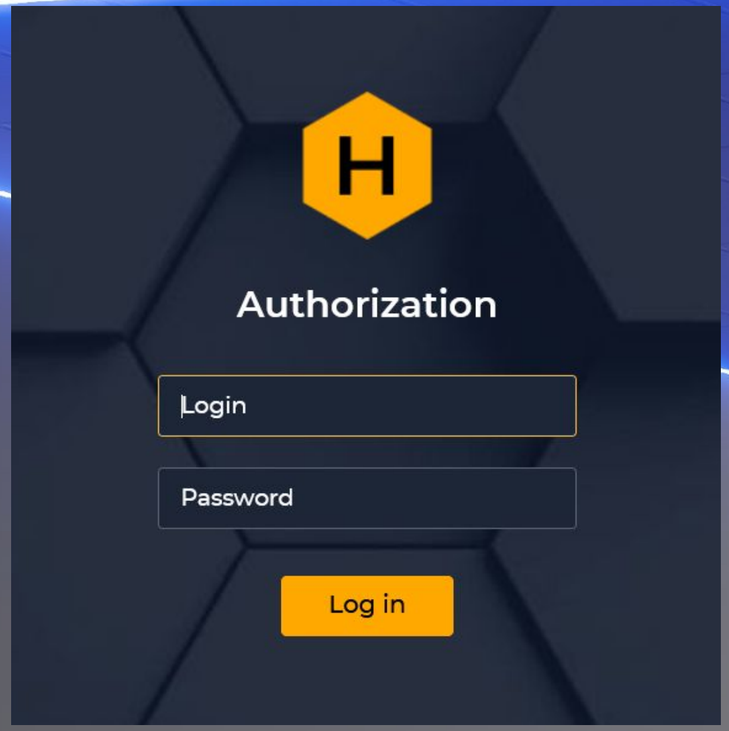
GROUP-IB



Inside the HIVE - LAC (Latin America & Caribbean)

Jesper Jurcenoks & Svetlana Ostrovskaya, FIRST May 4, 2022

GROUP-IB

Jesper Jurcenoks
Head of CyberSecurity
(CERT, DFIR, XDR,MDR)

t:@jesperjurcenoks
linkedin.com/in/jurcenoks

Svetlana Ostrovskaya
Principal DFIR Analyst

linkedin.com/in/lana-ostrovskaya/

Group-IB: 19 years of DFIR

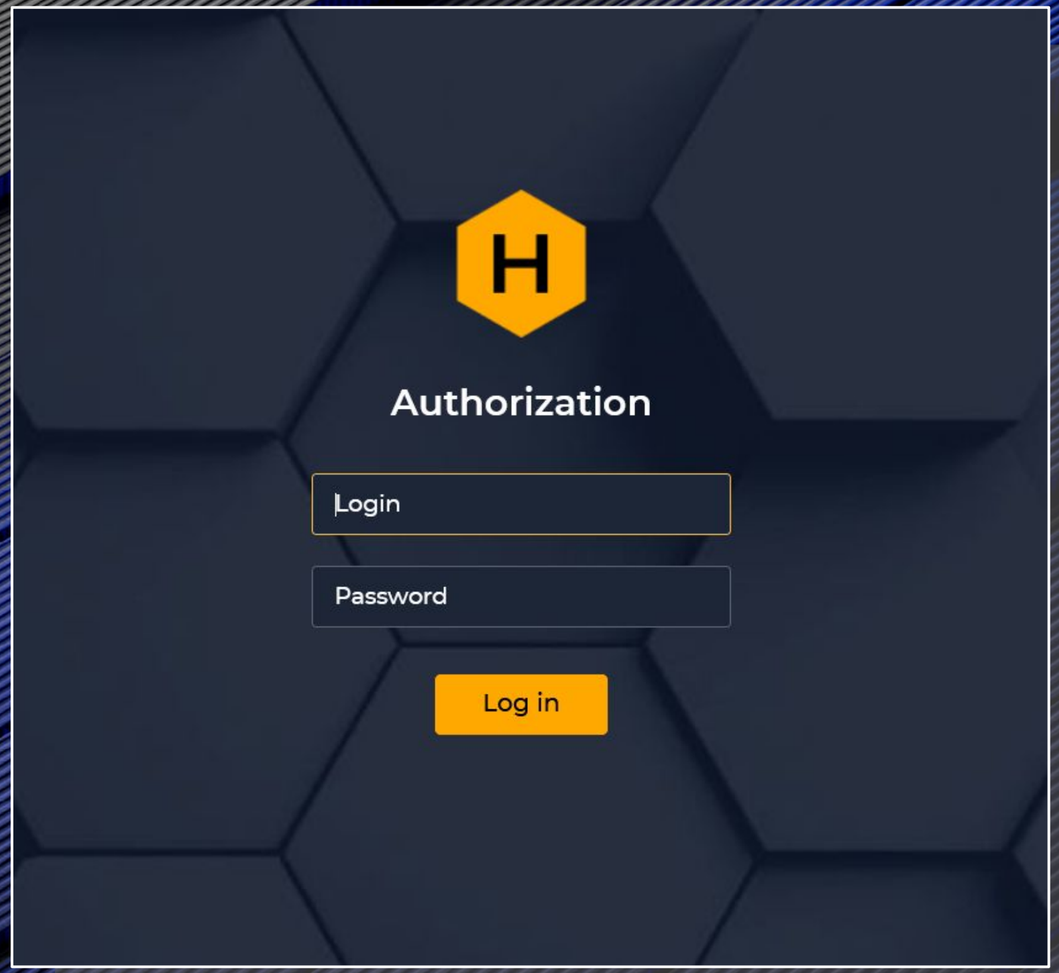
Ransomware in LAC Grew 127% 2020-2021

Focus on HIVE

Finance **Transport** InfoTech

Brazil

26.APR.2022



How do we know this?

How to we fight this?

Ransomware Kill-Chain - RaaS Extortion Chain

Cyber Kill-Chain - By Affiliate

Stage 1 - Outside network | **Stage 2 - Inside network** | **Stage 3**

Extortion Chain - By RaaS

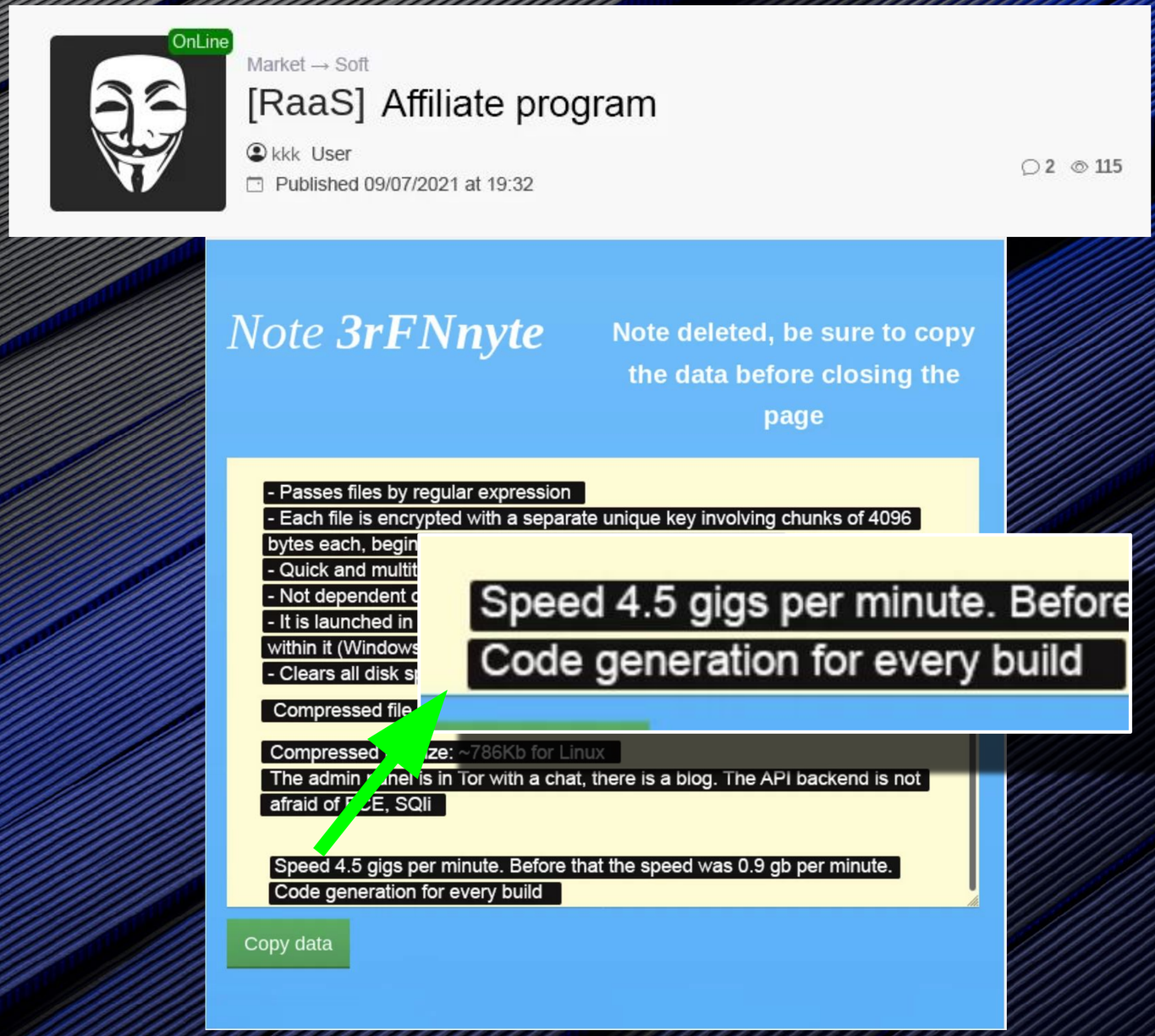
Negotiation | **Payment** | **Decryption**

Loot Split 80/20

24% of HIVE Victims Pay

HIVE’s Sales Pitch

1. Strong Encryption
2. Small encryptor file size
3. Low AV Detection Rate
4. Fast Encryption speed
5. Admin Panel
6. API
7. Live Chat support
8. Hive for VMWare ESXi
9. Double Extorsion with support for Data Leak Sites



Tracking HIVE activity

1) Most times the hacker downloads compromising information before encrypting, for later Blackmail in case on non-payment (Double Extorsion)

   13.5% of customers are exposed on HIVE Data Leak Site (DLS)

2) We fund a vulnerability in the Admin Panel, which allows us to enumerate all the victims worldwide 😉

The Demographics of the Hackers using HIVE RaaS

Unlike BlackCat RaaS which also does Attacks, HIVE is solely focused on RaaS.

Attack distribution and toolset (Estimate):

5%	State Actors	Own Distinct Tools
20%	Large Criminal Groups	
75%	Small Independent Hackers/Groups	Off-the-shelf tools: Cobalt Strike MetaSploit

HIVE Affiliates

GROUP-IB

Real-life DFIR on HIVE

by Svetlana Ostrovskaya

THE STORY BEGINS

- Windows infrastructure and VMWare ESXi nodes are encrypted
- The majority of servers and hosts are down
- Everyone is in a panic

