

# Cyberint Brand Guidelines

2020



01

# **Brand Strategy**



# Messaging Matrix

1. Our Core Principles
2. Elevator Pitch
3. Short Narrative
4. Our Values / Our Personality
5. Long Narrative / Our Differentiation
6. Tailored Messaging
7. What We Deliver
8. How We Do That / Value for Our Customers

# Core Principles

## Our Category

### Intelligence-Driven Detection and Response

#### Value We Deliver - Our Tagline

*Turning intelligence into actions to effectively and proactively protect your business.*

## Pillars of Differentiation

- Actioning intelligence
- Domain expertise
- Human & technology integration
- Continuous detection and response offering

## Our Values

- True Partnership
- Quality First
- Skin in the Game
- Relentless Response
- Context is King

## Our Mission

Cyberint's unique combination of proven technology platform and cyber and intelligence experts turns intelligence into actions.

We detect threats across the digital and organizational environment to be one step ahead by leveraging our analysts' expertise, market proven threat intelligence suite, digital presence monitoring, threat hunting and threat mitigation and response services.

## Our Vision

Being a cybersecurity partner to direct-to-consumer businesses with intelligence-driven detection and response.

Enabling businesses to act continuously against actual and potential threats.

Directing and prioritizing security efforts to be more effective whilst reducing their cybersecurity TCO and effectively protect what matters most to them.

## Our Positioning

Our modular offering is the only one to correlate cyber and business domain expertise to enable our customers to focus on the actual threats, directing and prioritizing security efforts to be most effective with real time visibility, while reducing cybersecurity TCO.

We continuously

- identify threats and risks in the cloud and digital environment;
- verify and assess if there was a compromise;
- close the loop with continuous mitigation and response actions in order to protect what matters most: your unique business mission, employees, customers and brand.

# Elevator Pitch

Cyberint is a cybersecurity partner to direct-to-consumer businesses with intelligence- driven detection and response.

We turn intelligence into actions by leveraging our analysts' expertise, market proven threat intelligence suite, digital presence monitoring, threat hunting and threat mitigation and response services.

Cyberint's unique combination of proven technology platform and human cyber and intelligence experts enables businesses to reduce their cybersecurity TCO and effectively protect what matters most to them – customers, employees, brand and business.

# Short Narrative

Cyberint is the unique provider of intelligence-driven detection and response solutions and services. Our offering is based on a modular automated threat intelligence suite combined with cyber analysts that identifies and prioritizes

- your threats
- weaknesses in the digital environment
- risks from 3rd party partners

Our cyber analysts holistically manage it for our clients, investigate events to alert with near zero-false positives, recommend or take mitigation steps on their behalf, enable immediate and effective response.

Leveraging our analysts' expertise, market proven threat intelligence suite, threat hunting and threat mitigation and response services we protect businesses' mission, employees, customers and brand.



# Our Values

## Collaborative Partnership

We focus on high-touch, long-term, trusted partnership with your team are the key to directing and prioritizing security efforts to be more effective

## Quality First

Managed services engagement model enables us to subside the noise and providing the alerts with near zero false positives

## Relentless Response

Our analysts are stepping in in collaboration with you and don't rest until threats are mitigated and incidents resolved

## Skin in the Game

We rely on high-touch delivery and providing expertise, real-time visibility and continuous prioritization of threats

## Context is King

Our intelligence-driven approach provides context to cyber incidents, unveiling the who, why and how is behind them to minimize dwell time and the potential impact

## Our Personality

Sharp

Direct

Agile

Collaborative

Trustworthy

## Long Narrative

Cyberint is the unique provider intelligence-driven detection and response offering, leveraging our market proven threat intelligence suite, threat hunting and threat mitigation and response services.

Our mission - turning intelligence into actions to proactively and effectively protect businesses against cyber threats.

Our customers get the full visibility of their threats and weaknesses in their digital environment, cloud, and associated risk from their 3rd party partners and receive actionable recommendations to respond to threats in the most effective way, with near zero-false positives, and detailed response actions, incl. take downs and incident containment.

We serve over 100 brands worldwide with a unique combination of proprietary technology and cyber and intelligence analysts.

## Our Differentiation

- Unique combination of proprietary technology and expert analysts
- Near zero false positives based on our managed services engagement model
- Reducing TCO (total cost of ownership) of in-house effort and costs of cybersecurity technology, operations, skilled manpower and training
- Full visibility of prioritized threats and weaknesses enabling faster time to remediate
- Unified platform with modular solutions: threat intelligence suite, with digital presence monitoring, threat hunting and continuous detection and response
- Best practices in direct-to-consumer businesses
- Augmenting services to assess enterprises' preparedness (Red Team/Purple team)

# Tailored Messaging

## CISO

Through configurable, automated, 24/7 monitoring of your environments, Cyberint's unique combination of technology and human cyber analysts enable you to know and act effectively according to the risk appetite, while reducing your cybersecurity total cost of ownership.

## CIO

Cyberint's iterative, comprehensive platform and processes integrate several point solutions, allowing for lower operational costs while enabling continuous adaptation to your changing business environment.

As you adopt new mobile applications, move your assets and infrastructure to the cloud, or interact with new third-party partners, you can count on us to quickly deploy and act on the intelligence as needed to protect your business continuity, operations, data and employees.

## CEO

Cyberint instills your customers with the utmost trust in their data security, enables your employees to focus on your organization's core competencies, and allows you to rest assured that your business continuity is protected with diligent managed cybersecurity.

## CMO

Our technology platform is operated by creative analysts in ongoing communication with your security team. This grants us unparalleled understanding of your changing business environment and enables us to make quick, continuous platform adaptations to meet your security needs.

# Tailored Messaging (Cont.)

## Retail

Cyberint deeply understands your consumers' digital journey to purchase, and works to protect their data across all channels, touchpoints, and third-party systems, enabling diligent protection from fraud and account takeover — even during holiday seasons.

Protecting more than just your customers, we ensure your employees are working on secured web interfaces across sales channels, inventory management and commerce platforms and enable your business operations and continuity.

## Finance

Cyberint has extensive experience with financial institutions around the world, and established the Cyber Defense Management directive for Israel's banking sector — the first directive of its kind in the industry. We protect your customers' financial data across touchpoints, while diligently monitoring your most pressing threats, such as business executive targeting, ATM targeting, or remote compromise of your data, operations and processes.

## Entertainment and Media

Cyberint empowers leading companies worldwide with highly secured platforms their players can trust. We understand the value of your high value gamers or your media stars who are prime targets for threat actors, and provide you with prioritized actionable insights to protect them with actionable insights and recommended mitigation steps.



## What We Deliver

Cyberint is the unique intelligence-driven detection and response provider, leveraging our market proven threat intelligence suite, threat hunting and threat mitigation and response services. It is based on a multi-tenant, modular SaaS platform with cyber analysts holistically managing it, recommending mitigation steps, enable immediate and effective response.

## Our Managed Services Include:

### Threat Intelligence

- Real-time alerts of targeted attacks, data leakage and stolen credentials compromising the organization
- Identifying threat actors targeting you in real time and providing contextual data about them
- Operational threat intelligence to enrich existing SIEM solutions
- Research and reporting on various attack campaigns targeting your industry and/or region with detailed analysis for the threat actors, their attack vectors and TTP (Tactics, Tools and Processes)

**Digital presence** discovery and monitoring the attack surface

**Threat hunting** services to assess if enterprises were compromised and containing incidents

**Mitigating threats and response** - with take downs, and specific response actions on behalf of our customers

## How We Do That

1. **Identify** and prioritize the threats, weaknesses and exposure in the cloud and digital environment, as well as risks from 3rd party partners' security assessment.
2. **Verify** if there was a compromise in the network with threat hunting and assess their teams' preparedness to breaches with red team and blue team services.
3. **Respond** with take downs, contain incidents when detected during hunts of threats in your network and provide detailed step-by-step remediation actions to enable your teams to act in the most effective way.

## Value for the Customers

Our customers get the support of dedicated cyber analysts and SMEs who provide through the Cyberint platform full visibility of their threats and weaknesses in their digital environment, cloud, and associated risk from their 3rd party partners.

The human cyber experts research, investigate and interact with threat actors to enable the most effective threat mitigation and response actions for verified threats.

Our customers receive detailed response steps as well as threat mitigation and incident containment services by Cyberint on their behalf.

This enables our customers to receive a bespoke service with near zero-false positives, and reduced TCO, to effectively protect what matters most: the customers, their data, employees and business goals.

02

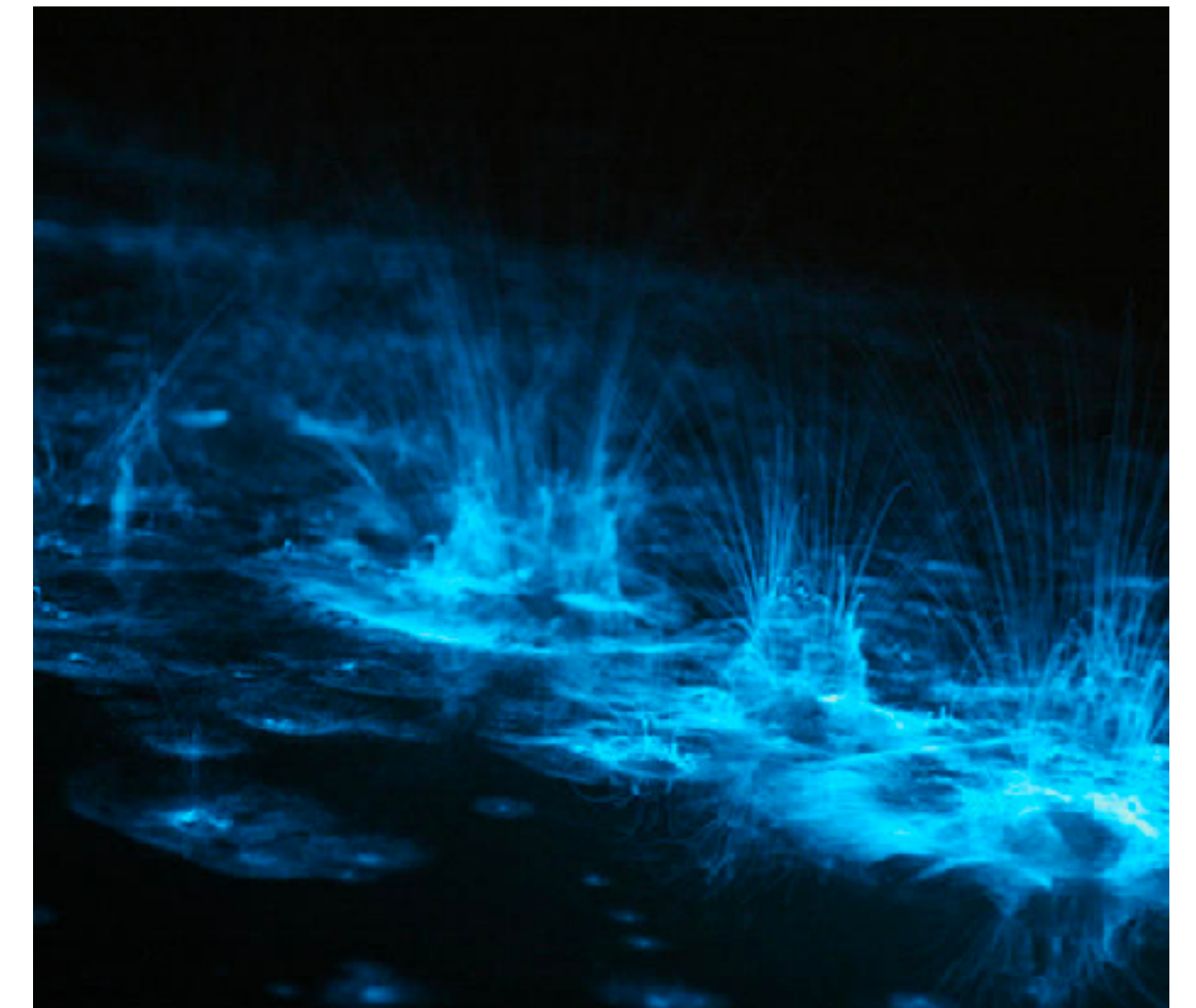
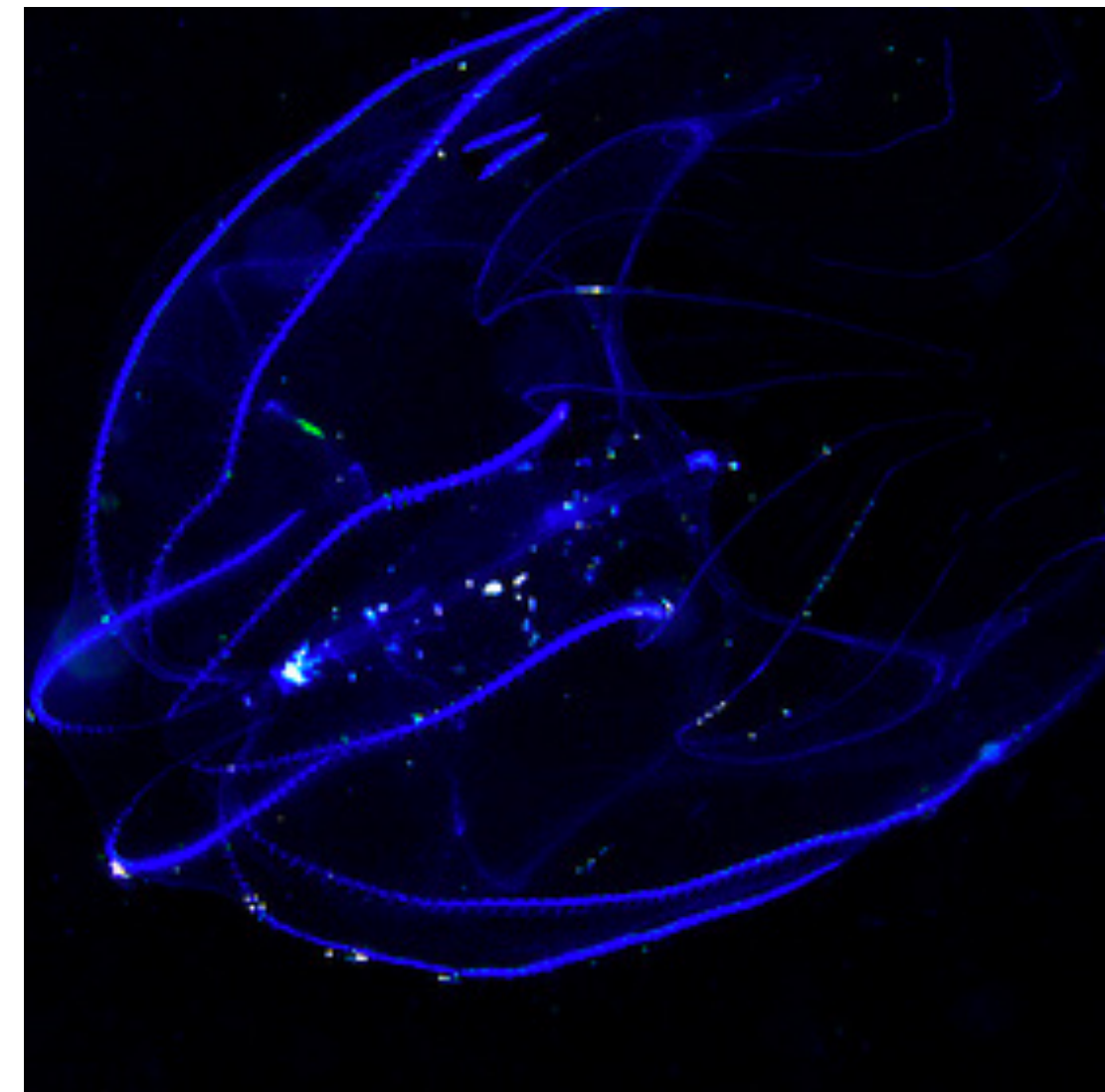
# Brand Assets





