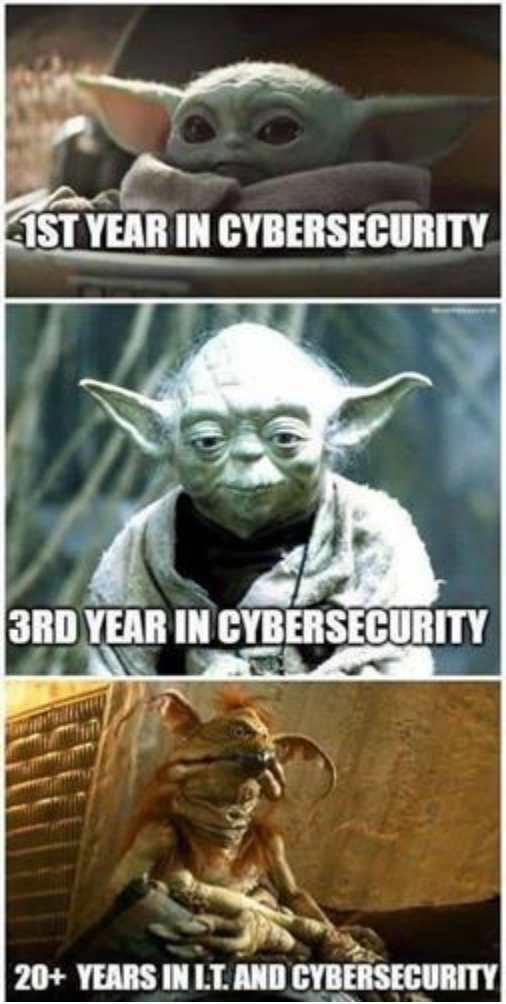
RAPID7

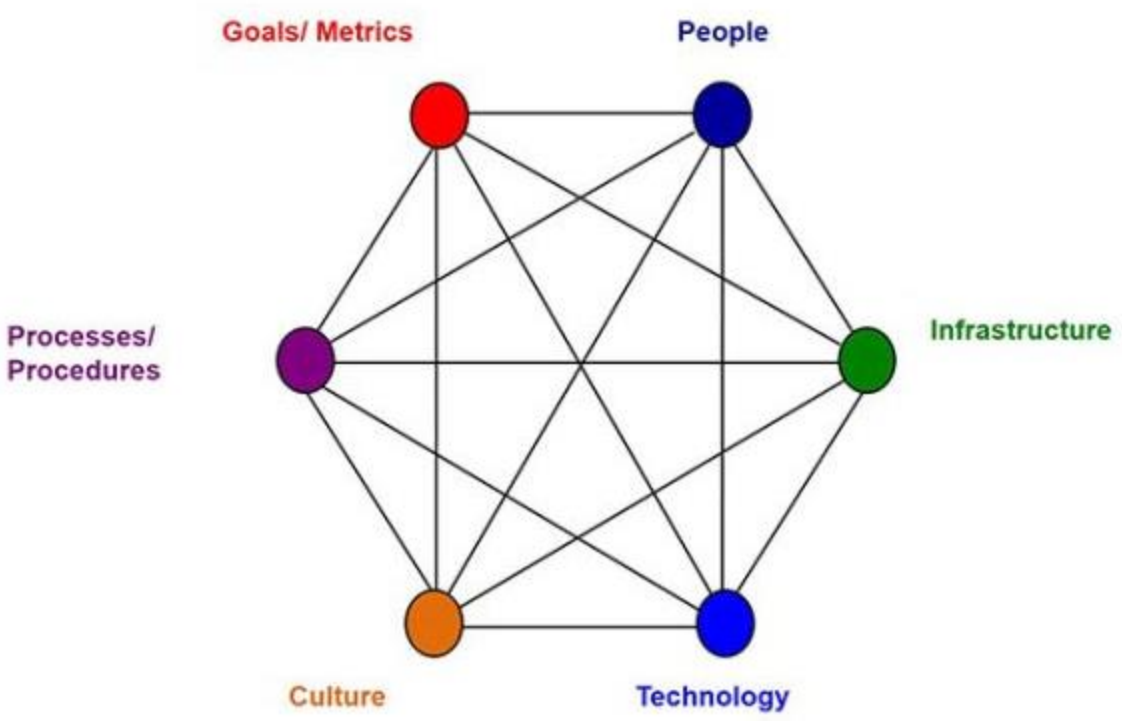
# The Human side of Security

**David Higgs - CISSP, C|EH**

Senior Security Solutions Engineer – Eastern Europe & Italy


1ST YEAR IN CYBERSECURITY
3RD YEAR IN CYBERSECURITY
20+ YEARS IN I.T. AND CYBERSECURITY

# Socio-technical Systems Theory



IT Operations

Server

Security Policies
Standards
Baselines

IT Operations

Security Team

Server

Vulnerability
Management

C-Level

Security Policies
Standards
Baselines

IT Operations
Manager