HIGHLIGHTS

RDP session

Non-privileged user, no source IP

SystemBC

Collection of system info, execution of scripts, commands, executable files

PowerShell

PowerShell scripts to download some malicious payloads

Shellcode

Shellcode to download Cobalt Strike

RDP

To move laterally

PC Hunter

To avoid detection

SSH

ESXI shell was enabled to access ESXI nodes

SCP

To move ransomware to ESXI nodes

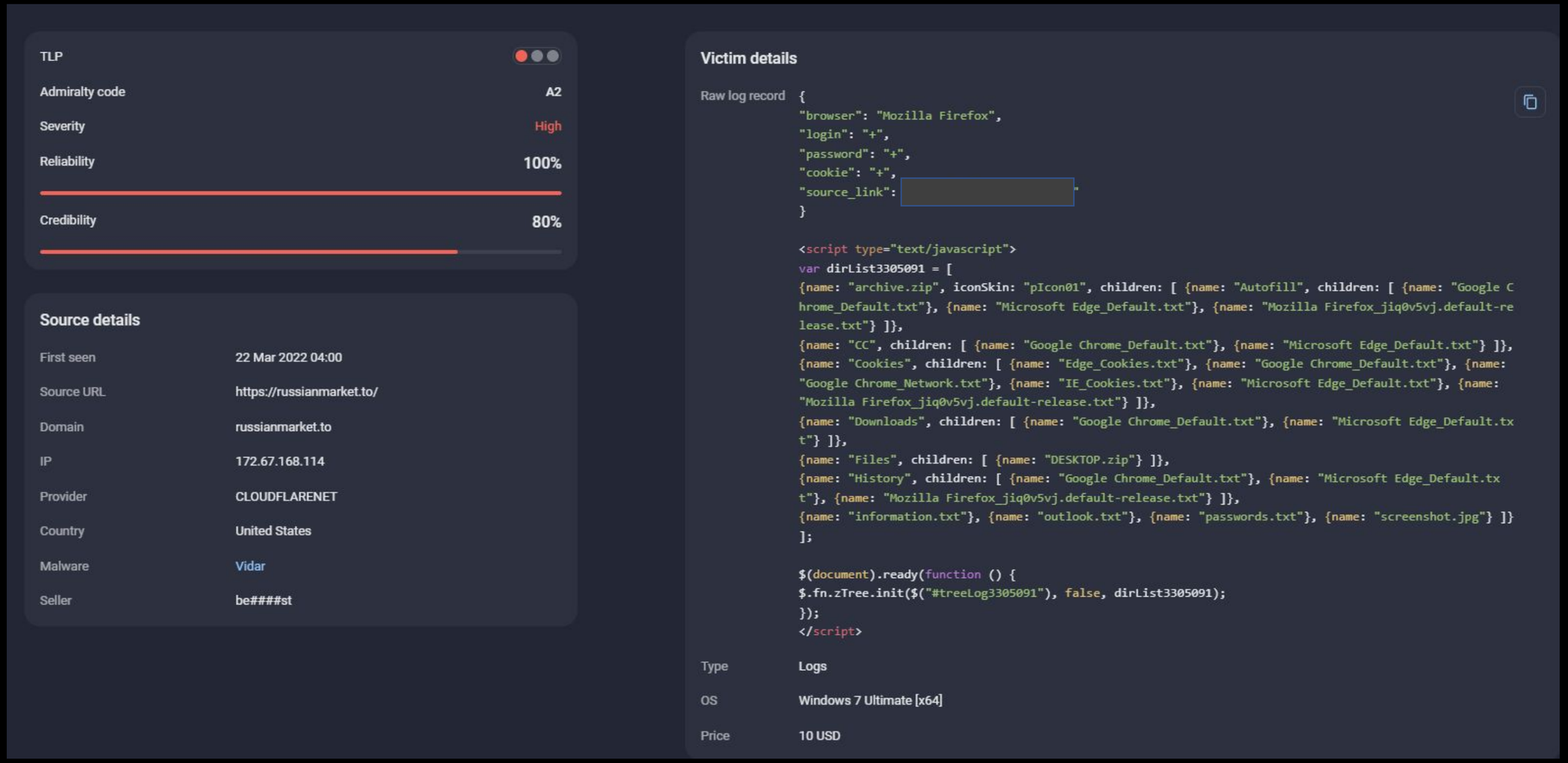
MYSTERY - How did they get in?

Vulnerable RDP

Phishing

VPN

SOLVED - RDP Credentials for Sale beforehand



TLP

Admiralty code A2

Severity High

Reliability 100%

Credibility 80%

Source details

First seen	22 Mar 2022 04:00
Source URL	https://russianmarket.to/
Domain	russianmarket.to
IP	172.67.168.114
Provider	CLOUDFLARENET
Country	United States
Malware	Vidar
Seller	be####st

Victim details

Raw log record

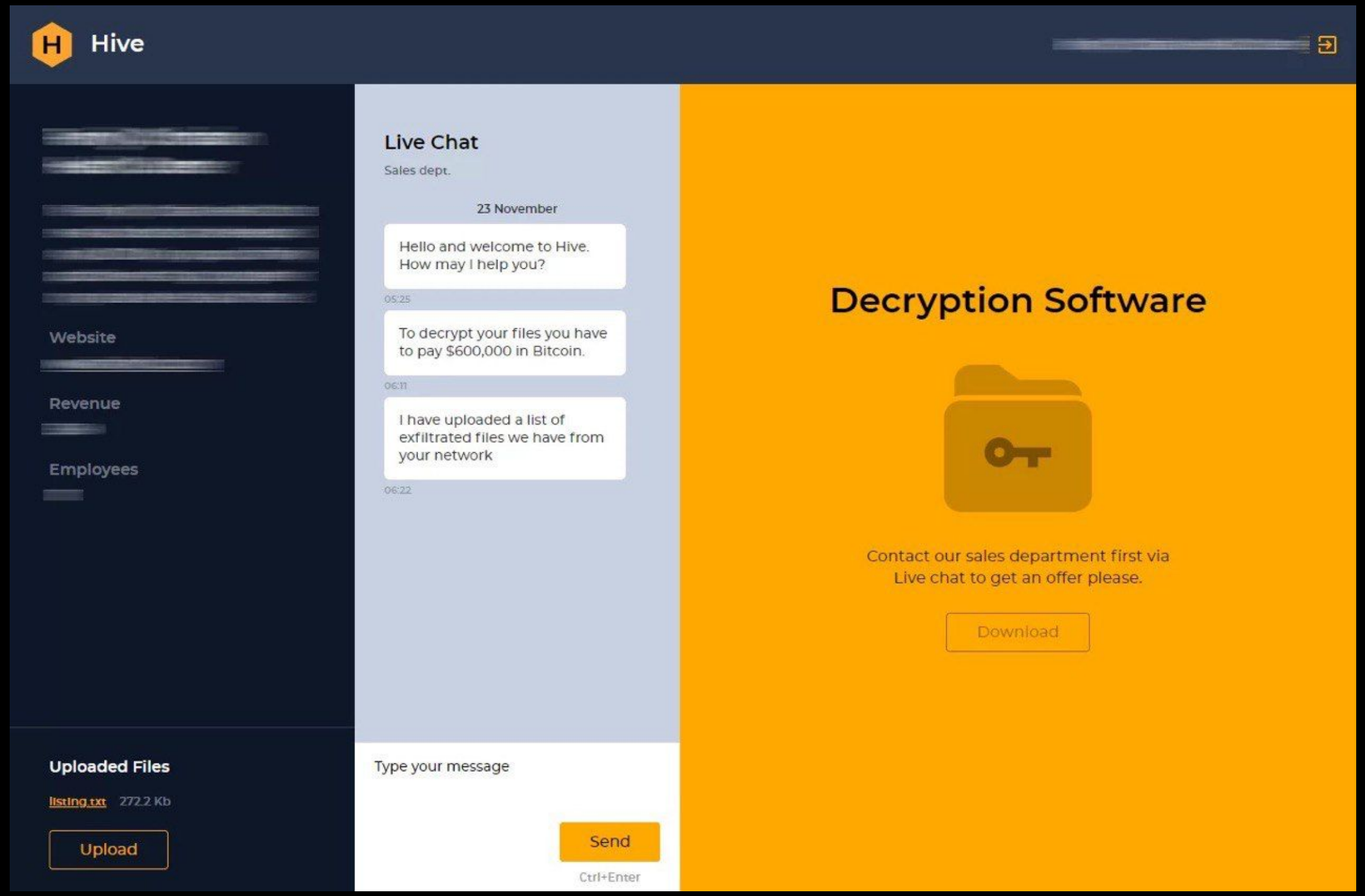

```
{
"browser": "Mozilla Firefox",
"login": "+",
"password": "+",
"cookie": "+",
"source_link": [redacted]"
}

<script type="text/javascript">
var dirList3305091 = [
{name: "archive.zip", iconSkin: "pIcon01", children: [ {name: "Autofill", children: [ {name: "Google C
hrome_Default.txt"}, {name: "Microsoft Edge_Default.txt"}, {name: "Mozilla Firefox_jiq0v5vj.default-re
lease.txt"} ]},
{name: "CC", children: [ {name: "Google Chrome_Default.txt"}, {name: "Microsoft Edge_Default.txt"} ]},
{name: "Cookies", children: [ {name: "Edge_Cookies.txt"}, {name: "Google Chrome_Default.txt"}, {name:
"Google Chrome_Network.txt"}, {name: "IE_Cookies.txt"}, {name: "Microsoft Edge_Default.txt"}, {name:
"Mozilla Firefox_jiq0v5vj.default-release.txt"} ]},
{name: "Downloads", children: [ {name: "Google Chrome_Default.txt"}, {name: "Microsoft Edge_Default.tx
t"} ]},
{name: "Files", children: [ {name: "DESKTOP.zip"} ]},
{name: "History", children: [ {name: "Google Chrome_Default.txt"}, {name: "Microsoft Edge_Default.tx
t"}, {name: "Mozilla Firefox_jiq0v5vj.default-release.txt"} ]},
{name: "information.txt"}, {name: "outlook.txt"}, {name: "passwords.txt"}, {name: "screenshot.jpg"} ]}
];

$(document).ready(function () {
$.fn.zTree.init($("#treeLog3305091"), false, dirList3305091);
});
</script>
```


Type Logs

OS Windows 7 Ultimate [x64]

Price 10 USD

What about decryption?



Some IOCs

Files
sk.zip
sk.exe
xxx.exe
PCHunter64.exe
a2122.exe
a42_34.exe.sa

C2
93[.]115.29.50:443
192[.]53.123.202:443
http://46[.]166.169.34:80/asdfg
http://185[.]8.105.112:80/asdfg

What to do if hit by Ransomware

1. Create memory dump if encryption is in progress
2. Isolate network
3. Call for help (to have proper incident response)
4. Start remediation activities
5. Improve your security

Expert Level info

SHA 256 hashes for all known versions of HIVE Encryptor
Version 1.0 - 5.2
OS: Windows, Linux, ESXi
Samples include: Encryptor, Dropper, Decryptor

https://github.com/rivitna/Malware/blob/main/Hive/Hive_samples.txt

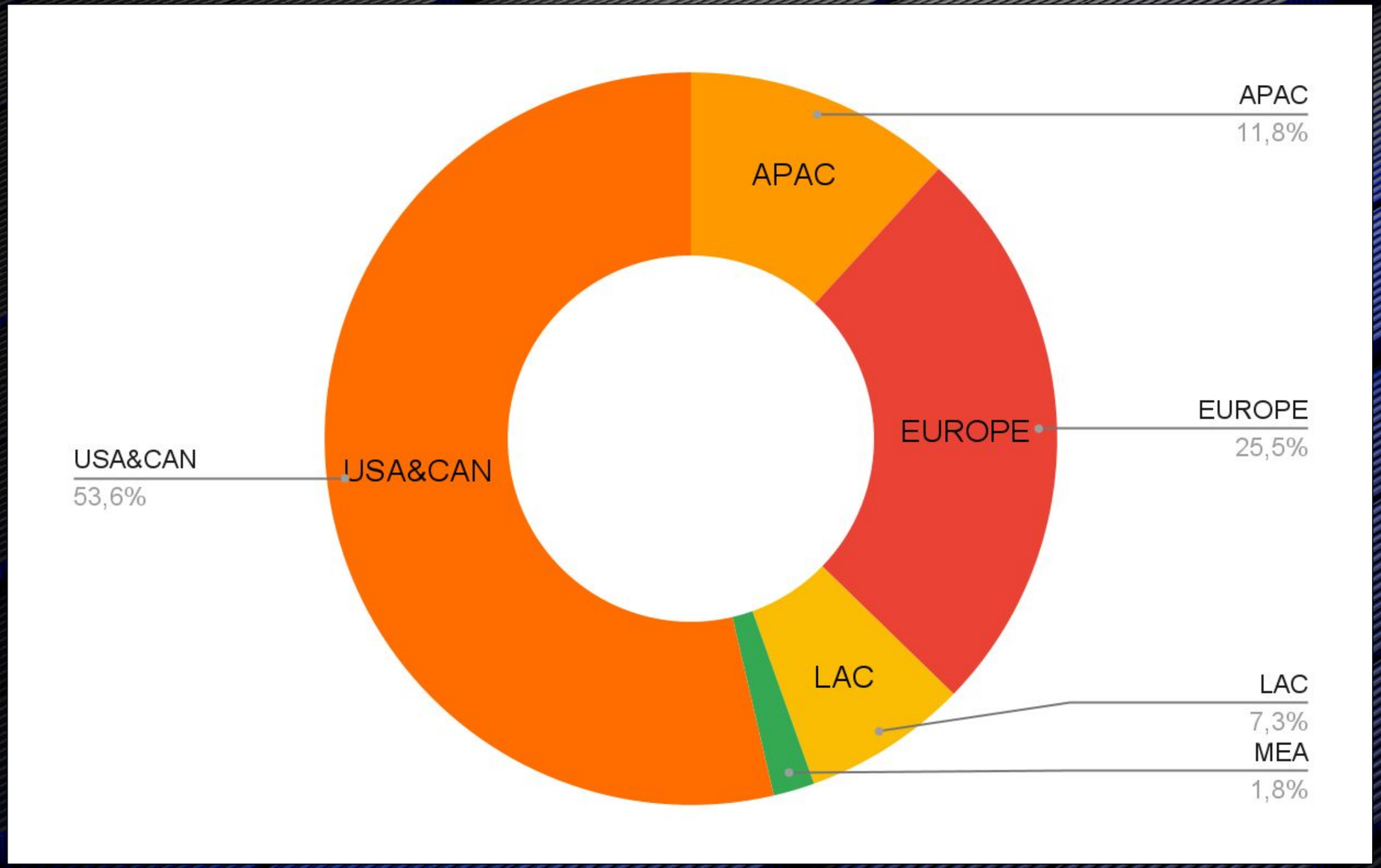
HIVE 5.2	f5d1acc98d62b3a3bfc640bfafd3144fa66112470512e26197cc9b643e438a0e