## Visual language

At the heart of the inspiration for the visual language is the idea of something that illuminates itself within the darkness, of a world of light, of contrast, and of the individual versus the many





## Visual language

The themes that came up throughout the strategy phase led to the development of a visual concept rooted in:

Focus: on one thing among many

Integration: the weaving of many elements into one

Movement and dynamism: Agility, constant search, adaptation to new threats and a changing environment



# Cyberint



## Logo

The Cyberint logo is a logotype, also known as a “word mark”.

The logotype is based on a font from the Bauhaus period, composed of the boldest, most fundamental geometric shapes - lines and circles.

The circle is a shape that repeats itself continuously in Cyberint’s visual language. This repetition allows for the creation of a visual scheme that can be both diversified and highly recognizable.



## Logo — minimum size

In order to ensure maximum readability of the logotype in all formats and platforms, the logo must meet the minimum sizing ideal for every implementation.

### Print

Minimum height of letter 30 mm

### Digital

Minimum height of letter 60 pixels



Cyberint

640 px

Cyberint

320 px

Cyberint

160 px

60 px

Cyberint



Cyberint

Cyberint

Cyberint

Cyberint

Cyberint

The logo for Cyberint, featuring the word "Cyberint" in a white, sans-serif font. The background is a dark blue gradient with a large, curved pink shape on the left side.

Cyberint



The image features a dark blue background with a large, semi-circular orange shape on the left side. The word "Cyberint" is written in white, sans-serif font in the center-right area.

Cyberint

## Logo — do's



Here are a number of examples of coloring do's and don'ts

Guiding principles:

The logo will always appear in one solid color, taken from the primary color palette of the brand

The secondary color palette must not be used for the logo

A high level of contrast must be retained between the logo color and background color



Cyberint

Cyberint

Cyberint

Cyberint

Cyberint

Cyberint



Cyberint



Cyberint



Cyberint



Cyberint



Cyberint



## Logo — dont's



Here are a number of examples of coloring do's and don'ts

Guiding principles:

The logo will always be in one solid color, taken from the primary color palette of the brand

The secondary color palette must not be used for the logo

A high level of contrast must be retained between the logo color and background color



## Color — primary palette

The main colors of the brand stem from three color spectrums.

A blue spectrum, an orange spectrum, and a grey spectrum, each with their range of colors.

Each shade from these spectrums can be used for the different implementations of the logo - as background colors, for the typography of the logo itself, and for primary and secondary headers.

Throughout the visual identity, these colors will be used in various integrations.



PANTONE 2768 C  
CMYK 100 / 97 /  
41 / 43 RGB 21 /  
21 / 70 #151546



PANTONE 2758 C  
CMYK 100 / 96 / 32 /  
22 RGB 27 / 20 / 100  
#1B1464



PANTONE 2738 C  
CMYK 98 / 89 / 5 /  
0 RGB 48 / 51 /  
137 #303389



PANTONE 2736 C  
CMYK 83 / 71 / 0 /  
0 RGB 69 / 82 /  
176 #4552B0



PANTONE 2727 C  
CMYK 73 / 57 / 0 /  
0 RGB 90 / 113 /  
214 #5A71D6



PANTONE 2718 C  
CMYK 44 / 23 / 0 /  
0 RGB 111 / 142 /  
255 #6F8EFF



PANTONE 485 C  
CMYK 9 / 100 / 100 /  
2 RGB 249 / 64 / 56  
#F94038



PANTONE 1585 C  
CMYK 0 / 74 / 97 /  
0 RGB 255 / 120 /  
22 #FF7816



PANTONE 151 C  
CMYK 0 / 53 / 88 /  
0 RGB 255 / 143 /  
29 #FF8F1D



PANTONE 7548 C  
CMYK 0 / 36 / 94 /  
0 RGB 255 / 193 /  
29 #FFC11D



PANTONE 101 C  
CMYK 4 / 13 / 81 /  
0 RGB 255 / 232 /  
118 #FFE876



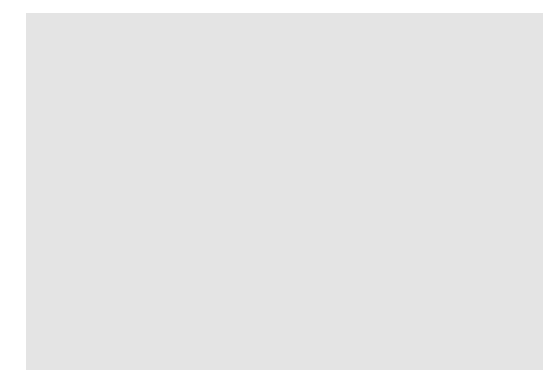
PANTONE BLACK  
7 C  
CMYK 73 / 58 /  
57 / 65 RGB 51 /  
51 / 51 #333333



PANTONE COOL GRAY  
9 C  
CMYK 55 / 45 / 45 / 32  
RGB 102 / 102 / 102  
#666666



PANTONE COOL  
GRAY 7 C  
CMYK 39 / 30 / 31 / 9  
RGB 151 / 151 / 151  
#979797



PANTONE 7527 C  
CMYK 18 / 13 / 14 / 0  
RGB 228 / 228 / 228  
#E4E4E4



## Color — secondary palette

The brand's secondary palette is composed of colors that are more bright, glowing and saturated.

It appears in minor touches and smaller doses than the primary palette.

These colors can be used mostly as part of the graphic spheres, to add 'points of light' or a hint of color on screens that are dark or monotone..

They can not be used for the logo, typography, or full solid-backgrounds.



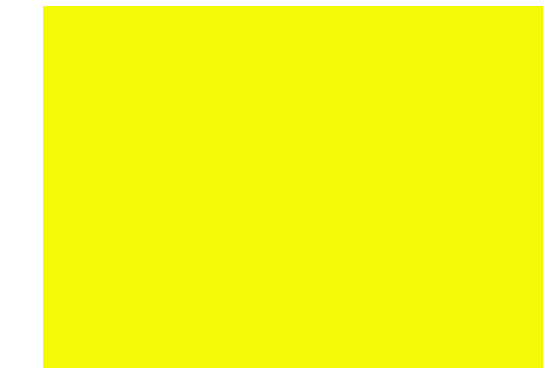
CMYK 69 / 0 / 14 / 0  
RGB 54 / 255 / 249  
#36FFF9



CMYK 68 / 0 / 60 / 0  
RGB 36 / 255 / 166  
#24FFA6



CMYK 67 / 0 /  
100 / 0 RGB 18 /  
255 / 83  
#12FF53



CMYK 8 / 0 / 100 /  
0 RGB 243 / 249 /  
6 #F3F906



CMYK 59 / 77 / 0 /  
0 RGB 206 / 49 /  
255 #CE31FF



CMYK 44 / 82 / 0 /  
0 RGB 231 / 68 /  
222 #E744DE



CMYK 10 / 84 / 0 /  
0 RGB 255 / 87 /  
188 #FF57BC



CMYK 7 / 64 / 0 / 0  
RGB 255 / 138 /  
216 #FF8AD8

## Color — severity spectrum

This is the precise color spectrum that can be used in any implementation that requires a visualization of a particular severity level.



CMYK 40 / 25 / 7 / 0	CMYK 63 / 45 / 0 / 0	CMYK 87 / 65 / 0 / 0	CMYK 83 / 71 / 0 / 0	CMYK 81 / 19 / 59 / 4	CMYK 72 / 0 / 100 / 0	CMYK 0 / 36 / 94 / 0	CMYK 0 / 53 / 88 / 0	CMYK 0 / 74 / 97 / 0	CMYK 9 / 100 / 100 /
RGB 166 / 180 / 212	RGB 111 / 133 / 194	RGB 50 / 90 / 166	RGB 69 / 82 / 176	RGB 24 / 145 / 122	RGB 72 / 172 / 51	RGB 255 / 193 / 29	RGB 255 / 143 / 29	RGB 255 / 120 / 22	2 RGB 249 / 64 / 56
#A6B4D4	#6E85C2	#325AA6	#4552B0	#18917A	#48AC33	#FFC11D	#FF8F1D	#FF7816	#F94038



## Typeface

# Lato

Naming Lato one of the 10 best Google Fonts for websites, art and design resource Creative Bloq writes, “The semi-rounded details of the letters give Lato a feeling of warmth, while the strong structure provides stability and seriousness.” Doesn’t that sound perfect for a business site?



**ABCDEFGHIJKLMN  
OPQRSTUVWXYZ  
abcdefghijklmn  
opqrstuvwxyz**

---

Lato  
Black

ABCDEFGHIJKLMN  
OPQRSTUVWXYZ  
abcdefghijklmn  
opqrstuvwxyz

---

Lato  
Regular

**ABCDEFGHIJKLMN  
OPQRSTUVWXYZ  
abcdefghijklmn  
opqrstuvwxyz**

---

Lato  
Bold

ABCDEFGHIJKLMN  
OPQRSTUVWXYZ  
abcdefghijklmn  
opqrstuvwxyz

---

Lato  
Light

***ABCDEFGHIJKLMN  
OPQRSTUVWXYZ  
abcdefghijklmn  
opqrstuvwxyz***

---

Lato  
Bold italic

*ABCDEFGHIJKLMN  
OPQRSTUVWXYZ  
abcdefghijklmn  
opqrstuvwxyz*

---

Lato  
Light Light



# Typography

Examples of typography with the proper use of different weights of Calibre.

## CUSTOMER JOURNEY

# Main touch points

Holistic security lorem ipsum dolor sit amet, zril suscipit cum ne. Pro suavitate intellegat lorem.



### USE CASE

#### The success of a leading online retailer

Deio deeply understands your customers' digital path to purchase, and works to protect their data across all channels, touchpoints, and third-party systems, enabling diligent prevention of fraud and account takeover — even during holiday season.

[Read more](#)

**“The challenge we had was to monitor over 1,600 digital assets and collecting OSINT based, actionable Threat Intelligence in real-time”**

Avraham Zerouk  
Head of Cyber and Info Security Unit, gema

## CASE STUDIES



### How online retailer ASOS tackles

MAY 11, 2019

## Reasons to work at Deio

### Creativity

We believe high-touch, long-term, collaborative partnerships with your team are the key to creating business-centered security you can

### Trust

We believe high-touch, long-term, collaborative partnerships with your team are the key to creating business-centered security you can

### Quality focused

We secure your business outside-in, inside-out, integrating internal and external threats to reveal unknown unknowns.

### Collaboration

Insight alone is not enough. Our dedicated, expert analysts take action for you and don't rest until threats are mitigated and incidents

### Courage

Our threat-led approach provides context to internal cyber incidents, unveiling the who, what, why and how that matter to your business.

### Secure

We subside the noise by providing the alerts your business needs to protect what matters most: your business mission, customers.



03

# Visual Elements



## Visual identity toolbox

There are a number of elements that compose the visual identity, which can be used according to need, platform and audience.

The elements are -

### Spheres & Dot sequences

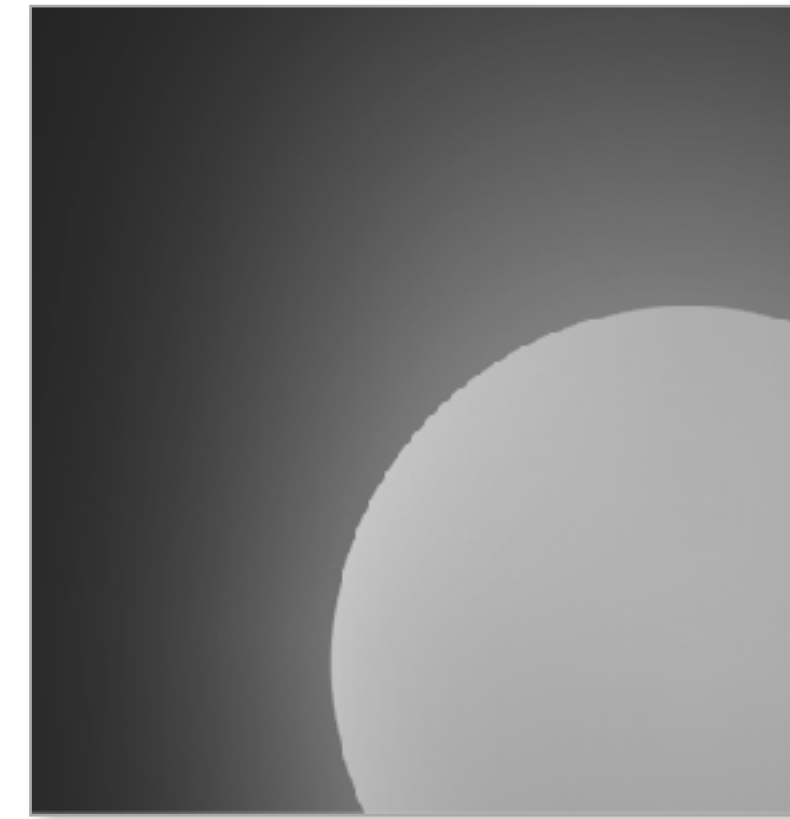
May be used separately or together. The dot pattern always appears as the frontmost layer (above the sphere). The elements can also appear in a variety of colors and sizes.

