WELCOME TO

SECURITY FIRST

CYBER SECURITY CONFERENCE 2023

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Today’s Host

Johanna Samuelson

#securityfirst2023

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Unveiling a New Era

Netsecure & Integrity360 Merger– Expanding Horizons and Expertise for Swedish Clients

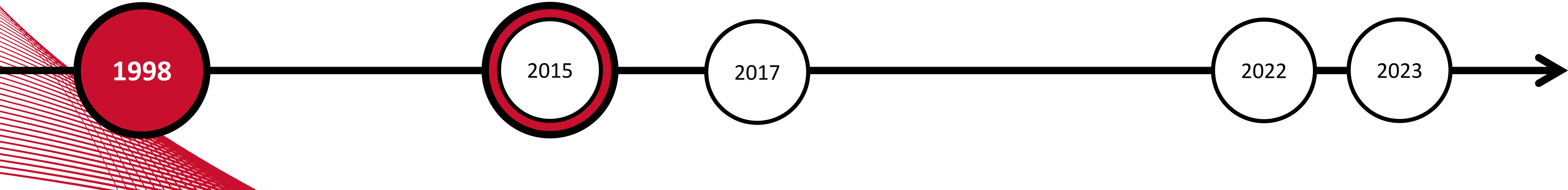
Jan Lindblom, CEO, Integrity360 Sweden

#securityfirst2023

En affärsidé tar form och Netsecure föds

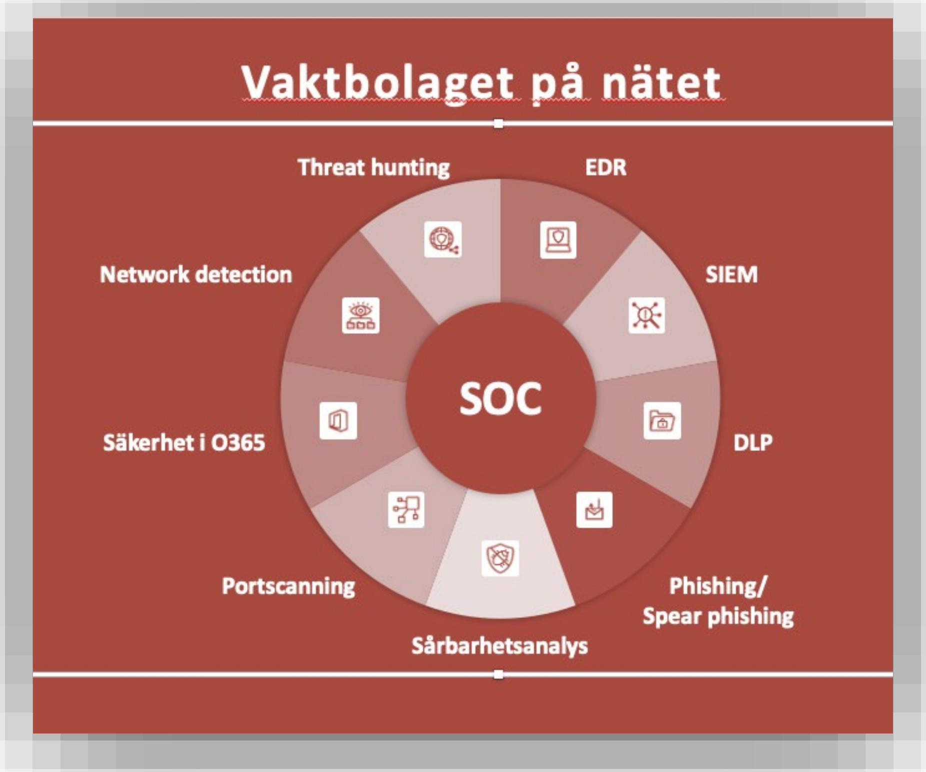
NETSECURE

För IT-säkerhetens skull

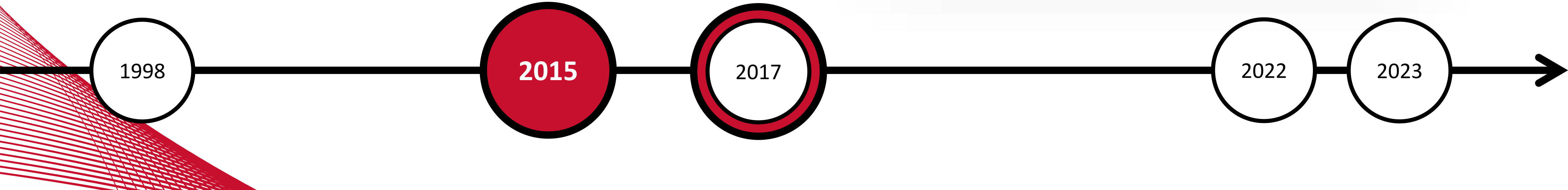


Vi utvecklas med branschen

NET SECURE

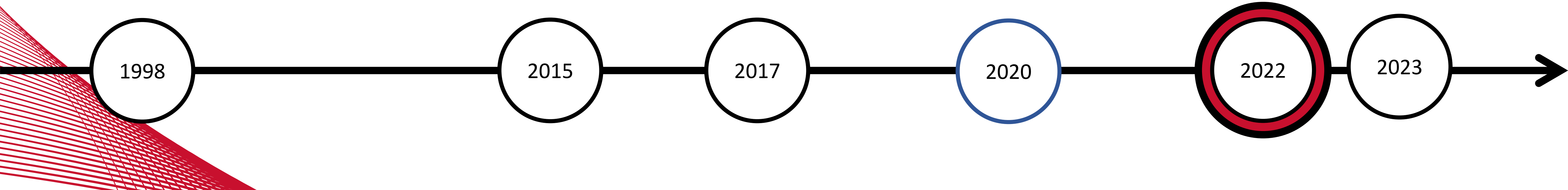


Vaktbolaget på nätet



netsecure

the cybersecurity company®



1998

2015

2017

2020

2022

2023

Integrity360

your security in mind

Vårt steg in i framtiden

1998

2015

2017