Use the hashes to download binaries from malware repositories like Virustotal for your own research and hidden nuggets

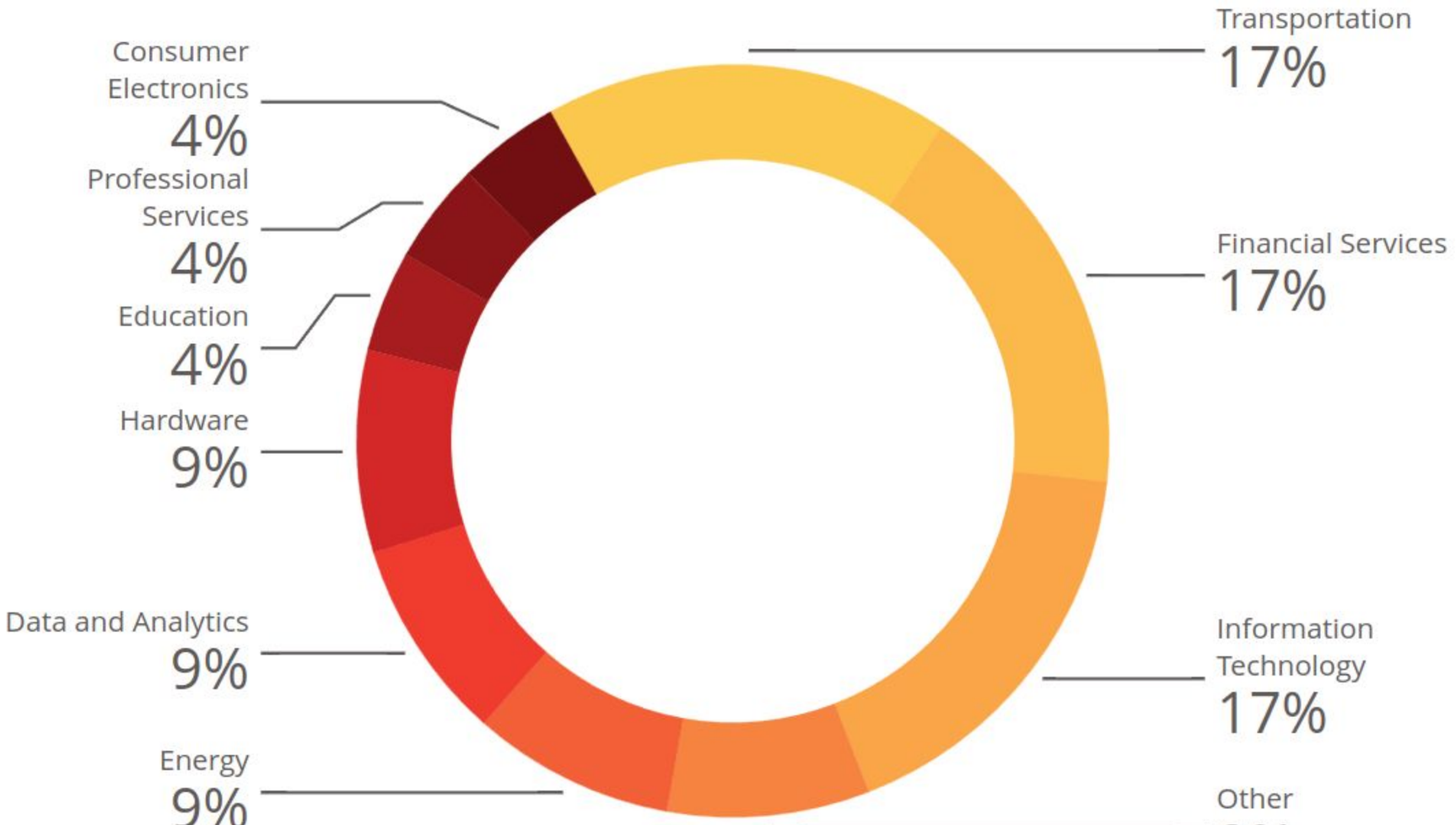
GROUP-IB

HIVE activity in LAC

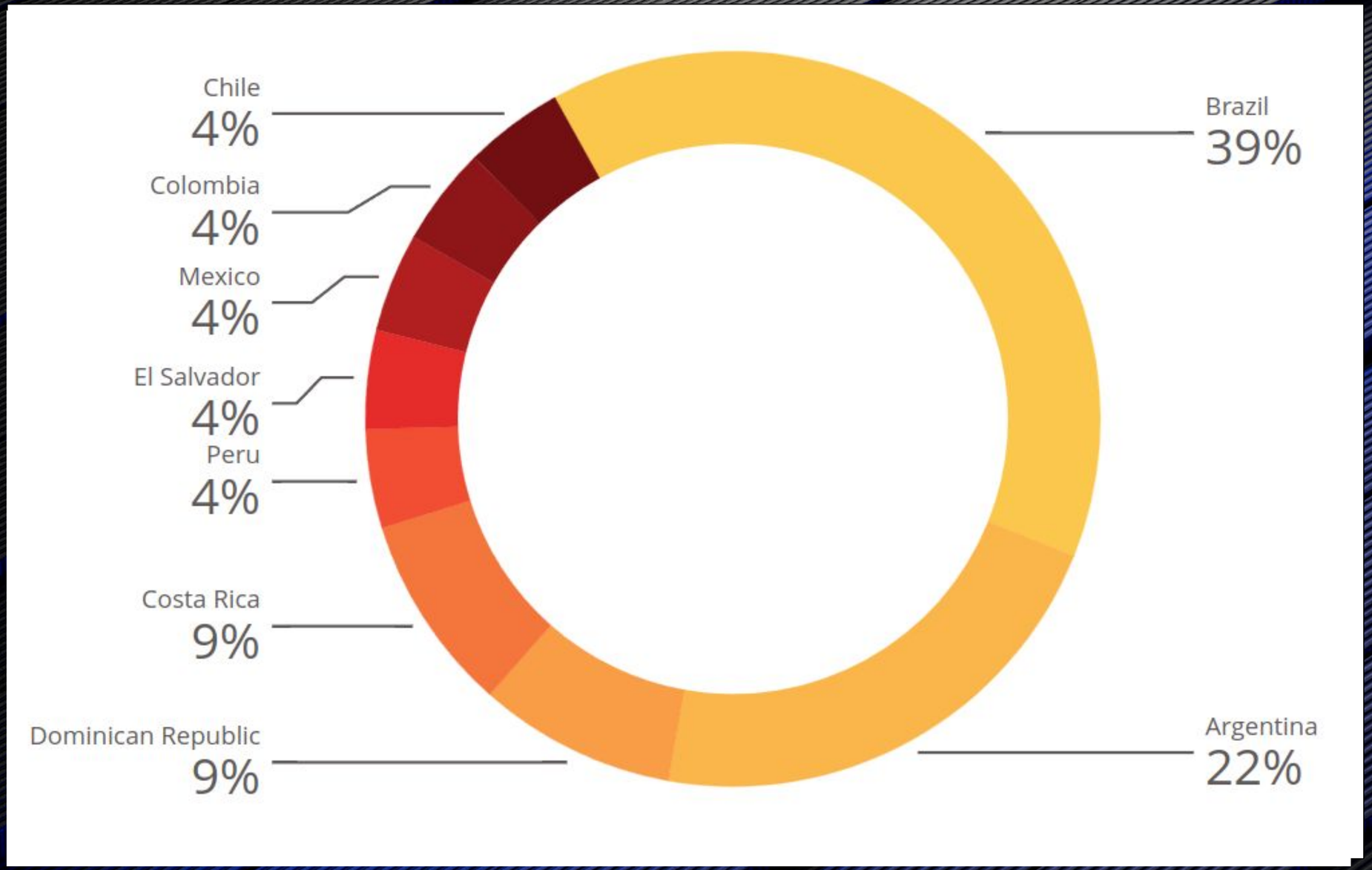
LAC represents 7.3% (Data Leak Sites)



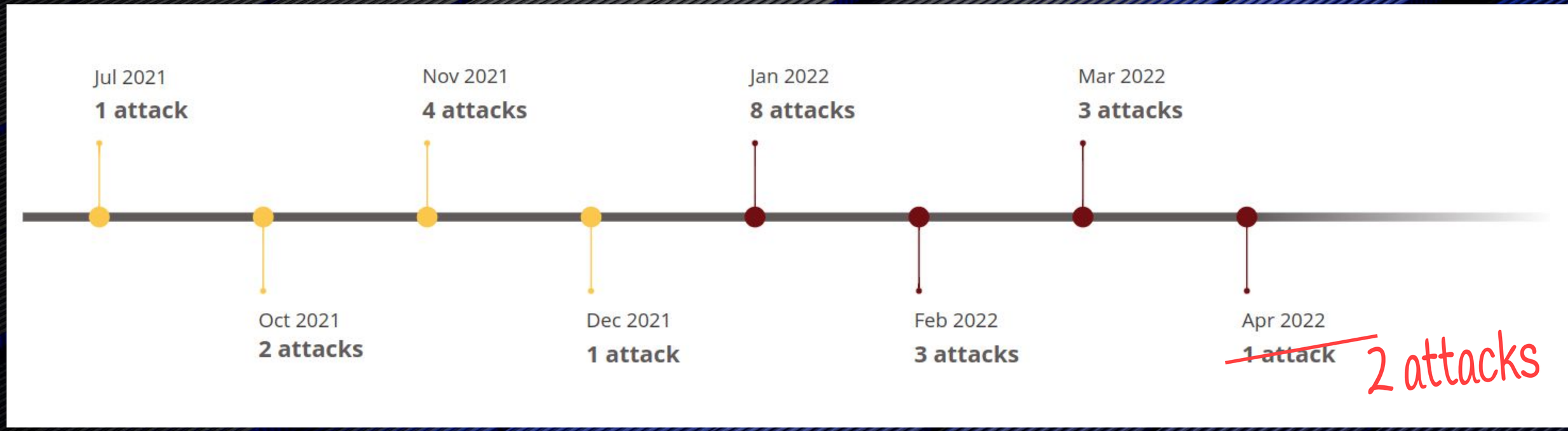
LAC Industry Break down (All sources)



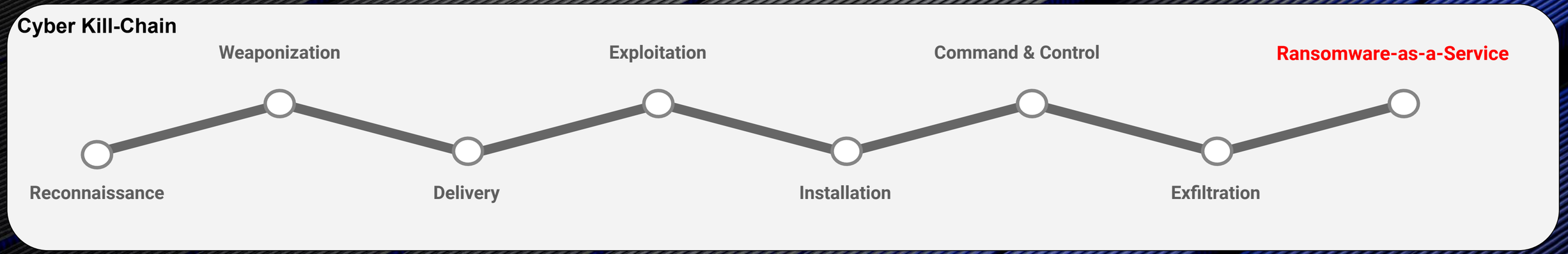
LAC Countries (All sources)



LAC HIVE Timeline



Ransomware Kill-chain

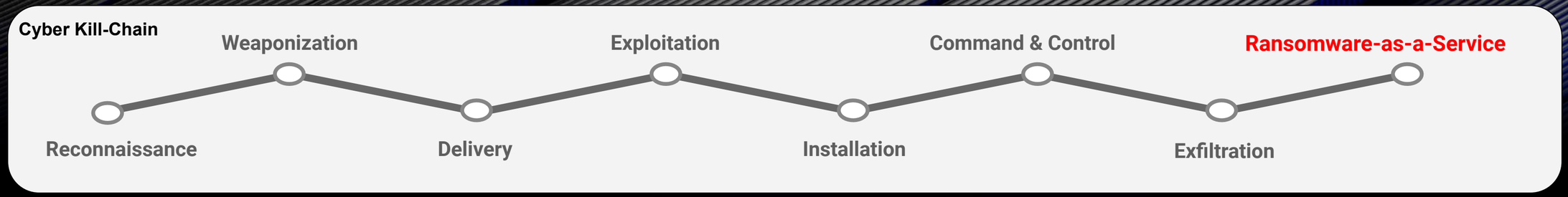


Stage 1	Stage 2	Stage 3

Average time in Stage 2 inside the network of before Encryption: **13 Days**

Time for Group-IB to detect 50% of Compromises: **<24 Hours**
Time for Group-IB to detect 99.9% of Compromises: **5 days**

Response to Ransomware for the individual org.



