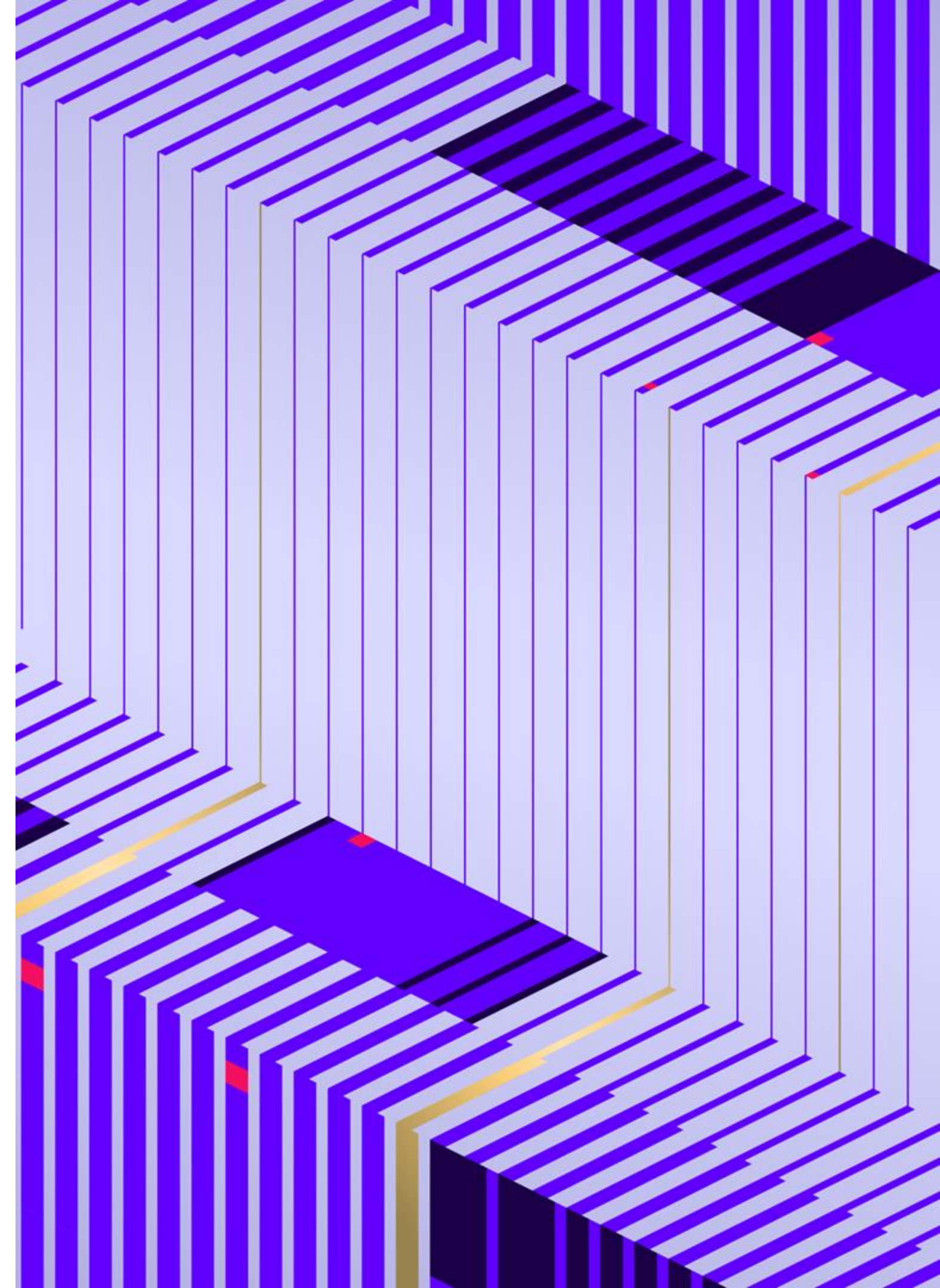


Harness the power of an Autonomous SOC to Combat the Evolution of Cybercrime.

Brett Williams

Solutions Engineering Manager



Illicit Underground Economy



E-crime is not new: A brief History



1834 - French Telegraph



1957 joybubble Phone Phreak



1969 - Rabbits Virus



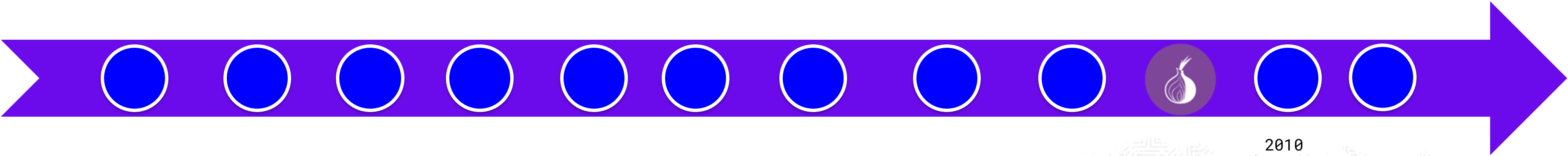
1973 Teller Embezzlement



1990 - 2003 AFP High Tech Crime Formed



2011 and beyond - APTs, Mass Breaches



1878- Early Telephone Hack NY



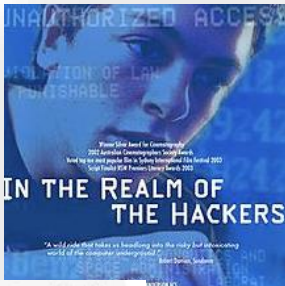
1962- Allan Scherr first Password Hack



1970 - Kevin Mitnick



1989-1990 Australian Hackers Electron/Phoenix Hack NASA and others



TOR Developed 2002



2010 Stuxnet



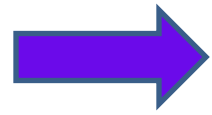
Cybercrime & State-Based Actors



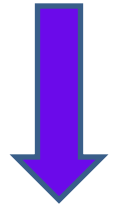
"For health and safety reasons, we'll be transitioning to cyber crime."