There are also 3 types of visual elements that can be used according to need, platform and audience:

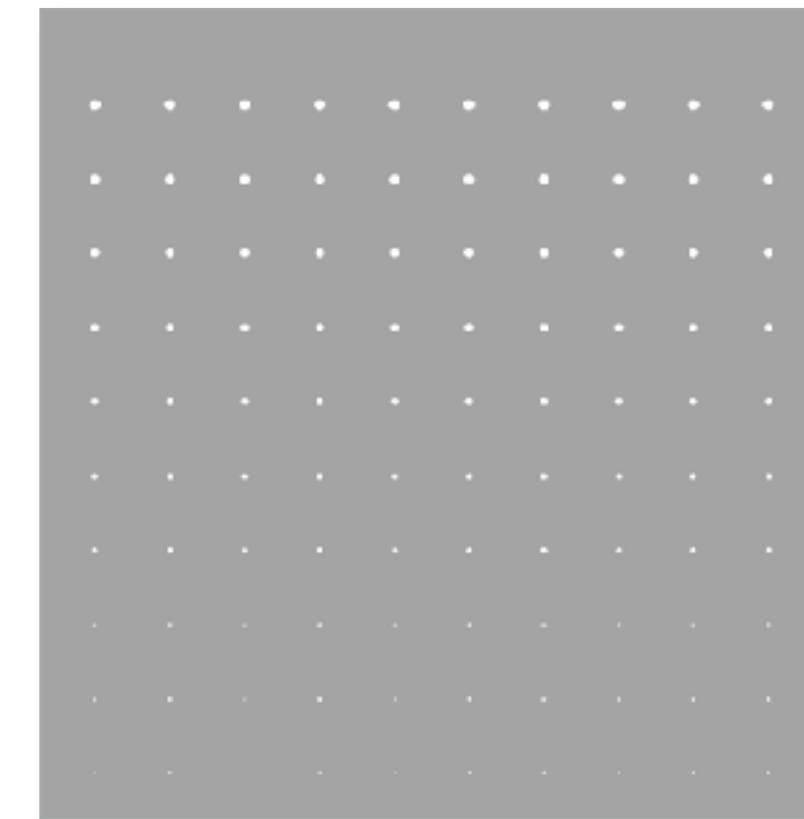
**Hidden nature photography** - these images will be used as general backgrounds. Further description follows.

**Two sides of a story** - these will be used in implementations for specific companies or industries. Further description follows.

**Product narratives** - A collage of product images. Further description follows.



Focus



Dot



Photography: Hidden



Photography: 2 sides



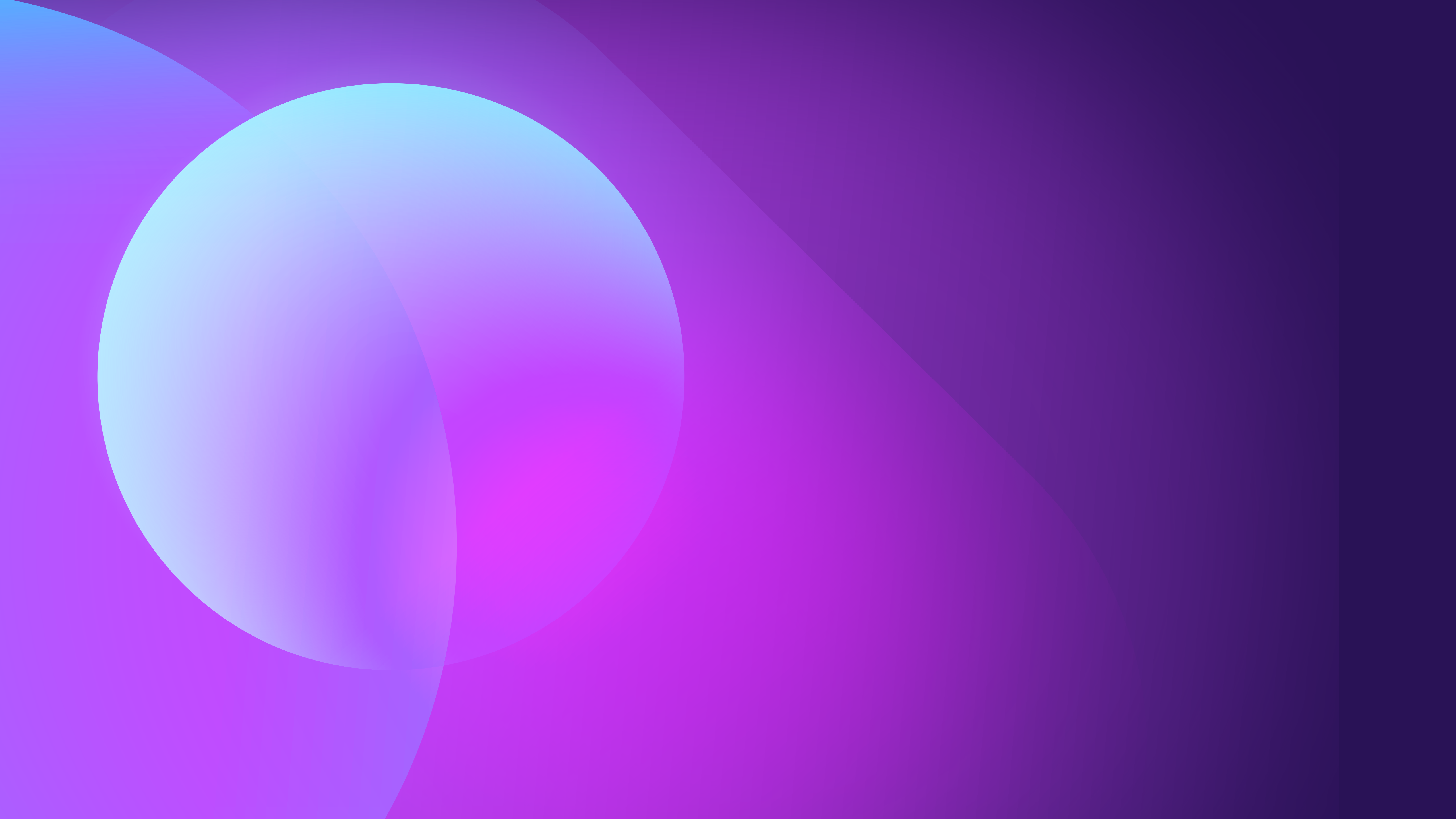
Images: Product narratives

## Imagery variants — Focus Spheres

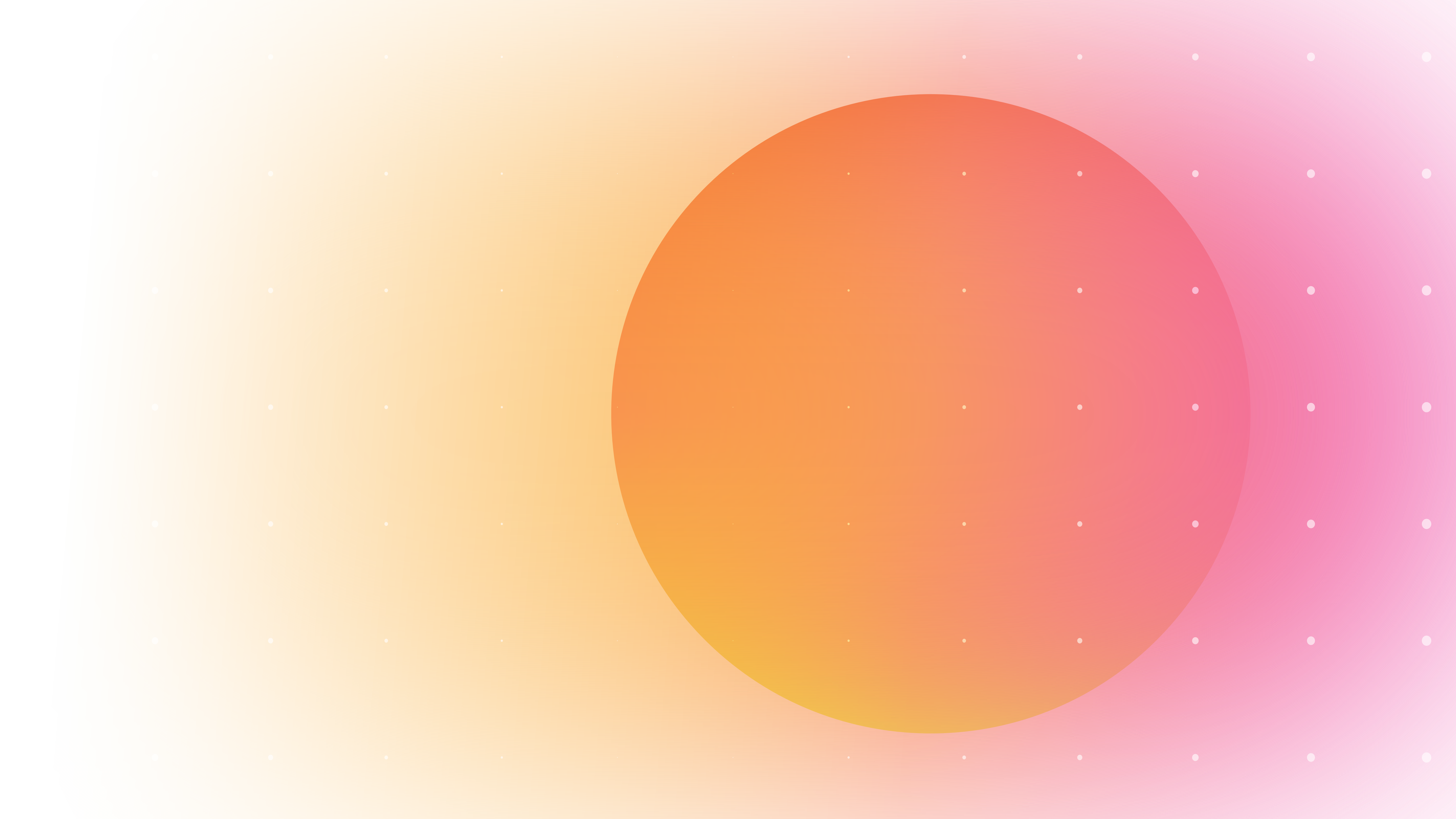
The round, glowing spheres are the leading graphic element of the language. They can appear in different sizes and colors, and in different compositions. They can appear large and be cut off the the format, or appear full in the centre of the frame. The spheres are shown static, or in dynamic movement, creating a spot light that is searching for threats.





















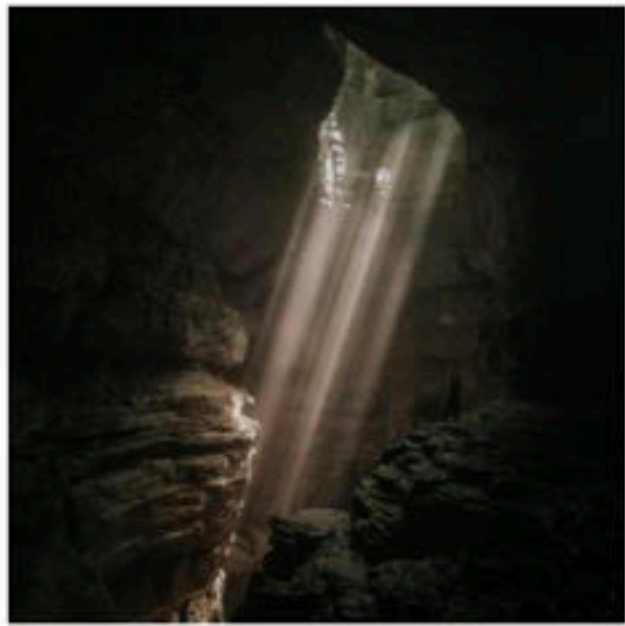


## Imagery variants – Hidden Nature

The idea behind “hidden nature” is the use of still, somewhat mysterious images in which there is something hidden, or imperceptible to the eye.