Stage 1

- Threat Intel on Targeted Recon,
  - Ransomware groups favorite Vulns
  - Detections of Major Raas service pre-encryption
- Track Exposed Assets - Both Direct and in the supply chain (47% of attacks)
- Business Email Protection, Malware Detonation
- NTA Detect “Soft
  of attacks) and C

Stage 2

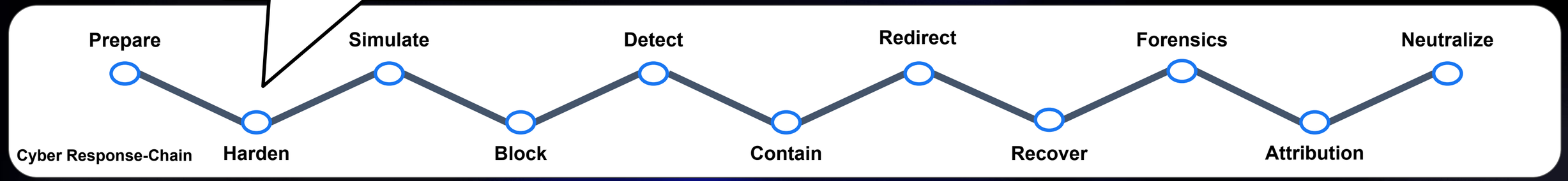
- EDR
  - Persistence
  - Windows Scripting
  - Application shimming
  - Powershell
  - Processes started from Office Programs
  - Procdump of lsass (31%)
- NTA
  - East-west spreading, ADFind (51%)
  - C&C traffic over covert channels

Stage 3

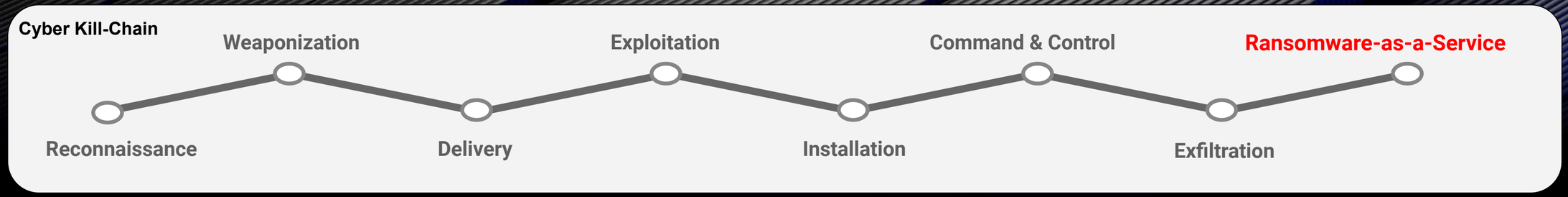
- EDR:
  - Detect and Block HIVE executable
  - Data Leak Prevention
  - End-point isolation
- DFIR
  - Attribution
  - Deanonymize
  - Report to InterPol, Europol

Off-line (and off-site) Backups

Pre-comp | **ntra-compromise Response** | **Post-compromise Response**



Response to Ransomware for the individual org.



Stage 1

- NTA On ISP Backbone
  - Detect “SoftPerfect Network Scanner” (71% of attacks) and Cobalt Strike (57%)
- Threat Intel:
  - Our Global sensors detect scanning activity targeting LACNIC Ranges
- BEC:
  - ISP Level Email url and attachment malware detection (Cobalt Beacon)

Stage 2

- EDR
  - Multi-customer ISP Level managed deployment
- NTA in SD-Wan/SASE
  - East-west spreading, ADFind (51%)
  - C&C traffic over covert channels
  - DNS resolution of suspicious domains

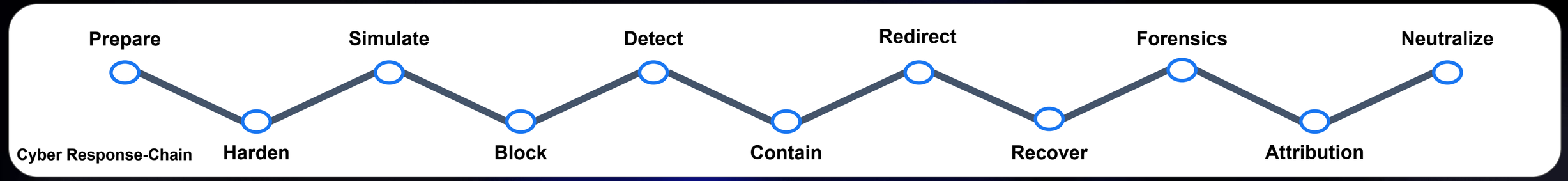
Stage 3

- DFIR
  - ISP provided DFIR, Forensics, Attribution and Neutralization backed by World Class Provider.

Pre-compromise Response

Intra-compromise Response

Post-compromise Response



Group-IB Tracks 51 “Ransomware as a Service” groups

Good News: Many groups have ceased operations and after the leaders behind REvil got arrested in January 2022, several smaller independent hackers who had used REvil’s RaaS also exited the Ransomware business.

Bad News: The number of Ransomware victims is unchanged so the remaining threat actors have grown to fill the vacuum.

As of May 2, we know 23 active RansomWare as a Service groups which hit victims in the previous 30-day period

More in HI-TECH CRIME TRENDS 2021/2022 PART II “**Corporansom**”

In Conclusion

We hope this has been an informative insight into:

- Ransomware-as-a-service in general
- HIVE Ransomware in particular
- Tools for fighting Ransomware
- How to respond to Ransomware

GROUP-IB

Jesper Jurcenoks
Head of CyberSecurity
(CERT, DFIR, XDR,MDR)

t:@jesperjurcenoks
linkedin.com/in/jurcenoks

Svetlana Ostrovskaya
Principal DFIR Analyst

linkedin.com/in/lana-ostrovskaya/

Happy Hunting

GROUP-IB

For Help on Ransomware attacks including:

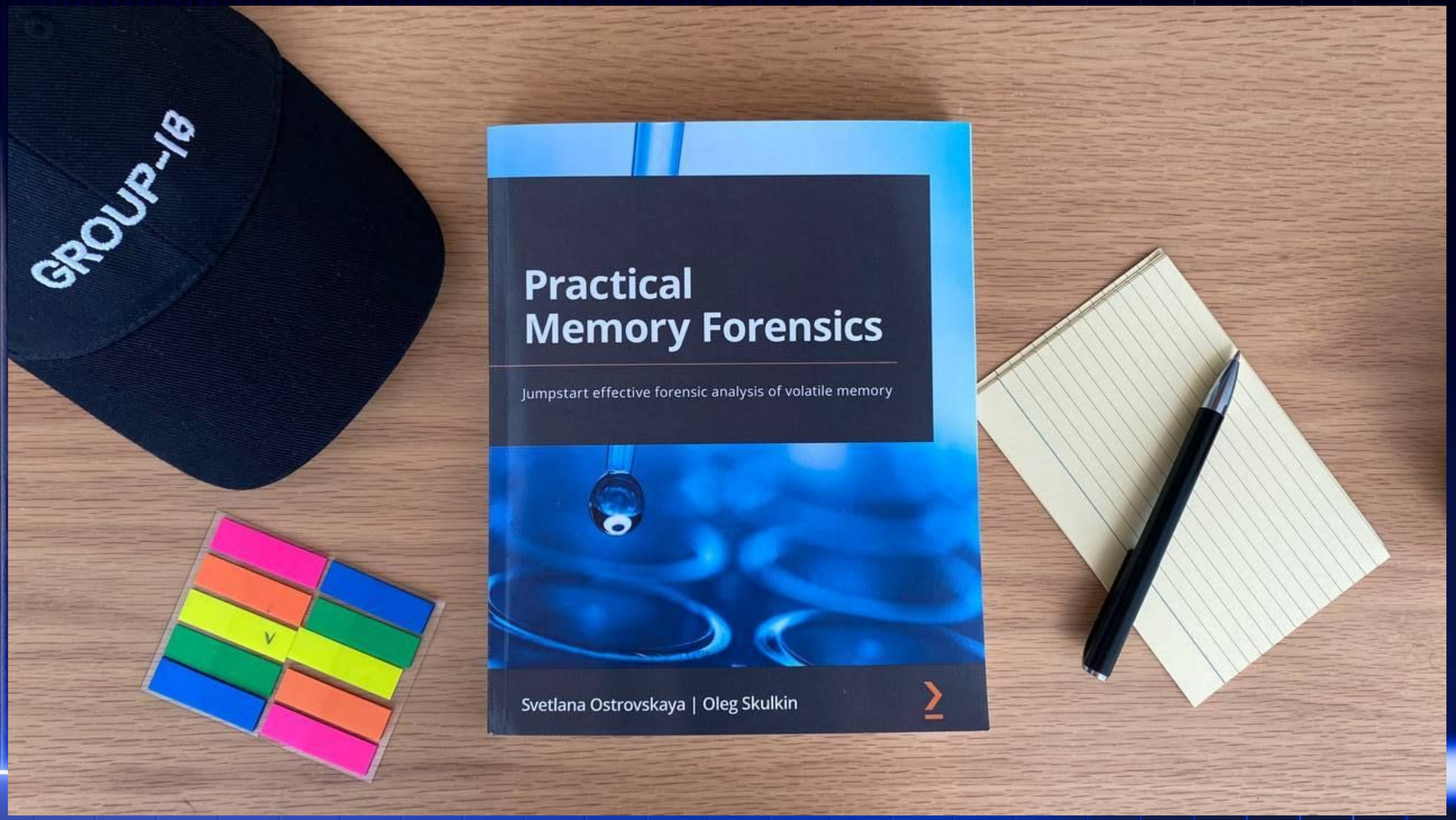
- Training for Digital Forensics Incident Responders, Threat Hunters
- ISP Level Malware traffic pattern detection
- Multi-region centralized ISP Level Malware detonation
- Latin America Country and Industry specific Threat Intel

Please contact Jesper Jurcenoks on

jurcenoks@group-ib.com

19 years of helping ISP and Enterprises response to CyberCrime

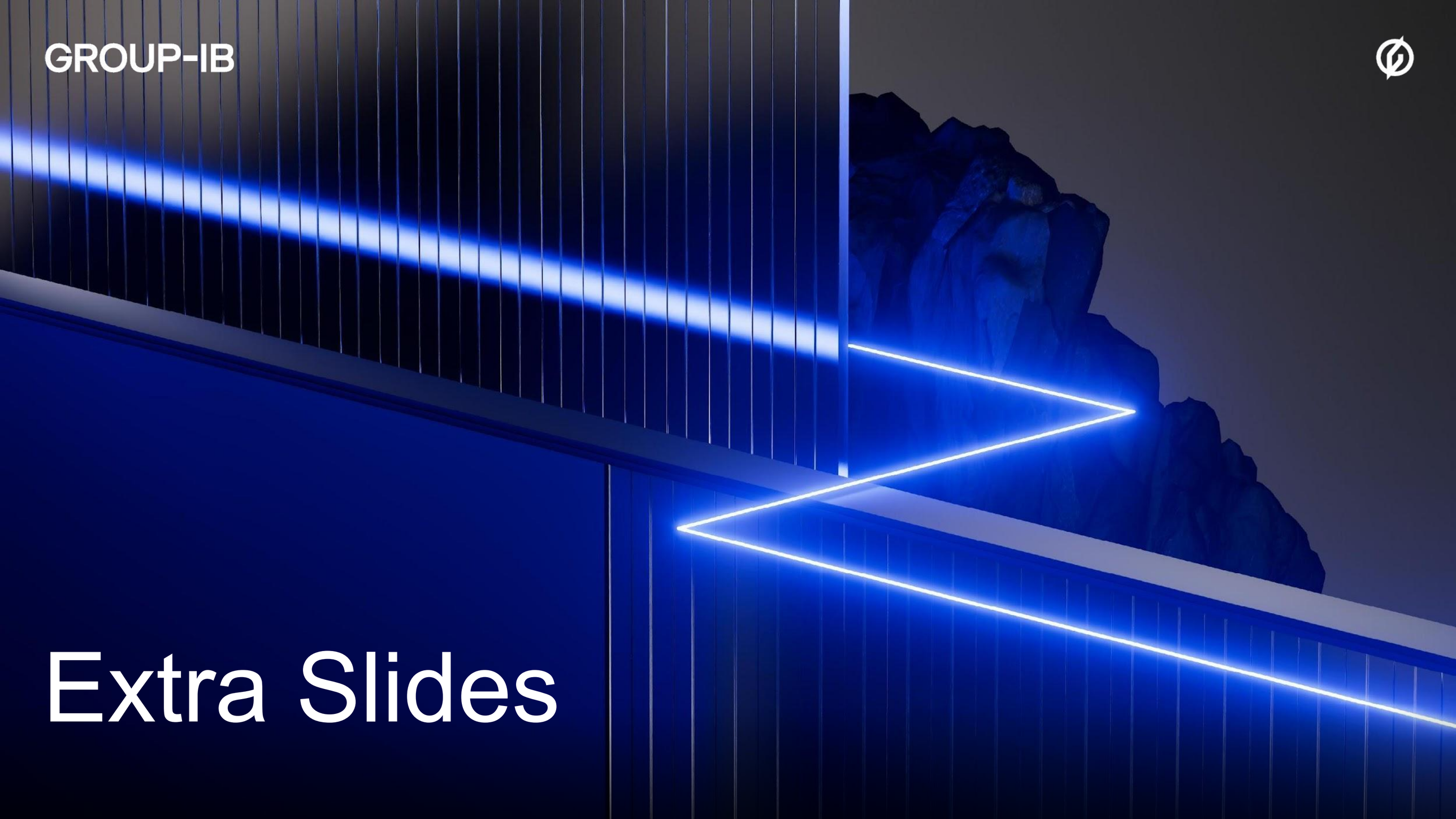
GROUP-IB



https://www.amazon.com/gp/product/B09RMYSGTZ/

Svetlana’s recent book

GROUP-IB



Extra Slides

THREAT INTELLIGENCE & ATTRIBUTION

System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure

Adversary-centric threat detection and proactive threat hunting

Advanced fraud detection and user authentication

Next-gen intellectual property protection

THREAT HUNTING FRAMEWORK

- Huntbox
  Sensor
  Sensor Industrial
  Polygon
  Huntpoint
  Decryptor

FRAUD HUNTING PLATFORM

- Processing Hub
  Preventive Proxy
  Web Snippet
  Mobile SDK

DIGITAL RISK PROTECTION

- Anti-Scam
  Anti-Counterfeiting
  Anti-Piracy
  Leak Detection
  VIP Protection