Providers



Services
&
Products



Buyers



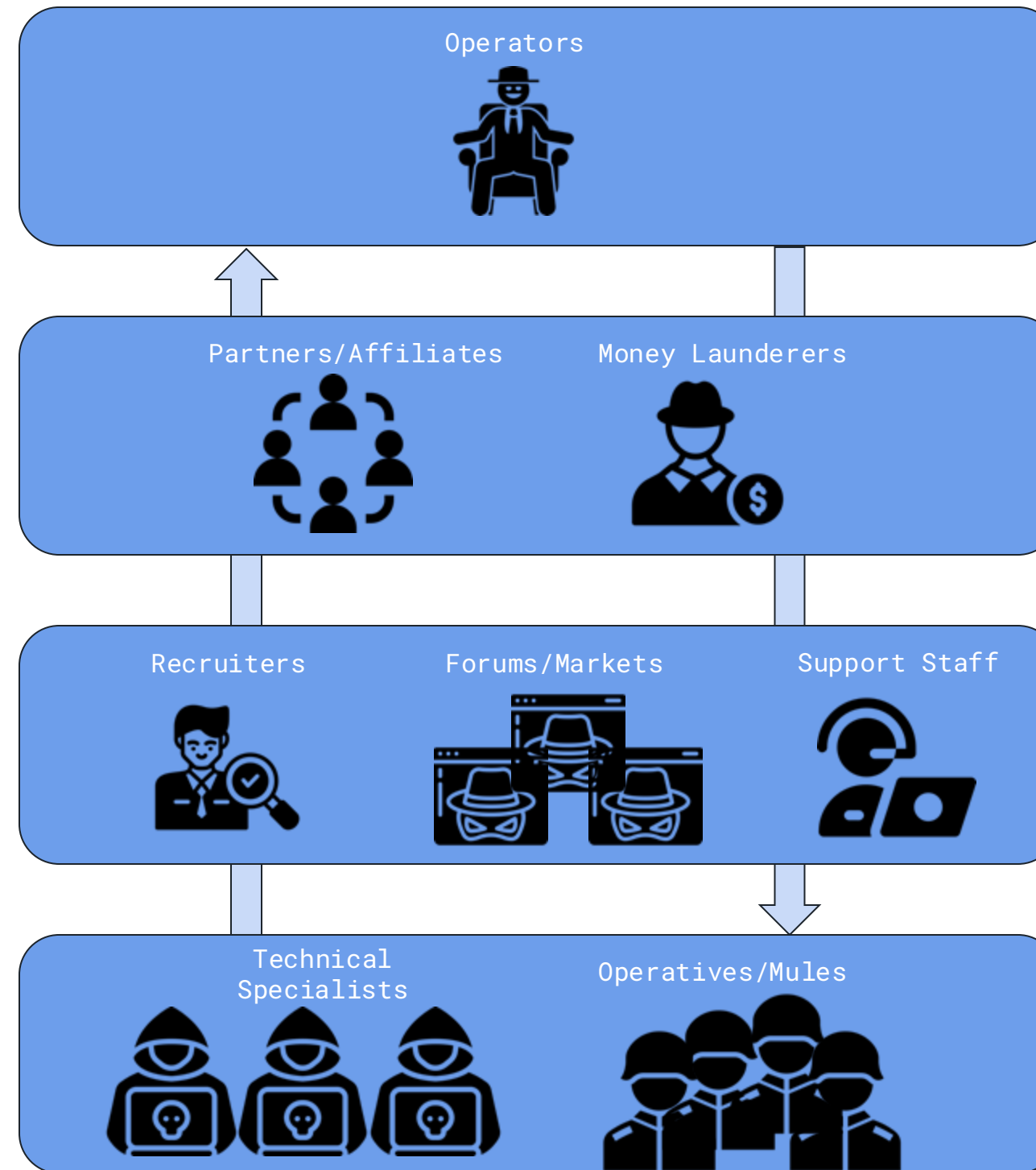
Channels

Tool Creation,
Negotiations,
Experts

Distribution &
Deployment

Remote Access
Services/Offerings

Initial Access
Brokers



\$500-\$10,000

*Exploitation & Attack Execution
Revenue Sharing*



\$200-\$5,000

Monetise Forum Access



\$10 - \$100

Initial Compromise

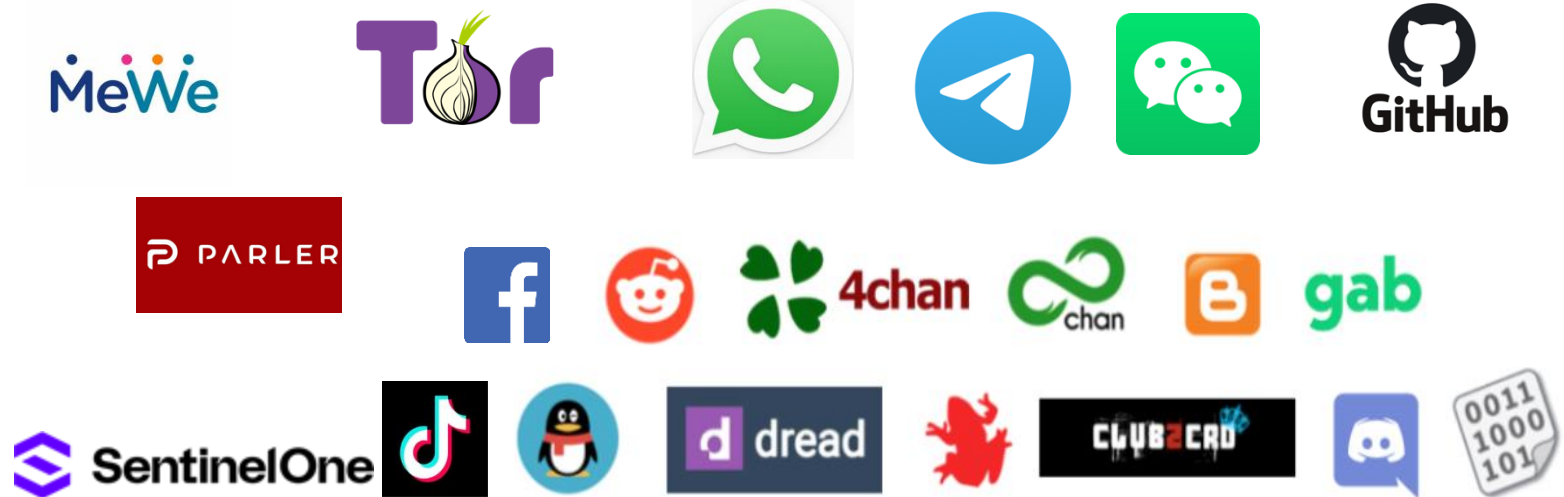
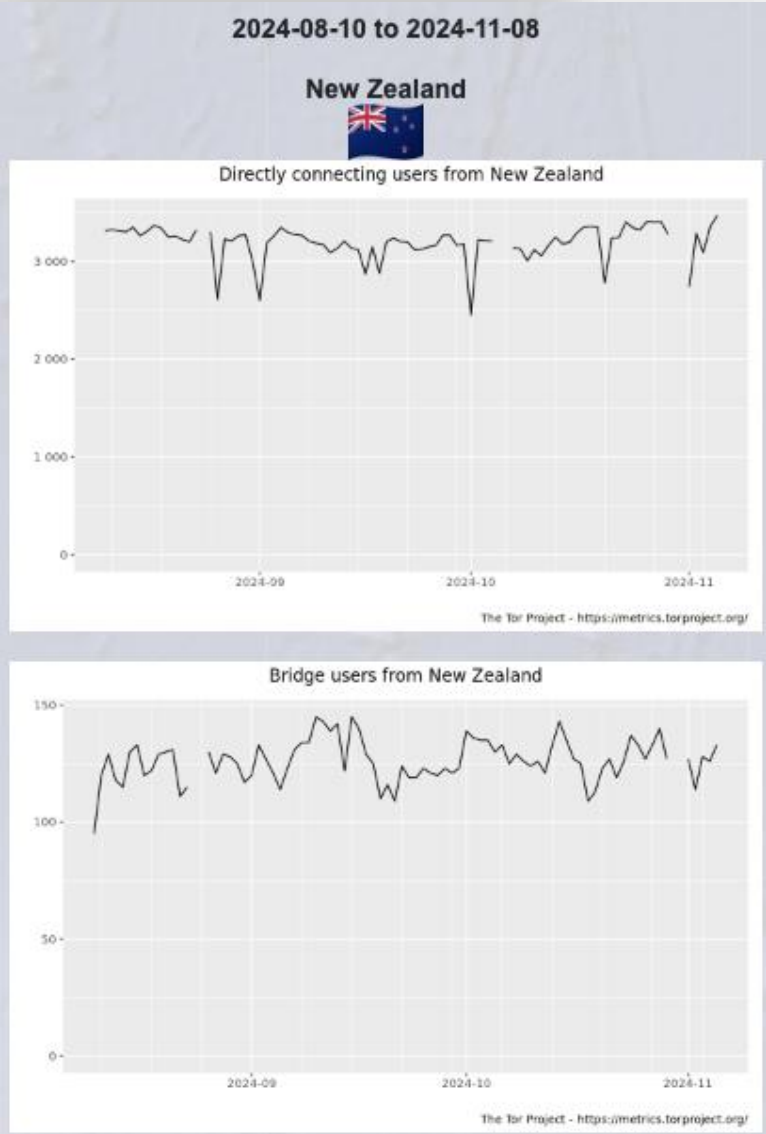
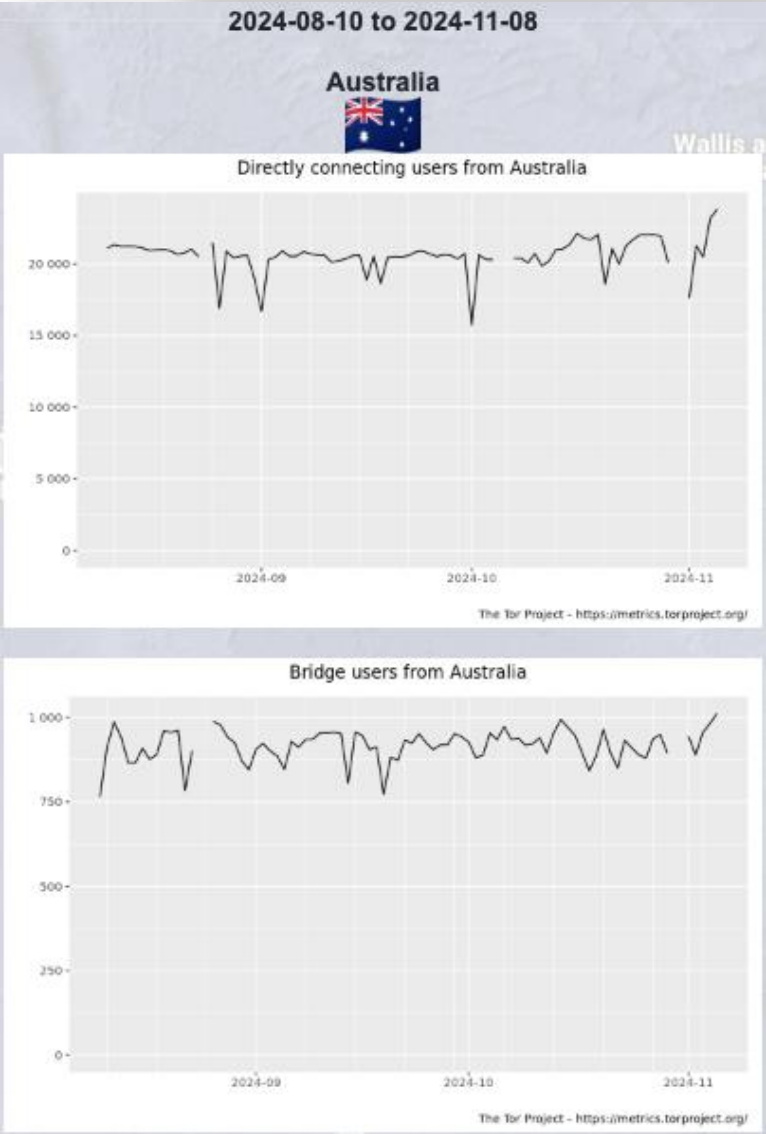
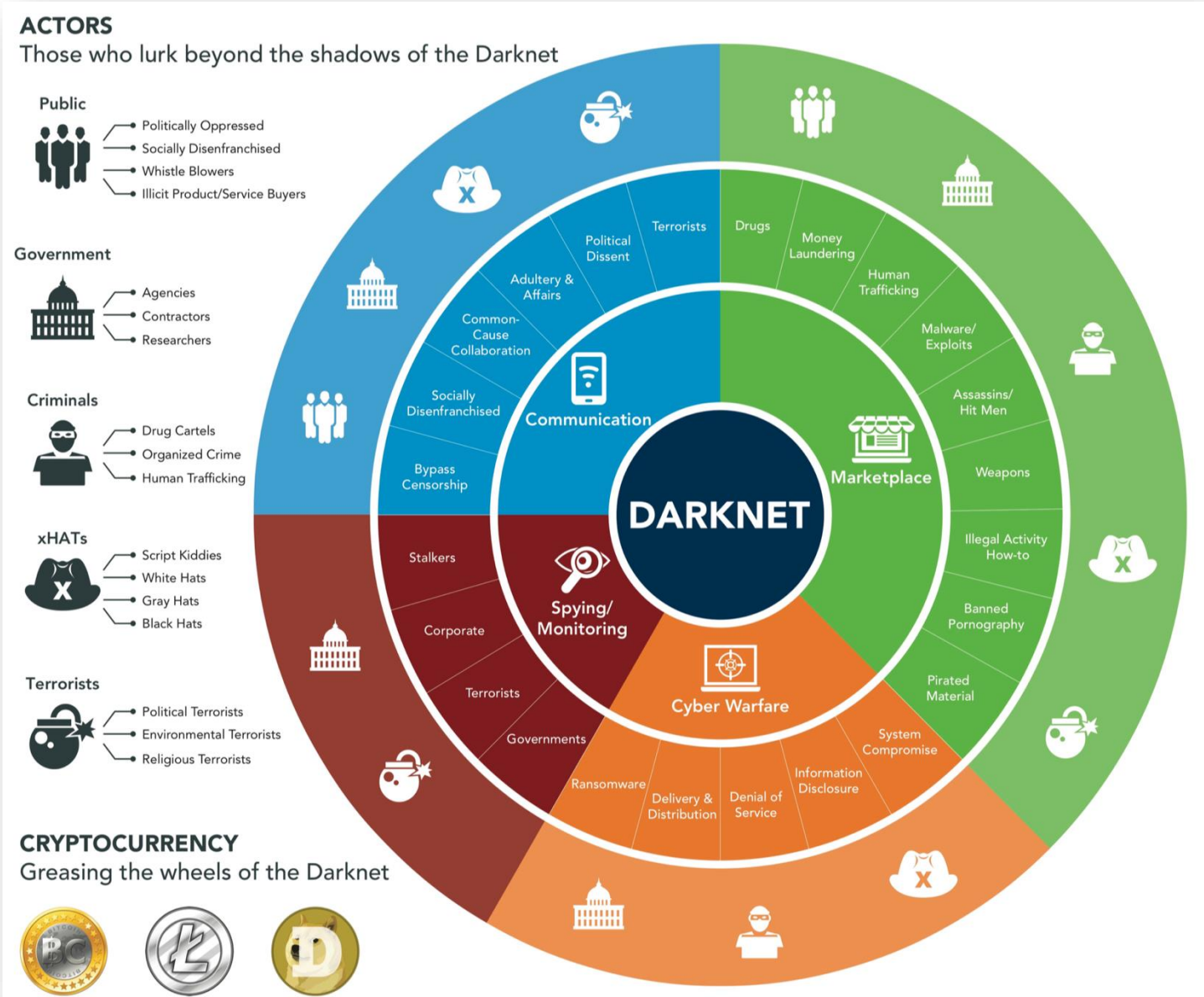
As a Service Offerings – Subscriptions