2022

2023

Integrity360
your security in mind

Thank you

Jan Lindblom
jan.Lindblom@integrity360.com

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

SECURITY FIRST

CYBER SECURITY CONFERENCE 2023

Gaining Visibility in an Always-on World

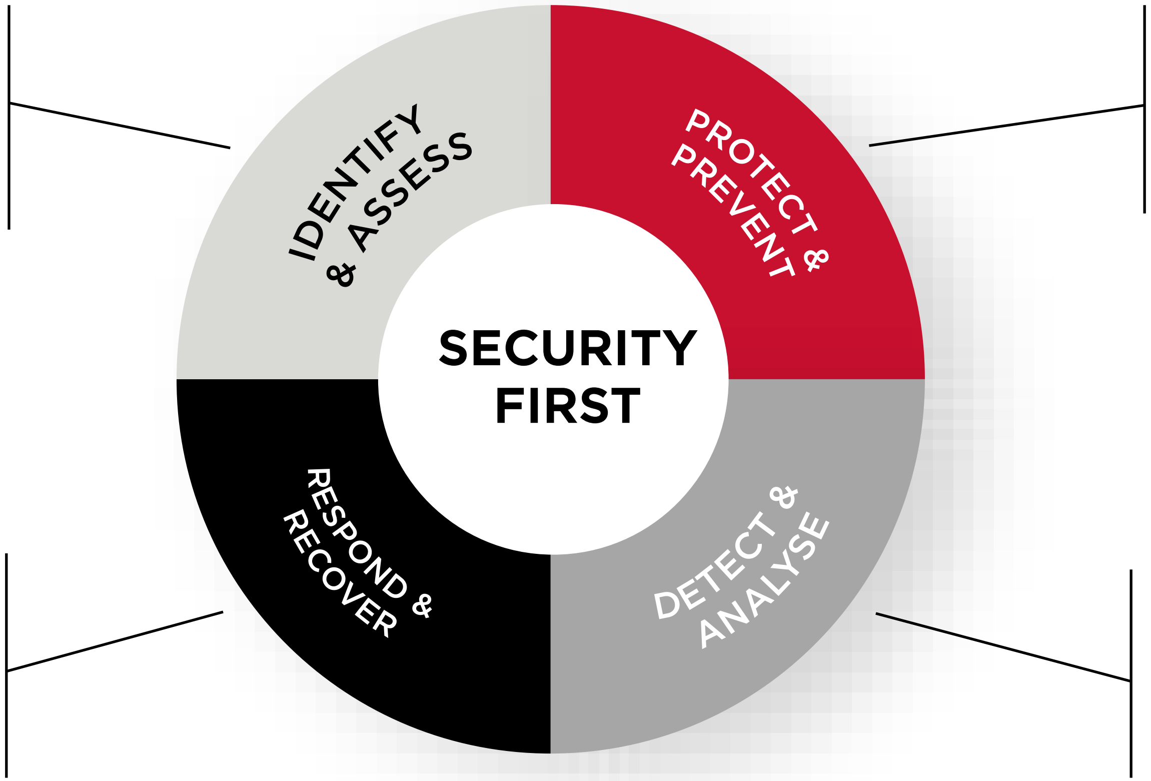
Richard Ford

Chief Technology Officer, Integrity360

#securityfirst2023

Visibility

Building an Effective Security Posture



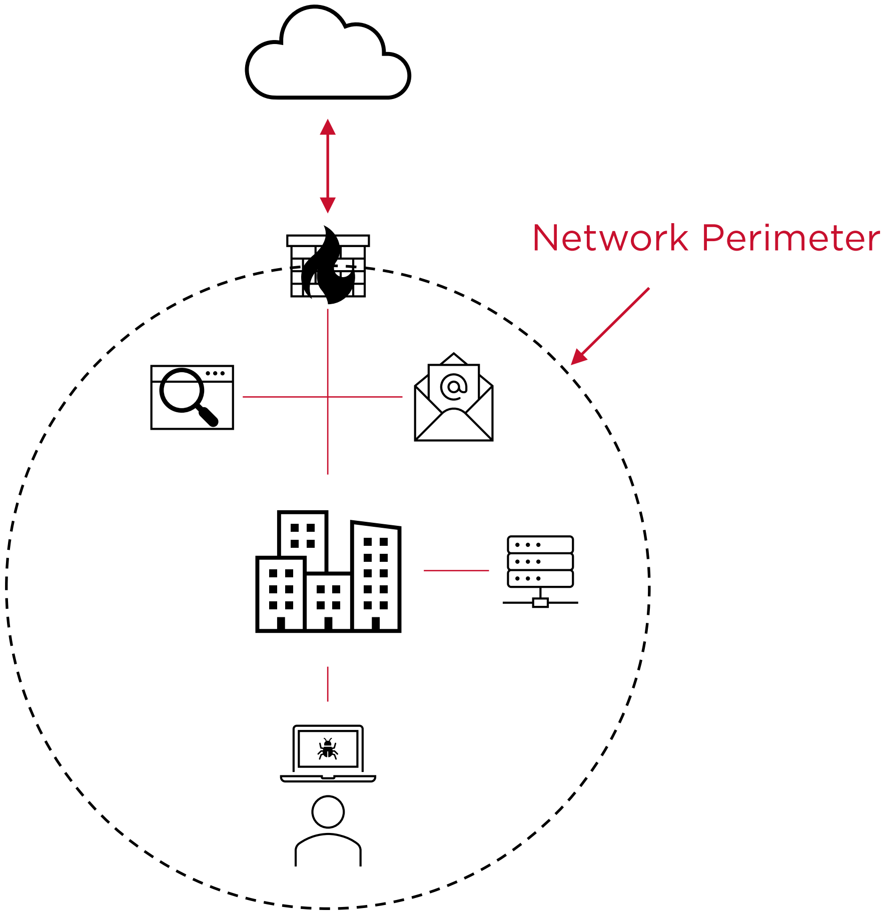
Identify threats, assets, and vulnerabilities, where you are, where you want to get to

Protect yourself as much as possible and prevent attacks from happening in the first place

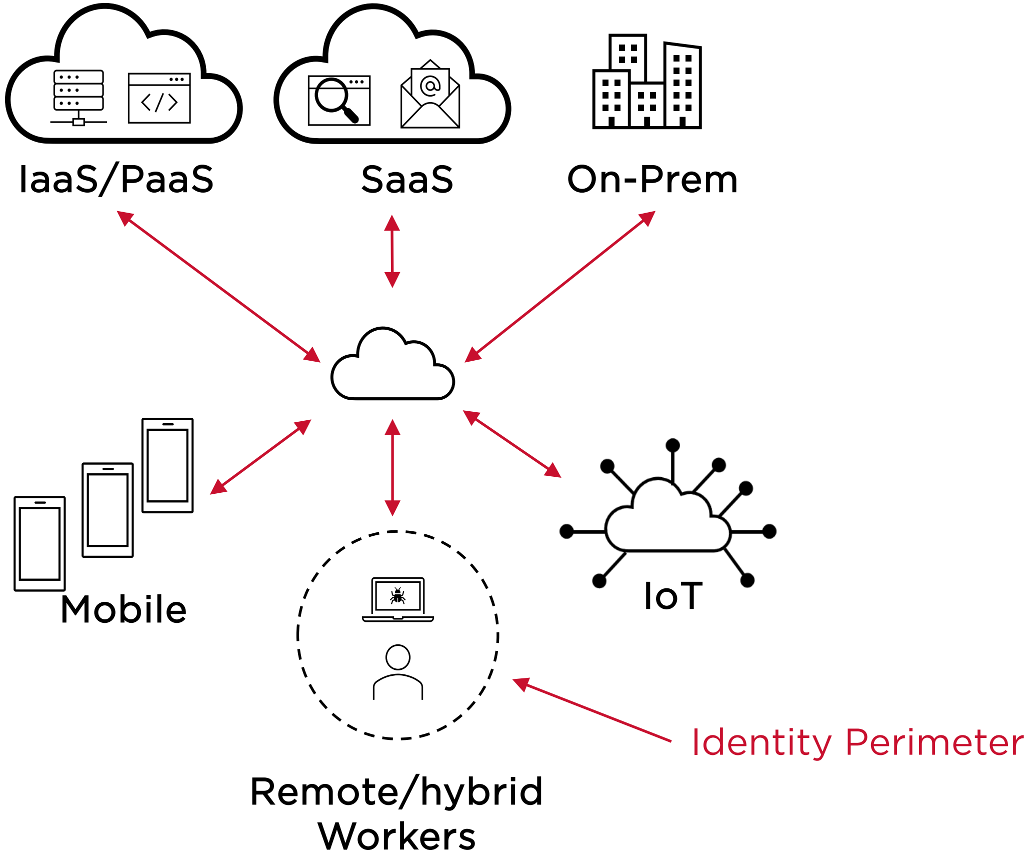
Have systems and processes in place to detect and analyse incidents as they occur

Be ready to quickly respond to and recover from incidents and breaches should they occur