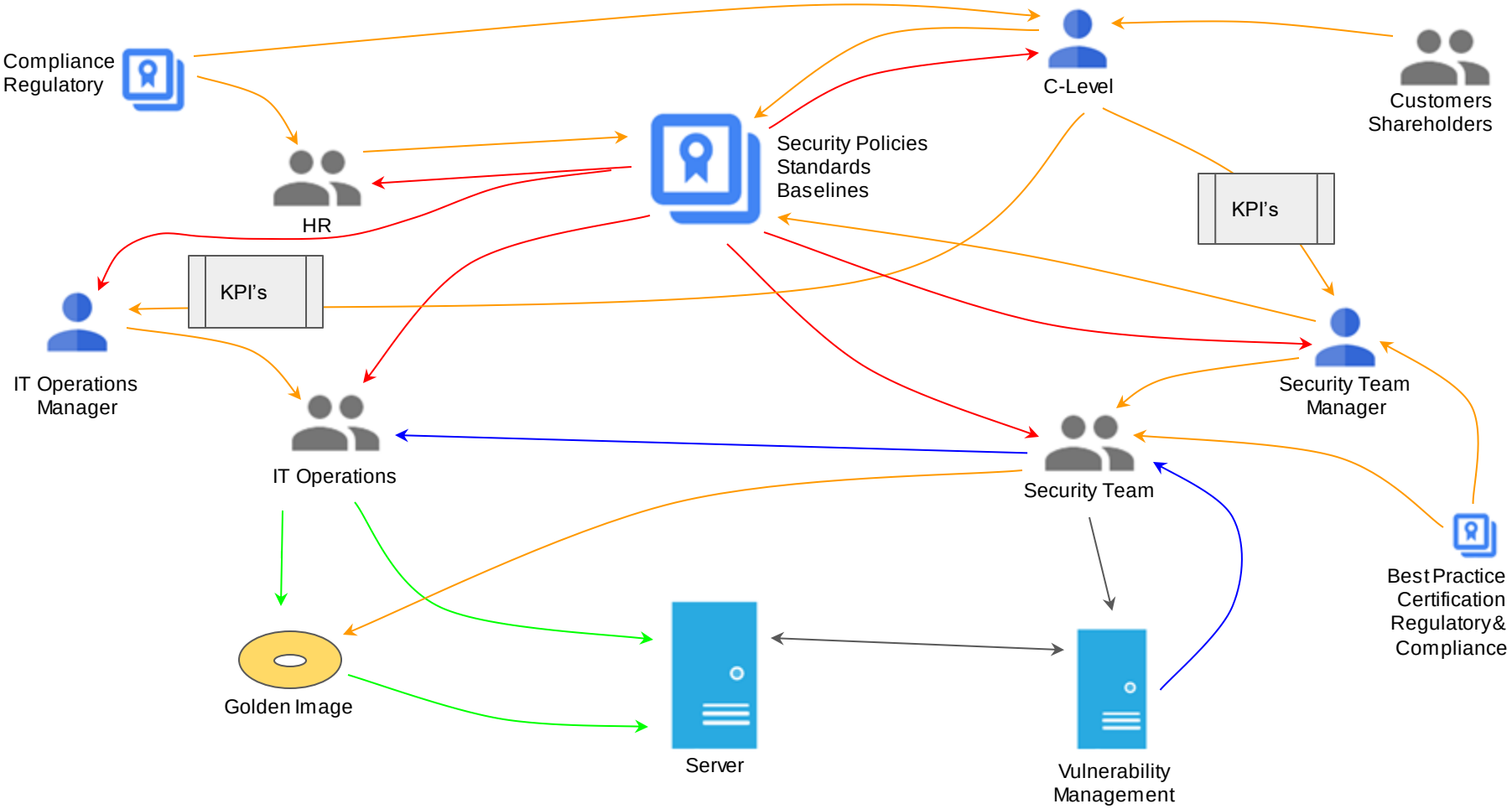
IT Operations

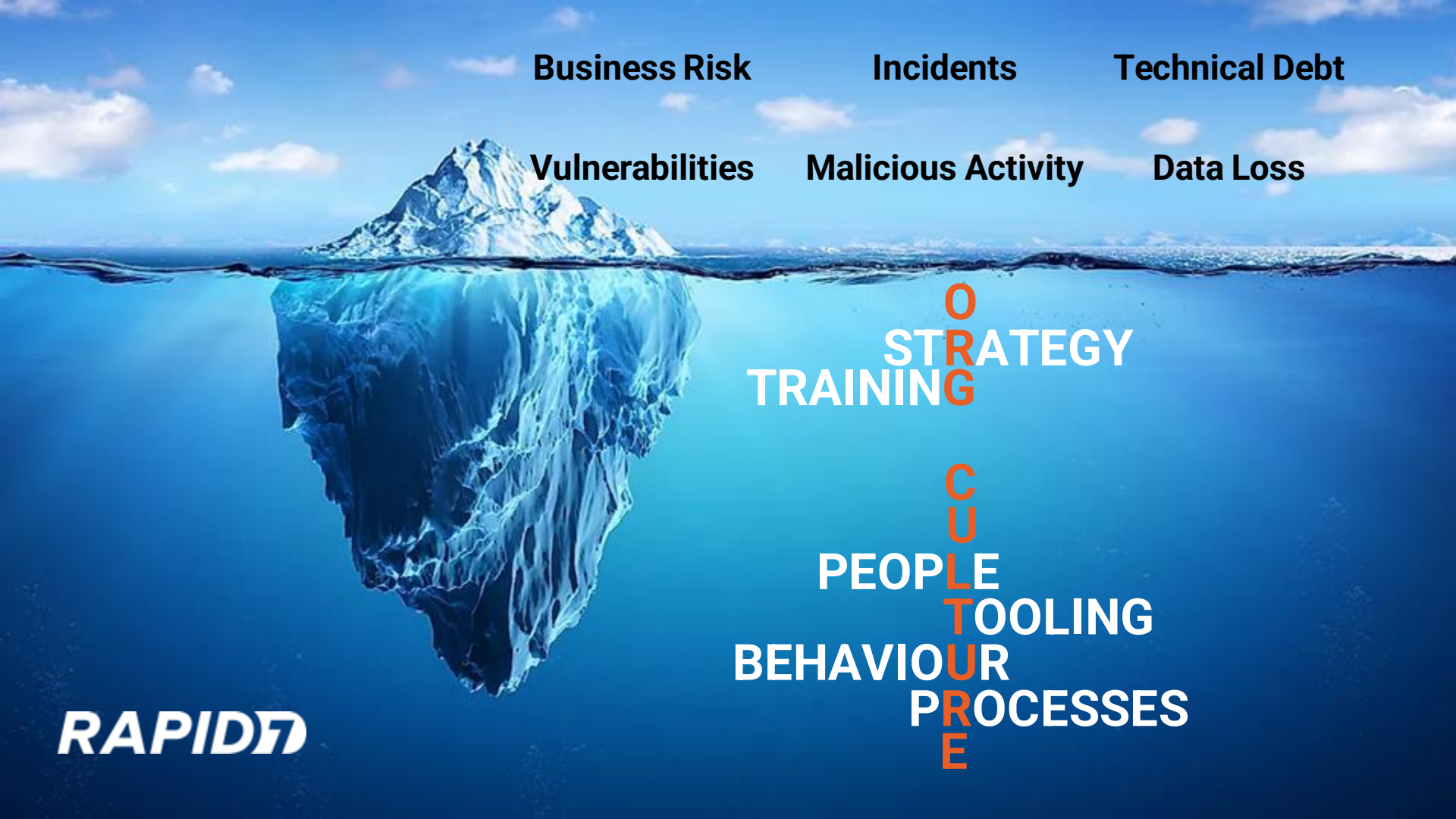
Security Team
Manager

Security Team

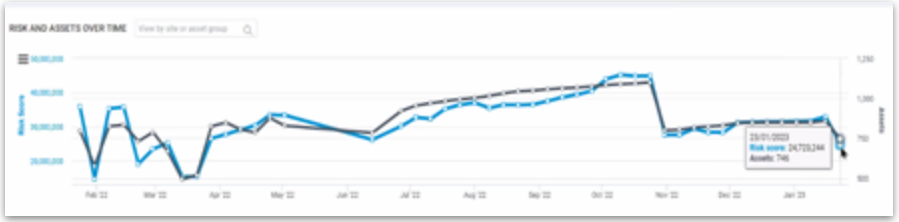
Server

Vulnerability
Management

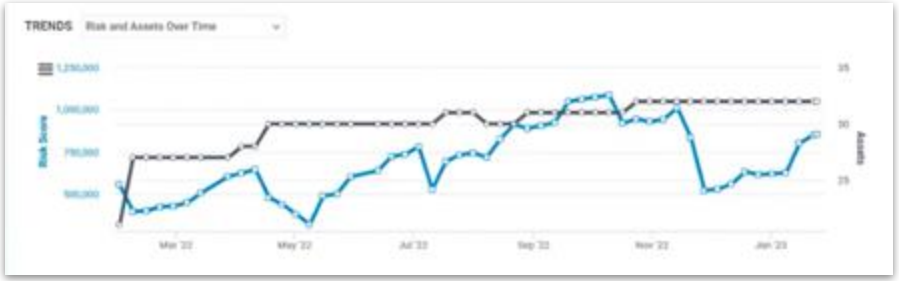

Compliance
Regulatory
C-Level
Customers
Shareholders
HR
Security Policies
Standards
Baselines
KPI's
KPI's
IT Operations
Manager
Security Team
Manager
IT Operations
Security Team
Best Practice
Certification
Regulatory&
Compliance
Golden Image
Server
Vulnerability
Management