Lumma Stealer


The screenshot displays the Lumma Stealer website's pricing page. At the top, there's a navigation bar with the Lumma Stealer logo and a 'Report a bug' link. The main section is titled 'Tariff plans' and features four distinct pricing cards. The 'EXPERIENCED' plan costs \$250 and is described as 'For mass spills'. The 'PROFESSIONAL' plan costs \$500, is marked with a green star icon, and is described as 'To strait with Google'. The 'CORPORATE' plan costs \$10000 and is described as 'For point spills'. The 'SOURCE' plan costs \$20000 and is described as 'Styler and panel source code'. Each plan includes a list of features: 'Viewing and uploading logs' (checked), 'Log analysis tools' (checked), 'Traffic analysis tools' (checked), and 'Proactive Defense Bypass' (unchecked). Below each list is a 'Choose a plan' button. The 'PROFESSIONAL' button is highlighted in green. At the bottom, there's a section titled 'Answers on questions' with a dropdown menu showing 'What's your takeaway?'.

Plan	Price	Description	Features
EXPERIENCED	\$250	For mass spills	✓ Viewing and uploading logs ✓ Log analysis tools ✗ Traffic analysis tools ✗ Proactive Defense Bypass
PROFESSIONAL	\$500	To strait with Google	✓ Viewing and uploading logs ✓ Log analysis tools ✓ Traffic analysis tools ✗ Proactive Defense Bypass
CORPORATE	\$10000	For point spills	✓ Viewing and uploading logs ✓ Log analysis tools ✓ Traffic analysis tools ✓ Proactive Defense Bypass
SOURCE	\$20000	Styler and panel source code	✓ Styler source code ✓ Panel source code ✓ Source code for all plugins ✓ Right to sell

Cyber Crime Ecosystem

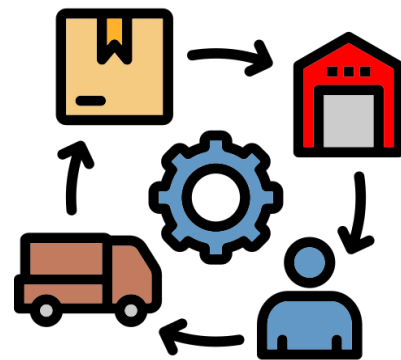


State of Cybercrime

The background of the slide features a photograph of server racks in a data center, with numerous blue indicator lights glowing. A large, solid blue triangle is positioned on the left side, pointing towards the right, and it serves as a backdrop for the white text.

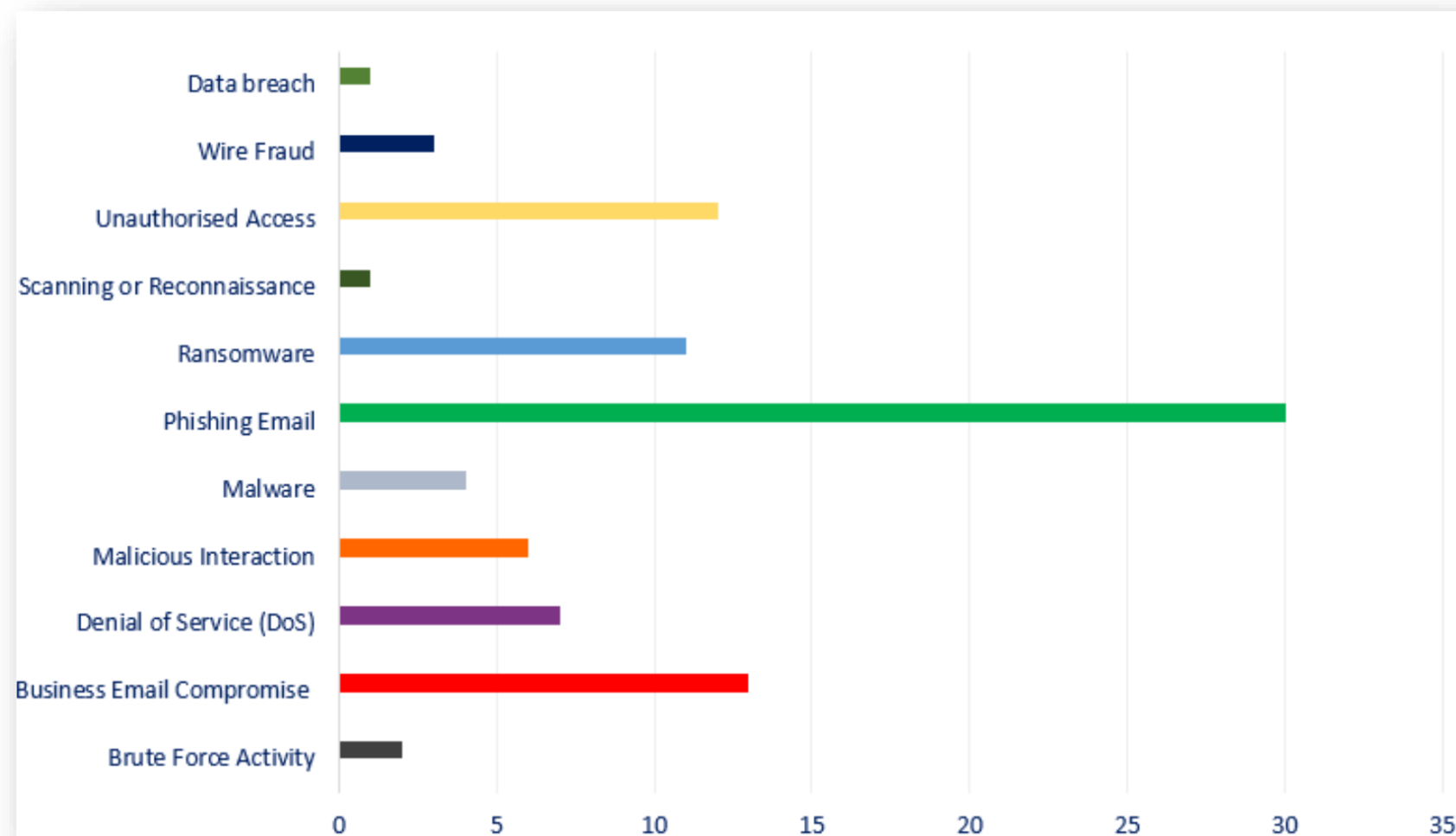
Global Scale Espionage & Layers of Cybercrime

- Derivative Attacks
- Supply Chain Compromise
- Critical Infrastructure
- Human Based Exploits
- Ransom Attacks
- Compromised Credentials
- BEC, Scams & Crypto
- Deep (MFA) Phishing/Bots