Challenge: IT Landscape



Network Perimeter



IaaS/PaaS

SaaS

On-Prem

Mobile

IoT

Identity Perimeter

Remote/hybrid
Workers

Pillars of Visibility

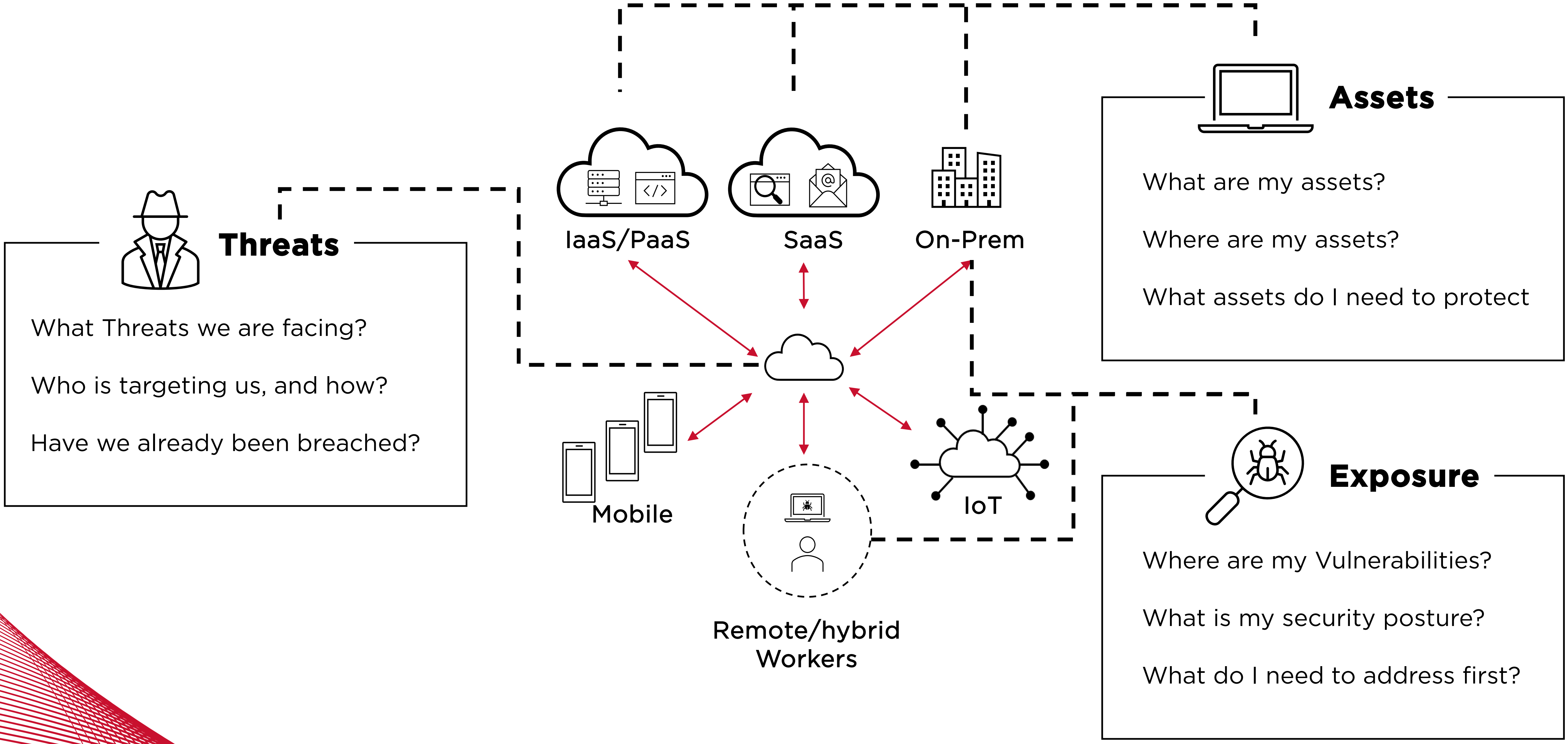
Attack Surface

Threat Activity

Control Effectiveness

Attack Surface

Attack Surface



Threats

What Threats we are facing?

Who is targeting us, and how?

Have we already been breached?

Assets

What are my assets?

Where are my assets?

What assets do I need to protect

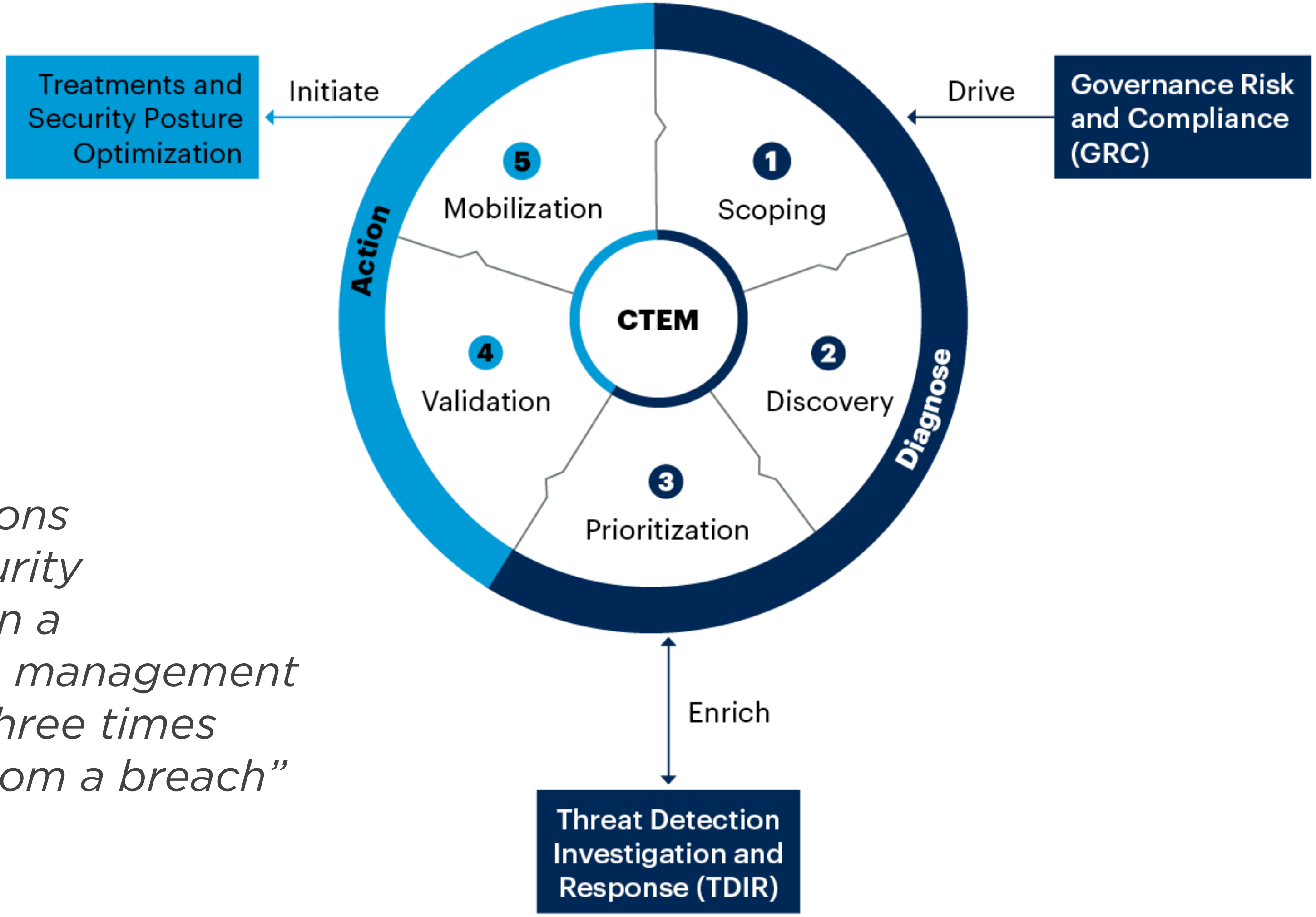
Exposure

Where are my Vulnerabilities?

What is my security posture?

What do I need to address first?