Business Risk
Incidents
Technical Debt
Vulnerabilities
Malicious Activity
Data Loss
STRATEGY
TRAINING
PEOPLE
TOOLING
BEHAVIOUR
PROCESSES
CULTURE
RAPID7

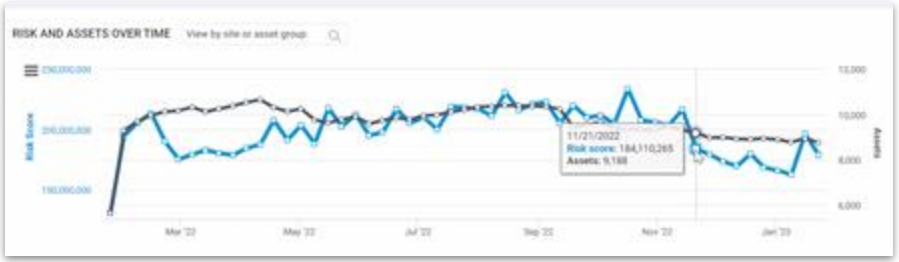
# Process Maturity Levels




Org 1

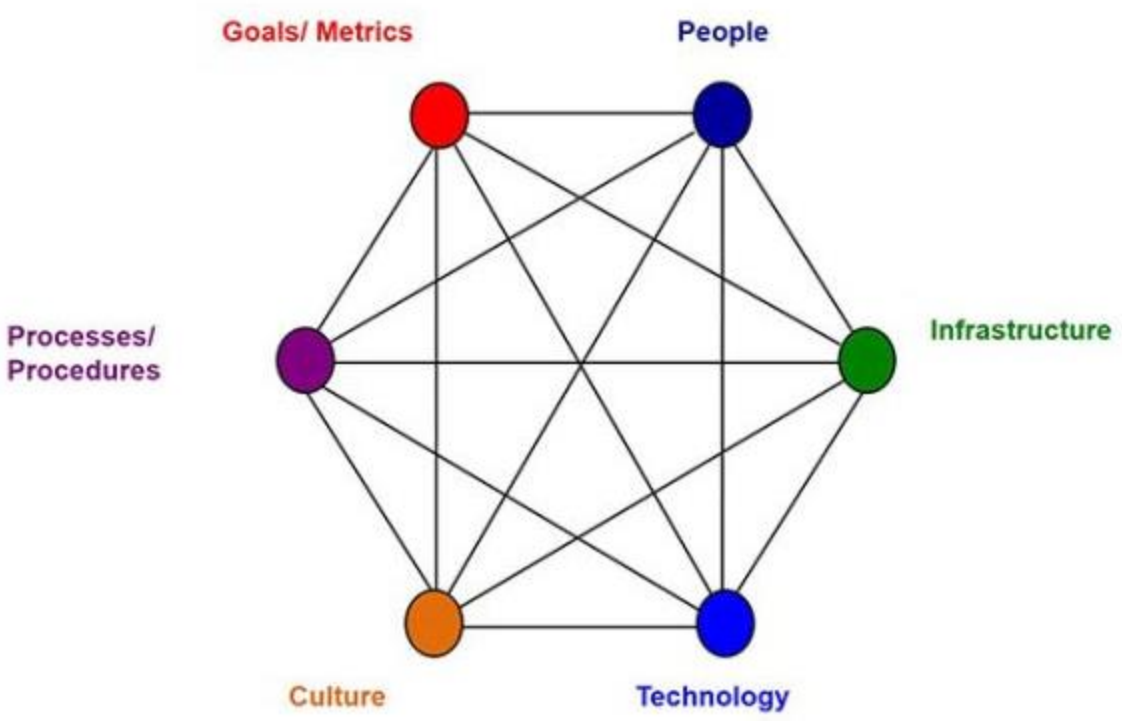


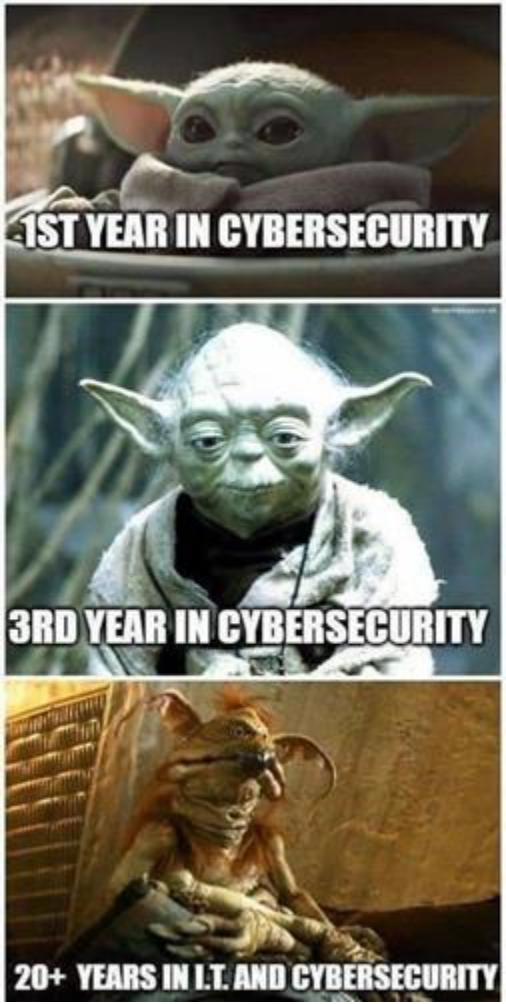

Org 2




Org 3

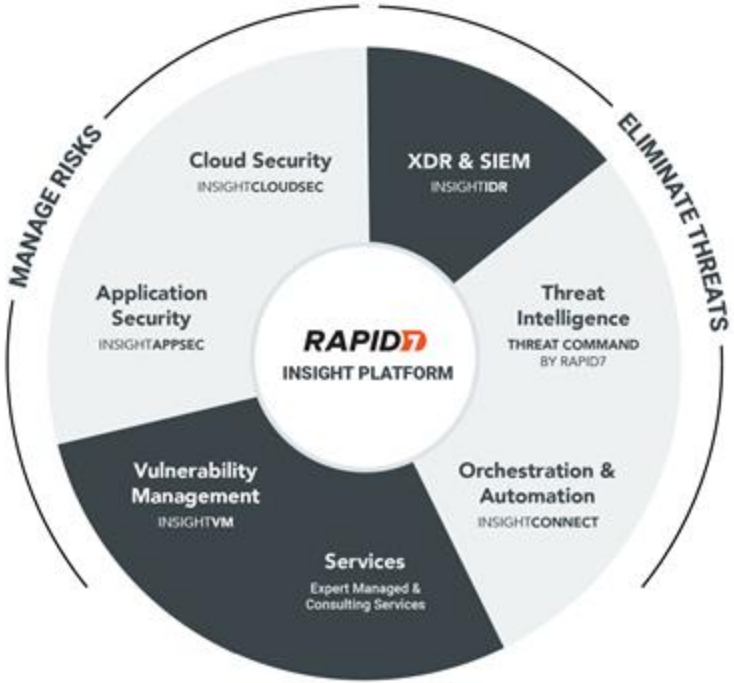
# Socio-technical Systems Theory




1ST YEAR IN CYBERSECURITY
3RD YEAR IN CYBERSECURITY
20+ YEARS IN I.T. AND CYBERSECURITY