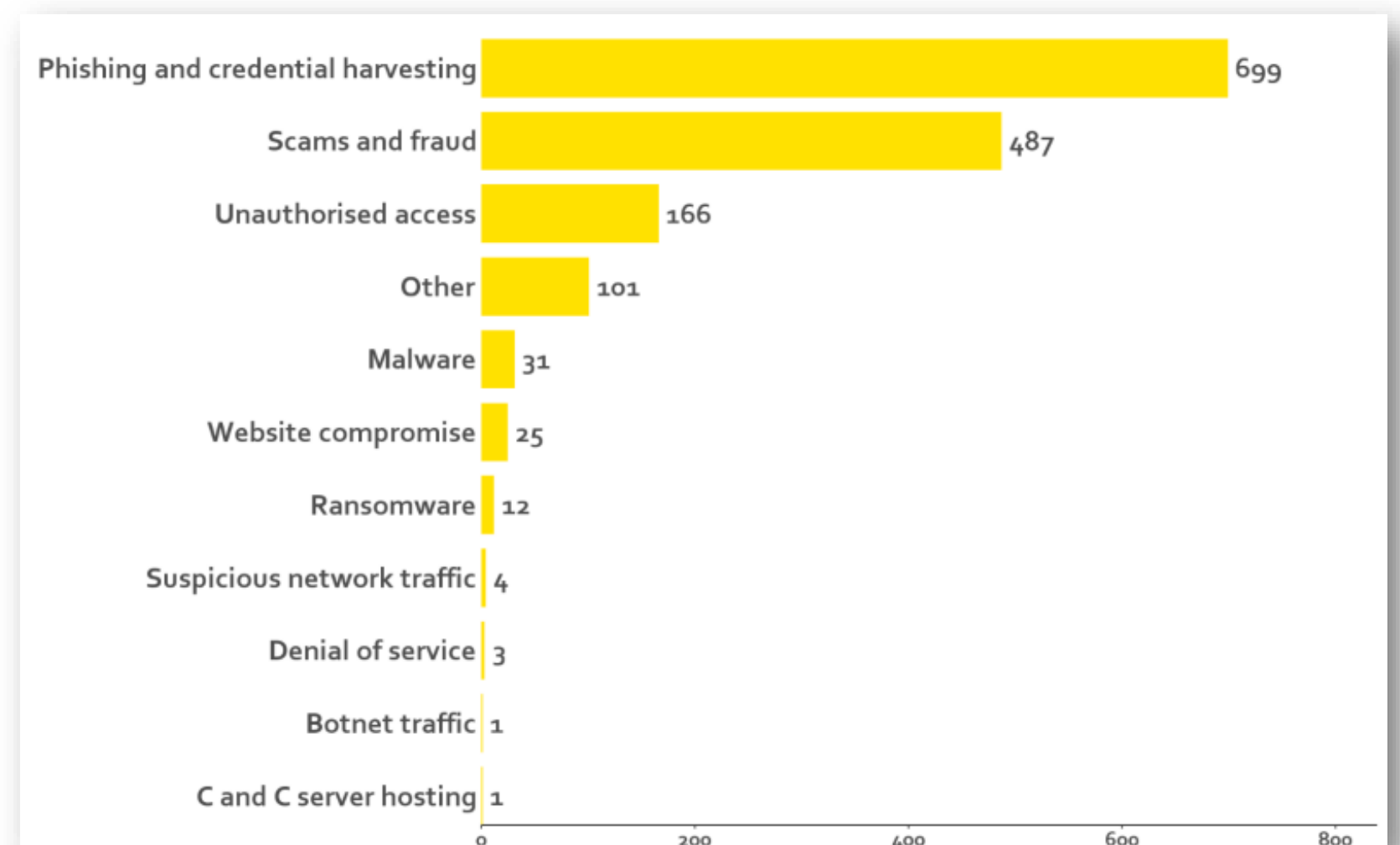
90 Incidents (June 2024)

Up 7.1% since May
2024

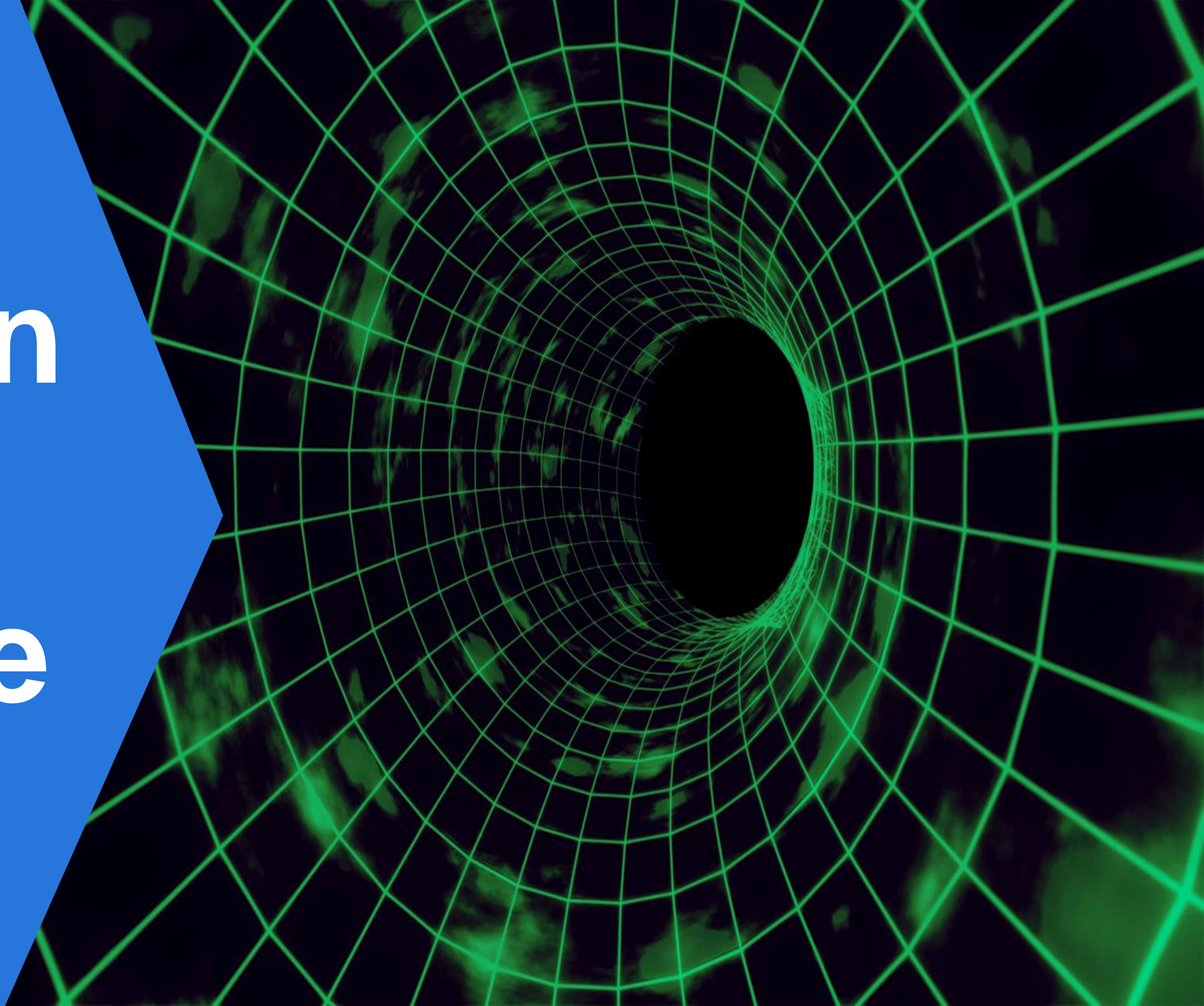


1537 Incidents (Q1 2024)

Down 19% since Q4 2023



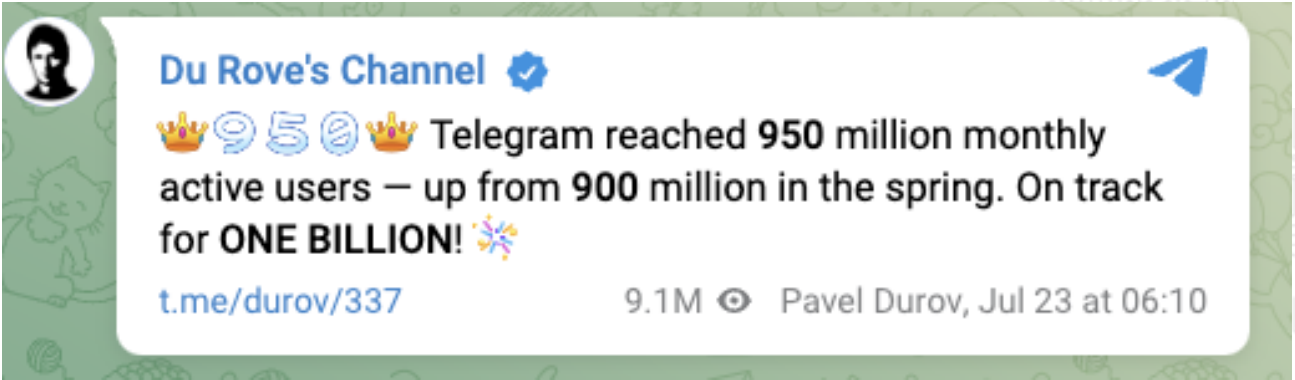
Common Threat Example



The trend to Chat Services



2017



2020 >

Chat Services & Cyber Crime

- Spreading malware
- Hosting malicious content
- Sharing phishing tutorials
- Controlling malware
- Facilitating credit card theft
- Exposing user information
- Developing AI-powered tools for cybercrime