CTEM: Continuous Threat Exposure Management



Treatments and Security Posture Optimization
Initiate
Drive
Governance Risk and Compliance (GRC)
Action
Diagnose
5 Mobilization
1 Scoping
CTEM
4 Validation
2 Discovery
3 Prioritization
Enrich
Threat Detection Investigation and Response (TDIR)

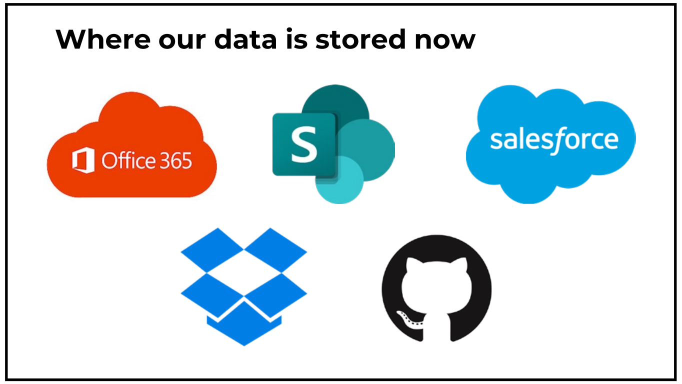
"By 2026, organizations prioritising their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach"
- Gartner 2022

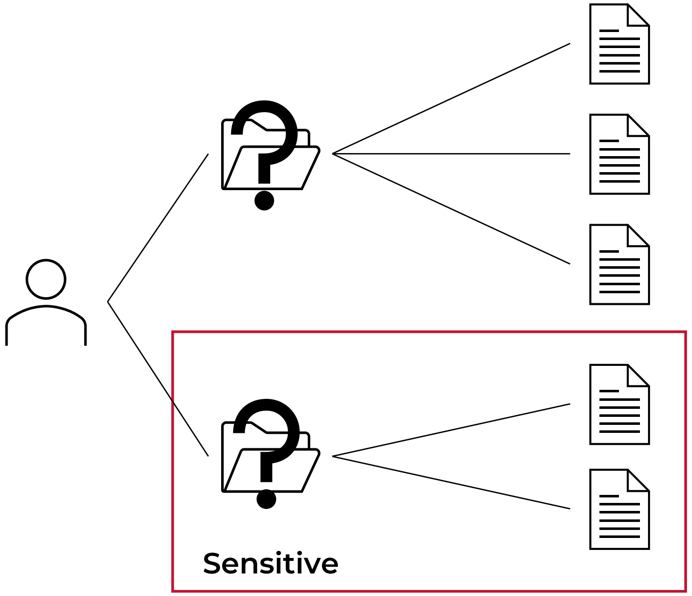
Our Most Valuable Asset: Data

Two Key Questions:

- Where our Data is?
- Who has access to our Data?

Where our data is stored now

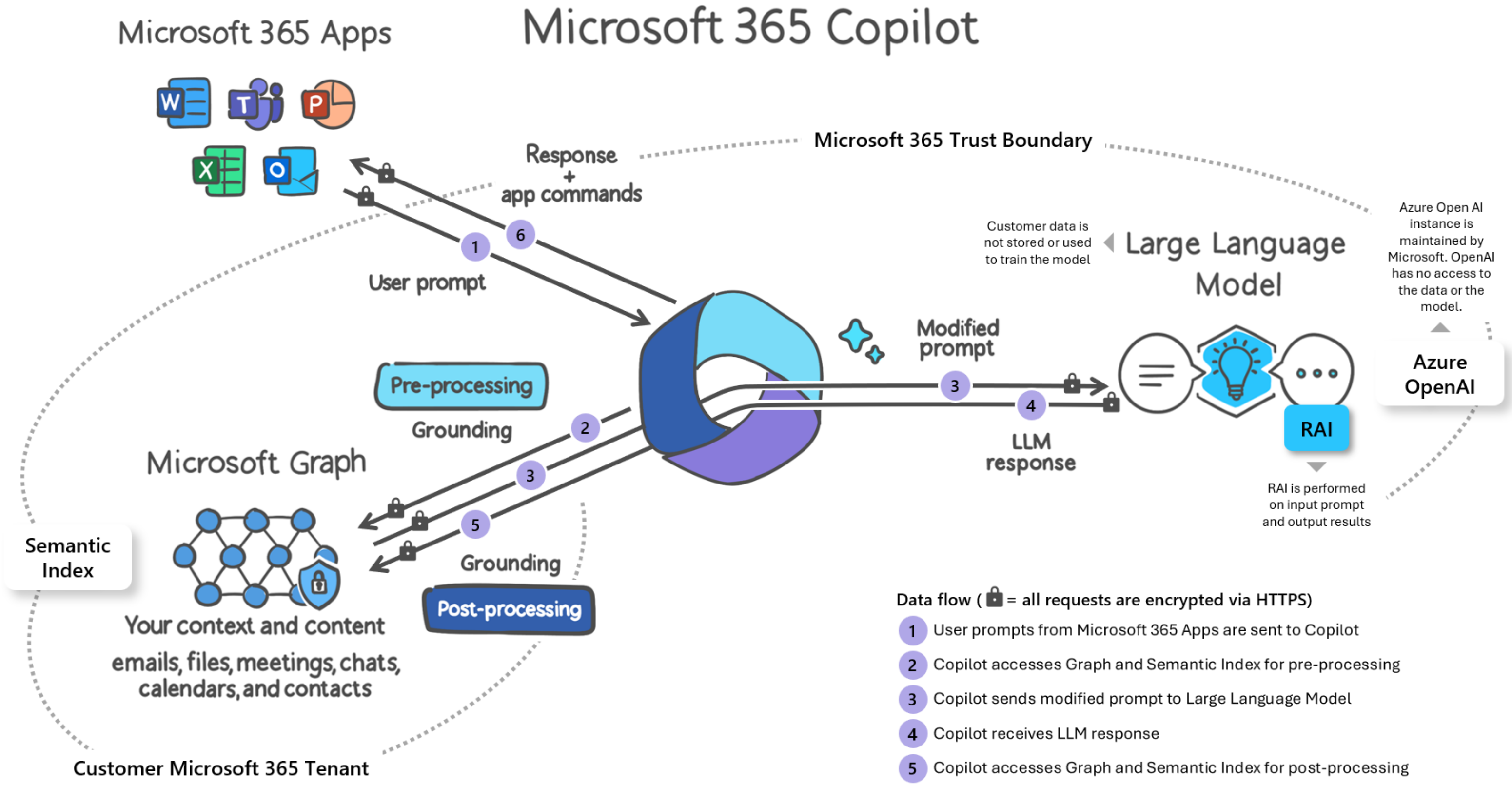




Data: Impact of Generative AI

GenAI will turbo charge our organisations, harnessing the power of the data we have access to and generate content. And there is the problem:

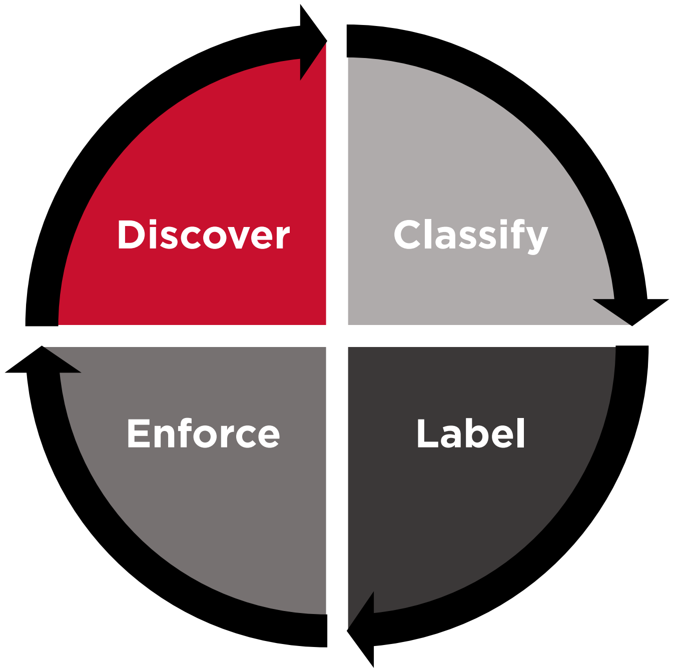
- ***Permissions***
- ***Labels***
- ***Humans***


Microsoft 365 Apps
Microsoft 365 Copilot
Microsoft 365 Trust Boundary
Response + app commands
6
1
User prompt
Customer data is not stored or used to train the model
Large Language Model
Azure Open AI instance is maintained by Microsoft. OpenAI has no access to the data or the model.
Azure OpenAI
Modified prompt
3
4
LLM response
RAI
RAI is performed on input prompt and output results
Pre-processing
Grounding
2
Microsoft Graph
3
5
Grounding
Post-processing
Semantic Index
Your context and content
emails, files, meetings, chats, calendars, and contacts
Customer Microsoft 365 Tenant