# What are Rapid7 doing about it?

# The Rapid7 Threat Complete Offer




**Unlock a unified risk and threat experience with proactive, detective, and responsive security:**

- Know your exposure
- Find threats earlier
- Respond with confidence

Two solutions. One Partner. Complete coverage.

Gartner
Peer Insights Vuln. Assessment, 2020
**CUSTOMERS' CHOICE**

FORRESTER
VRM Wave, Q4 2019
**LEADER**

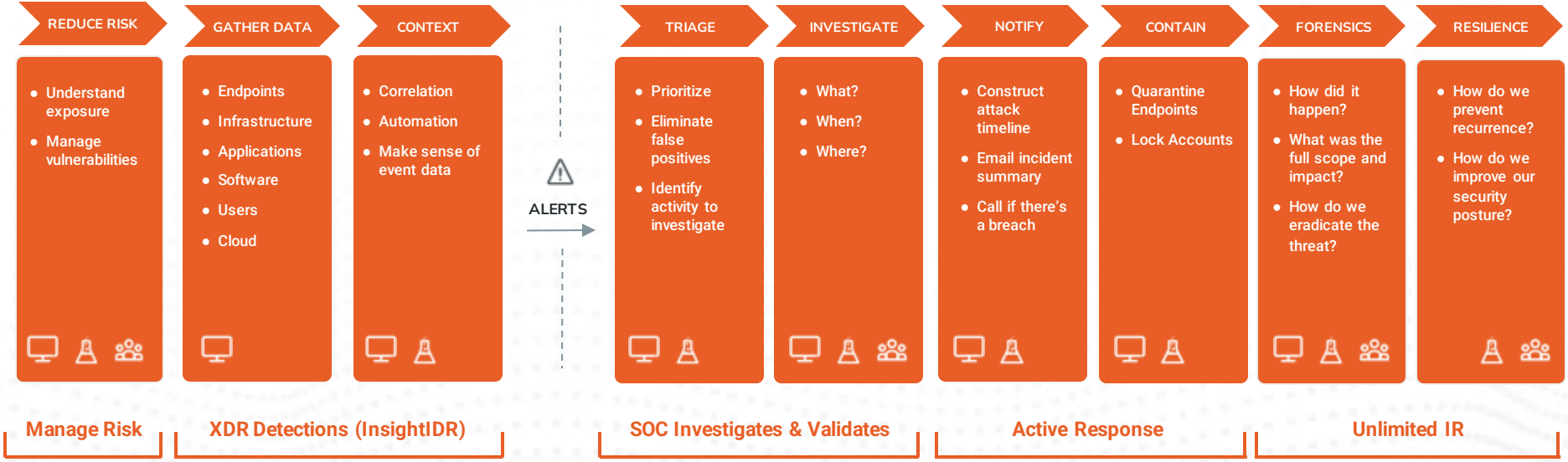
Gartner
SIEM Magic Quadrant, '20 & '21
**LEADER**