Immediate - Secure - Real-Time - Communities

Telegram founder vows to tackle 'illicit activities' following French arrest

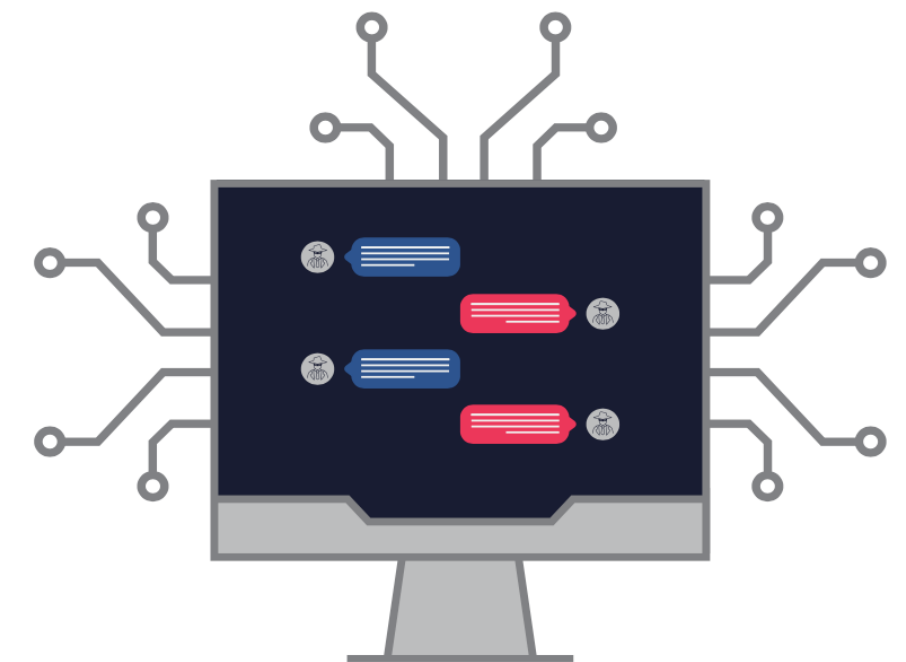
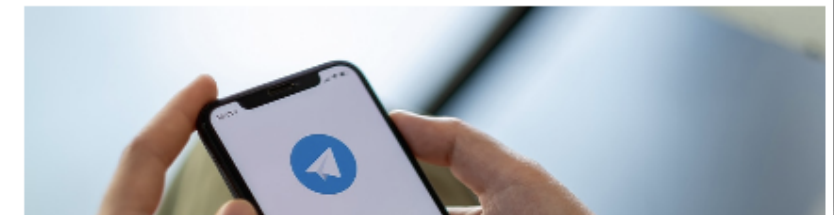
Pavel Durov acknowledges criminal elements on Telegram and announces changes to moderation on the platform.



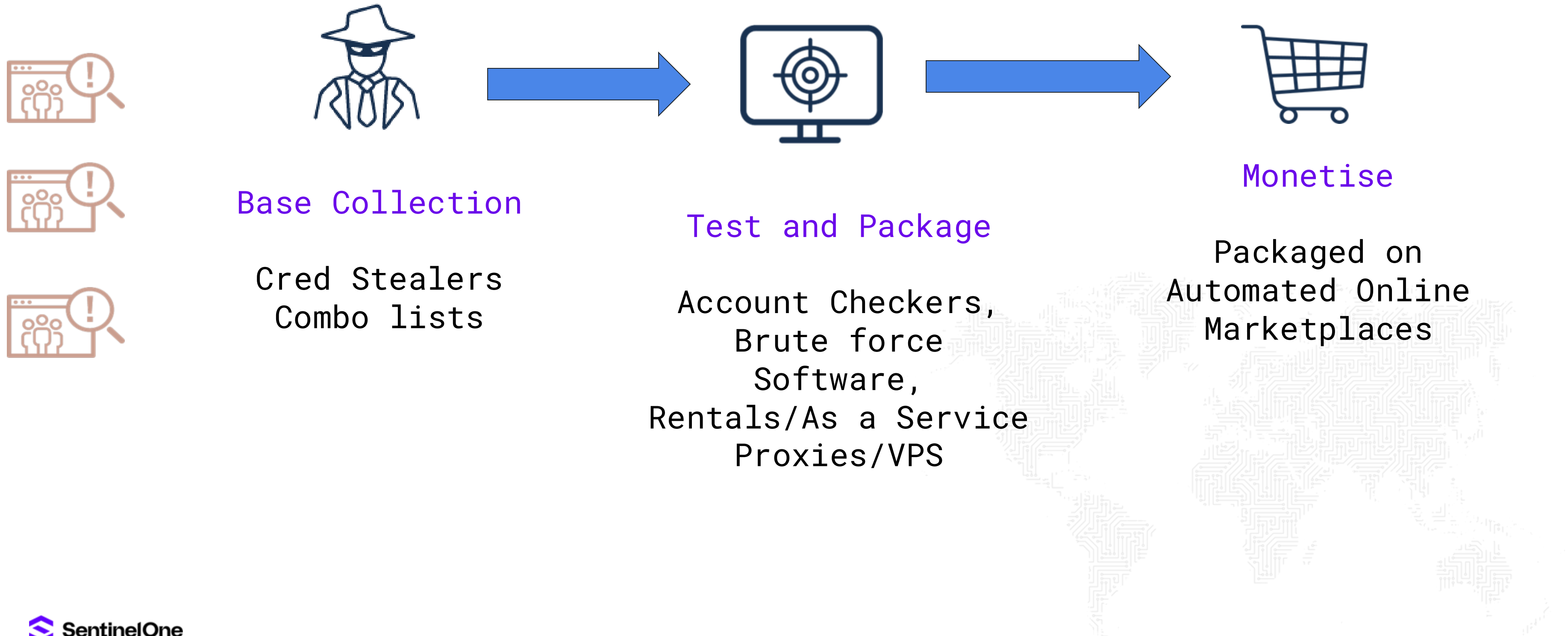
David Hollingworth • Mon, 09 Sep 2024 • CULTURE

SHARE


Russian-born tech entrepreneur Pavel Durov broke his silence late last week, promising changes to Telegram's platform to fight "illicit activities that, he says, are creating a bad image of the platform."




The Credential Economy









REDLINE Стиллер Pro
150,00 \$ – 900,00 \$
Выберите параметры




Dark Crystal RAT
75,00 \$
В корзину




Agrat stealer
100,00 \$ – 260,00 \$
Выберите параметры




Prynt Stealer
50,00 \$ – 1000,00 \$
Выберите параметры




Aurora Stealer
135,00 \$ – 2500,00 \$
Выберите параметры




Meta stealer
150,00 \$ – 1000,00 \$
Выберите параметры




Taurus Стиллер
150,00 \$
В корзину




Stealer BlackGuard 5.0
500,00 \$ – 1200,00 \$
Выберите параметры




Mars Stealer
140,00 \$ – 160,00 \$




AZORult Стиллер
200,00 \$ – 1000,00 \$



Vidar PRO Стиллер
130,00 \$ – 750,00 \$



Raccoon Stealer v2
125,00 \$ – 275,00 \$



REDGlade
Local
Joined: Feb 14, 2020
Messages: 88
Reaction score: 26
Points: 249

Feb 20, 2020

If you purchase HP FORUM OR WARRANTIES OF THE FORUM 20% DISCOUNT FOR ALL KINDS SERVICES

Write only, and only here <https://t.me/REDLINESUPPORT> and require confirmation by PM Forum

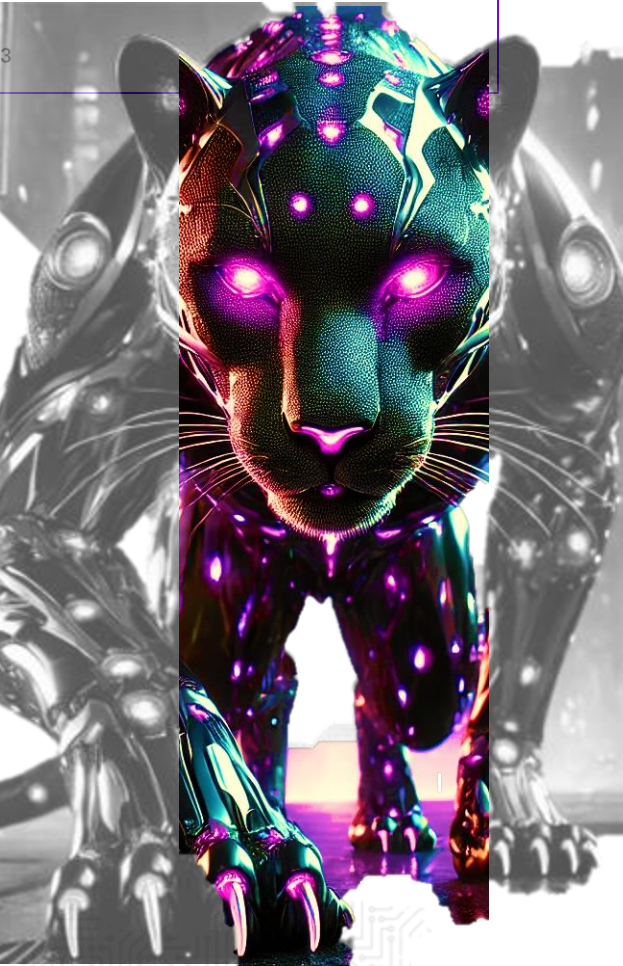
I would like to present you a stealer tailored for convenient work with logs. Collects the most popular information for v in all areas. The program was written taking into account all the wishes of people who are professionally involved in the field of carding.