SERVICES THAT GIVE AN ACCESS TO “BATTLE FIELDS”

- Security & Risk Assessment
  Red Teaming Testing
  24/7 CERT-GIB
  Internal & External Threat Hunting
  Incident Response
  Digital Forensics & Malware Analysis
  Hi-tech Crime Investigations
  Cyber Education

GROUP-IB OVERVIEW

OUR COMPANY IN NUMBERS:

1,300+
investigations of high-tech cybercrime cases

600+
employees

450+
enterprise customers from

60
countries worldwide

11
key services

6
products

120+
patents and applications

4
regions with research centers Singapore, UAE, Russia, Netherlands

GROUP-IB GLOBAL PARTNERSHIPS:

INTERPOL

EUROPOL

GROUP-IB: RECOGNIZED BY TOP INDUSTRY EXPERTS

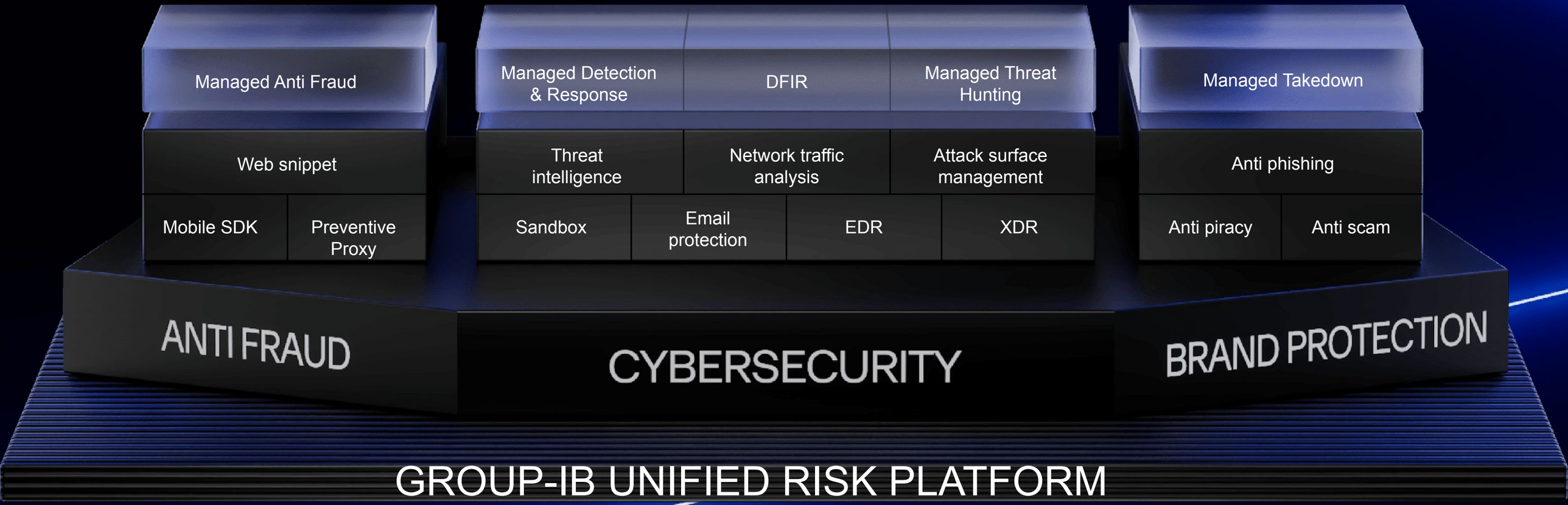
FORRESTER® IDC Gartner

kuppingercole ANALYSTS

FROST & SULLIVAN

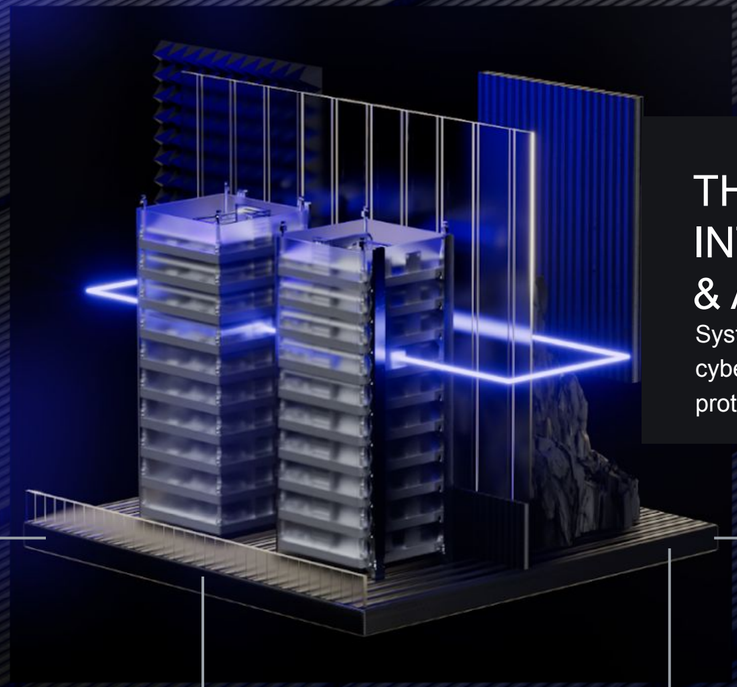
GROUP-IB TECHNOLOGIES

Unified Risk Platform:



TECHNOLOGIES WITH DETECTIVE DNA

State-of-the-art innovations and extensive service portfolio powered by the best-in-class Threat Intelligence solution



THREAT INTELLIGENCE & ATTRIBUTION

System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure

THREAT HUNTING FRAMEWORK

Adversary-centric detection threats within the infrastructure and beyond

FRAUD HUNTING PLATFORM

Real-time client-side digital identity protection and fraud prevention

ATMOSPHERE

Patented email security technology that blocks, detonates and hunts for the most advanced email threats

CLOUD ANTIBOT

SOON

Bot preventive proxy for SME market

DIGITAL RISK PROTECTION

AI-driven platform for digital risk identification and mitigation

ASSETZERO

Intelligence-driven attack surface management that continuously discovers all external-facing IT assets

Discover your external attack surface, manage risk and prevent breaches.

INTELLIGENCE-DRIVEN SERVICES

- Managed Detection & Response
- Digital Forensics and Incident Response
- Managed Threat Hunting
- Managed Anti Fraud
- Managed Takedown
- Red Teaming
- Security, Compromise and Pre-IR assessments

GROUP-IB SERVICES PORTFOLIO

PREVENTION

Red Teaming
Real-life simulation of targeted attacks using the technologies from hackers' arsenals

Compliance Audit
Unbiased evaluation of your company's security posture against industry's best practices and standards

Cyber Education
Training courses relevant for all organizations, conducted by certified specialists

Security Assessment
Assessments performed with advanced technologies and conducted by our team of experts

Compromise Assessment
Proactive detection of attack intention, compromise or attacked and damaged assets

Pre-IR Assessment
Evaluation of your incident response capabilities and your team's readiness

RESPONSE

Incident Response
Network traffic analysis, forensic analysis, malware analysis conducted by incident experienced response team

Managed Threat Hunting
Threat Hunting service powered by Group-IB technology

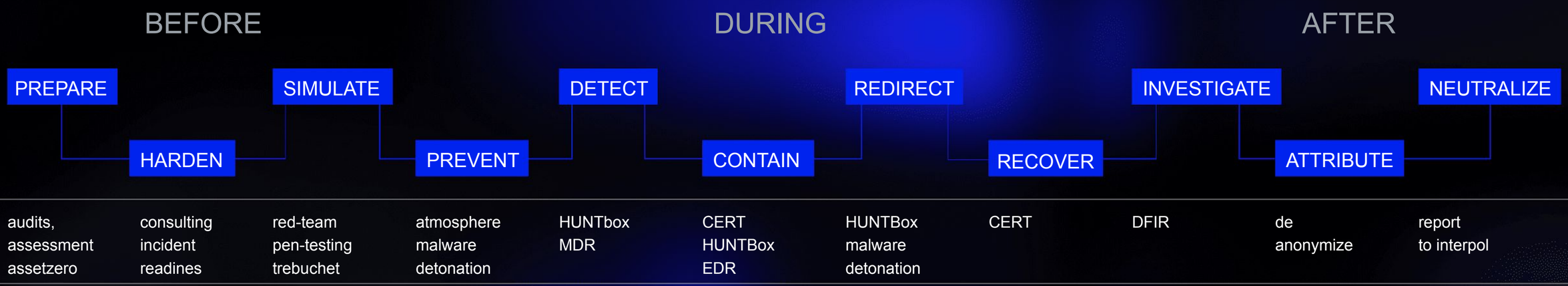
Managed Detection & Response
Detection & Response service powered by Group-IB technology

INVESTIGATION

Investigations
World-class investigations bringing criminals to justice

Digital Forensics
Top experts with 18+ years of experience dissecting cyber incidents

THE GROUP-IB SERVICES PORTFOLIO COVERING ALL STAGES OF CYBER RESPONSE CHAIN:



ABOUT CERT-GIB

CERT-GIB IS:

Round-the-clock computer security incident response team First private CERT in Russia founded in 2011
70 000+ hours of incident response
60+ certified experts and analysts
The biggest laboratory in Eastern Europe Information exchange among teams in 78 countries

CERT-GIB COMPRISES:

24/7 incident response Rapid takedown of dangerous websites in 2500+ domain zones Close cooperation with CERT teams, domain registrars and hosting providers from 150+ countries globally Collection, analysis and preservation of digital evidence Full support on every stage of incident response and investigation Preparation of required documentation for court

INTERNATIONAL COOPERATION AND RECOGNITION

ACCREDITED MEMBER OF FIRST

The largest global network of IR teams. encouraging cooperation in incident prevention and reaction, information sharing among teams in 78 countries.

MEMBER OF APWG

Anti-phishing working group, an international coalition unifying the global response to cybercrime

PARTNER OF THE IMPACT

IMPACT serves as a politically neutral global platform that brings together governments of the world, industry and academia to deali with cyber threats

ACCREDITED MEMBER OF TRUSTED INTRODUCER

The Trusted Introducer Service - was established by the European CERT community in 2000 providing vital support for all security and IR teams.

MEMBER OF OIC-CERT

OIC-CERT is the Computer Emergency Response Team for Organisation of Islamic Cooperation (OIC) member countries

GROUP-IB AS A RECOGNIZED LEADER

2014	2015	2016	2017	2018	2019	2020	2021
Gartner Market Guide	Gartner Competitive Landscape	IDC Russia	Forrester Vendor Landscape	Forrester New Wave	Gartner Market Guide	Forrester Now Tech Gartner Market Guide	Forrester Total Economic Impact Forrester Wave Frost & Sullivan Frost Radar

ABOUT GROUP-IB

BUSINESS INSIDER

The firm's Threat Prevention & Investigation Department has been a prominent factor leading Group-IB toward becoming the go-to expert on Russian cybercrime.

Defenders of the web: The people behind 7 influential security companies (2015)

THREAT INTELLIGENCE & ATTRIBUTION

FROST & SULLIVAN

Group-IB is one of the few vendors in the market that conducts intelligence collection in line with customers' requirements.

Group-IB is one of the most innovative vendors in the market and a leader on the Frost Radar leading CTI vendors.

Frost Radar™: Global Cyber Threat Intelligence Market, 2021

THREAT HUNTING PLATFORM

kuppingercole ANALYSTS

Group-IB's TDS is one of the most feature-rich NDR solutions in the market. It exceeds expectations for NDR functionality. Organizations that need a full range of NDR capabilities, especially for industrial applications, should consider Group-IB TDS.

Kuppingercole: Leadership Compass Report - NDR, 2020

THREAT INTELLIGENCE & ATTRIBUTION

FORRESTER®

With Group-IB TI&A, fraud prevention on payment cards became available instantly, and that resulted in large savings. Before, it would not have been possible for us to replicate that effort.