Data flow (🔒 = all requests are encrypted via HTTPS)

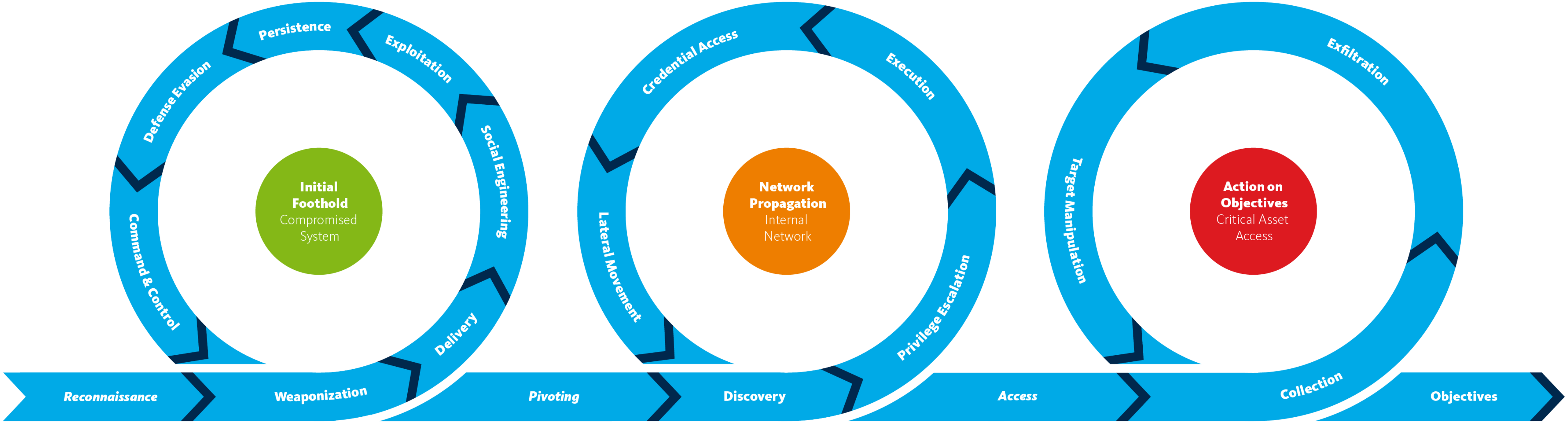
1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps

Data Classification Process



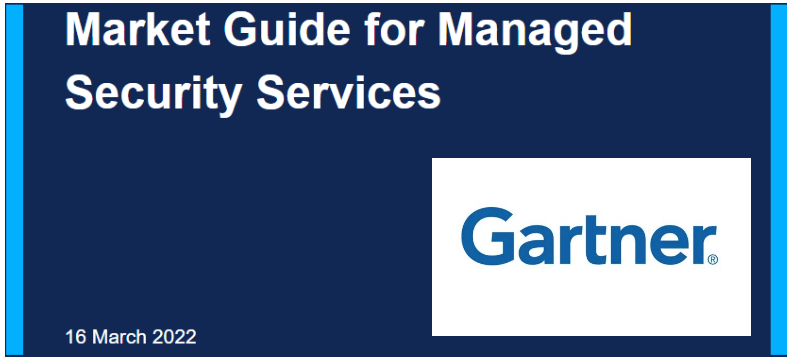
Threat Activity

Unified Kill Chain



Gartner Recognition

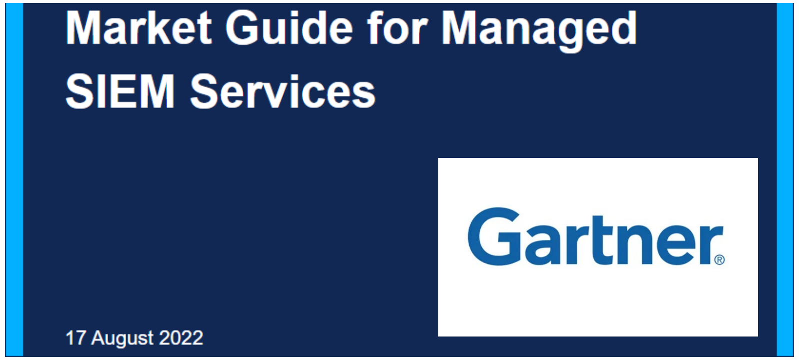
2022



Market Guide for Managed Security Services

Gartner.

16 March 2022



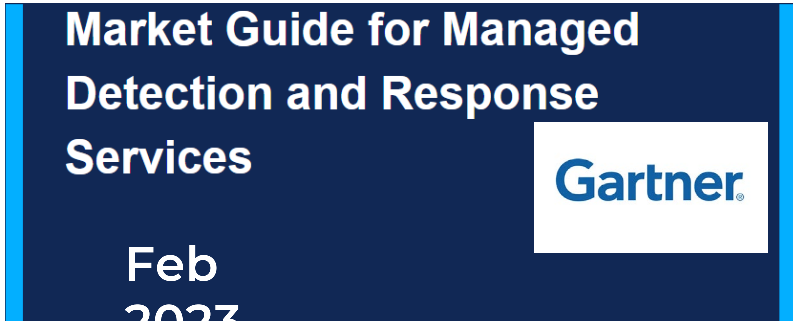
Market Guide for Managed SIEM Services

Gartner.

17 August 2022

✓ Integrity360 named as representative vendor in the last 2 market guides for Managed Security Services

✓ Integrity360 named as representative vendor in the market guide for Managed SIEM Services



Market Guide for Managed Detection and Response Services

Gartner.

Feb 2023

✓ **Integrity360 has been listed as a representative vendor in the new Market Guide for Managed Detection and Response Services, published 14/Feb/2023**

2023

https://info.integrity360.com/gartnermdr

Detection & Response Challenges

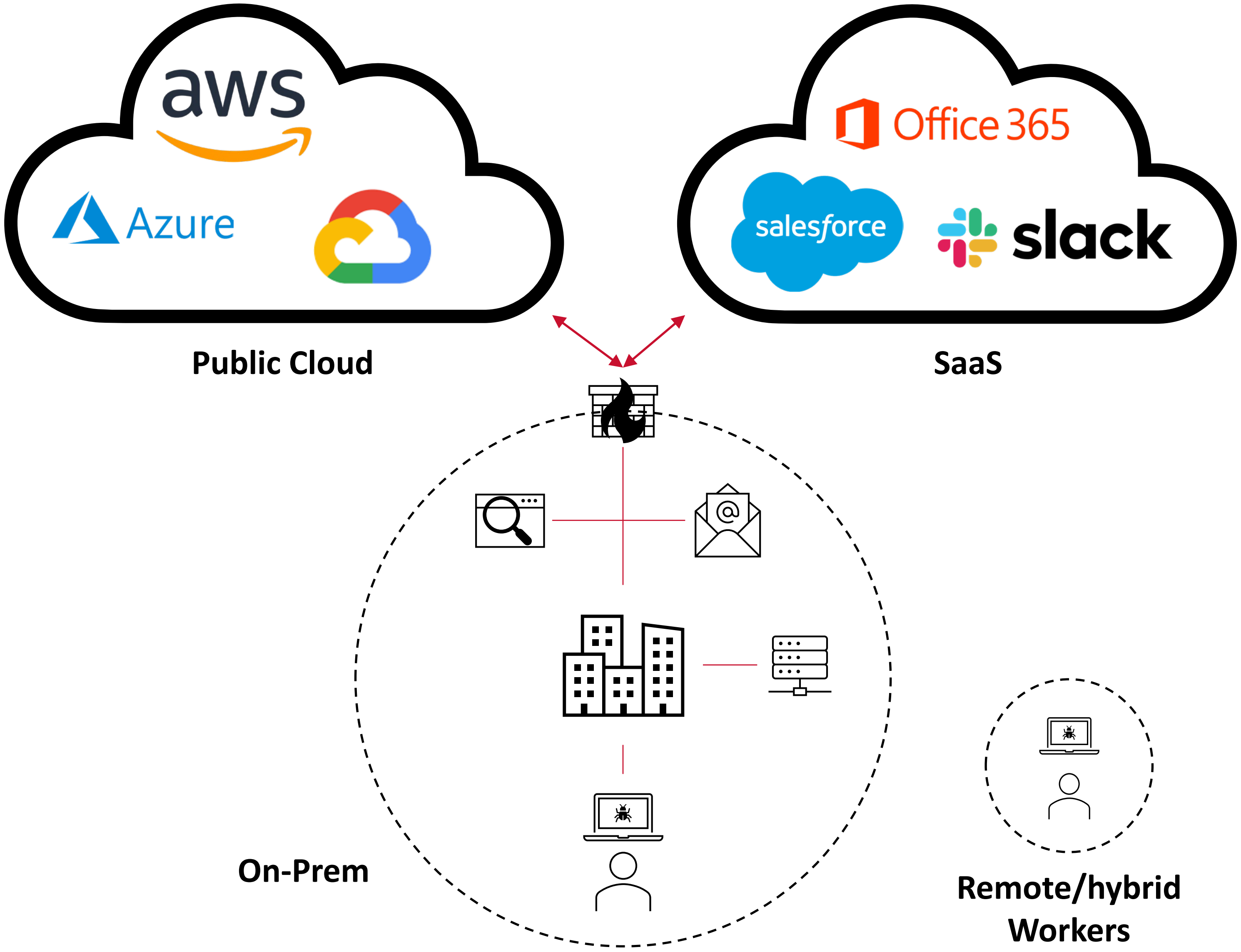
Do we have the right tools?

