HUMANIZE

SAFEGUARDING DIGITAL BEHAVIOR

# SALIENCE

# WHITEPAPER

SALIENCE

www.humanize.security

# Table of Contents

# Introduction

Cyber risks top  business concerns in 2022 worldwide.

The threat of ransomware attacks, data breaches, or major IT outages bothers companies even more than business and supply chain disruption, natural disasters, or the COVID-19 pandemic.

Cyber attacks on all businesses, particularly on small to medium-size businesses, are becoming more frequent, targeted, and complex.

**43%**

of cyber attacks target small businesses.

**$1.07 mln**

Organizations that have adopted remote working spend an additional $1.07 million responding to data breaches.

**$2.72 mln**

unfilled roles in cybersecurity.

**$4.24 mln**

The average data breach cost increased from $3.86 million in 2020 to $4.24 million in 2021.

## Why cybersecurity is the new black in the business world?

- **Number of cyberattacks are increasing**

  Cyberattacks are becoming more common and the nature of those attacks are more sophisticated.

- **New risks brought by remote work and geopolitical tensions**

  Cyberwarfare and the trend of remote working have generated new cyber risks, which are ringing bells for businesses.

- **There is a huge skills gap in cybersecurity**

  The world is lacking 3 million cybersecurity professionals, according to the latest report by the World Economic Forum (WEF).

- **Small and medium-sized businesses are widely targeted by opportunistic adversaries or nation-state groups**

  Frail cyber security due to the limited budget has made small and medium-sized businesses the most vulnerable target for threat actors and nation-state sponsored groups.

# Industry-specific challenges

## HEALTHCARE SECTOR

The healthcare sector is a top target among adversaries. Cyber-attacks can expose sensitive patient information and result in substantial financial losses and regulatory penalties.

## GOVERNMENTAL AGENCIES

Government bodies always remain over the radar of threat actors which is why they are under high cyber risk. Cybercriminals target government data, networks and systems, and cyber-attacks are often politically motivated.

## FINANCIAL SECTOR

Cybersecurity is a top challenge in the financial industry.
With the active digital transformation of financial institutes, there is a noticeable surge in cyber threats and fraudulent activities in the financial sector.

## CORPORATE & ENTERPRISE

Identifying and quantifying cybersecurity risks is the modern challenge in corporations now. C-levels are alarmed by the increasingly sophisticated and broad nature of cyber-attacks which are causing regulatory compliance Issues and affecting decision making.

## INSURANCE

Insurance companies are being challenged to embrace cyber innovation and update their systems and infrastructure. Consequently, they store substantial amounts of business and personal information about their policyholders online.

## TELECOM & IOT

Telecom & IoT is a critical infrastructure that is growing exponentially and has many internet facing assets and customers that communicate, process, and store enormous amounts of sensitive data.

# Modern cyber challenges for business leaders

Cybersecurity is no longer a problem that only security teams should consider. The rapid growth of cyber-attacks and increase in the average cost of data breaches are alarming companies' **executives and board members.**

As reported by business leaders, the main challenges they face when it comes to cybersecurity are: complexity, unawareness, poor budget.

1.

## Complexity

They do not understand the complex language of cybersecurity. Cybersecurity solutions fail to use easy-to-understand and human readable concepts, for all most C-level executives.

2.

## Unawareness

They are not aware of what company assets are exposed to cybercriminals, what cyber threats pose critical or high risks and what is their financial impact.

3.

## Poor Budget

To prevent cyberattacks, a company needs a proper cyber budget for both hiring an internal security team and external services (audit, penetration testing, etc.). However, small and medium companies usually lack that budget.

# SAAS AS A SOLUTION

By positioning itself as **quantified cyber risk management solution**, Humanize is transforming the cybersecurity landscape.

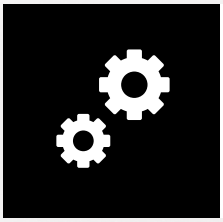
Humanize makes cybersecurity easy for business leaders and provides them the opportunity to be in control of their cybersecurity posture.

Our platform, called **Salience**, has a simplified user-friendly interface that provides **easily understandable** and **human readable analysis** for non-technical individuals. Hence, we got the name “Humanize Security”, human-readable cybersecurity for C-Suite executives to understand and control their organization’s cybersecurity priorities independently and make decisions accordingly.

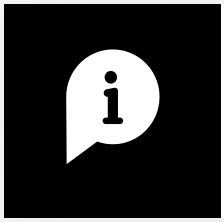
Salience gives a clear understanding to C-Suite what could be at stake.

Eventually, **what business leaders want** is to see the risks associated with security issues, what they mean to their business (impact) and what operational, financial, regulatory, or reputational risk they may face.