FORRESTER
Security Analytics Wave '20
**STRONG PERFORMER**

FORRESTER
MDR Wave '21
**STRONG PERFORMER**

IDC
MDR Marketscape '21
**LEADER**

# Only Rapid7 takes detection and response from end to end without limits

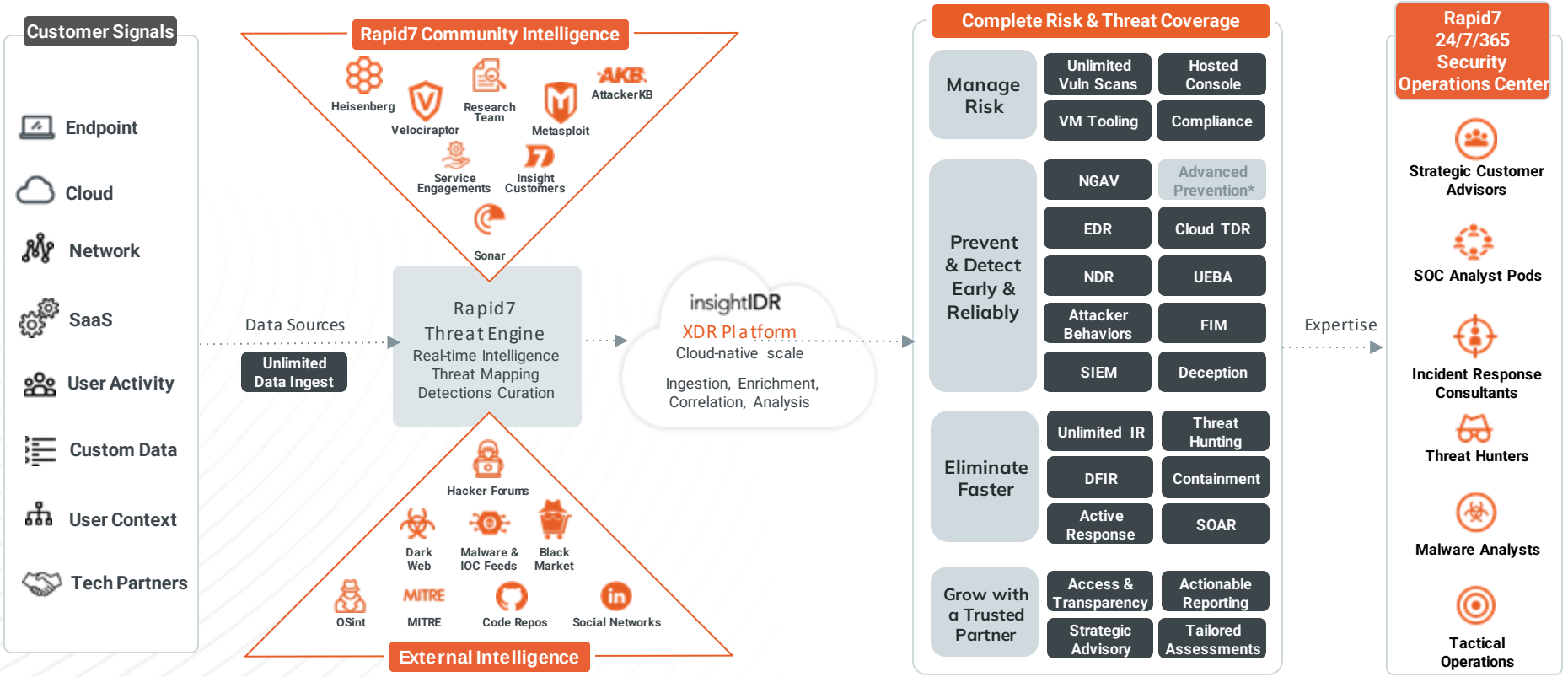



**Rapid7 handles EVERY incident, no matter how large or complex. With us, there is no line. We're there for you when you need it.**

Technology / Tooling

# Managed Threat Complete

## No matter where threats start, threats end with Rapid7 Managed Threat Complete

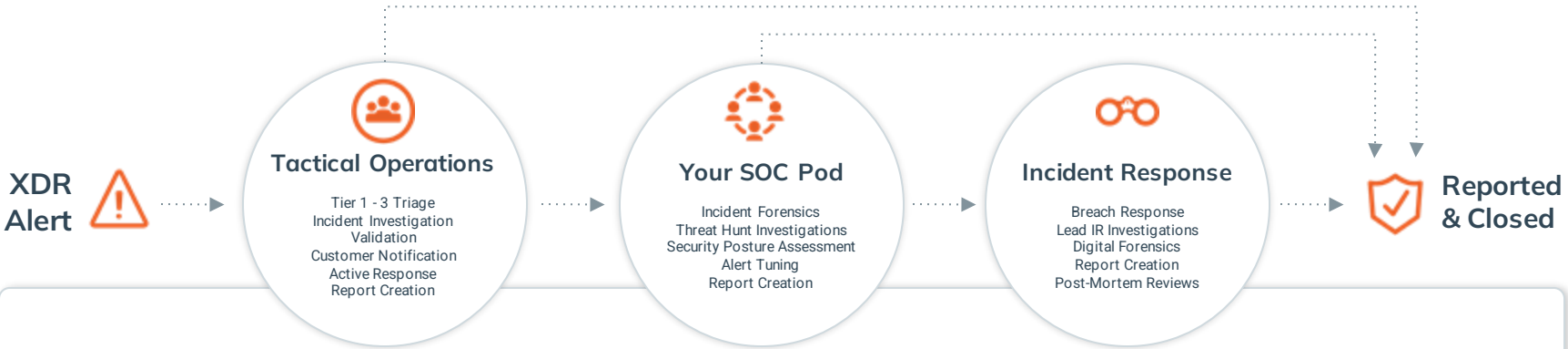


# Customers extend their team with D&R experts

**95%+**
3-Year Analyst Retention Rate

**4**
Global SOCs (FTS coverage)

**7-10**
Analysts per SOC pod



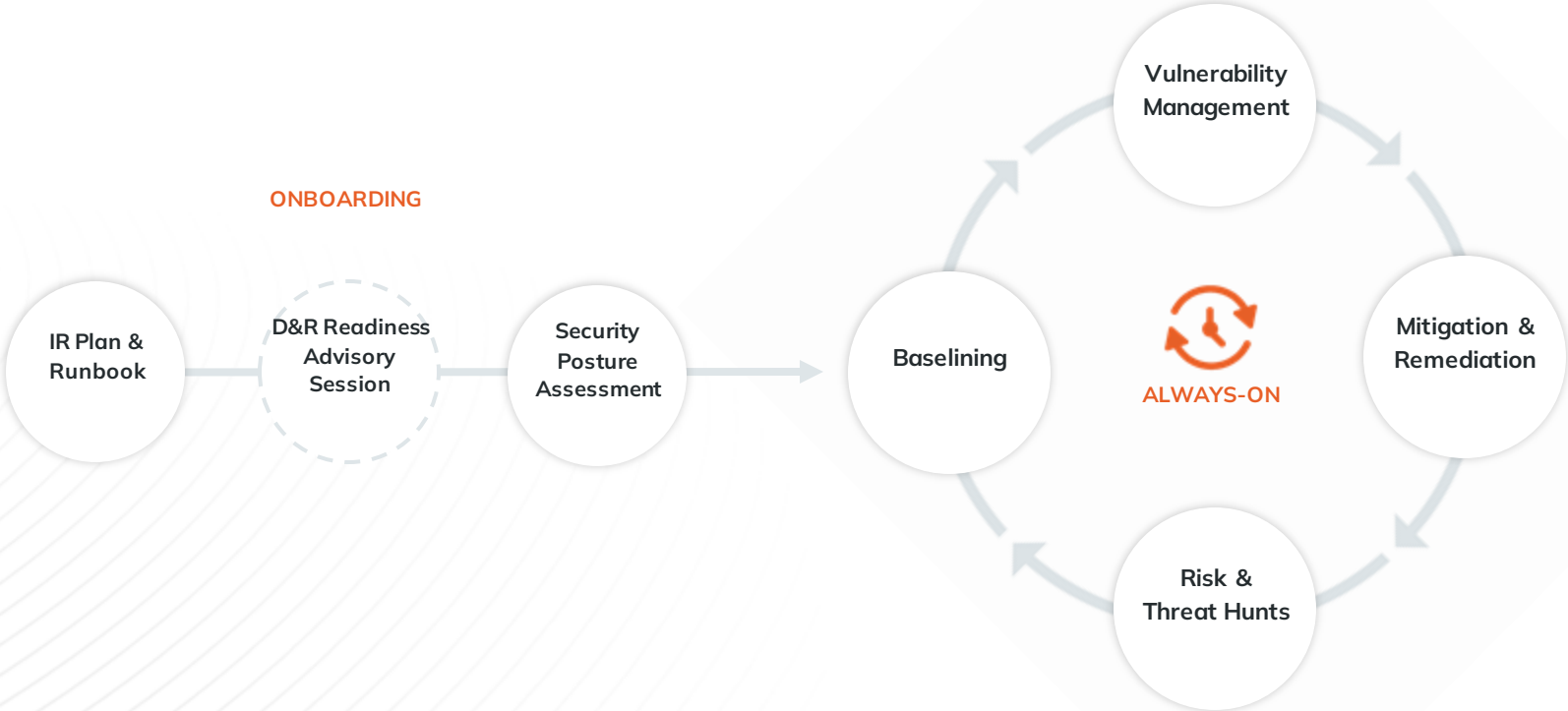

## Managed Threat Operations

Proactive Threat Hunting | Malware Analysis | Threat Intelligence | Detection Engineering | Managed Services Labs