Forrester: Total Economic Impact report, 2021

FRAUD HUNTING PLATFORM

kuppingercole ANALYSTS

Exhaustive device intel capabilities, advanced bot management available, sophisticated array of ML detection models and excellent fraud analyst interface"

Kuppingercole: Leadership Compass Report - FRIP, 2021

DIGITAL RISK PROTECTION

FROST & SULLIVAN

Group-IB keeps a close watch on customers' needs. For instance, the company has included brand protection and digital footprint monitoring in MSSP and MDR Partner's Program in response to partner's end-clients demand."

Frost Radar™: Digital Risk Protection Innovation Excellence, 2020

MEET GROUP-IB GLOBAL TEAM OF EXPERTS

The Group-IB team comprises cybersecurity professionals in different areas:

We created a distributed and repeatable team structure across the world to provide our clients with a tailored and robust protection and continuous service.

- Threat hunting
- Digital forensics and incident response
- Malware reverse engineering
- Penetration testing
- Security assessment
- Investigations

60 countries of presence	600+ experts internationally	135 Cyber security certifications
1 300 investigations worldwide	18+ languages spoken by analysts	70K hours of incident response

GLOBAL PRESENC

OUR PRINCIPLES

PROUDLY PRESENTING GROUP-IB’S FIVE PRINCIPLES, THE CORE VALUES OUR TEAM STANDS FOR

Zero tolerance to cybercrime

Fighting against all cybercrime: no matter geography, origin or victim choice

Doing things right and doing the right things

Acting the right way, standing for good, supporting our customers, partners, friends and mutually help each other.

Researching and investigating

Being vigilant, ready to combat cyber criminals and bring them to justice no matter what is your role in a team at Group-IB.

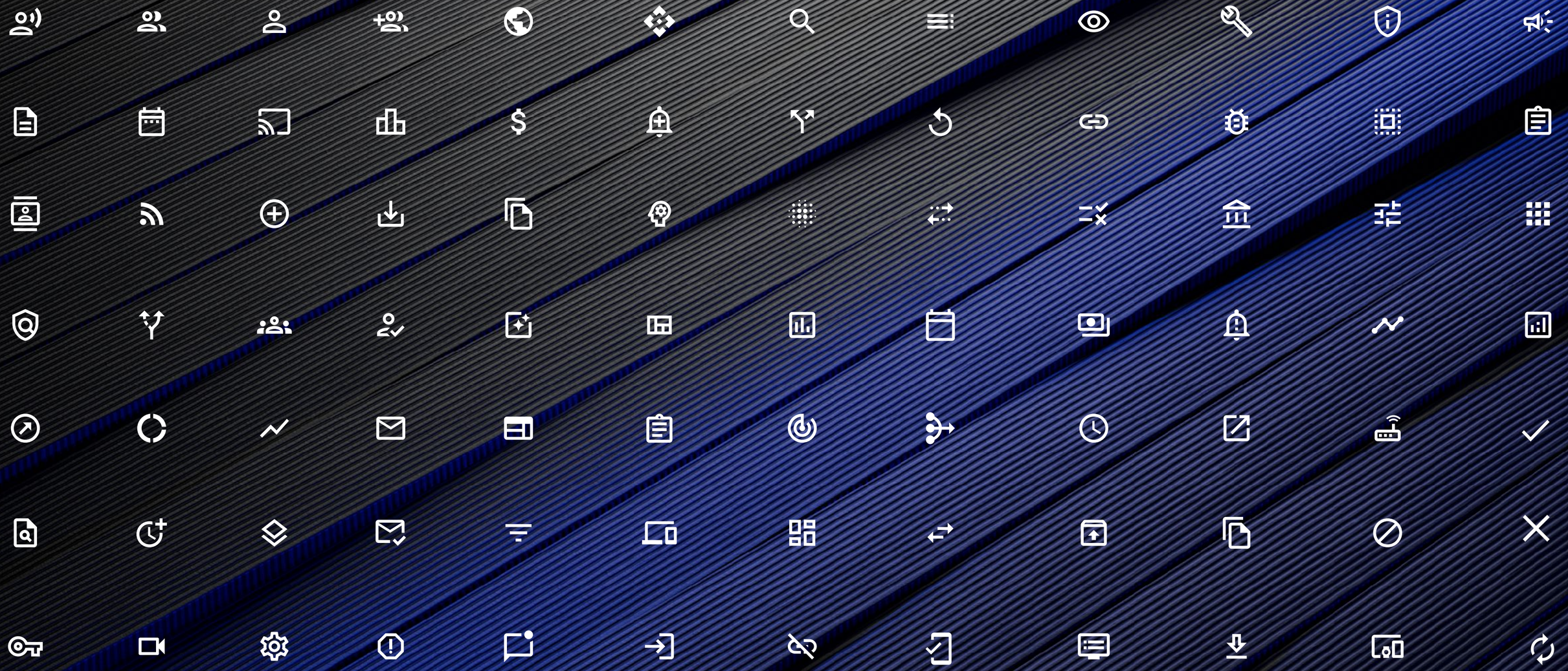
Inventing and innovating

Continuously innovating and improving our technologies, products and services in order to make a difference and proactively fight against cyber criminals.

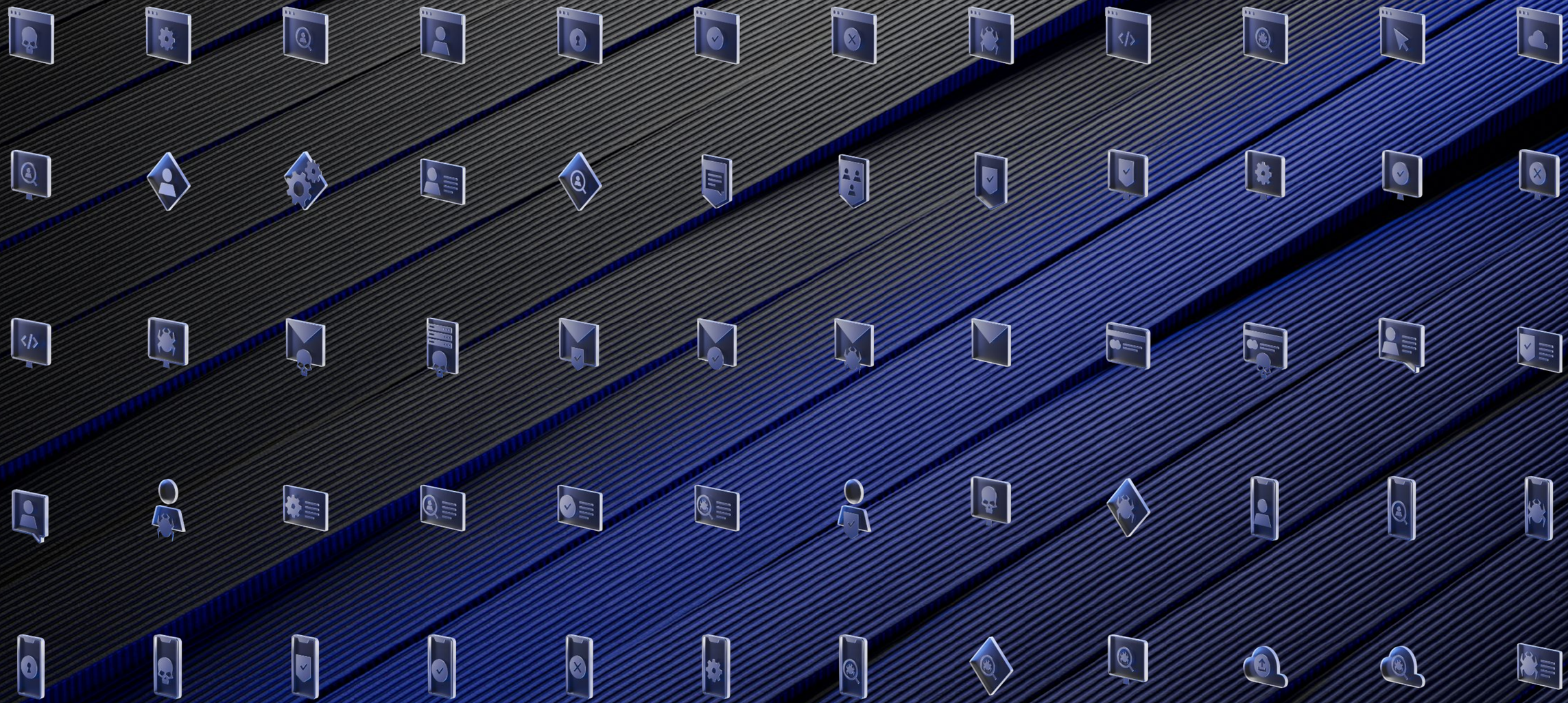
Earning honestly and investing in cyber safe culture

We reinvest our gains to build research centers in regions of presence, hire new talents to study local threat landscape. Supporting us, our clients also contribute to cybersafety of their regions.

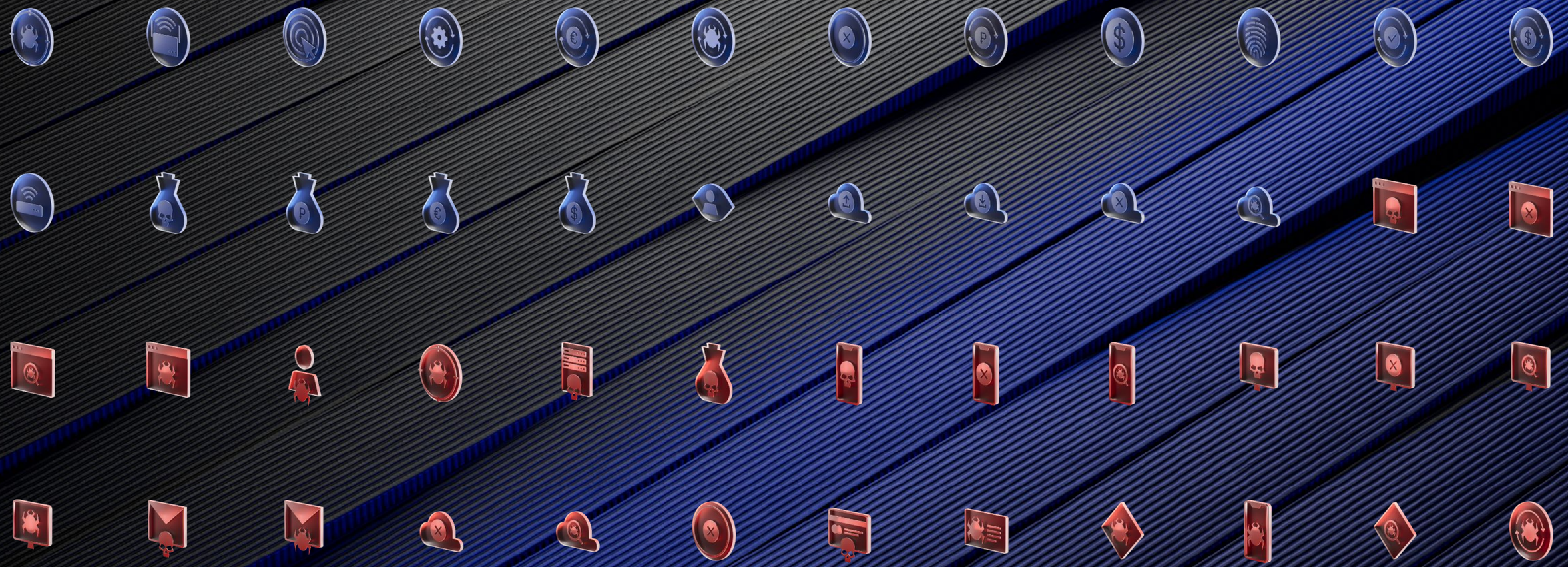
ICONS 01



ICONS 02

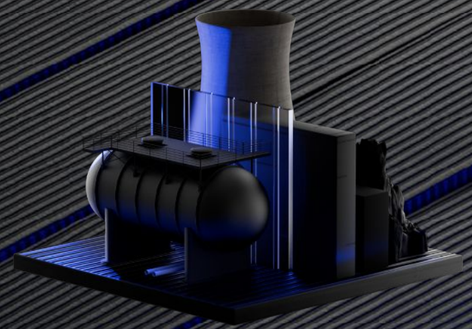


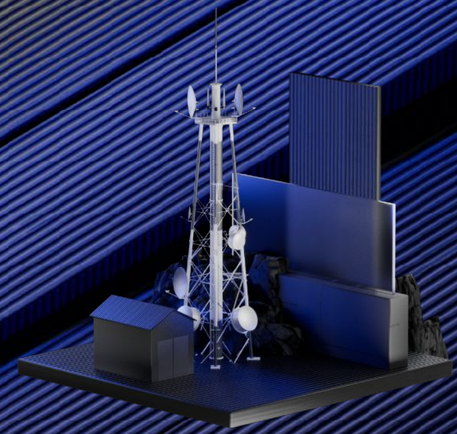
ICONS 03



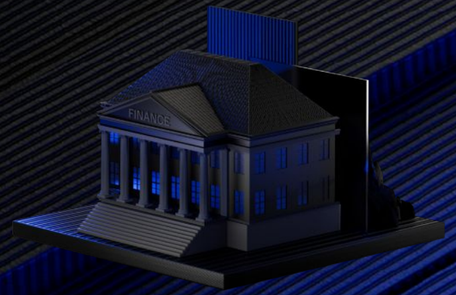
* The main glass icons are blue icons, red ones are recommended to be used only in case of acute necessity.