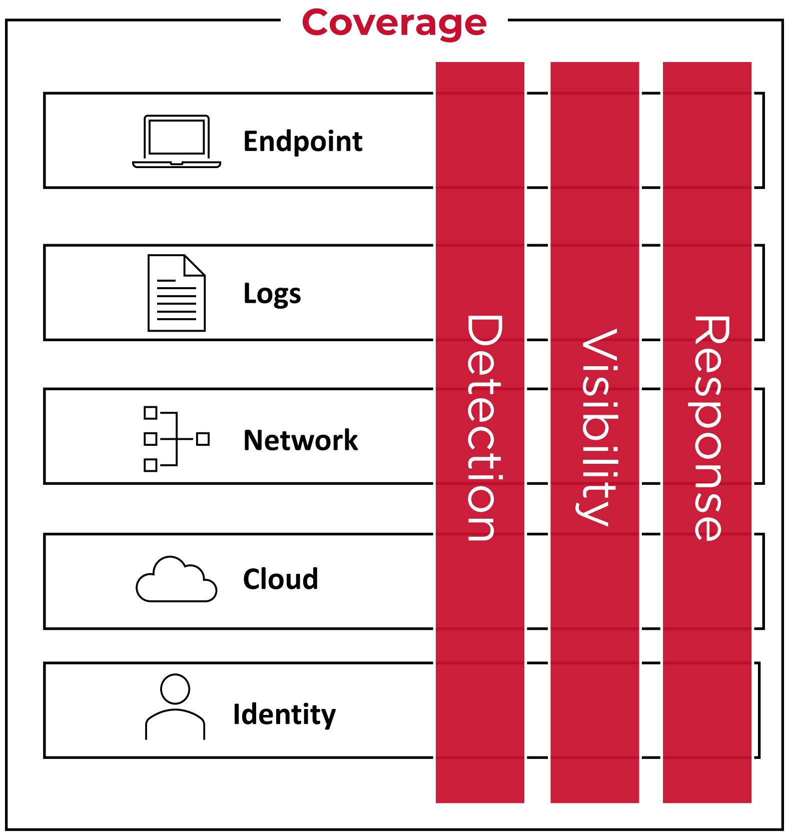
Do we have the right processes?

Do we have the right people?

Do we have the right tools?

Detection & Response Landscape





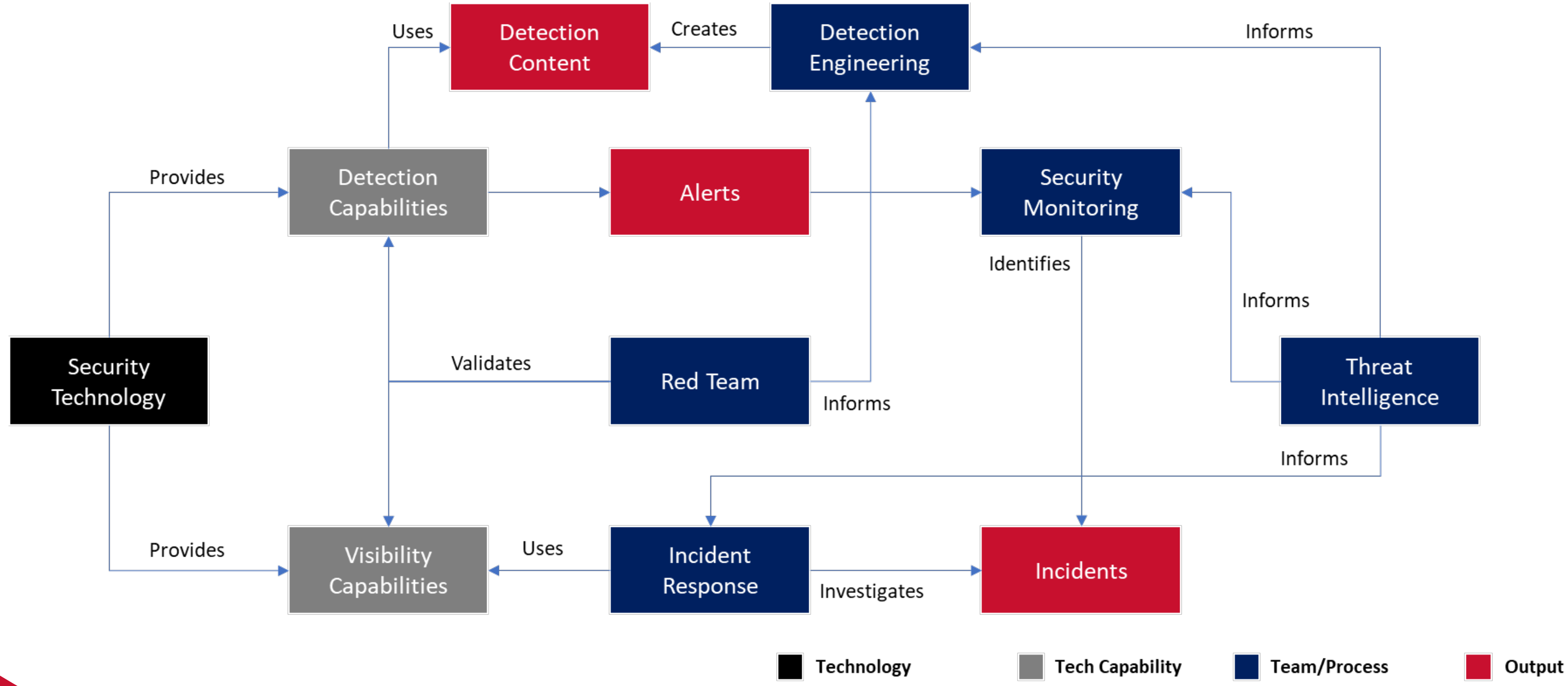
Detection vs. Visibility

Detection

Detection capabilities are used to generate alerts when active threat activity is detected within the environment.

Visibility

Visibility capabilities support the IR process during the investigation of incidents, and enable threat hunting activity.



Tactical vs. Strategic Detection

Tactical

Detection of common threats is tactical

Common: Threats common across all organisations, particular vertical or geographic location.