The nature imagery used should be unfiltered, and create a sense of stillness alongside the feeling that something is present which can't be seen. Images of a world hidden from the surface (in the water, underground) or of one thing hiding another (clouds blocking something behind them, an eclipse, etc')

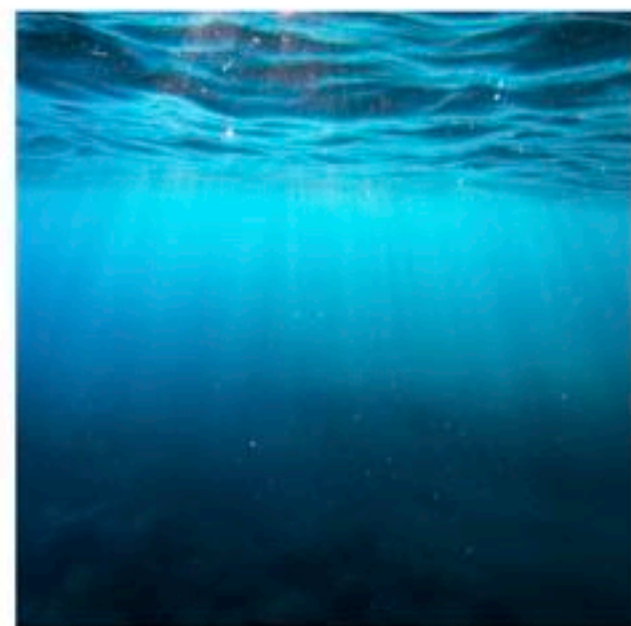




**Managed threat hunting**

PROFFETIONAL SERVICES

Cyberint



**Managed threat hunting**

PROFFETIONAL SERVICES

Cyberint



**Managed threat hunting**

PROFFETIONAL SERVICES

Cyberint



**Managed threat hunting**

PROFFETIONAL SERVICES

Cyberint

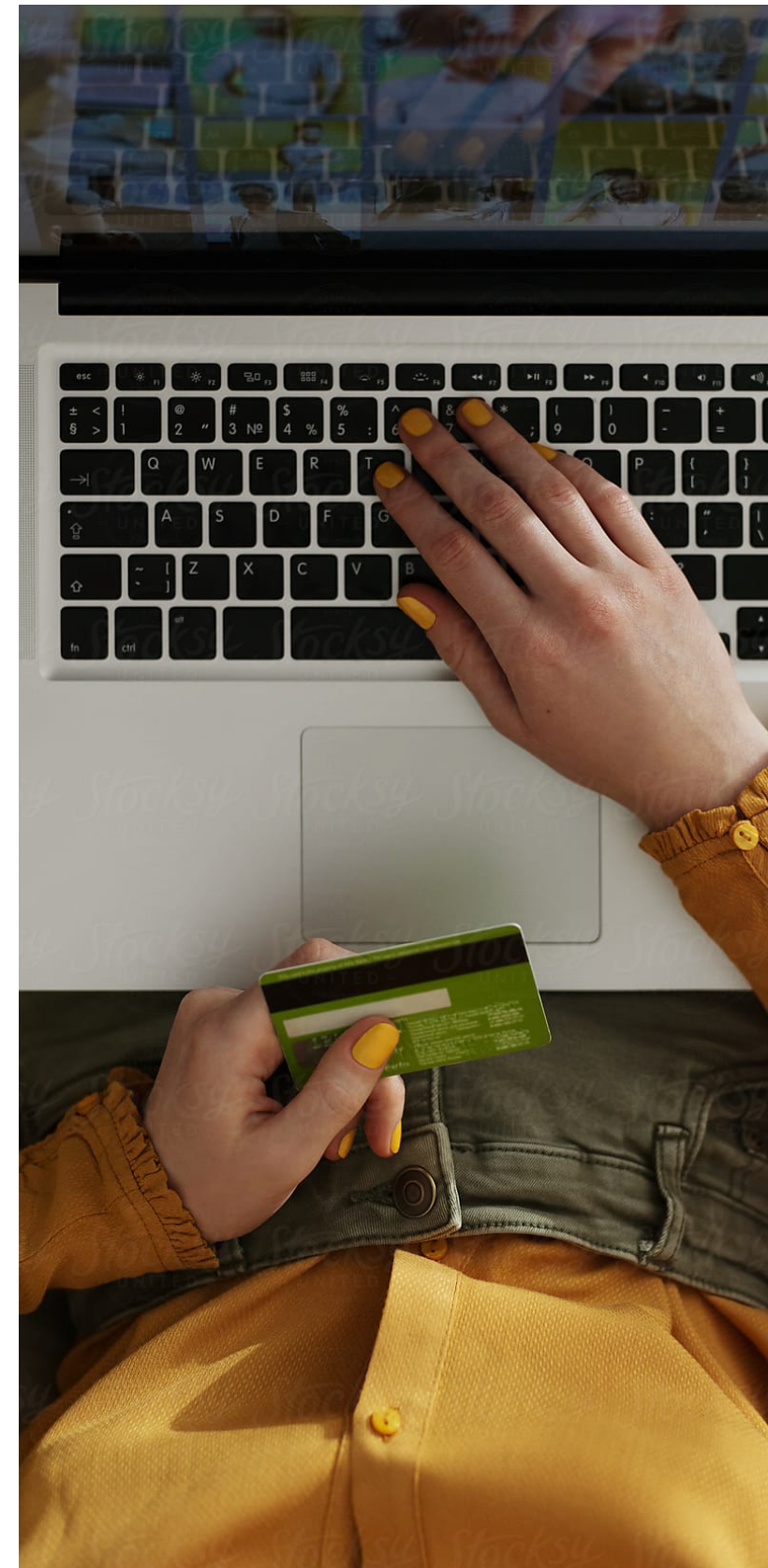


## Imagery variants — “2 sides of the story” image system

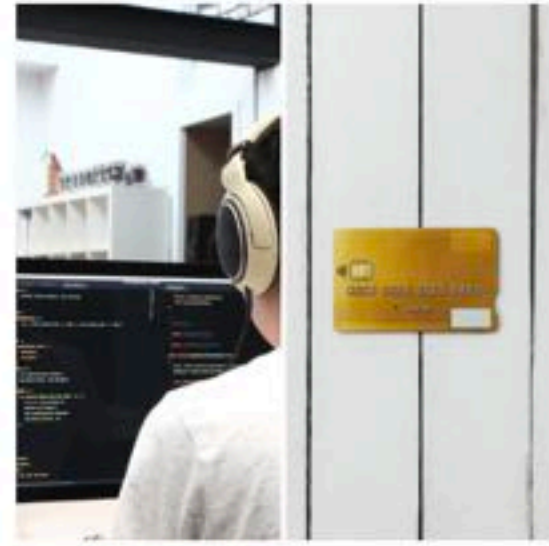
We can tell the story of a specific industry using a composition of two images.

The right hand side is used to envision the industry, while the left hand side demonstrates the aspect related to Cyberint: for example, a critical moment in the customer journey (such as entering credit card details), the analyst, the backend of the product, etc.

The square composition can also be created with an image on the right hand side, and a rectangle of solid color on the left. In this option, the composition of right and left doesn't have to be 50-50, and can be in uneven proportions.