Build features:

- 1) Collects from browsers:
 - a) Login and passwords
 - b) Cookies
 - c) Autocomplete fields
 - d) Credit cards
- 2) Supported browsers:
 - a) All Chromium-based browsers (Even Chrome latest version)
 - b) All Gecko-based browsers (Mozilla, etc.)
- 3) Collecting data from FTP clients, IM clients
- 4) Customizable grabber file by criteria Path, Extension, Search in subfolders (can be configured to the desired cold wallets, steam, etc.)
- 5) Sample by country. Configuring the blacklist of countries where the build will not work
- 6) Configuring anti-duplicate logs in the panel
- 7) Gathers information about the victim's system:
 - IP
 - Country
 - City
 - Current username
 - HWID
 - Keyboard layouts
 - Screenshot of the screen Screen resolution
 - Operating system
 - UAC settings
 - Is the current build running with rights administrator
 - User-Agent
 - Information about the components of the PC (video cards, processors)
 - Installed antiviruses

Predator AI | ChatGPT-Powered Infostealer Takes Aim at Cloud Platforms

ALEX DELAMOTTE / NOVEMBER 7, 2023



A new malware **#stealer** known as "Ada Stealer" has surfaced on multiple **#Darkweb** forums in October 2024. It first appeared on the Cracked forum on October 1st, and then on October 9th, 2024, it was spotted on other **#darkweb** forums. Here's a rundown of the features of the Ada Stealer as shared (Screenshot#1):

- **Ada Stealer Overview**:**
- "Ada" is an undetected stealer now public after a year of private use.
 - Operations are currently managed via Telegram, but a custom panel is under development.
 - Every stub is heavily obfuscated, and group chat links are protected by a server to prevent direct reporting.
 - User data is stored in memory, leaving no system logs behind.
 - Supports both Chromium and Gecko-based browsers, including lesser-known browsers.
 - Captures browser logs that contain Cookies, Passwords, Credit Cards, and Autofills.
 - Steals data from over 80 crypto wallets,

RedLine Takedown and Arrests (Maxim Rudometov)

OPERATION MAGNUS

On the 28th of October 2024 the Dutch National Police, working in close cooperation with the FBI and other partners of the international law enforcement task force *Operation Magnus*, disrupted operation of the Redline and META infostealers. Involved parties will be notified, and legal actions are underway.



OPENBAAR MINISTERIE

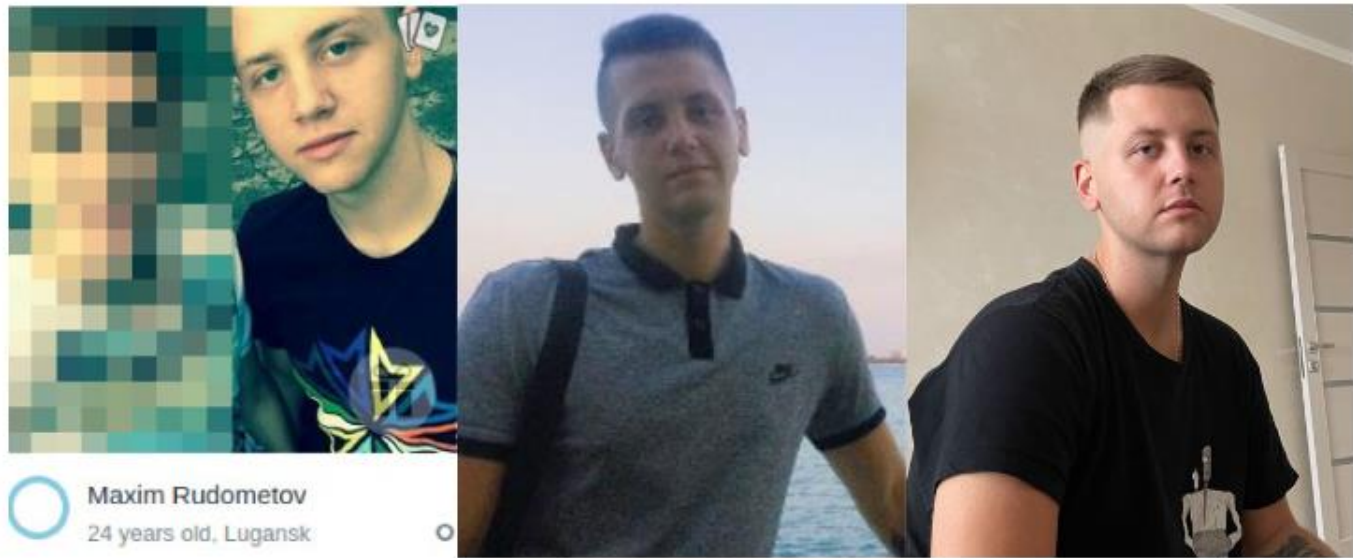


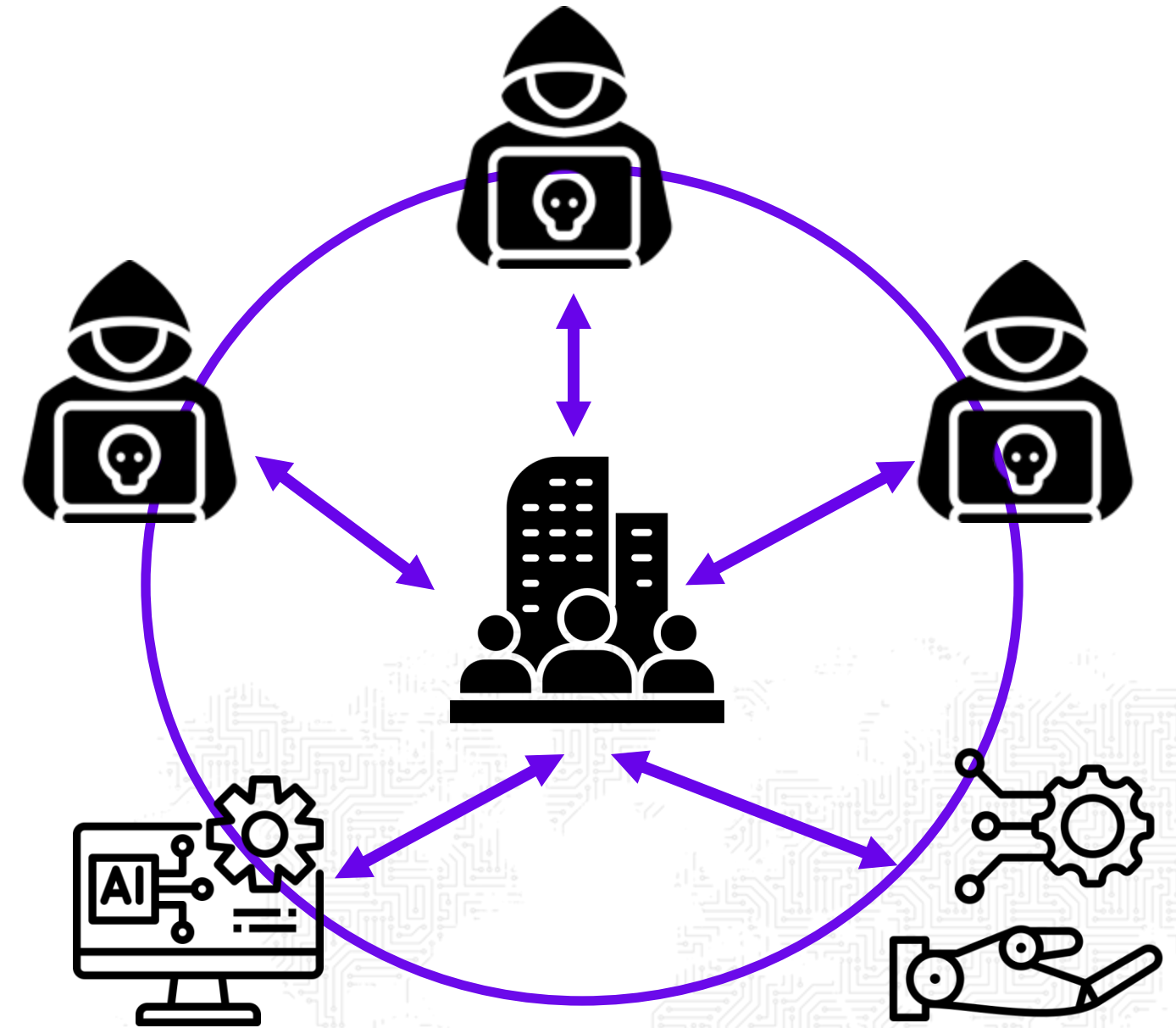
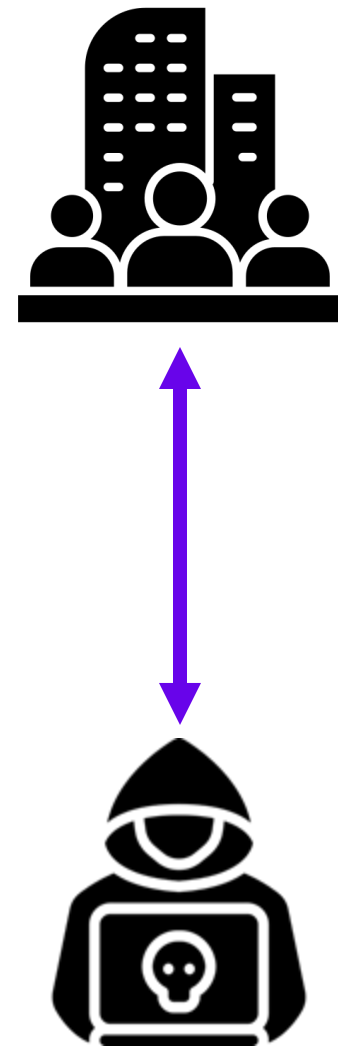
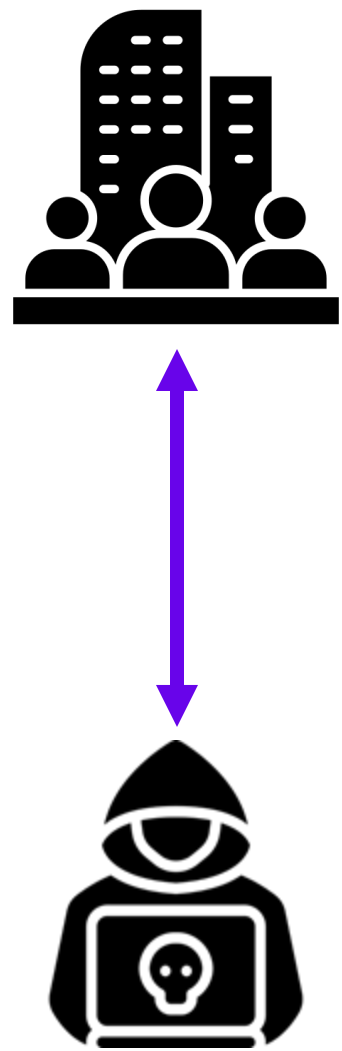
Figure 5: Comparison photos of Maxim; from VK profile (top-left), advertisement for C# stealer training (top-center), an Apple account registered by the Yandex Email Account (top-right), and dating profile (bottom).