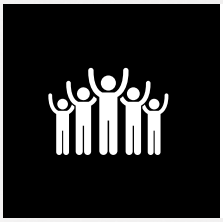
## What digital assests a company has:



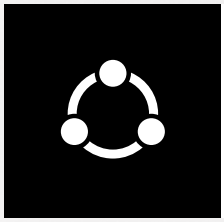
TECHNICAL



INFORMATIONAL



HUMAN



THIRD-PARTY

# SALIENCE ENTERPRISE

## Salience Technology

Salience assesses an organization's attack surface the same way an adversary will look to compromise or attack a target. Salience uses the same adversary tools and techniques in an automated way to discover and analyze the risks or threats an organization is exposed to adversaries.

Salience provides an automated, close-to-real-time view of attack surface threats of organizations, vendors, and partners.

- **MetaDiscovery**

  Continuously hunt for security flaws and new threats.

- **MetaThreat**

  With the use of artificial intelligence (AI), Salience will discover the threat and list down its severity, likelihood, business impact, and more factors.

- **MetaAction**

  Continuous and automated safe-attack mechanism to test and verify the cybersecurity weaknesses and vulnerabilities of the organization.

- **MetaProtect**

  Quantified cyber risks mitigation for C-Suite to make confident decisions and smooth planning.

# Salience Process

**Attack Surface Management: MetaAction & MetaDiscovery**

During **MetaDiscovery** process, with the help of MetaAction technology, Salience runs passive and active safe attacks on 4 types of assets of a company:

- Technical assets
- Informational assets
- Human assets
- 3rd party assets

**MetaAction**

Afterwards, the data is visualized and presented in 3 types of reports, with an option for customization:

- Risk assessment reports,
- Audit reports,
- Financial risks reports,
- Board reports.

**Risk Analysis & Scoring: MetaThreat**

In **MetaThreat** process, our technology analyzes the discovered security weaknesses and vulnerabilities using the power of artificial intelligence (AI). Afterwards, it scores severity, likelihood, and business impact of those weaknesses, vulnerabilities and misconfigurations of attack surface.

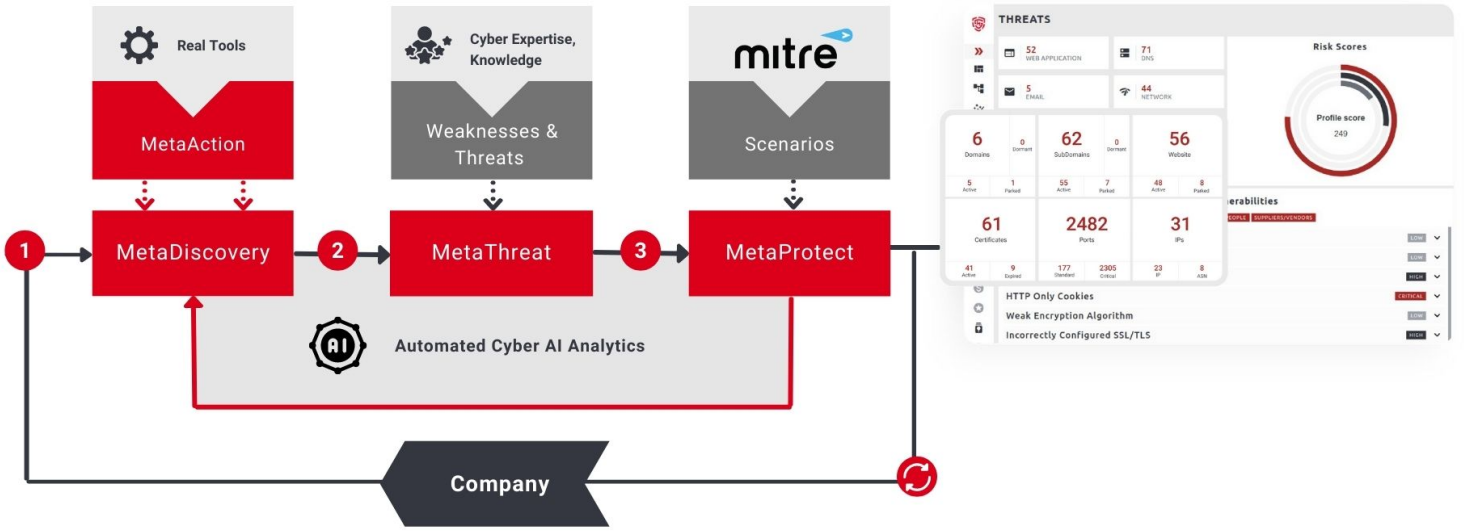
By analyzing the data, the technology quantifies the Technical, Financial & Compliance risks.