Cyberscore report  
BPI Bank

Cyberint

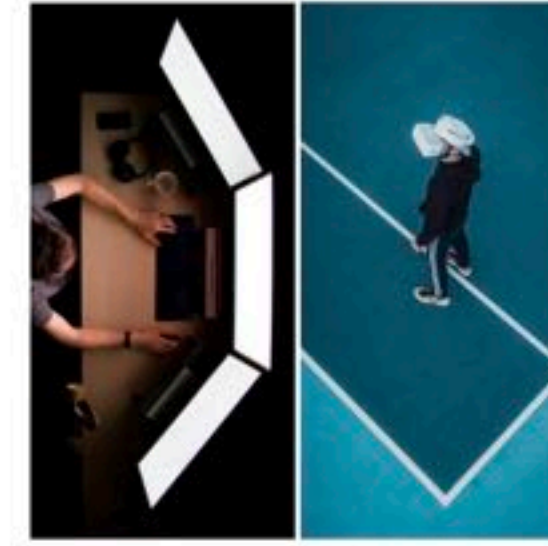
DEC 2019



Cyberscore report  
Asos

Cyberint

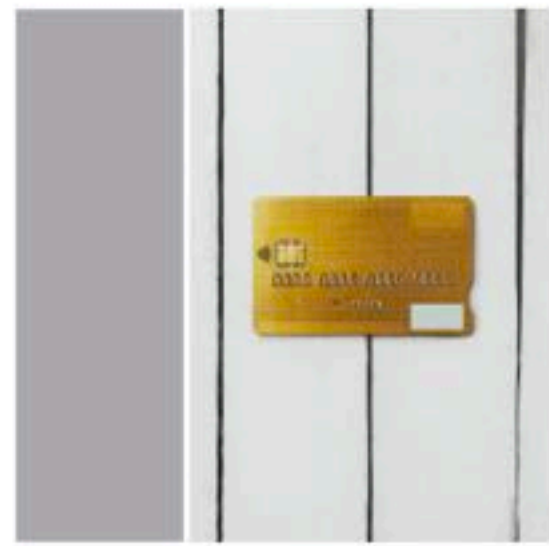
DEC 2019



Cyberscore report  
Playtika

Cyberint

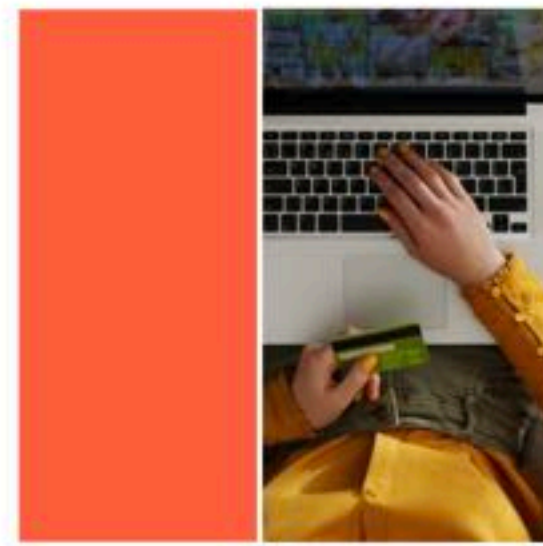
DEC 2019



Cyberscore report  
BPI Bank

Cyberint

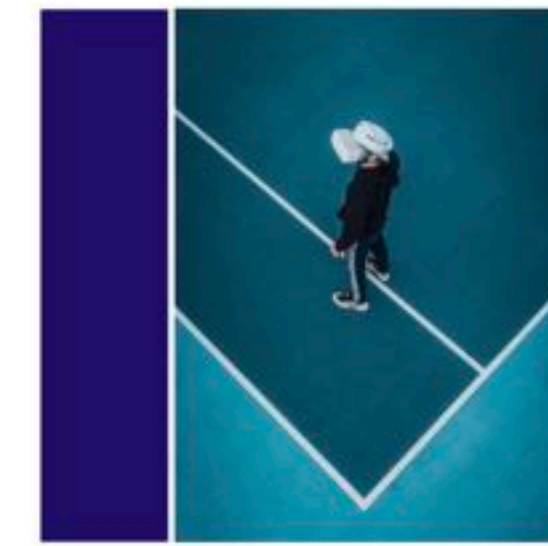
DEC 2019



Cyberscore report  
Asos

Cyberint

DEC 2019



Cyberscore report  
Playtika

Cyberint

DEC 2019

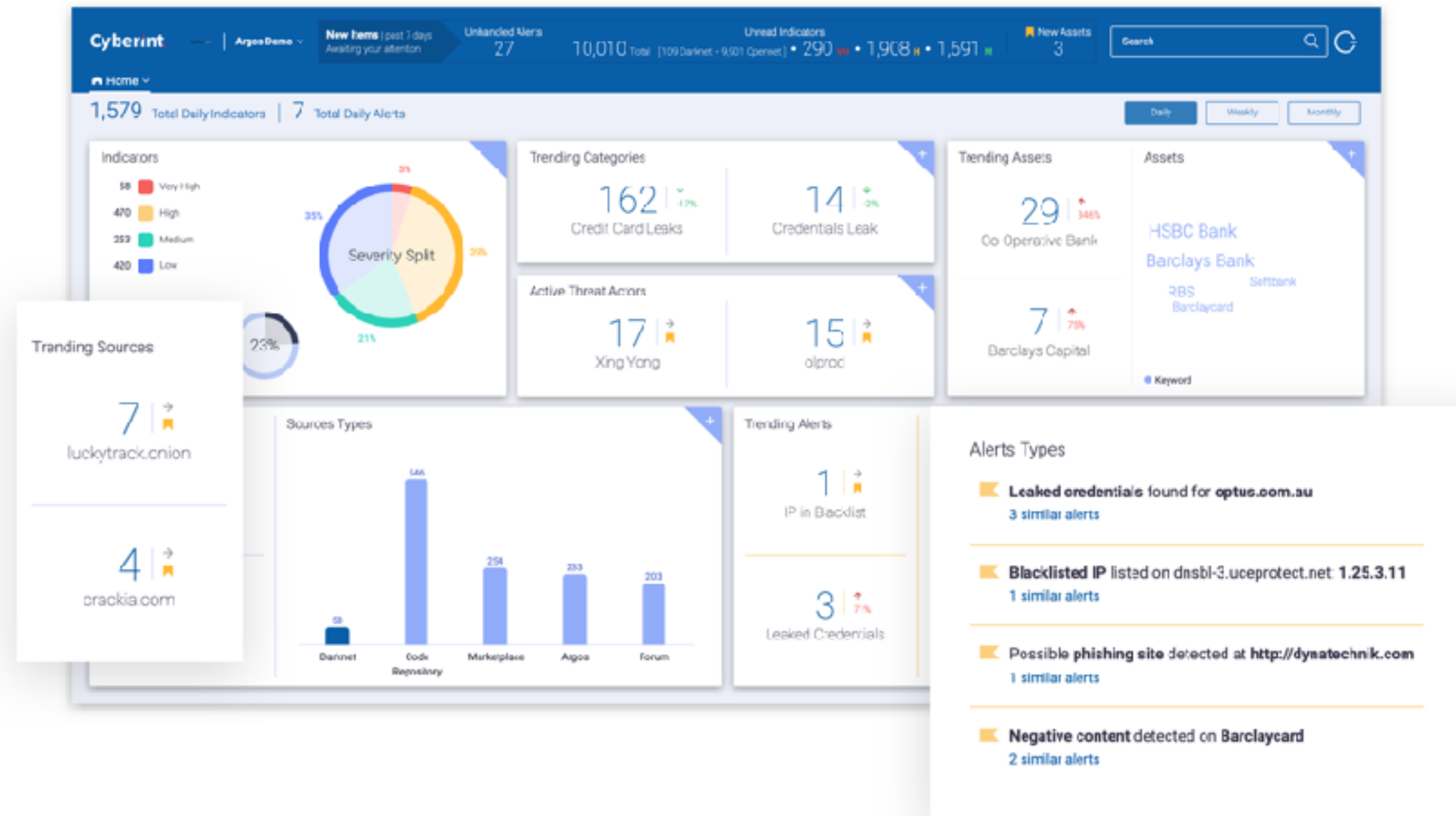


# Imagery variants – Product Narratives

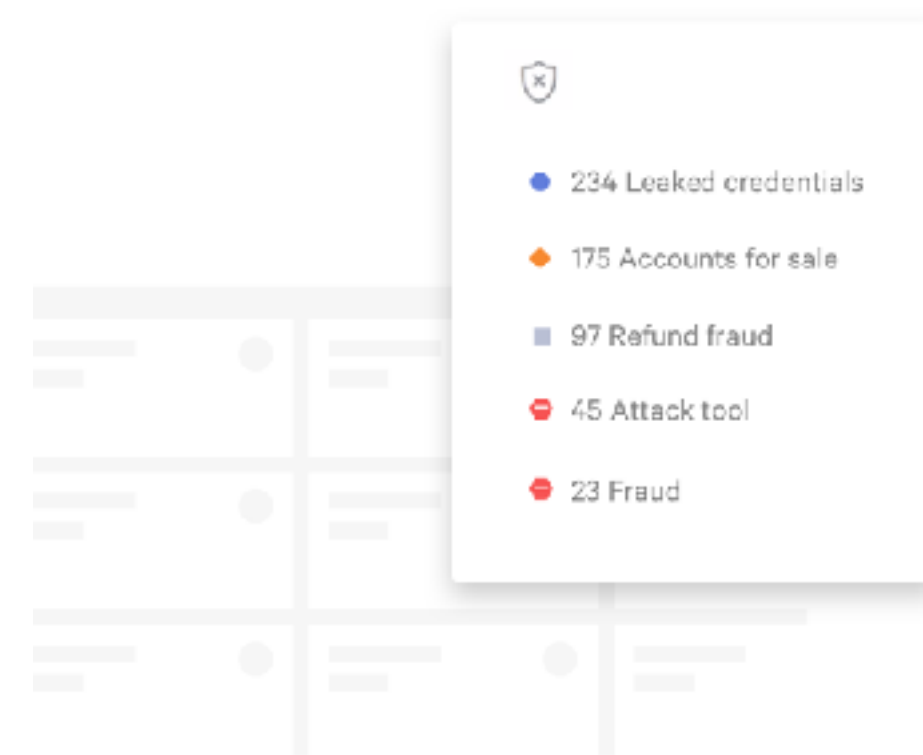
In order to tell a story about our product, features or the way they work, we use a collage of product screenshots and call-out website or interface elements.

Using these collages, we may focus on a particular actual or simplified Cyberint screenshot, and use several call-outs to give it context.

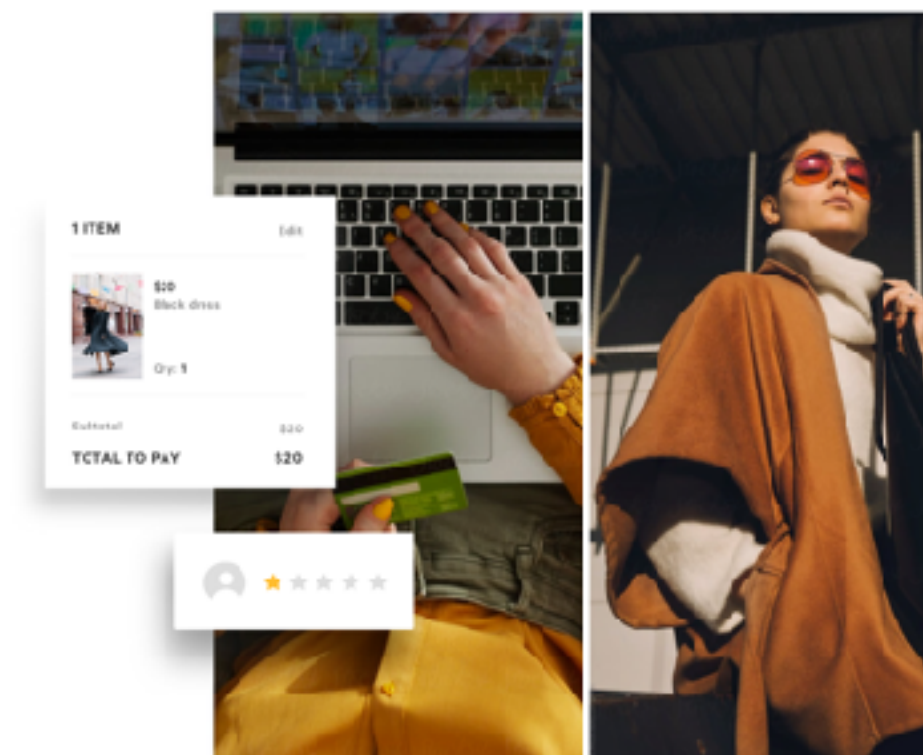
Call-outs may be taken from the screenshot itself, or illustrate different moments of a client’s customer journey online.



Cyberint screenshot with two call-outs taken from the product



Simplified screenshot (background) with call-outs



Simplified screenshot (background) with call-outs

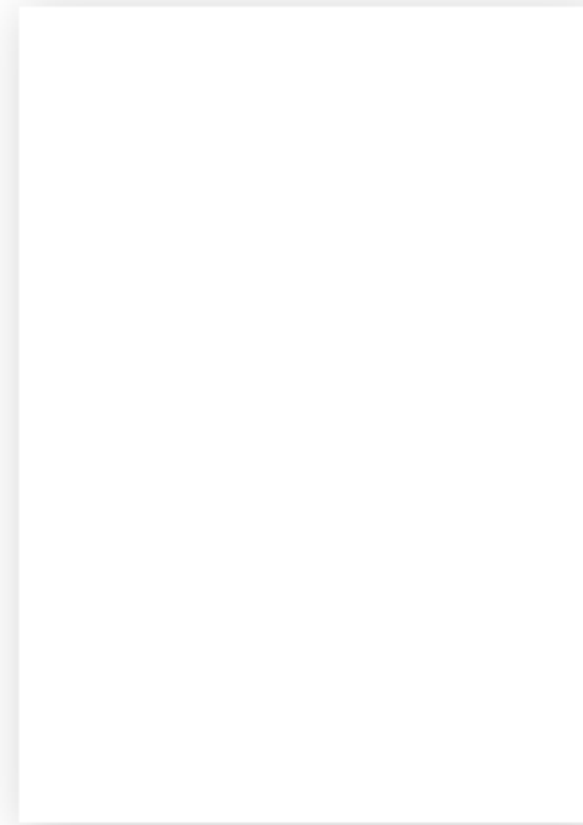
## Visual layouts

There are a number of optional layouts that can be used as a way to embed an image -

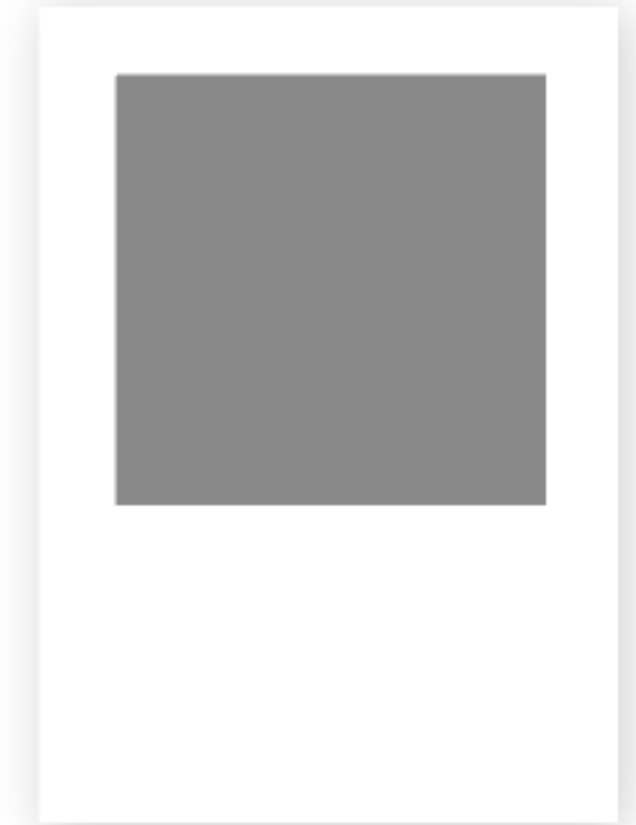
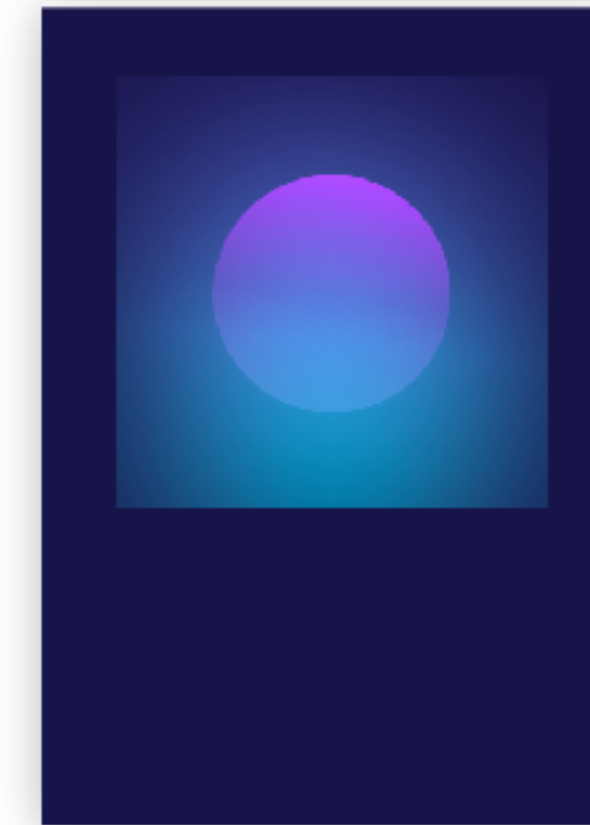
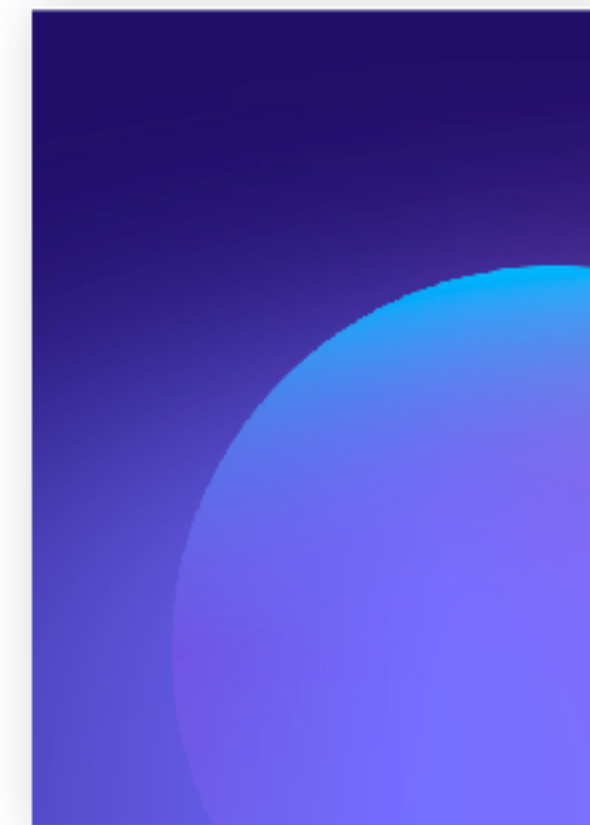
1. A solid color (dark or light)
2. A colourful sphere used as full-frame background or placed within a square.

In the following pages are examples of layout usages.

1.



2.





## Imagery variants – Reports/Brochures styles

A number of options for layouts used with different graphic elements:

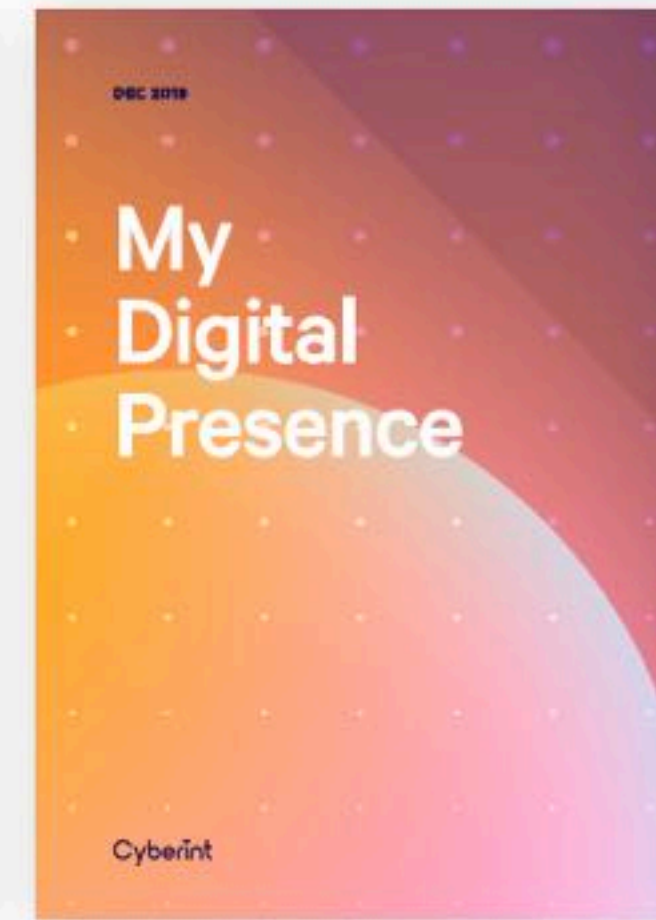
1. A round sphere on a colorful background,  
with or without the dot pattern
2. Use of spheres in motion/spotlights
3. Single color background

Typography color can be negative or positive according to the background color - light when the background is dark, and dark when the background is light.