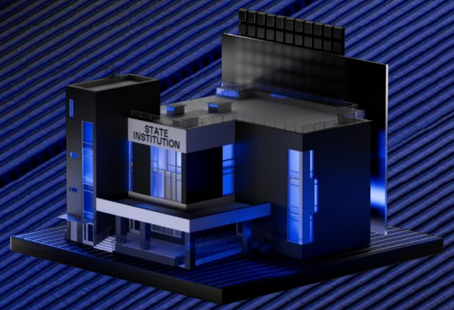
FACTOIDS 01



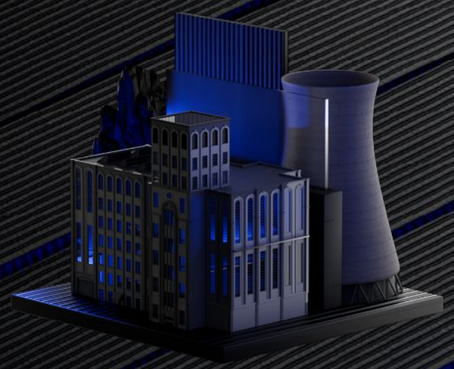


FACTOIDS 02

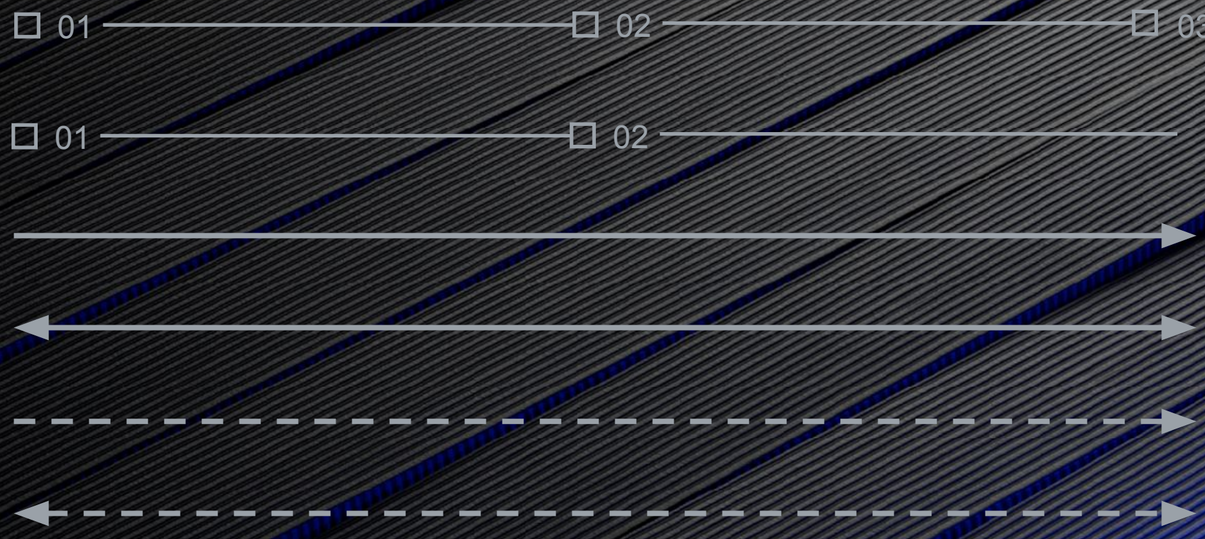




FACTOIDS 03



OTHER ELEMENTS 01



Small tags

GARTNER
IDC
FROST & SULLIVAN
GARTNER
INTERPOL
EUROPOL

Medium tags

GARTNER
IDC
FROST & SULLIVAN
INTERPOL
EUROPOL
GARTNER

18 yr

spent building the industry's best threat database

11 mln

threat actors are mapped and tracked

OTHER ELEMENTS 02

Fraud Hunting Platform

BY GROUP-IB

- Compromised credentials
- Compromised devices
- Compromised websites
- Fraudster IP addresses
- Fraudster devices
- Fraudster profile
- Compromised credit Cards

Group-IB Investigation team

BY GROUP-IB

01	Deep knowledge of criminal schemes	Enables us to immobilize the attackers before businesses suffer major damage
02	Individual approach by special project team	Project team consists of eDiscovery and Forensic analysts, economic security, financial audit, corporate law specialists, financial crime experts.
03	Proprietary technologies for criminal's detection	We accelerate investigations using in-house tools for pattern analysis, network analysis, tactical profiling.
04	Collaboration with law enforcement agencies	Work with international police in combating various types of crimes from computer-based crimes to murders and missing people

450+

enterprise customers around the world

550+

employees worldwide

1,300+

successful investigations of hi-tech cybercrime cases

70,000+

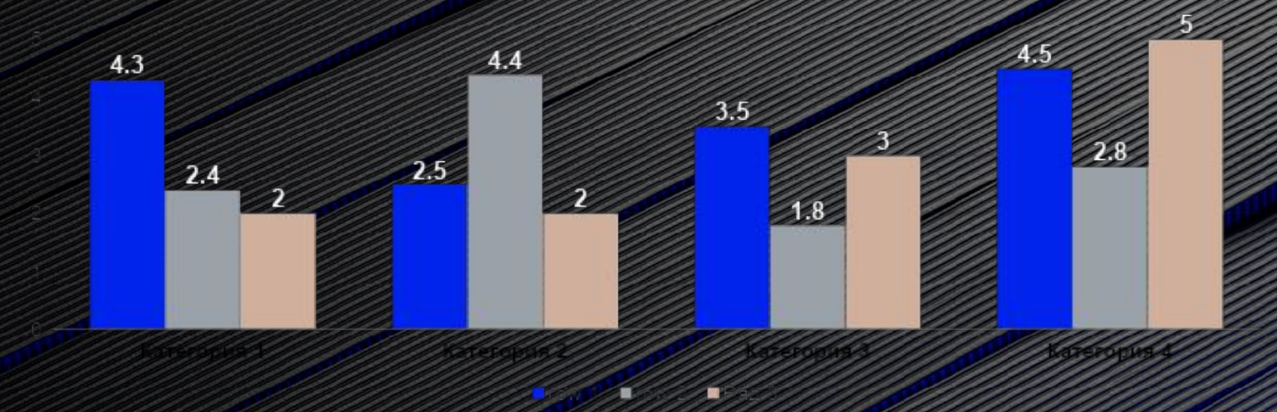
hours of hands-on Incident Response

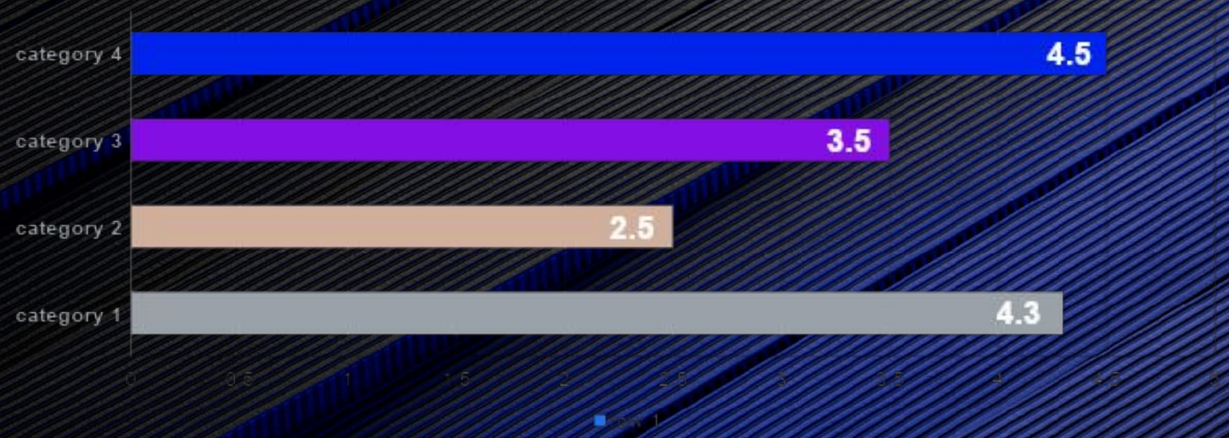
DIAGRAMS 01


Stolen user data for 2020-2021
sales: 32%
sales: 32%
sales: 11%
sales: 9%
sales: 8%
quarter. 1
quarter. 2
quarter. 3
quarter. 4
quarter. 5
quarter. 6

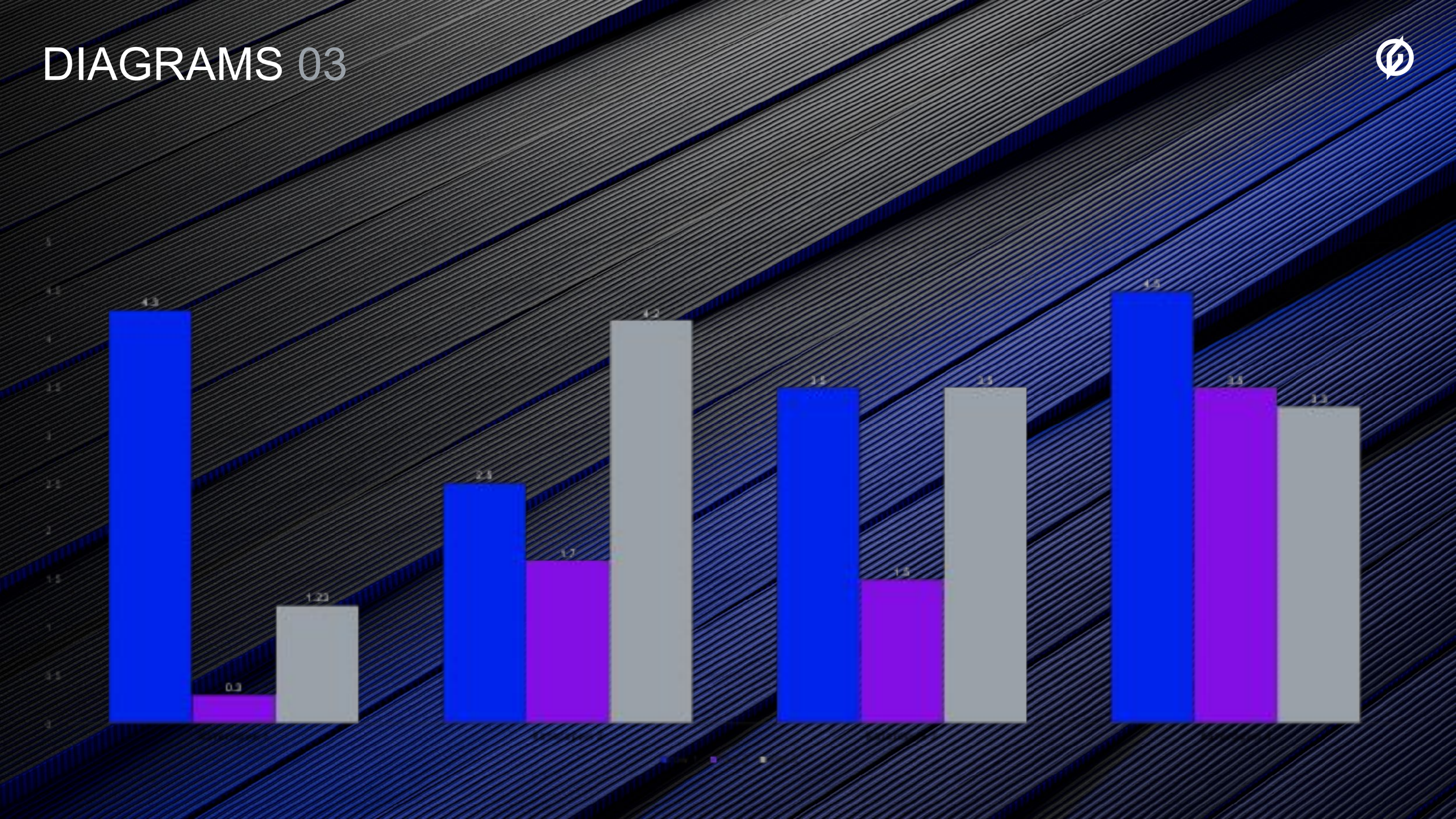

Stolen user data for 2020-2021
32%
32%
11%
9%
8%
quarter. 1
quarter. 2
quarter. 3
quarter. 4
quarter. 5
quarter. 6

DIAGRAMS 02


4.3
2.4
2
2.5
4.4
2
3.5
1.8
3
4.5
2.8
5
Категория 1
Категория 2
Категория 3
Категория 4


category 4
4.5
category 3
3.5
category 2
2.5
category 1
4.3

DIAGRAMS 03



GROUP-IB

TEMPLATES

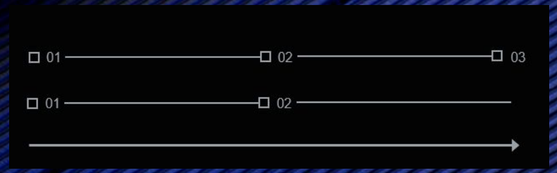
USEFUL LINKS TO SLIDES

In other words, fast navigation

The standard icons are on **this slide**

The glass icons are on **this** and the slides following it.