**Remediation & Recommendations: MetaProtect**

Lastly, **MetaProtect step**, Salience generates a remediation playbook that includes:

- Guides for vulnerability management,
- Prioritization of top vulnerable assets,
- Recommendations how to fix the issues,
- Industry based recommendations.

# Salience Flow




# Methodology & Frameworks

We are intelligently automating the adversary approach based on MITRE Attack, OWASP and WASC frameworks using real life adversary tools manipulated by our Cyber AI module.

In the toolchain, we have tools written in C/C++, Phyton, Go, JS, Shell and Bash Scripts.

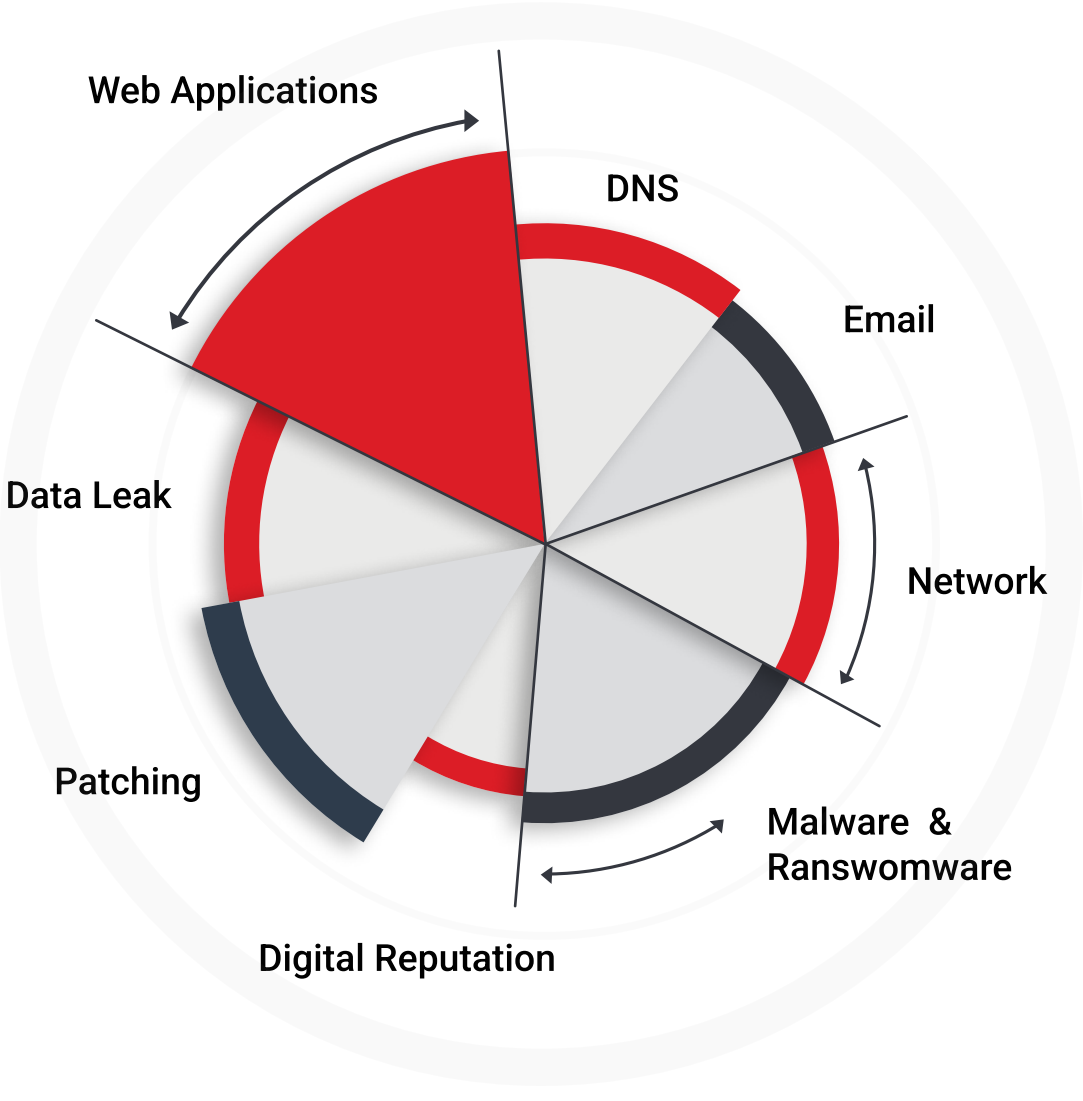
The Salience Platform is designed using a microservices architecture with a message/event driven approach and dynamically scalable architecture. The technology stack of the platform frontend is ReactJS SPA connected to the backend over APIs and Socket connections. The backend consists of a number of microservice and Containerization.