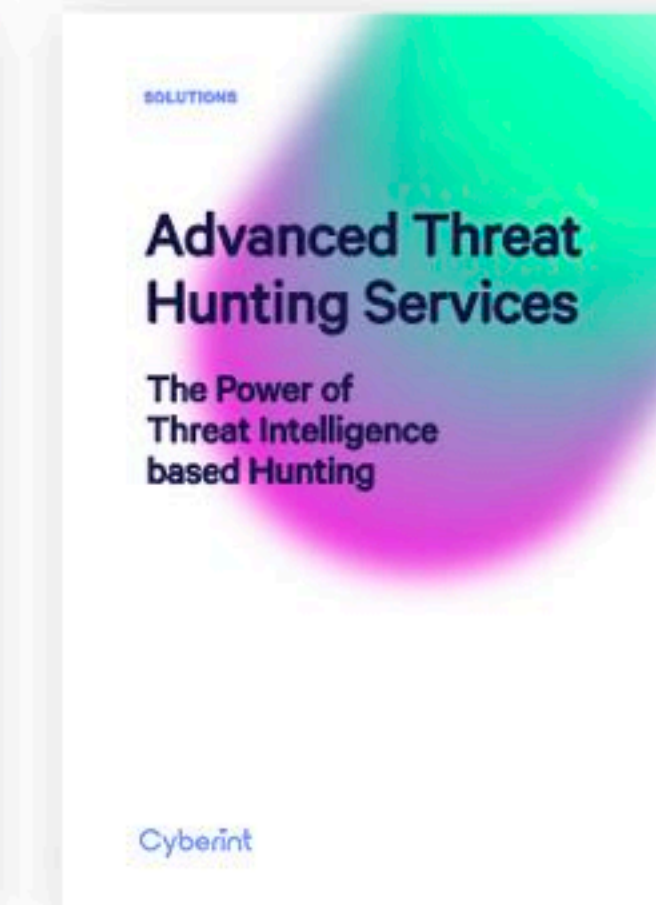
The color of the logotype should be treated in the same way



1.



2.



3.





## Imagery variants – Reports/Brochures styles

A number of options for layouts using a square and graphic elements

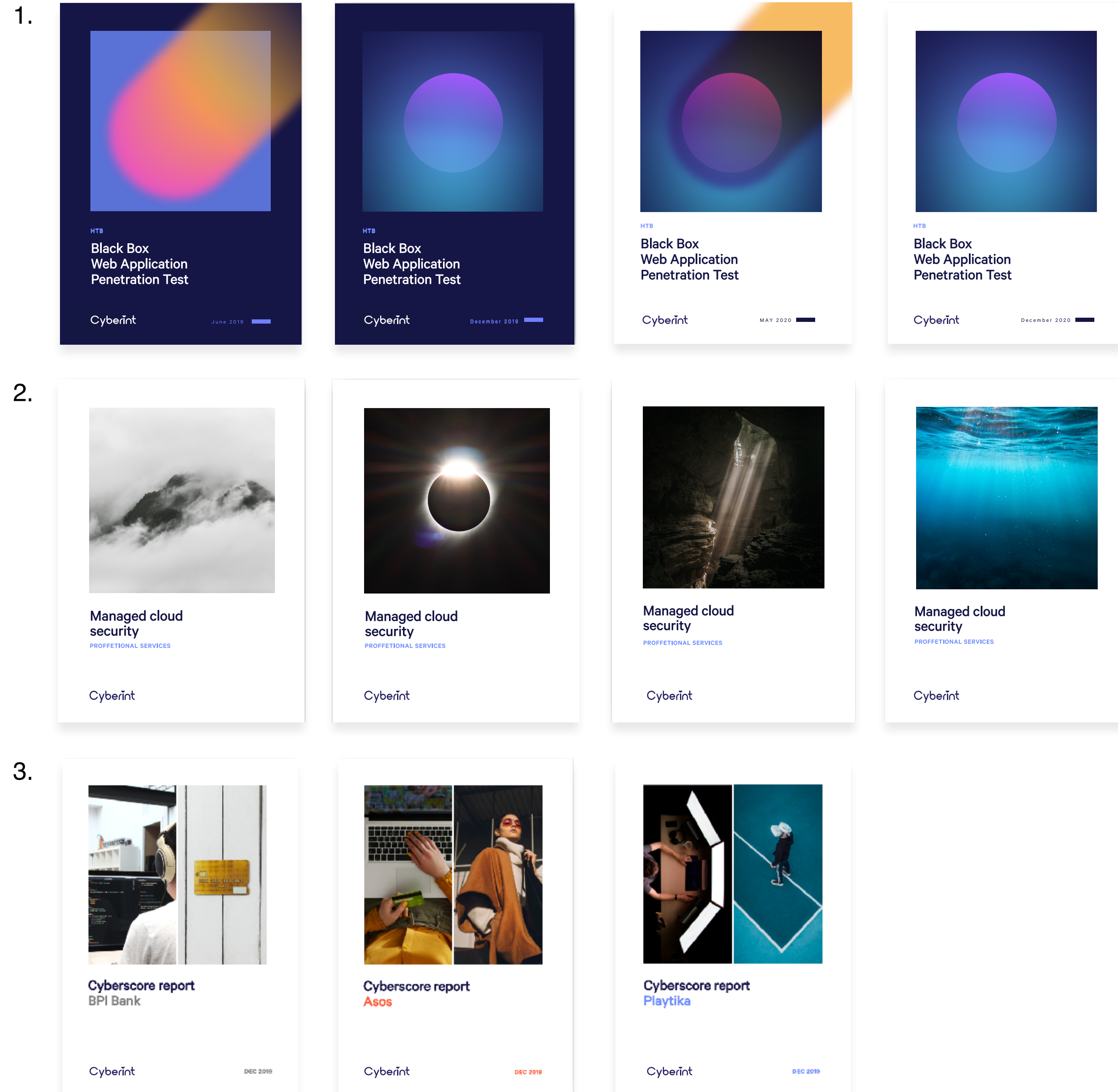
1. Spheres within a square. A dark or light background can be used according to typography color

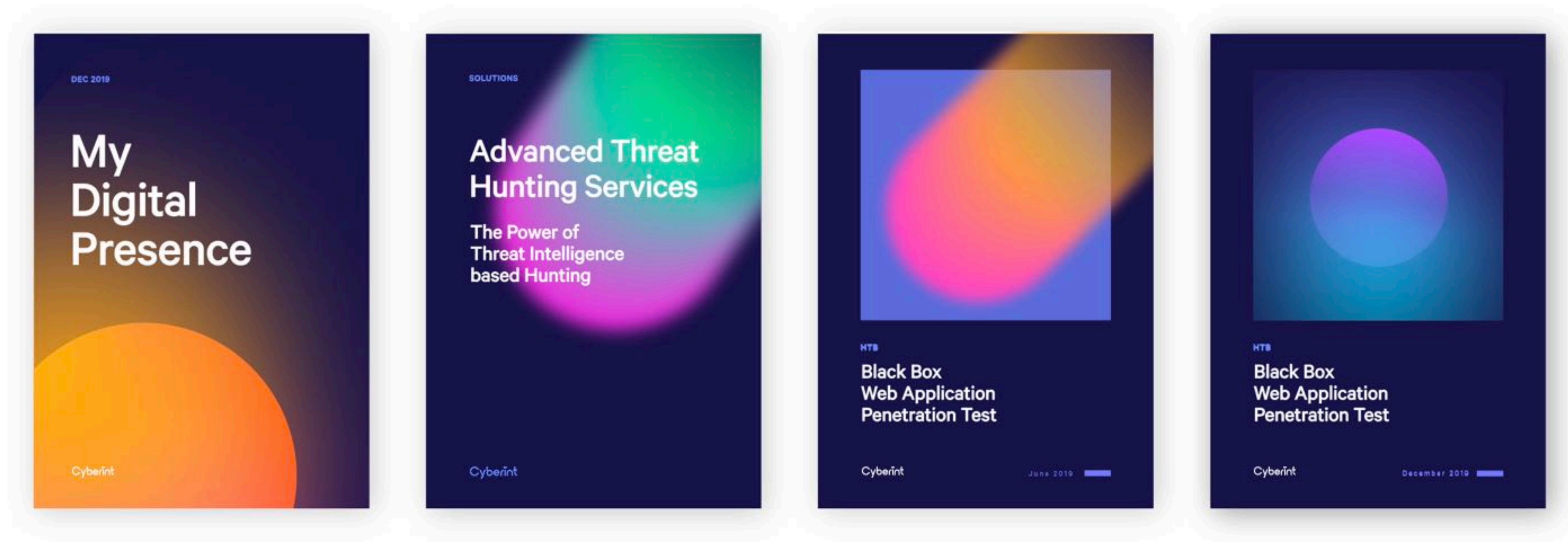
The sphere can remain within the square, or a sphere in motion can be used to break out of the square

2. A full single image of hidden nature within the square

3. Two images that together create a square

In the square layout, the typography must always appear outside of the square

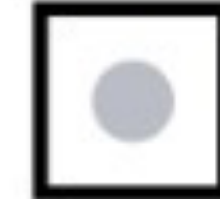
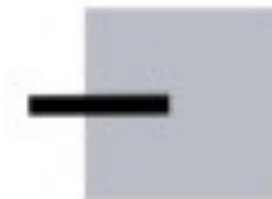




## Icon style 1 – Grayscale icons

Geometrical, minimalistic,  
simple, two-toned.

We use the two color icon style  
to visually illustrate features,  
journey moments and offering  
constructs.

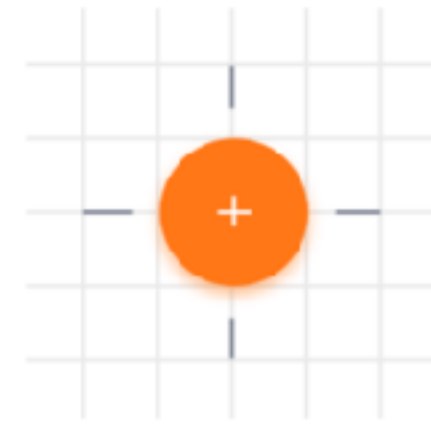




## Icon style 2 – Offering icons

Color + grays, geometrical shapes that are more complex, use of angles, and a grid background.

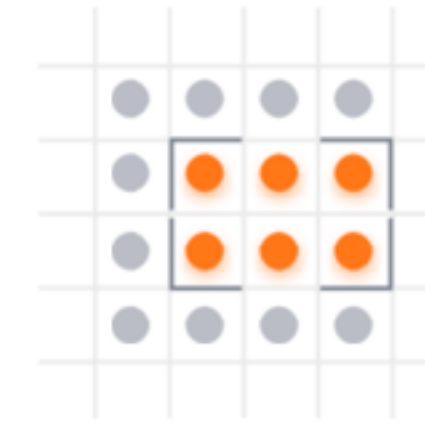
We use the offering icon style to provide a consistent visual representation of our solutions.



Identify



Verify



Respond



04

# Sample implementations





Cyberint

Itai Margalit  
CEO

M+972.54.7769500  
T+972.3.728.6777

itai@deio.com  
www.deio.com

Cyberint

Cyberint

Daniela Perlmutter  
VP Marketing

M+972.54.7769500  
T+972.3.728.6777

daniela@deio.com  
www.deio.com

Cyberint

Cyberint

Solutions

Markets

Company

Blog

Get a demo

# Business centered insight & action

Get a demo

Cyberint



# Business centered insight & action

Get a demo

MacBook

# Automated platform with cyber experts

Leave the buzzwords behind, expert analysts  
deliver concrete results



Business assurance

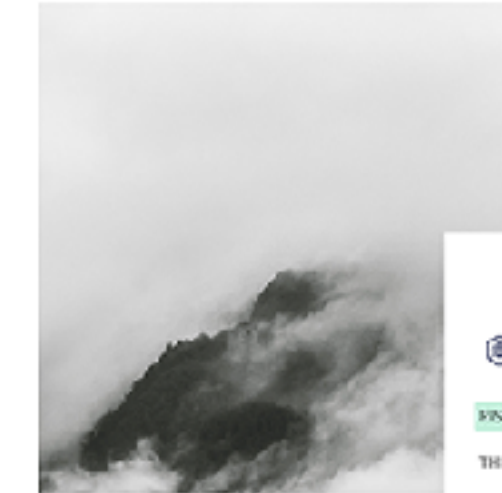
Threat detection

Incident detection & response

Proactive defense

## Penetration testing, red & purple team

We secure your business outside-in, inside-out,  
integrating internal activity and lorem ipsum dolor sit





## Cyber expertise across customer journeys, business processes & cyber threats

Protecting your customers, employees, business, and  
brand across domains and industries

[Learn more](#)



**Finance & banking**  
Feel safe online



**Retail & ecommerce**  
Threat-free customer journeys



**Games & entertainment**  
Being 1-step ahead



**More**  
Protect what matters

## Automated platform with cyber experts

Holistic security lorem ipsum dolor sit amet, zril  
suscipit cum na. Pro suavitare intollegat lorem

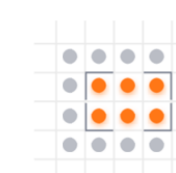
[Learn more](#)



Identify



Verify



Respond



# Presentation Title

Subheadline

Cyberint

VIZIO





Managed threat hunting  
PROFFETIONAL SERVICES



Records  
773,000,000  
users in  
'collection 2'