Максим Рудомётов (navi_ghacking)



персональный гороскоп
VK
Максим лайкнул 89 человек, всего лайкнул: 105 фоток
Ещё никто не признался в любви, будьте первым.
Получил: 668 лайков от 481 человека.
Заходил в VK: 12.06.2015 10:02:40
обновить
Страница: <http://yourmoneyforppl.blogspot.com/>
День рождения: [redacted] Овен
Подписчиков: 3737 человек
Подписался: 175
Друзей: 55
Профиль зарегистрирован: 11.04.2012 10:11:35
В сети: 9 лет.
Введите ваше сообщение для Максим
оставить сообщение
Анонимно
Фотографий: 9

From Targeted to Automated



Autonomous SOC



Evolution of Security Operations

Early 2000's

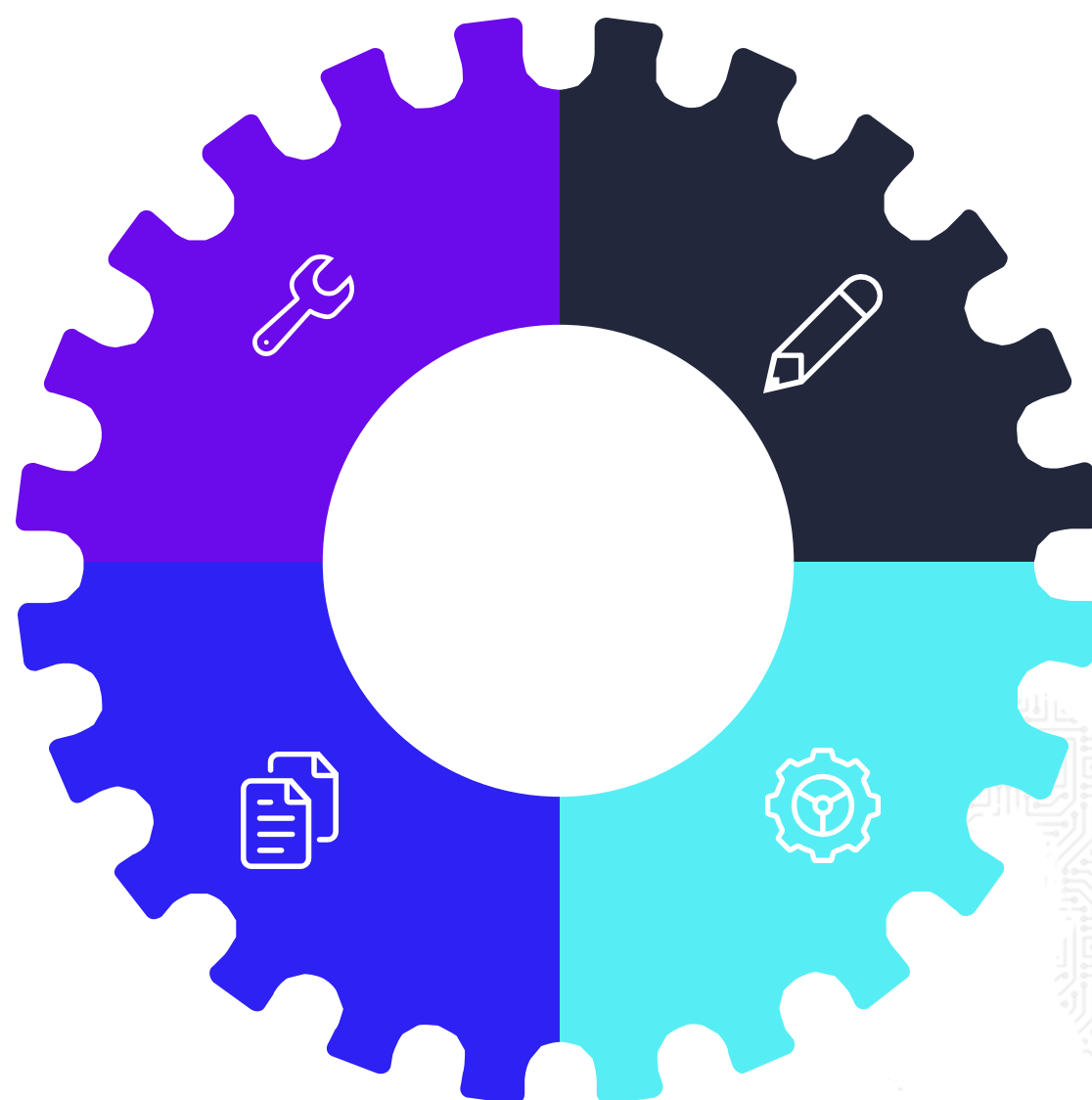
Basic Log Visibility

Tool Explosion and Complexity

2016 to Today

Security Automation

Playbooks and Integrations



2010

Log Platforms and Scripts

Very little detections

2015

Ad-Hoc Automation

Rules Library

Triage

Investigate

Respond

Remediate

Proactive Threat
Hunting



Very Happy



Happy



Neutral



Frustrated



Very Frustrated

The **Frustrating** “Day in the life” of a Security Analyst





SOC Challenge and AI Assistance



- | | | | | |
|---|--|--|--|---|
| <ul style="list-style-type: none">▪ Incomplete Visibility▪ Normalisation | <ul style="list-style-type: none">▪ Anomaly Detection▪ Multi Signal Detection | <ul style="list-style-type: none">▪ Ambiguous Alerts▪ Query Complexity▪ High Skill Threshold▪ Poor Prioritisation▪ Limited Hunting | <ul style="list-style-type: none">▪ Slow Response▪ Limited Automation | <ul style="list-style-type: none">▪ Groundhog Day |
|---|--|--|--|---|



Data Ingestion



Analysis



Investigation



Action



Improvement



- | | | | | |
|---|--|--|---|--|
| <ul style="list-style-type: none">▪ Rogue Detection of data sources▪ Intelligent Parsing | <ul style="list-style-type: none">▪ Behavioural Analysis▪ Automated Correlation▪ Threat Intelligence | <ul style="list-style-type: none">▪ Contextual Awareness▪ Natural Language Queries▪ Guided Investigations▪ Risk Assessment▪ Guided Hunts | <ul style="list-style-type: none">▪ Decision Support▪ Automated Response | <ul style="list-style-type: none">▪ Self-Improvement |
|---|--|--|---|--|

Reimagining the Way the SOC Works

Incident Response

Accelerates incident responses
with automated playbooks

Automated Workflows

Reduces manual intervention

AI-Enhanced Alerts

Identifies patterns and
anomalies



Ingestion

Detect threats on ingestion.
Use connectors for expanded
visibility. OCSF Native
support.