The elements that can be quickly copied are **here**

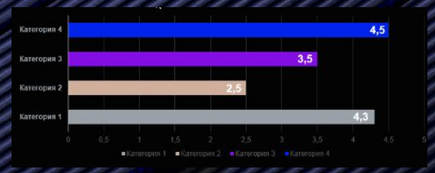


The factoids are on **this** and the following slides after that

The tables on **this** and the following slides

Условия	Пакет «Лайт»
Длительность	1 год
Краткое описание	100% предоплата

Diagrams can be found on **this slide** and the following slides after that



EXAMPLE OF A COMPLETED TEMPLATE

01

this is how the lead text is filled in, this is the text to fill in, you can change it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

EXAMPLE OF A COMPLETED TEMPLATE

02

this is how the lead text is filled in, this is the text to fill in, you can change it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

JUST AN EXAMPLE OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

JUST AN EXAMPLE OF A FILLED HEADER

- this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it
- this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it
- this is just an example of filling in the text, in order to show how an already filled slide looks, you can change the text, but please do not repaint it

EXAMPLE OF A COMPLETED TEMPLATE 03

JUST AN EXAMPLE
OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks

JUST AN EXAMPLE
OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks

JUST AN EXAMPLE
OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks

JUST AN EXAMPLE
OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks

JUST AN EXAMPLE
OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks

JUST AN EXAMPLE
OF A FILLED HEADER

this is just an example of filling in the text, in order to show how an already filled slide looks

EXAMPLE OF A COMPLETED TEMPLATE 04

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

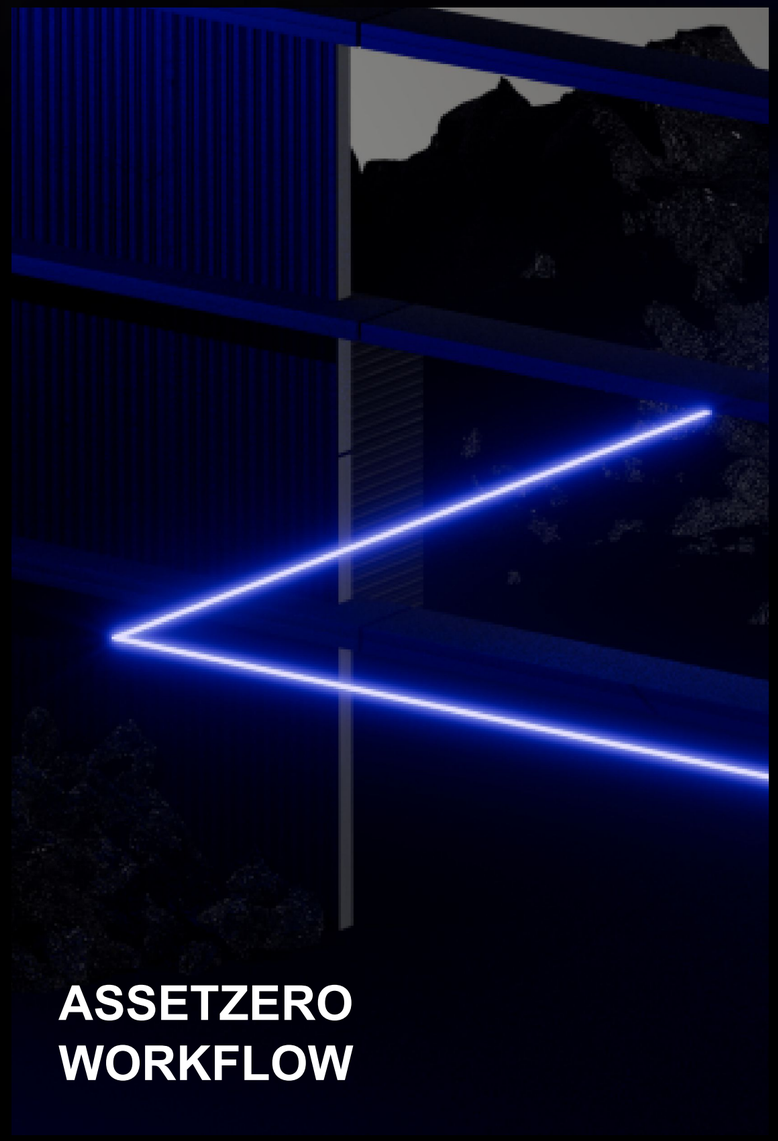
this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

EXAMPLE OF A COMPLETED TEMPLATE 05



this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

this is just an example of filling in the text, in order to show how an already filled slide looks

EXAMPLE OF A COMPLETED TEMPLATE 06

this is how the lead text is filled in, this is the text to fill in, you can change it

JUST AN EXAMPLE OF A FILLED HEADER

- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach
- Cross-channel complex digital footprint
  Wider digital attack surface
- Digital assets are increasingly exposed
  and harder to control

JUST AN EXAMPLE OF A FILLED HEADER

- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach
- Cross-channel complex digital footprint
  Wider digital attack surface
- Digital assets are increasingly exposed
  and harder to control

JUST AN EXAMPLE OF A FILLED HEADER

- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach
- Cross-channel complex digital footprint
  Wider digital attack surface
- Digital assets are increasingly exposed
  and harder to control

EXAMPLE OF A COMPLETED TEMPLATE 06

this is how the lead text is filled in, this is the text to fill in, you can change it

JUST AN EXAMPLE OF A FILLED HEADER

- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach
- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach
- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach

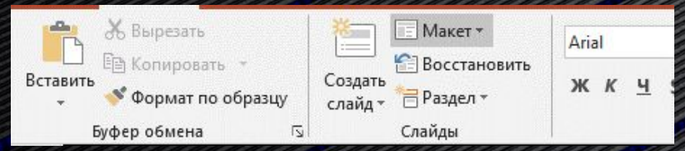
SAMPLE IMAGE

JUST AN EXAMPLE
OF A FILLED HEADER

WHERE THE OTHER SLIDES?

All other templates you can
find here (look at the steps below)

01



02

03

CHOOSE THE ONE YOU NEED!

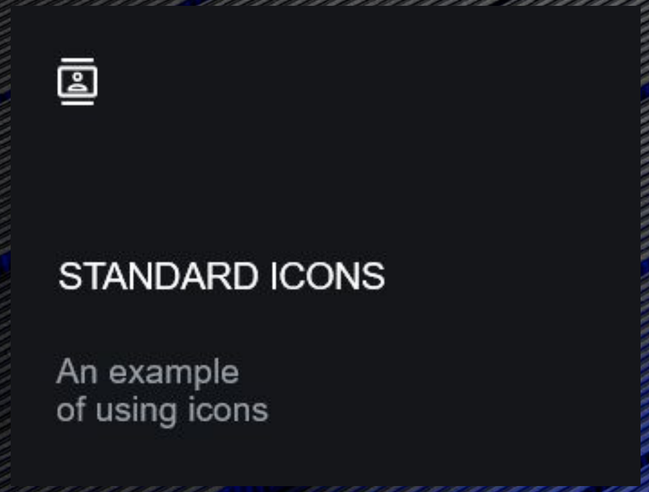
GROUP-IB

TEMPLATES USAGE

HOW TO USE ICONS?

There are two basic rules

Firstly, we use standard icons on black cards and do not repaint them



The standard icons are on **this slide**

The second rule is that we use glass icons for schemes

The glass icons are on **this** and the slides following it

EXAMPLE OF USING A TEMPLATE 01

NO CLARITY ABOUT AT-RISK ASSETS

Alerts without context do not facilitate adequate prioritization of mitigation activity. Our industry and attackers have moved beyond CVSS.

ONLY PERIODIC EXTERNAL DISCOVERY

Intermittent vulnerability assessments provide outdated and incomplete assessments of the attack surface.

SCATTERED DIGITAL FOOTPRINT

Keeping up-to-date data on all external assets and services is near impossible. Manual inventory struggles to map resources for automated validation & management.

LIMITED VIEW OF THE ATTACK SURFACE

Security scanners only scan known resources & active scanning is often not used across all resources because it can disrupt business processes.

55%+

of all Group-IB IR cases are due to perimeter-based vulnerabilities and insecure infrastructure

173%

growth in the number of RDP access sales to large corporate networks (Group-IB Intelligence)

1.5 bln+

files were available online on Amazon S3, rsync, SMB, and FTP servers from periodic reviews

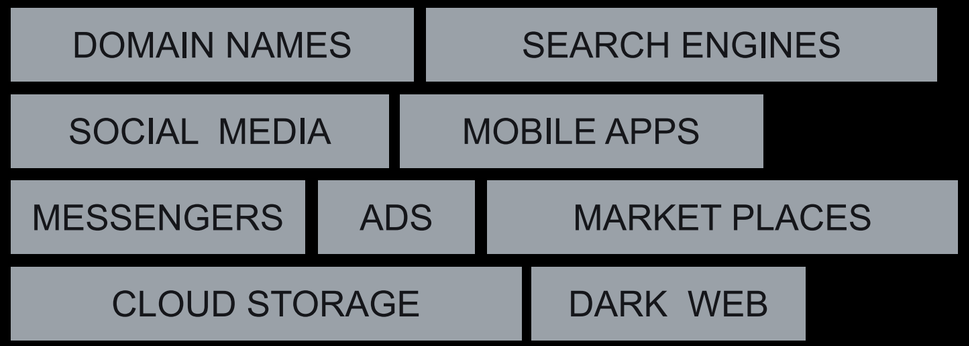
EXAMPLE OF USING A TEMPLATE 02

Lead example

52%	50-100X	520K
of global GDP will come from digitally transformed business by 2023	quicker will be developing of new products	new apps and services will be developed by 2024

EXAMPLE OF USING A TEMPLATE 03

Identify in what ways you are exposed and understand the threats to critical assets across all your platforms.



ATTACK SURFACE

- Discovers and classifies your assets
  Identifies Shadow IT
  24/7 Monitoring
  Catches external threats like leaks, dark web & malware connections
  Issues alerts regarding infrastructure risk
  Maps to remediation & workflows
  Tracks and baselines security posture over time

ATTACK SURFACE

- Discovers and classifies your assets
  Identifies Shadow IT
  24/7 Monitoring
  Catches external threats like leaks, dark web & malware connections
  Issues alerts regarding infrastructure risk
  Maps to remediation & workflows
  Tracks and baselines security posture over time

EXAMPLE OF USING A TEMPLATE 04

Example of lead

AssetZero is Group-IB's intelligence-driven External Attack Surface Management solution. This is a fully cloud, software-as-a-service solution with no agents required for use. It discovers and inventories all known and unknown Internet-facing assets related to your organization. Group-IB AssetZero provides full visibility of your External Attack Surface, thoroughly evaluates its risk & vulnerability, allowing prioritised remediation.

HOW DOES ASSETZERO MAP YOUR ATTACK SURFACE?

- Discovers and classifies your assets
  Identifies Shadow IT
  24/7 Monitoring
  Catches external threats like leaks, dark web & malware connections
  Issues alerts regarding infrastructure risk
  Maps to remediation & workflows
  Tracks and baselines security posture over time

EXAMPLE OF USING A TEMPLATE 05

Many companies are becoming increasingly digital and expanding the online side of their business

- Growth requires creation of safe digital platforms and ecosystems to scale and extend the digital reach
- Cross-channel complex digital footprint
- Wider digital attack surface
- Digital assets are increasingly exposed and harder to control

Digital Risk Protection identifies where and how your assets are exposed and protects your brand from digital threats

2X growth number of online offers

40 percent of sales via social media channel

4,6 billion internet users

4,3 billion mobile internet users

4,2 billion social media users

ACT NOW WITH ASSETZERO

Take control of your
external attack surface

Baseline and track
external security posture

Build new services
& deliver value

Protect your organization
from avoidable risks

**YOU CAN CHANGE
TEXT HERE PLEASE USE IT**

IMMEDIATE VISIBILITY & FAST RESULTS

AssetZero requires no installation of software and is 100% agentless. Our process is fully automated, and alerts flow to your clients, either directly or through your team as a managed service.

PREVENT AVOIDABLE INCIDENTS

AssetZero identifies, tracks and alerts you on the risks and vulnerable infrastructure of your organisation. Take back control and get ahead of attackers.

FRICTIONLESS SERVICES

The easy-to-use portal and dashboards help quickly manage issues and prioritize critical risks for proper remediation.

PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+65 3159 37 98

LINKEDIN FACEBOOK TWITTER INSTAGRAM

GROUP-IB

PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

Contributor name

PLACE QR-CODE