Cyberint

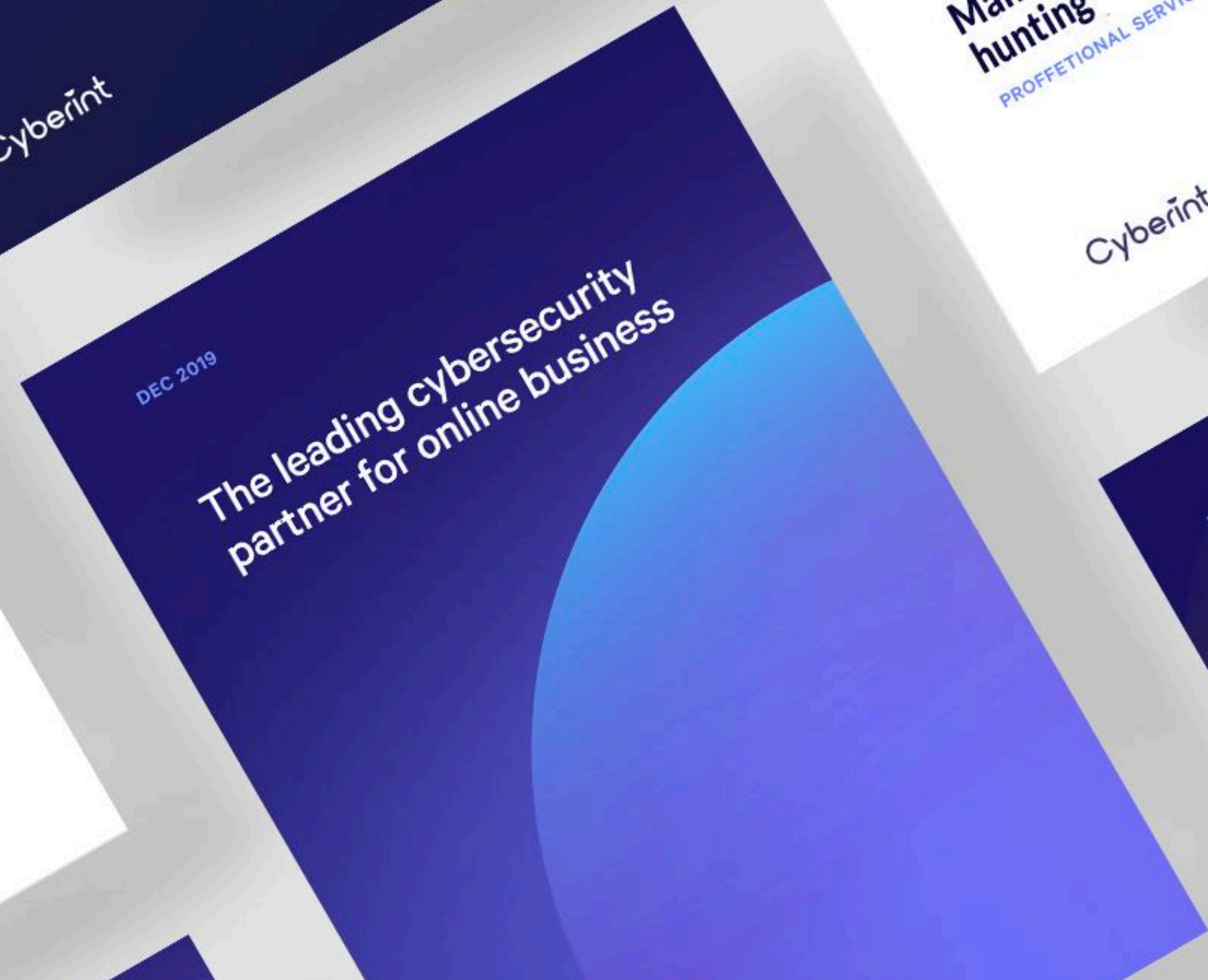
MAY 2019



DEC 2019

The leading cybersecurity  
partner for online business

Cyberint



Managed threat  
hunting

PROFFETIONAL SERVICES

Cyberint



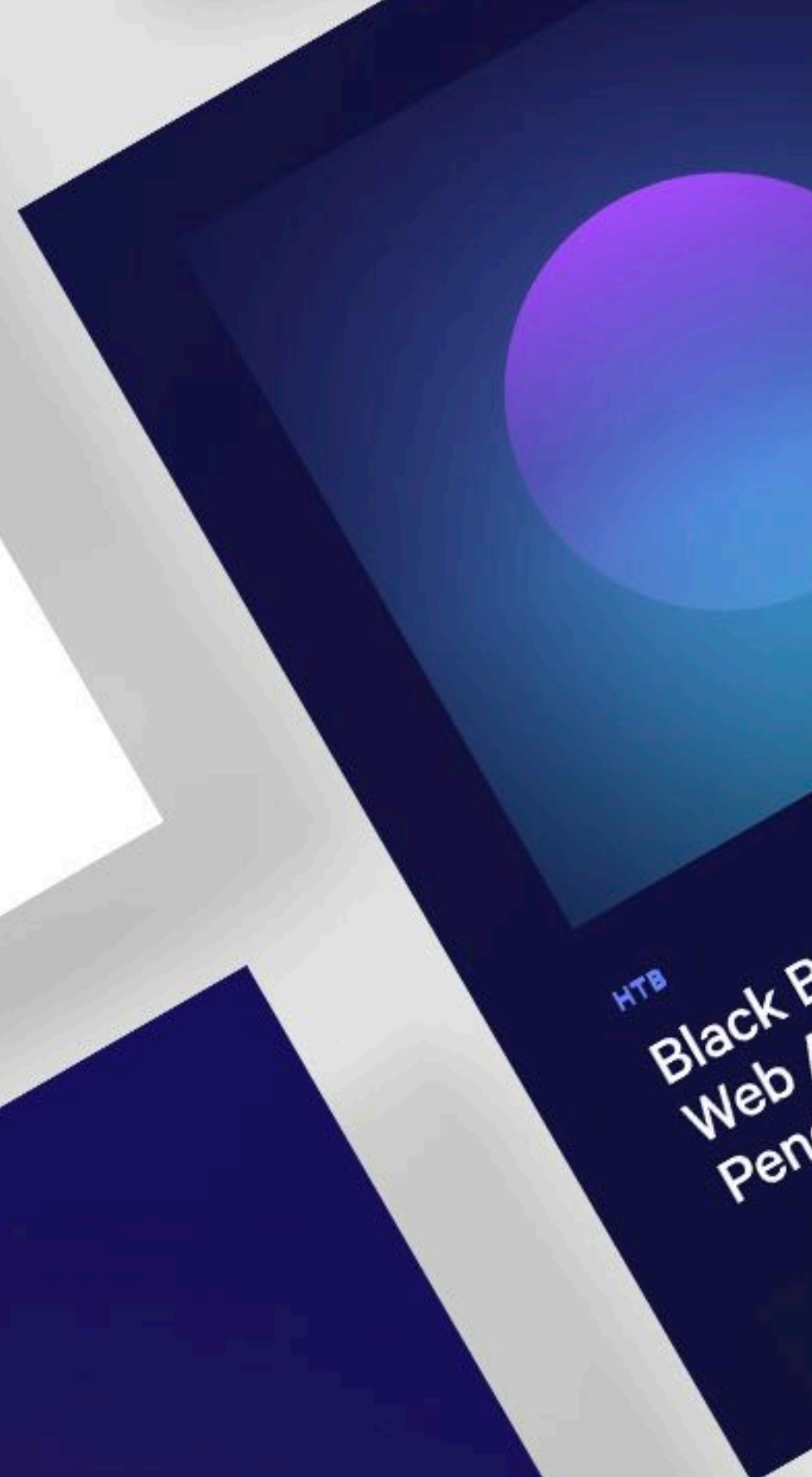
DEC 2019

My  
Digital  
Presence



HTB

Black P  
Web  
Pen





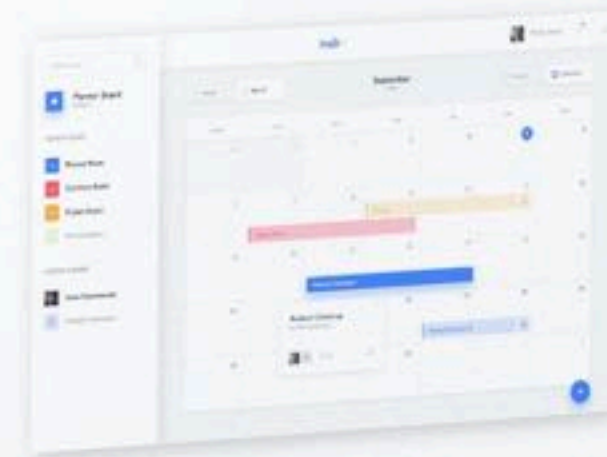
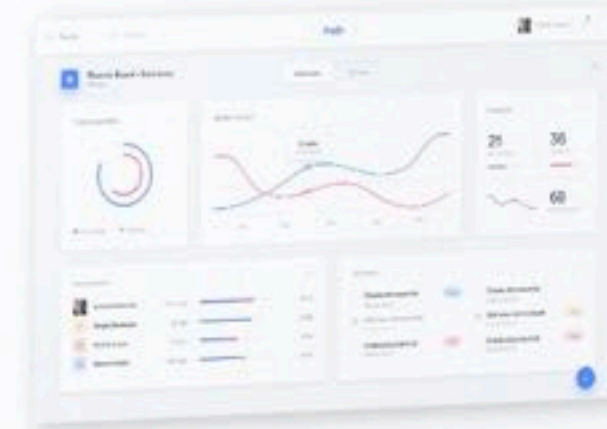
DEC 2019

# My Digital Presence

Cyberint

In today's rapidly changing business landscape, cybersecurity has become an increasingly shifting target, with new threats emerging daily. The race to detect and protect has transformed the cybersecurity dialogue into one of fear and damage prevention.

Current providers are responding to the evolving landscape with more solutions: more alerts, features, and data to ensure you keep up with attackers. These create more noise and greater anxiety, and often prevent you from actually identifying threats and attacks.



Cyberint

05

# **typography & layout guidelines**





# Reports/Brochures typography & layout style (cover pages)



Image

Subhead ← **PROFFETIONAL SERVICES**

Header ← **Managed threat Hunting**

Cyberint

deio copyright  
© all rights reserved

Logo

Copyrights

Subhead

Image

Header → **Records of 773,000,000 users in 'collection 1'**

DATA DUMP ANALYSIS  
by DEIO / 2019

Cyberint

deio copyright  
© all rights reserved

# Reports/Brochures typography & layout style (content pages)

Subsection Header Bar

Header

Body text (main)

Body text (expanded)

subhead separator line

Image

Cyberint

Logo

Caption

Copyrights

**ANALYSIS**

The initial data dump, aptly named 'Collection #1' based on the directory structure, is comprised of over 12,000 text files and SQL database dumps that total over 87GB of credential data. Within this, almost 773 million unique email addresses feature in over 1.1 billion unique credential combinations.

Whilst the source of each leaked credential cannot be fully determined, over 3,300 domains were identified from filenames within the leak and likely indicate that a service on that domain was compromised at some point in the past. Additionally, filenames containing names such as 'Dropbox', the file-hosting service that suffered a 68 million credential leak in August 2016, suggest that the collection contains data curated over the course of several years from both public and private data sources.

**DATA ORIGIN**

Comprised of multiple data sources, this data was originally advertised for sale for just US\$76 by a threat actor named 'Sanix' on various nefarious forums as part of a larger collection of 'combos' (Figure 2).

Based on subsequent forum discussions, a threat actor using the alias 'C0rpz', an individual with an apparent former business relationship, decided to leak the data set due to 'Sanix' reportedly scamming people (Figure 3).

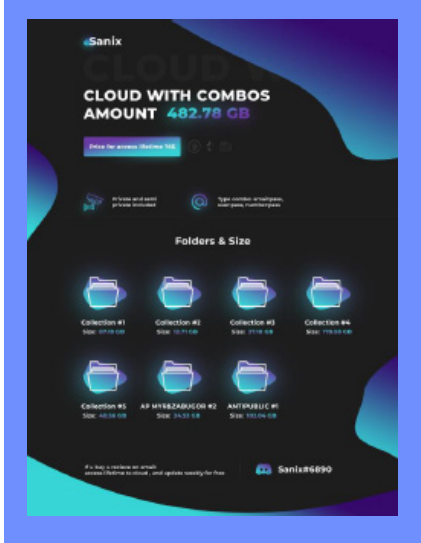




Figure 2 - Original 'collection' sale (https://shopyygg/product/rb9FKhm)

Figure 3 - Reason for the collection leak

deio copyright © all rights reserved

## WHAT ARE THE PAIN POINTS?

### Cloud Environment Visibility and Control Are Limited

Multi-cloud environments make it difficult to monitor data in motion in its entirety; data may be stored or pooled in multiple services and even locations, often not based on a long-term vision but on current objectives instead. Without a comprehensive cloud strategy and established security management tools at the core of processes, all of these factors weaken data transparency, visibility and control grip.

### Generic and Multiple Guidelines and Legislation

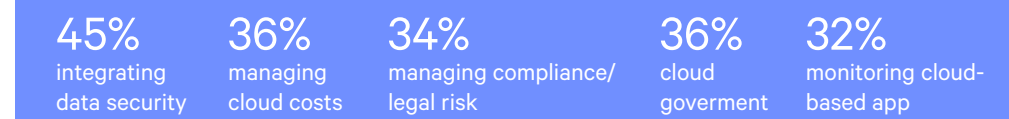
Alignment of the cloud infrastructure with internal guidelines is a challenge for any company: hardening, data security, and access control policies traditionally developed for the organization aren't applicable and relevant to cloud services. It only gets worse when data privacy regulations come into play. It's no surprise that security issues and concerns are expanding – the introduction of GDPR is one of recent key contributors to this trend. Trying to adapt to one specific regulation will most likely cause a major security impact on the company's entire IT infrastructure.

### Poor Level of Cyber Expertise and Professionals

The rise of the cloud approach significantly increased the demand for high-level expertise among the organization's IT professionals, who see the bigger picture while maintaining control and detecting vulnerabilities. Security talent is already at an all-time deficit. The human element remains the weakest link in cloud security. In cloud computing, human error risk multiplies, as misappropriated or compromised credentials are able to play havoc with significant cloud data and applications.

## TOP 5 CHALLENGES IN SECURING YOUR BUSINESS

source: Accenture 2018



Cyberint

deio copyright © all rights reserved

Information box



# Format #1



PROFFETIONAL SERVICES

## Managed threat Hunting

Cyberint

deio copyright  
© all rights reserved

### WHAT ARE THE PAIN POINTS?

#### Cloud Environment Visibility and Control Are Limited

Multi-cloud environments make it difficult to monitor data in motion in its entirety; data may be stored or pooled in multiple services and even locations, often not based on a long-term vision but on current objectives instead. Without a comprehensive cloud strategy and established security management tools at the core of processes, all of these factors weaken data transparency, visibility and control grip.