# 8D cybersecurity profile

Salience provides an 8-dimensional security profile to discover how secure the company is and what weaknesses and vulnerabilities are in each classified dimension presented in their severity and impact levels.

These classified dimensions help business leaders have a helicopter view of the company's attack surface in the identification and mitigation process.

- Web Applications
- Digital Reputation
- DNS
- Malware & Ransomware
- Email
- Patching
- Network
- Data Leak



# Features

## 01 ATTACK SURFACE MANAGEMENT

Continuous and automated process of discovery, classification, prioritization, and security monitoring of the company's IT assets that contain, transmit, or process sensitive data and could be seen by attackers looking in from outside to compromise

## 02 VULNERABILITY ASSESSMENT & PRIORITIZATION

Automated and continuous analysis of weaknesses based on severity, asset criticality, exploitability, exposure and business impact. Dynamic calculations and assignment of straightforward, normalized security scores to each asset. Prioritization of weaknesses that will have the biggest impact on risk remediation

## 03 VULNERABILITY INTELLIGENCE

Automatically customized attack vector analysis is focused on the aggregation of discovered threats that may put the company at cyber risk

## 04 AUTOMATED PENETRATION TESTING

Automated process of detecting weaknesses, misconfigurations and vulnerabilities performed with real-life penetration testing methods & tools

## 05 AUTOMATED & CONTINUOUS RED TEAMING

Automated and continuous process of launching simulated safe-attacks on company's internet-facing assets to test the attack surface on daily basis

## 06 CYBER RISK QUANTIFICATION

Evaluating the potential financial impact of discovered cyber weaknesses and threats based on Open FAIR model. Calculated and normalized financial risk score for each threat vector enables C-Suite and security/IT teams to talk numbers

## 07 SECURITY RISK SCORING & PRIORITIZATION

Security Risk Score is calculated and used to rank the priority relative to the discovered weaknesses and threats. Risk prioritization is the automated process of determining which risk should be remediated first based on likelihood and impact

## 08 THIRD PARTY RISK MANAGEMENT

Automatic and continuous monitoring of third party organizations' quantified risk scores that are potential threats to company's employees, customer & financial data or operations continuity from the supply-chain perspective

## 09 RISK REMEDIATION PLAYBOOK

Dynamically generating recommendations for each weakness and vulnerability on how-to-remediate and overcome providing a clear understanding of detected threats mitigation before a security incident

## 10 ROLE-BASED REPORTING

Multi-purpose reporting allows different stakeholders to get risk and security performance metrics from outside look. Reports translate the relevant complex security data for C-Suite (CEO, CFO, COO, etc.) in different roles to make important risks mitigation decisions independently

## 11 ALERTS & NOTIFICATIONS

Automated alerts based on triggers that can be enabled and customized by a user. Notifications can be sent via email as well

## 12 BUSINESS/ EXPERT MODE

Business mode is a humanized version of Expert mode for C-Suite to take control of their companies' external attack surface. Meanwhile Expert mode is designed for IT/ security teams providing professional functionality and features

# SOLUTIONS

## Vulnerability Management

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.

**Salience identifies vulnerabilities on 4 types of assets:**

- TECHNICAL
- HUMAN
- INFORMATIONAL
- THIRD-PARTY

With an 8-dimensional cybersecurity profile, Salience provides an overview of the company's cyber posture and the criticality level of vulnerabilities.

## Quantified Risk Management

Salience evaluates the security risks of organizations and provides a mitigation playbook to fix the issues before adversaries exploit them.

It conducts risk assessment analysis using **ISO27k, NIST, PCI DSS, OWASP, and other technical and compliance standards** mapped to the FAIR Institute's quantitative information risk model to produce the value of risk for cybersecurity and operational risks.

# Third Party Risks

Our solution has enormous potential to help enterprises in various industries who are constantly struggling to keep on top of their risk profile. The old method of running 3rd party vendor due to diligence questionnaires, point-in-time penetration tests, or annual red teaming only provides a snapshot view of risk and getting a sense of risky suppliers and vendors.

Our approach is quite easy to onboard onto the platform. The enterprise provides their known suppliers, we obtain the consent of assessing their systems and then Salience starts with identifying and quantifying the risk of those organizations, finding what other 3rd parties or technologies are linked to, and assessing those.

The platform can be easily incorporated into a vendor onboarding process without heavy investment and time needed to continuously manage and assess the risks.

# CONCLUSION

Humanize Salience is one-stop solution for C-Suite executives of small to medium size businesses when it comes to cybersecurity. With the help of Salience human readable analytics, whole cybersecurity landscape of an organization will be concluded in easily understandable format. This will ultimately help you make efficient and confident decisions. Salience Meta family will continually prevent your valuable assets from cyber criminals.

HumanizeInc humanize-inc @HumanizeInc

www.humanize.security