## Security Accelerator

Customer Advisor | Monthly Meetings | Security Posture Assessment | CIS Security Benchmark Assessment | Trend & ROI Reporting

# Mitigate risk and contain impact




* Available with MTC Advanced package

# Practitioner-first approach that delivers answers

Monthly Service Report


Incident Report


Security Posture Assessment


Top 25 Remediations by Risk

Critical Controls Assessment


Executive & Trend Reports



View all reports: https://docs.rapid7.com/services/mtc-deliverables/

# Something was missing…

# 360° Expert Threat Detection Coverage

## Identify the earliest threat signals, pinpoint active threats across your attack surface

**MANAGED**
**Digital Risk Protection**

### Proactively thwart attack plans

- Anticipate targeted threats against your organization earlier in attack chain
- Minimize exposure time with expert takedowns
- Protect your company, employees, and brand across the clear, deep, and dark web


**MANAGED**
**Threat Complete**

### Pinpoint and eliminate active threats

- Expert 24/7, follow-the-sun monitoring as an extension of your team
- High fidelity XDR alerts for endpoint-to-cloud coverage
- Unlimited DFIR delivers complete end-to-end results

# Managed Threat Complete

## ESSENTIALS

24x7 Expert Threat Monitoring and UNLIMITED Incident Response

**Highlights:**

- Complete transparency with access to InsightIDR Ultimate, Rapid7 XDR platform
- Detections Content Service powered by Rapid7 Threat Engine
- 24x7 Threat Monitoring
- Active Response automation
- Unlimited Incident Response
- Comprehensive Reports
- Managed Risk powered by leading leading vulnerability management, InsightVM

## ADVANCED

Advanced Threat Detection & Response for Modern Environments

**Highlights:**

- Dedicated Customer Advisor
- Monthly Service Meetings
- IR Planning Assistance
- Customized Quarterly Executive Reports

## Ultimate

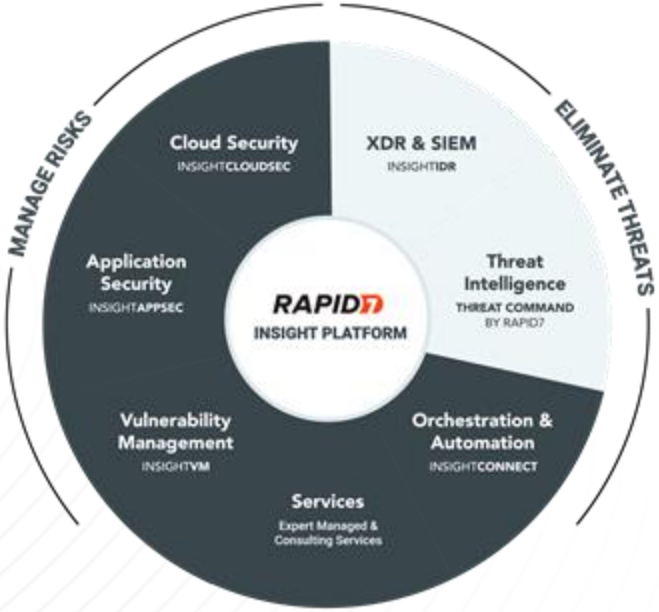
Unlock Holistic Security Leadership & Ransomware Coverage

**Highlights:**

Everything in Managed Threat Complete Advanced PLUS:

- Managed Vulnerability Management
- Managed Digital Risk Protection
- Hosted Velociraptor Integration

# Rapid7's Cloud Risk Complete Offer




**Experience the only practitioner-first security platform with Rapid7. Your partner to future proof your business.**

- Unlimited Users and Automated Workflows
- Unlimited Vulnerability Management
- Unlimited Application Security Testing

**STRONG PERFORMER**
Cloud Workload Security, Q1 2022
FORRESTER

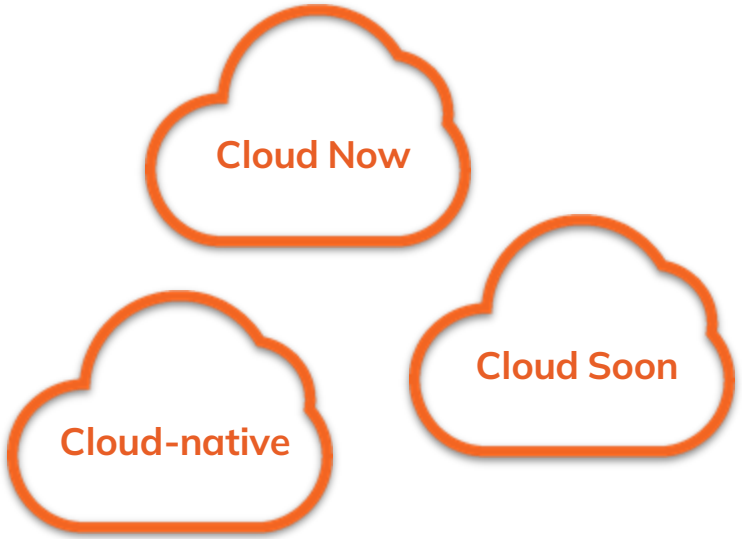
**VISIONARY**
AppSec Magic Quadrant 2021, 2022
Gartner

**CUSTOMERS' CHOICE**
Peer Insights Vuln. Assessment, 2020
Gartner

**LEADER**
VRM Wave, Q4 2019
FORRESTER

# What's driving your cloud journey?

- Born in the cloud from the start
- Digital Transformation / Innovation
- Direct to Consumer Engagement
- CapEx to OpEx
- Outsourcing Strategy
- Mergers & Acquisitions
- Runaway engineering, product, marketing and/or big data teams




Innovators → Early Adopters → Early Majority → Late Majority → Laggards

# How easy is it to find a public S3 or Blob in the real world??

S3 & Blob have a format that allows us to use specific google search operators

virtual

- http://{bucket}.s3.amazonaws.com
- http://{bucket}.s3-{aws-region}.amazonaws.com