#### Generic and Multiple Guidelines and Legislation

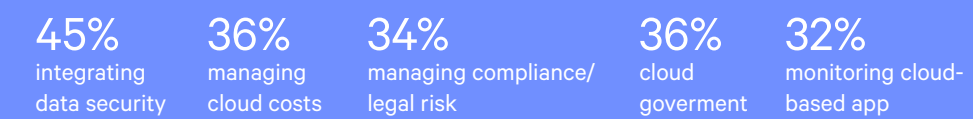
Alignment of the cloud infrastructure with internal guidelines is a challenge for any company: hardening, data security, and access control policies traditionally developed for the organization aren't applicable and relevant to cloud services. It only gets worse when data privacy regulations come into play. It's no surprise that security issues and concerns are expanding – the introduction of GDPR is one of recent key contributors to this trend. Trying to adapt to one specific regulation will most likely cause a major security impact on the company's entire IT infrastructure.

#### Poor Level of Cyber Expertise and Professionals

The rise of the cloud approach significantly increased the demand for high-level expertise among the organization's IT professionals, who see the bigger picture while maintaining control and detecting vulnerabilities. Security talent is already at an all-time deficit. The human element remains the weakest link in cloud security. In cloud computing, human error risk multiplies, as misappropriated or compromised credentials are able to play havoc with significant cloud data and applications.

### TOP 5 CHALLENGES IN SECURING YOUR BUSINESS

source: Accenture 2018



Cyberint

deio copyright  
© all rights reserved

### CONTACT US

**UK**  
+442035141515

**Israel**  
+442035141515

**USA**  
+442035141515

**Singapore**  
+442035141515

[sales@deio.com](mailto:sales@deio.com)

Cyberint

deio copyright  
© all rights reserved





# Format #1

**Page 1:**

- Image: 16.4 cm x 16.4 cm
- Subhead: **8.5 pt Bold (Subhead) UPPER CASE** → **PROFFETIONAL SERVICES**
- Headline: **38 pt Semibold (Headline) Title case** → **Managed threat Hunting**
- Footer: **10 pterodactyls Regular (Copyrights)**

**Page 2:**

- Section Header: **18 pt Bold (Headline) UPPER CASE** → **WHAT ARE THE PAIN POINTS?**
- Text: **12 pt Semibold (Subhead) Title case** → **Cloud Environment Visibility and Control Are Limited**
- Text: **12 pt Regular (Text) Title case** → **Generic and Multiple Guidelines and Legislation**
- Text: **12 pt Regular (Text) Title case** → **Poor Level of Cyber Expertise and Professionals**
- Section Header: **16.4 cm** → **TOP 5 CHALLENGES IN SECURING YOUR BUSINESS**
- Text: **16 t Bold (Headline) UPPER CASE** → **45%**
- Text: **12 pt Regular** → **36%**
- Text: **12 pt Regular** → **34%**
- Text: **24 pt Regular (Numbers)** → **36%**
- Text: **24 pt Regular (Numbers)** → **32%**
- Text: **10 pterodactyls Regular (Copyrights)**

**Page 3:**

- Section Header: **16 pt Bold (Subhead) UPPER CASE** → **CONTACT US**
- Text: **12 pt Regular (Information)** → **UK**
- Text: **12 pt Regular (Information)** → **Israel**
- Text: **16 pt Bold (Information)** → **USA**
- Text: **16 pt Bold (Information)** → **Singapore**
- Text: **10 pt Regular (Copyrights)** → **sales@deio.com**
- Text: **10 pterodactyls Regular (Copyrights)**





# Format #2



888 HOLDINGS 10/12/2020 08:15

## Cyberscore Report

Cyberint deio copyright  
© all rights reserved

### WEB APPLICATION SECURITY A

One of the most vulnerable attack surface with-in the organization is public-facing web applications, with an external interface that can exploited by an attacker. The technical skillset required to perform such an attack is basic and documentation of such methods are publicly available. As a first step of Advance Persistence Threat (APT), an attacker can exploit a web application in order to gain control over internal systems, with higher privileges. Most of the Web applications are usually front-ends for databases and contain user-specific data.

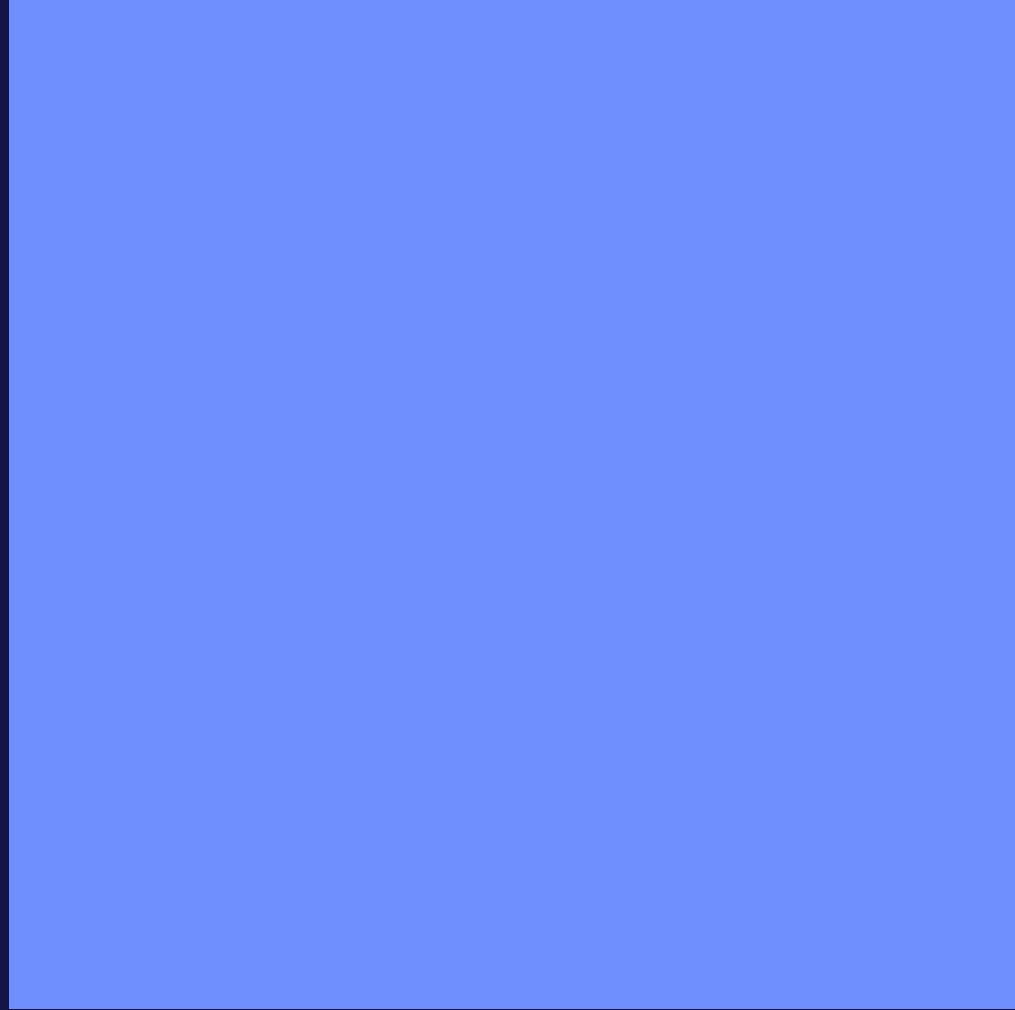
Increasing businesses' adoption of the web combined with attackers' ingenuity to find new attacks methods, are making web application one of the most vulnerable assets of the enterprise. Securing the organization's web application is somewhat challenging, as it involves not only advanced isolation and application hardening – infrastructure securing is also mandatory, as part of a secured application development lifecycle (SDLC).

#### Key Findings

■ **Missing HTTP Headers**

- 183 assets are missing content-security-policy security header
- 182 assets are missing x-content-type-options security header
- 25 assets are missing strict-transport-security security header
- 183 assets are missing x-xss-protection security header
- 180 assets are missing x-frame-options security header

Cyberint deio copyright  
© all rights reserved



**CONTACT US**

<b>UK</b> +442035141515	<b>Israel</b> +442035141515
<b>USA</b> +442035141515	<b>Singapore</b> +442035141515

[sales@deio.com](mailto:sales@deio.com)

Cyberint deio copyright  
© all rights reserved



# Format #2

Thumbnail image of a report cover. The cover has a dark blue background. At the top, there is a dark blue header bar. Below it is a large, light gray square with a white 'X' shape and a circular logo in the center. The square is labeled '16.4 cm (Image)'. Below the square is a dark blue footer bar containing the text '888 HOLDINGS', 'Cyberscore Report', and 'Cyberint'. The date '10/12/2020 08:15' is also visible. Dimensions and annotations are shown with dashed lines and arrows.

Annotations:

- Top-left corner: 2.3 cm
- Top-right corner: 2.3 cm
- Bottom-right corner: 2.3 cm
- Bottom-left corner: 2.3 cm
- Text '888 HOLDINGS': 8.5 pt Bold (Subhead) UPPER CASE
- Text 'Cyberscore Report': 38 pt Semibold (Headline) Title case
- Text '10/12/2020 08:15': 16 pt Regular (Date)
- Text 'Cyberint': 10 pt Regular (Copyrights)

Thumbnail image of a report page. The page has a white background. At the top, there is a dark blue header bar. Below it is a large, light blue square with a white 'X' shape and a circular logo in the center. The square is labeled '16.4 cm (Image)'. Below the square is a dark blue footer bar containing the text 'Cyberint'. The date '10/12/2020 08:15' is also visible. Dimensions and annotations are shown with dashed lines and arrows.

Annotations:

- Top-left corner: 2.3 cm
- Top-right corner: 2.3 cm
- Bottom-right corner: 2.3 cm
- Bottom-left corner: 2.3 cm
- Text 'WEB APPLICATION SECURITY': 18 pt Bold (Headline) UPPER CASE
- Text 'Cyberscore Report': 12 pt Regular (Text)
- Text 'Cyberint': 10 pt Regular (Copyrights)
- Text '10/12/2020 08:15': 16 pt Regular (Date)
- Text 'Key Findings': 12 pt Semibold (Subhead) Title case
- Text 'Missing HTTP Headers': 10 pt Regular (Section Header)
- Text '183 assets are missing content-security-policy security header': 10 pt Regular (Text)
- Text '182 assets are missing x-content-type-options security header': 10 pt Regular (Text)
- Text '25 assets are missing strict-transport-security security header': 10 pt Regular (Text)
- Text '183 assets are missing x-xss-protection security header': 10 pt Regular (Text)
- Text '180 assets are missing x-frame-options security header': 10 pt Regular (Text)

Thumbnail image of a report page. The page has a white background. At the top, there is a dark blue header bar. Below it is a large, light blue square with a white 'X' shape and a circular logo in the center. The square is labeled '16.4 cm (Image)'. Below the square is a dark blue footer bar containing the text 'CONTACT US', 'UK', 'Israel', 'USA', 'Singapore', 'sales@deio.com', and 'Cyberint'. The date '10/12/2020 08:15' is also visible. Dimensions and annotations are shown with dashed lines and arrows.

Annotations:

- Top-left corner: 2.3 cm
- Top-right corner: 2.3 cm
- Bottom-right corner: 2.3 cm
- Bottom-left corner: 2.3 cm
- Text 'CONTACT US': 16 pt Bold (Subhead) UPPER CASE
- Text 'UK': 12 pt Regular (Information)
- Text 'Israel': 12 pt Regular (Information)
- Text 'USA': 12 pt Regular (Information)
- Text 'Singapore': 12 pt Regular (Information)
- Text 'sales@deio.com': 16 pt Bold (Information)
- Text 'Cyberint': 10 pt Regular (Copyrights)
- Text '10/12/2020 08:15': 16 pt Regular (Date)



# Format #3

**DATA DUMP ANALYSIS**  
by DEIO / 2019

# Records of 773,000,000 users in 'collection 1'

**Cyberint** deio copyright © all rights reserved

## ANALYSIS

The initial data dump, aptly named 'Collection #1' based on the directory structure, is comprised of over 12,000 text files and SQL database dumps that total over 87GB of credential data. Within this, almost 773 million unique email addresses feature in over 1.1 billion unique credential combinations.

Whilst the source of each leaked credential cannot be fully determined, over 3,300 domains were identified from filenames within the leak and likely indicate that a service on that domain was compromised at some point in the past. Additionally, filenames containing names such as 'Dropbox', the file-hosting service that suffered a 68 million credential leak in August 20164, suggest that the collection contains data curated over the course of several years from both public and private data sources.

### DATA ORIGIN

Comprised of multiple data sources, this data was originally advertised for sale for just US\$76 by a threat actor named 'Sanix' on various nefarious forums as part of a larger collection of 'combos' (Figure 2).

Based on subsequent forum discussions, a threat actor using the alias 'C0rpz', an individual with an apparent former business relationship, decided to leak the data set due to 'Sanix' reportedly scamming people (Figure 3).



Folder	Size
Collection #1	100 MB
Collection #2	100 MB
Collection #3	100 MB
Collection #4	100 MB
Collection #5	100 MB
Collection #6	100 MB
Collection #7	100 MB
Collection #8	100 MB



Creation Date: Jan 21st 2019 - 13:30:35  
Published: Jan 21st 2019 - 12:47:28

ok dm me xDDD  
Discord: C0rpz#5867

Creator of "Collection #1"  
There are 7 Collections, and 5 leaked.  
The reason for the leak was simply: "Sanix#1165", he used to resell my Collections & Scammed people so I leaked them.  
But not #7 and #6 :)  
And now it got viral on the media.  
#NullSec | Hacking Squad |  
<https://www.troyhunt.com/the-773-million-ata-reach-more-passwords-may-be-at-risk/>

Leak Hack

**Cyberint** deio copyright © all rights reserved

## CONTACT US

<b>UK</b> +442035141515	<b>Israel</b> +442035141515
<b>USA</b> +442035141515	<b>Singapore</b> +442035141515

**sales@deio.com**

**Cyberint** deio copyright © all rights reserved



# Business card typography & layout style