- Named attacks & threat actor groups (e.g. APT40)
- Threats against common platform vulnerabilities (e.g. Windows)
- Mitre Att&ck technique

Off the shelf detection

EPP | EDR | NDR | XDR

Strategic

Detection of uncommon threats is strategic

Uncommon: Threats unique only to your organisation, business process or internal applications

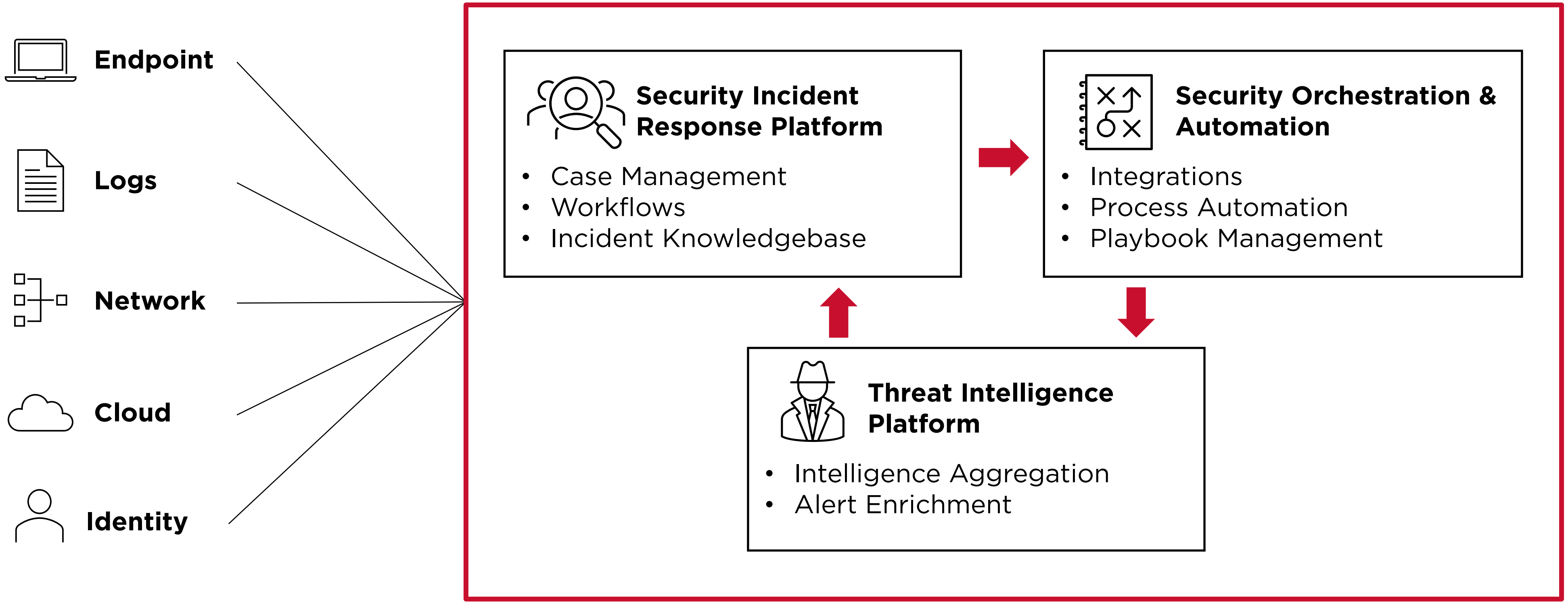
- Unique business risks
- Unique application risks
- Behaviour risks
- Company policy violation

Customised detection

SIEM

Bringing it all together

SOC Operations Tooling



Security Incident Response Platform

- Case Management
- Workflows
- Incident Knowledgebase

Security Orchestration & Automation

- Integrations
- Process Automation
- Playbook Management

Threat Intelligence Platform

- Intelligence Aggregation
- Alert Enrichment

Response

Endpoint

CROWDSTRIKE cynet

Trellix Microsoft

- Isolate Host
- Kill Process
- Execute Command

Network

CHECK POINT

FORTINET

paloalto NETWORKS

- Block Network Connection

Identity

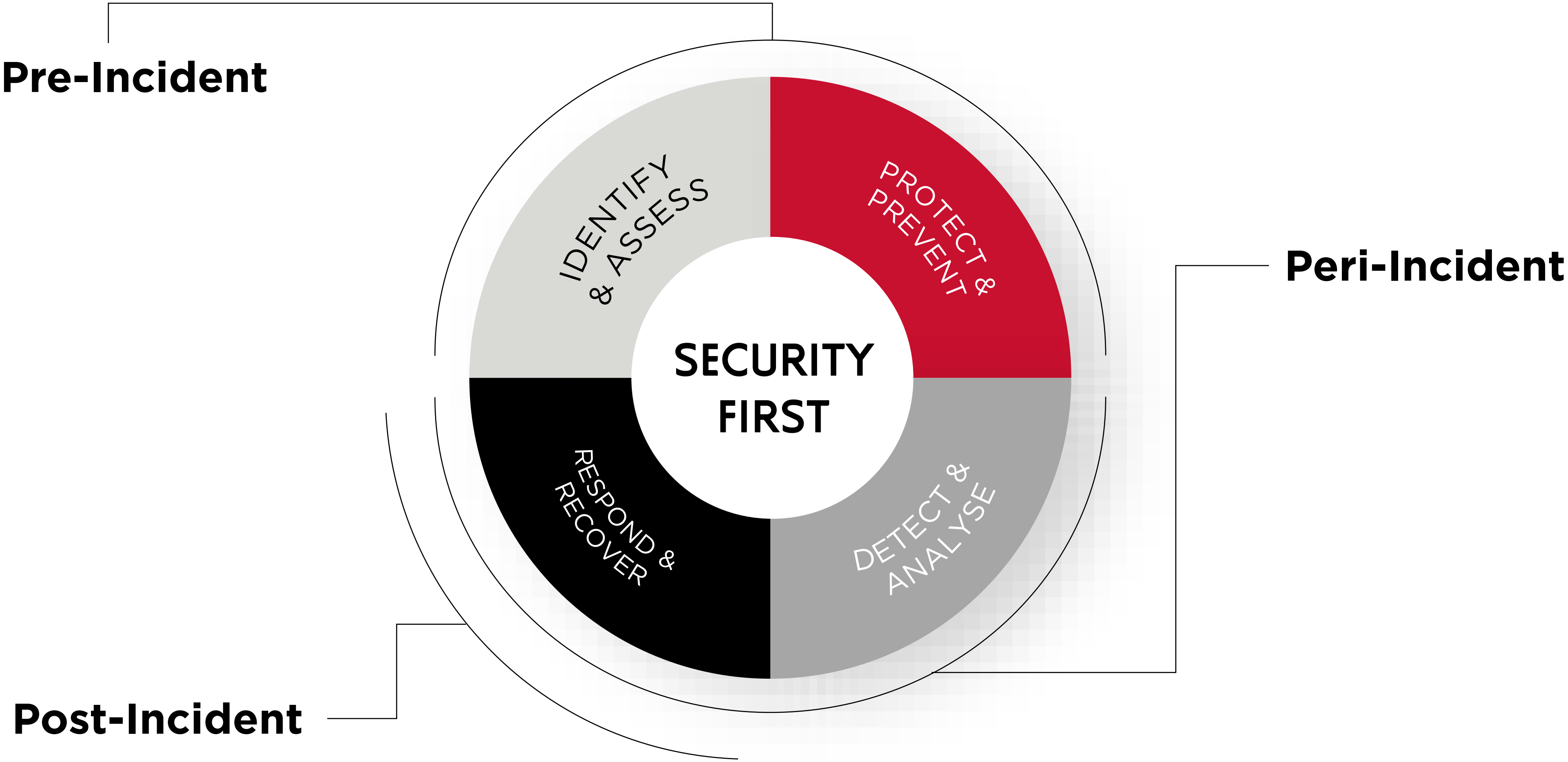
Azure Active Directory

Microsoft Active Directory

- Disable user account
- Log user out
- Change group membership

Do we have the right Processes?