Path

- http://s3-{awsregion}.amazonaws.com/{bucket}

*What are google "dorks"*

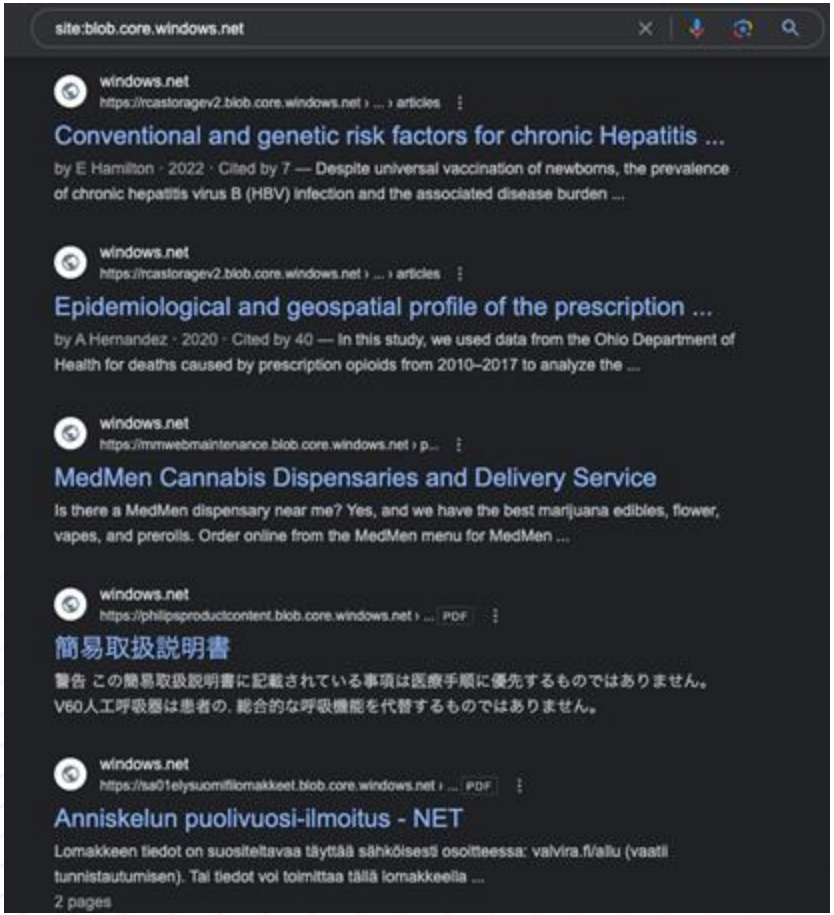
*If I type "site:rapid7.com" it will only return results from rapid7.com. If i type "site:rapid7.com filetype:pdf" it will only return pdf's from rapid7.com in the results*

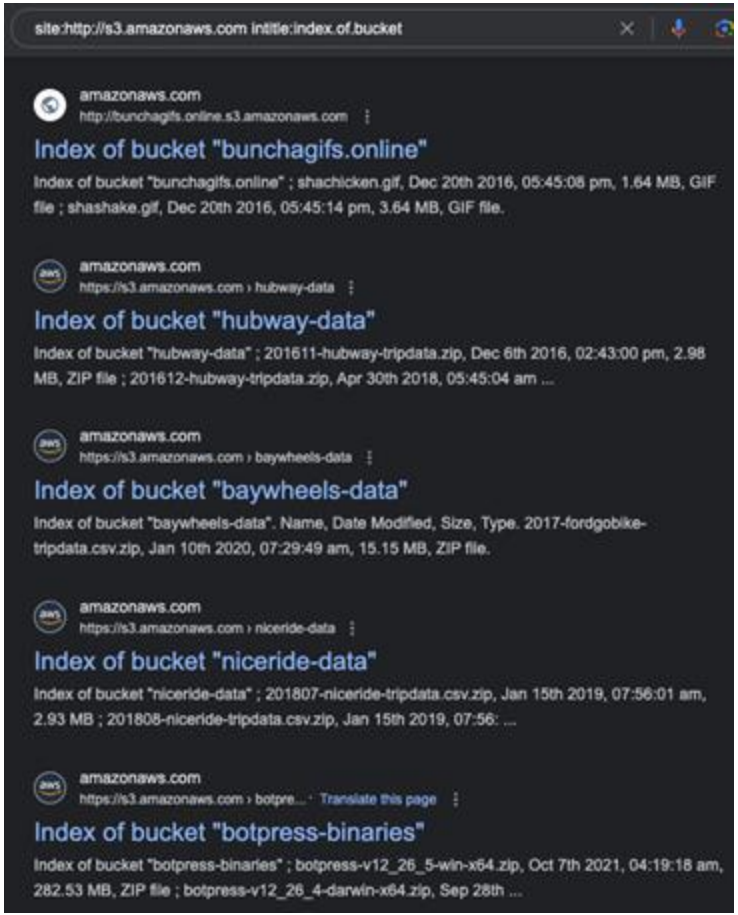
## How easy is it to find a public S3 or Blob in the real world??