Dashboards

Provides comprehensive views
of events

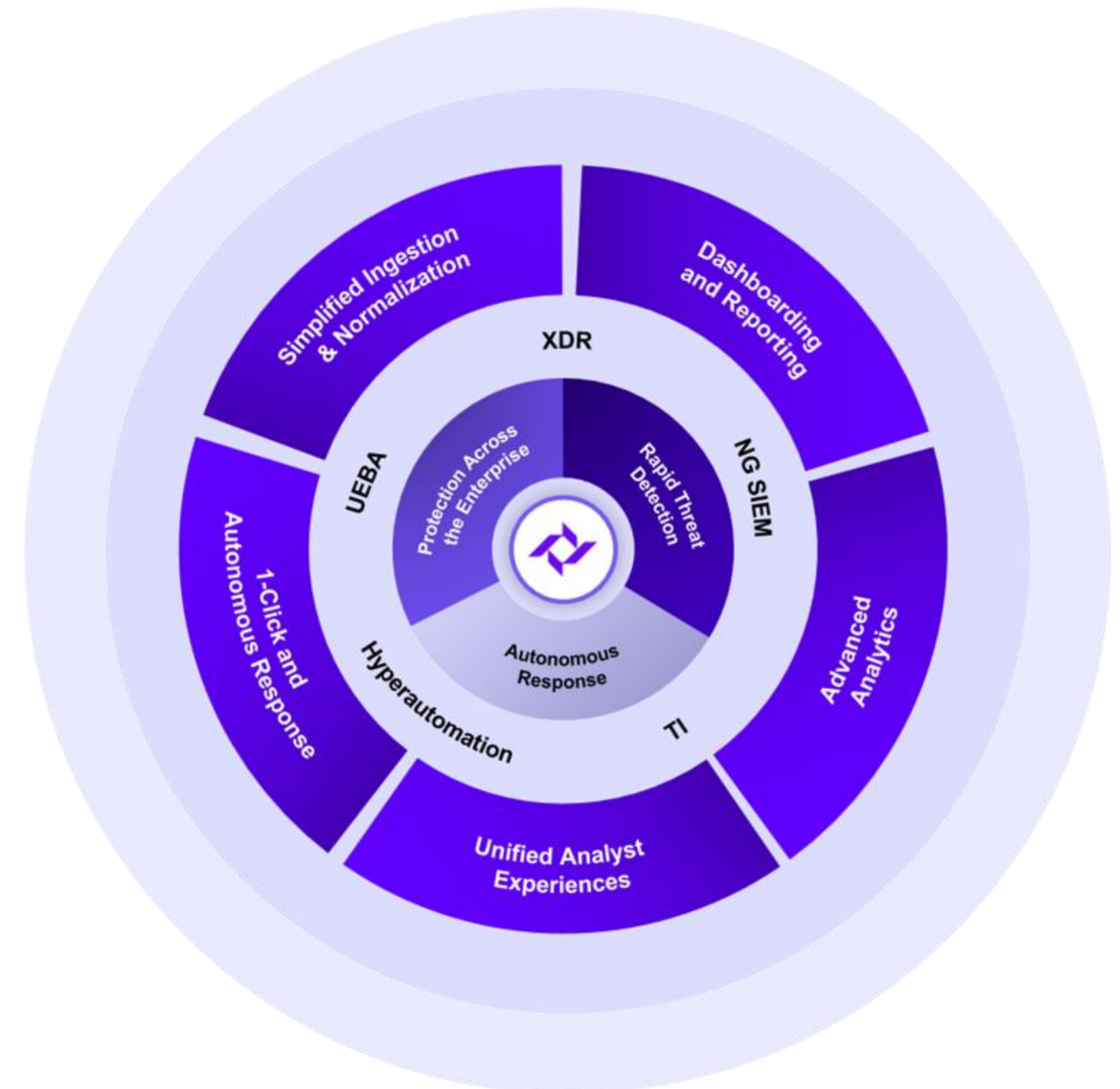
Threat Intelligence

Stays up-to-date on the latest
threats and vulnerabilities

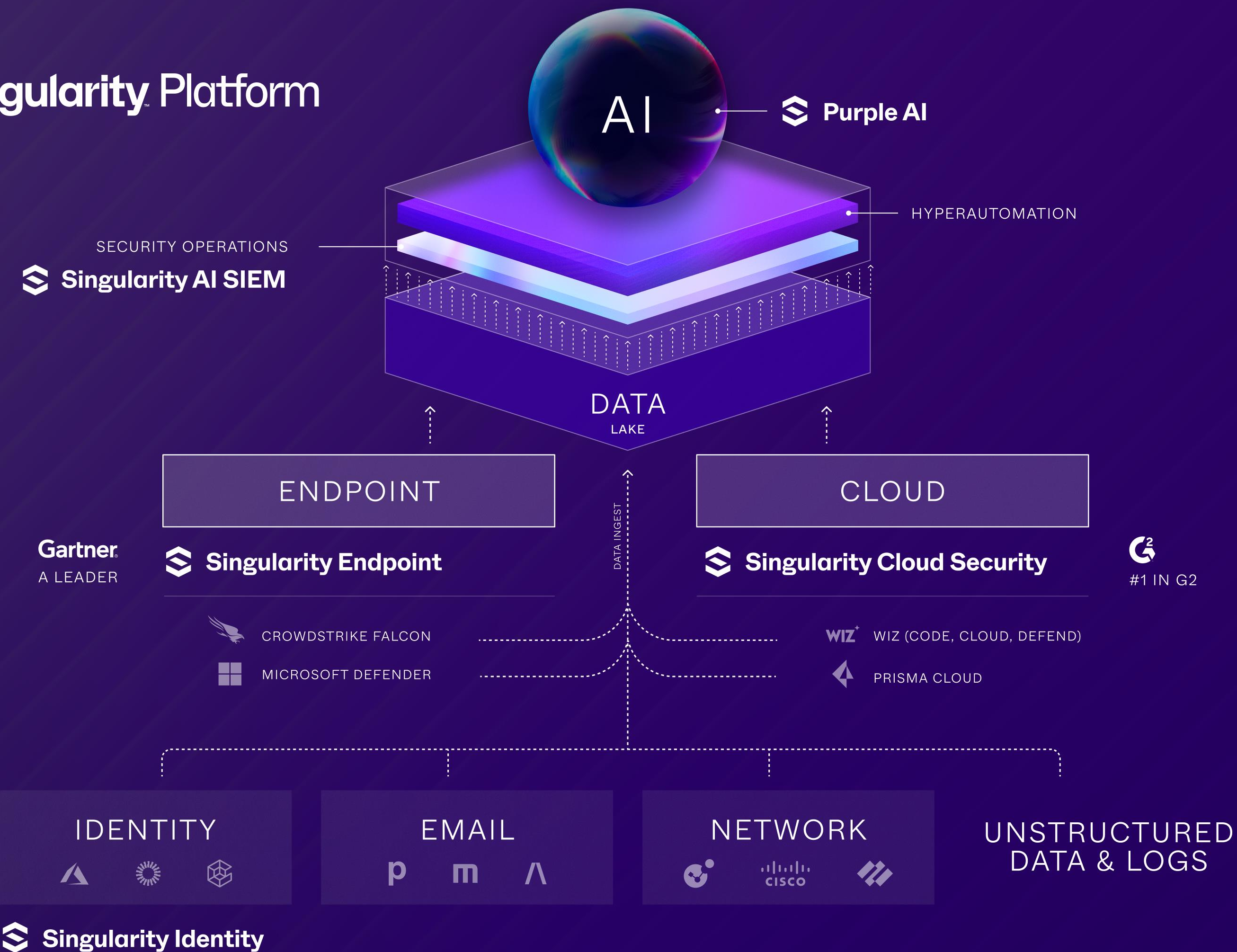
Singularity AI SIEM

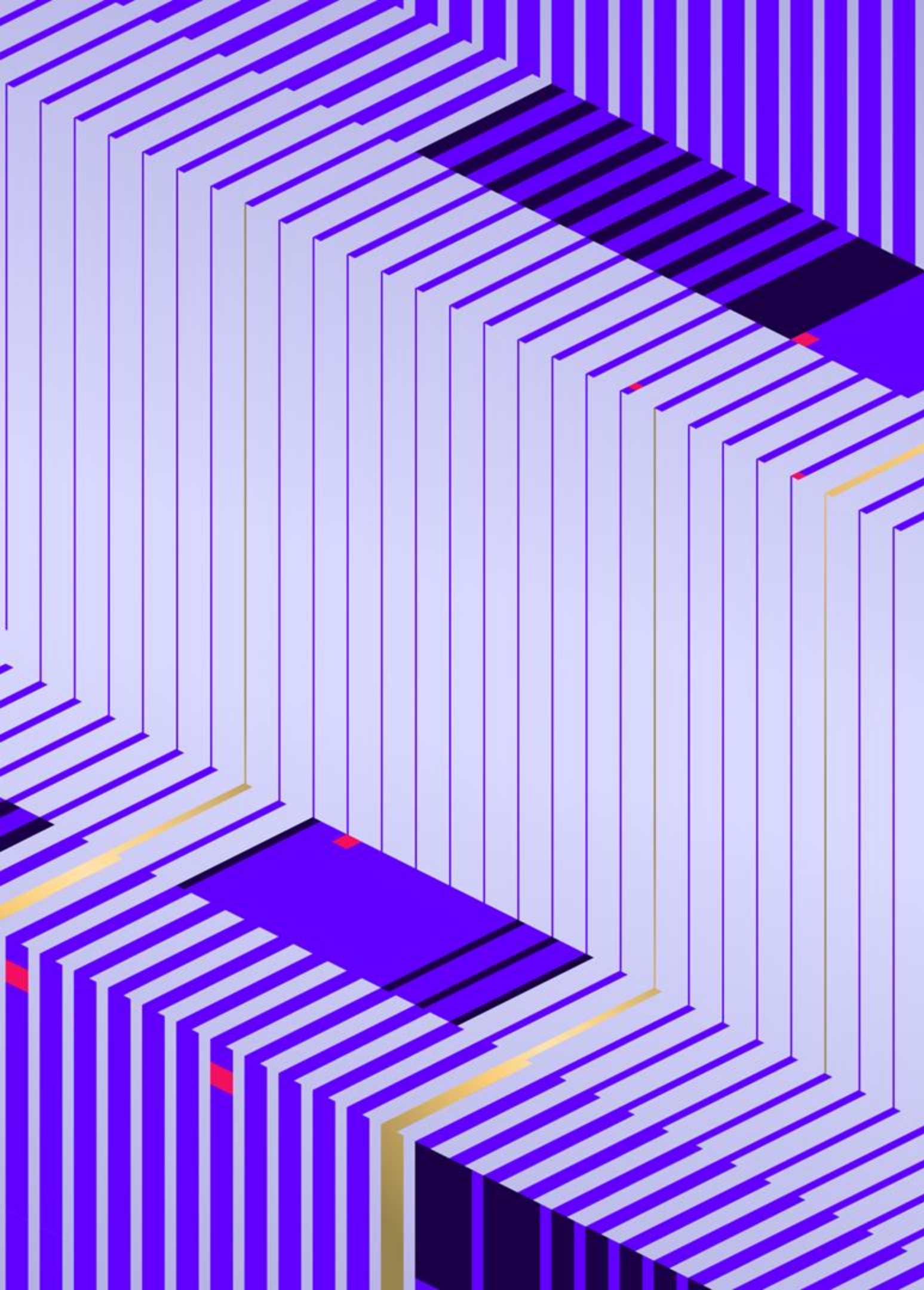
Simplified, Autonomous Security Operations

- **One Security Operations Platform**
streamlining daily operations with converged SecOps capabilities delivering comprehensive protection and efficiency.
- **One Data Architecture**, unifying every endpoint, identity, cloud, 3rd party data source for seamless integration, comprehensive visibility, speed, and scale.
- **One User Interface** with centralized security operations workflows to enhance security posture and enable rapid threat detection and response.



Singularity Platform





Sentinelone.com