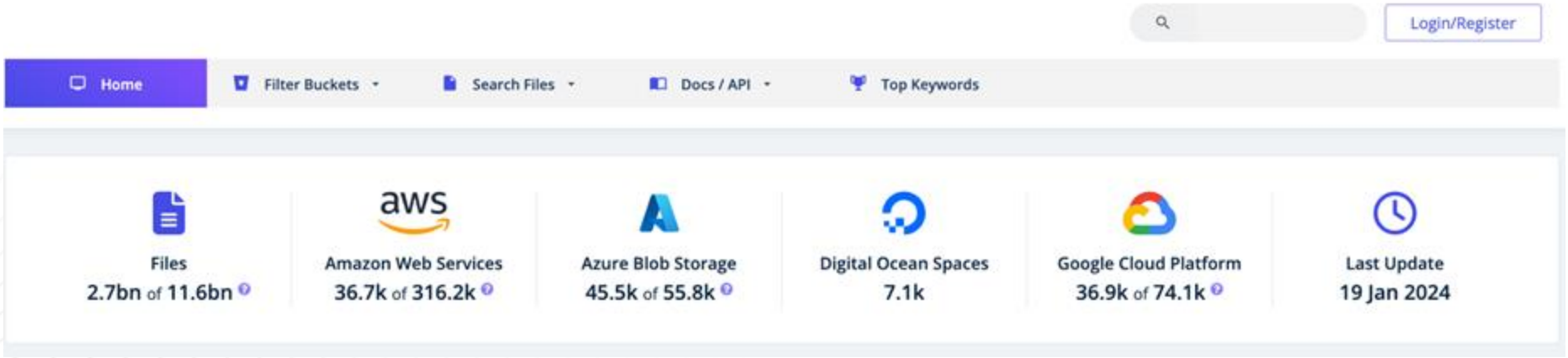
# Just Google it…

*site:http://s3.amazonaws.com intitle:index.of.bucket*

*site:blob.core.windows.net*


site:blob.core.windows.net
windows.net
https://rcasloragev2.blob.core.windows.net › ... › articles
Conventional and genetic risk factors for chronic Hepatitis ...
by E Hamilton · 2022 · Cited by 7 — Despite universal vaccination of newborns, the prevalence of chronic hepatitis virus B (HBV) infection and the associated disease burden ...
windows.net
https://rcasloragev2.blob.core.windows.net › ... › articles
Epidemiological and geospatial profile of the prescription ...
by A Hernandez · 2020 · Cited by 40 — In this study, we used data from the Ohio Department of Health for deaths caused by prescription opioids from 2010–2017 to analyze the ...
windows.net
https://mmwebmaintenance.blob.core.windows.net › p...
MedMen Cannabis Dispensaries and Delivery Service
Is there a MedMen dispensary near me? Yes, and we have the best marijuana edibles, flower, vapes, and prerolls. Order online from the MedMen menu for MedMen ...
windows.net
https://philipsproductcontent.blob.core.windows.net › ... PDF
簡易取扱説明書
警告 この簡易取扱説明書に記載されている事項は医療手順に優先するものではありません。
V60人工呼吸器は患者の、総合的な呼吸機能を代替するものではありません。
windows.net
https://sa01elysuomifiomakkeet.blob.core.windows.net › ... PDF
Anniskelun puolivuosi-ilmoitus - NET
Lomakkeen tiedot on suositeltavaa täyttää sähköisesti osoitteessa: valvira.fi/allu (vaatii tunnistautumisen). Tai tiedot voi toimittaa tällä lomakkeella ...
2 pages

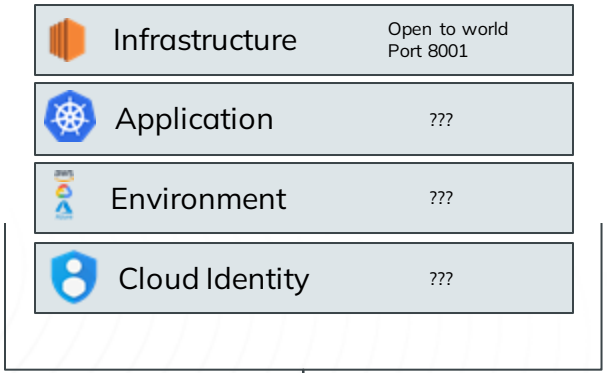

site:http://s3.amazonaws.com intitle:index.of.bucket
amazonaws.com
http://bunchagifs.online.s3.amazonaws.com
Index of bucket "bunchagifs.online"
Index of bucket "bunchagifs.online" ; shachicken.gif, Dec 20th 2016, 05:45:08 pm, 1.64 MB, GIF file ; shashake.gif, Dec 20th 2016, 05:45:14 pm, 3.64 MB, GIF file.
amazonaws.com
https://s3.amazonaws.com › hubway-data
Index of bucket "hubway-data"
Index of bucket "hubway-data" ; 201611-hubway-tripdata.zip, Dec 6th 2016, 02:43:00 pm, 2.98 MB, ZIP file ; 201612-hubway-tripdata.zip, Apr 30th 2018, 05:45:04 am ...
amazonaws.com
https://s3.amazonaws.com › baywheels-data
Index of bucket "baywheels-data"
Index of bucket "baywheels-data". Name, Date Modified, Size, Type. 2017-fordgobike-tripdata.csv.zip, Jan 10th 2020, 07:29:49 am, 15.15 MB, ZIP file.
amazonaws.com
https://s3.amazonaws.com › niceride-data
Index of bucket "niceride-data"
Index of bucket "niceride-data" ; 201807-niceride-tripdata.csv.zip, Jan 15th 2019, 07:56:01 am, 2.93 MB ; 201808-niceride-tripdata.csv.zip, Jan 15th 2019, 07:56: ...
amazonaws.com
https://s3.amazonaws.com › botpre... · Translate this page
Index of bucket "botpress-binaries"
Index of bucket "botpress-binaries" ; botpress-v12_26_5-win-x64.zip, Oct 7th 2021, 04:19:18 am, 282.53 MB, ZIP file ; botpress-v12_26_4-darwin-x64.zip, Sep 28th ...


Login/Register
Home
Filter Buckets
Search Files
Docs / API
Top Keywords
Files
2.7bn of 11.6bn
Amazon Web Services
36.7k of 316.2k
Azure Blob Storage
45.5k of 55.8k
Digital Ocean Spaces
7.1k
Google Cloud Platform
36.9k of 74.1k
Last Update
19 Jan 2024

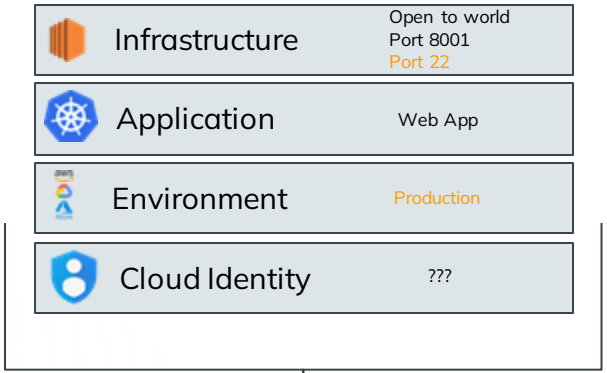
# Act Faster With Unlimited Risk Coverage

Remediation is completed well before alternative solutions even detect risk in your environment.

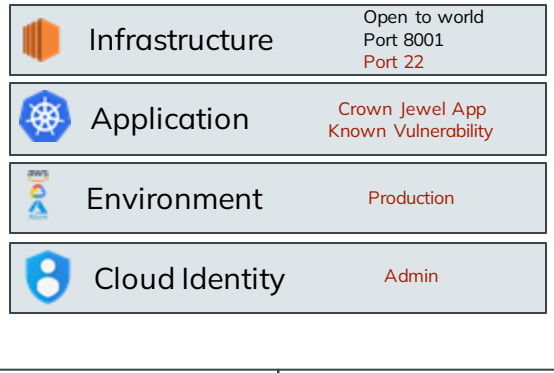
# Make Context-driven Decisions With Layered Context




**Risk :** N/A
**Action:** Notify




**Risk:** Medium
**Action:** Escalate




**Risk:** High
**Action:** Automate

# Visualize toxic combinations with Attack Path Analysis

## Visualize Your Attack Surface in Real Time

Visualize risk across your cloud environments in real-time, mapping relationships between compromised resources and the rest of your environment.

## Identify Avenues to Sensitive Resources and Data

Prioritize remediation efforts by understanding the toxic combinations that provide bad actors paths to access to business-critical resources or and data.

## Communicate Risk to Non-technical Stakeholders

Report on risk and potential impact of an exploit to non-technical stakeholders with easy-to consume attack path visualizations.

# Manage and Communicate Risk Across Hybrid Environments with Executive Risk View

## Communicate Risk Posture and Progress

Achieve a unified view of risk across your hybrid environments to effectively communicate risk across the organization and track progress.

## Define Risk Consistently

Establish a consistent definition of risk across your organization, aggregating insights and normalizing scores from on-premises and cloud assessments.

## Make Informed Decisions

Take a data-driven approach to decision making, capacity planning and drive accountability for risk reduction across the entire business.

# Thankyou

# Questions