Security First: Process Mapping



Pre, Peri & Post Incident Processes

Pre-Incident

- Threat Intelligence
- Security Engineering
- Detection Engineering
- Continuous Testing

Peri-Incident

Alert Management

- Alert Triage
- Alert Enrichment

Incident Handling

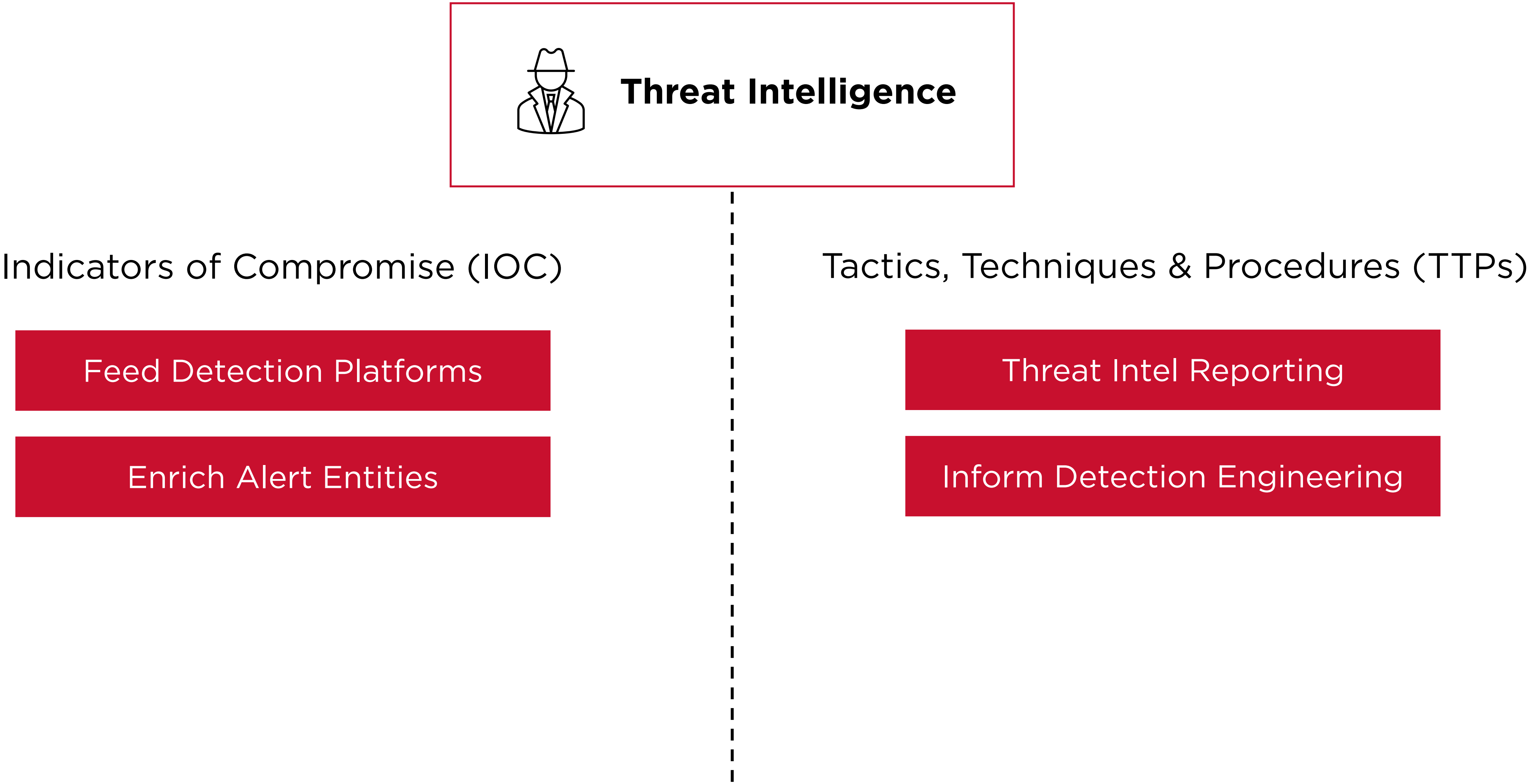
- Incident Analysis
- Containment & Response

- Threat Hunting

Post-Incident

- Forensic Analysis
- Eradication
- Root Cause Analysis

Threat Intelligence



Threat Intelligence

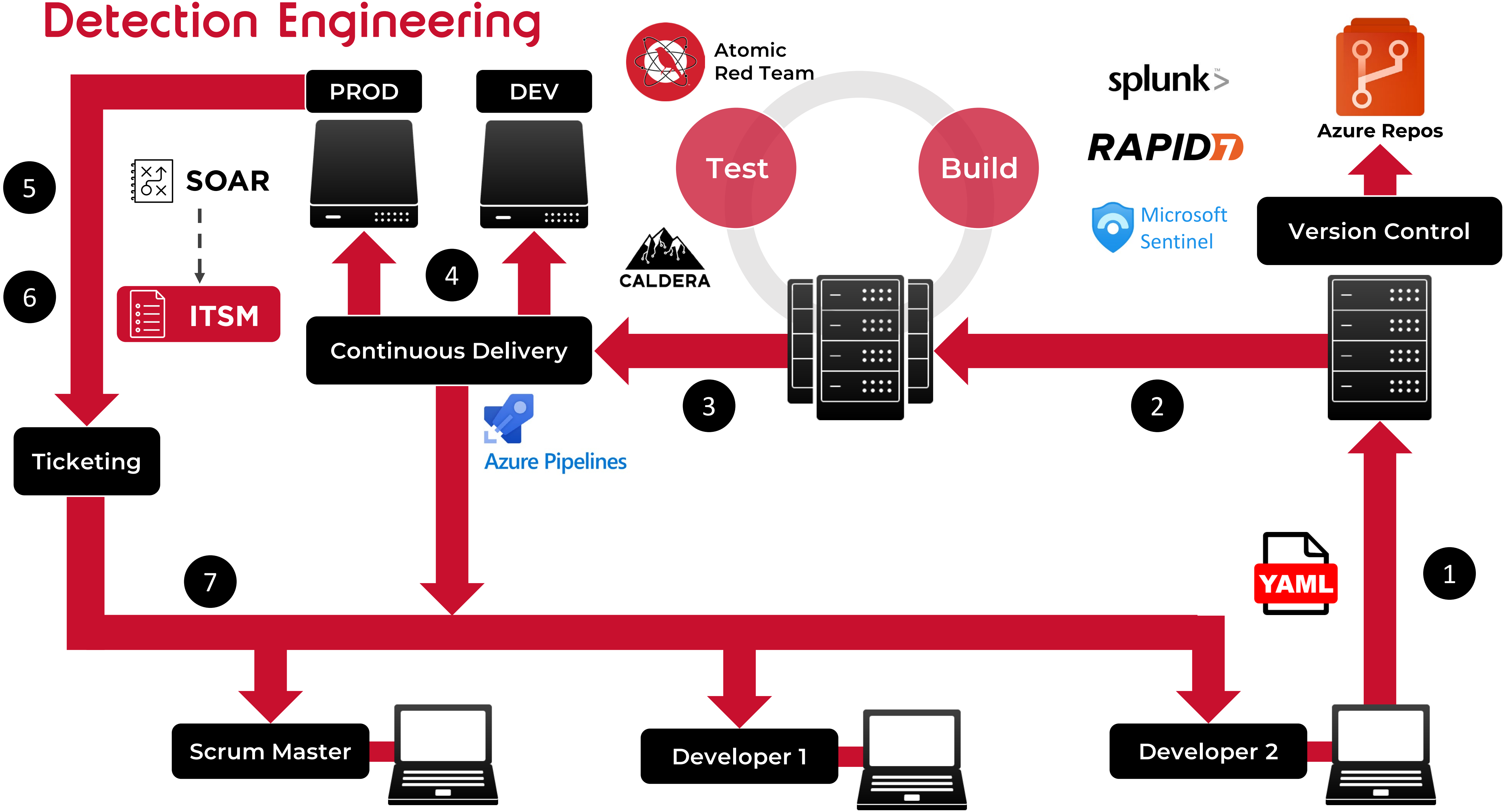
Indicators of Compromise (IOC)

- Feed Detection Platforms
- Enrich Alert Entities

Tactics, Techniques & Procedures (TTPs)

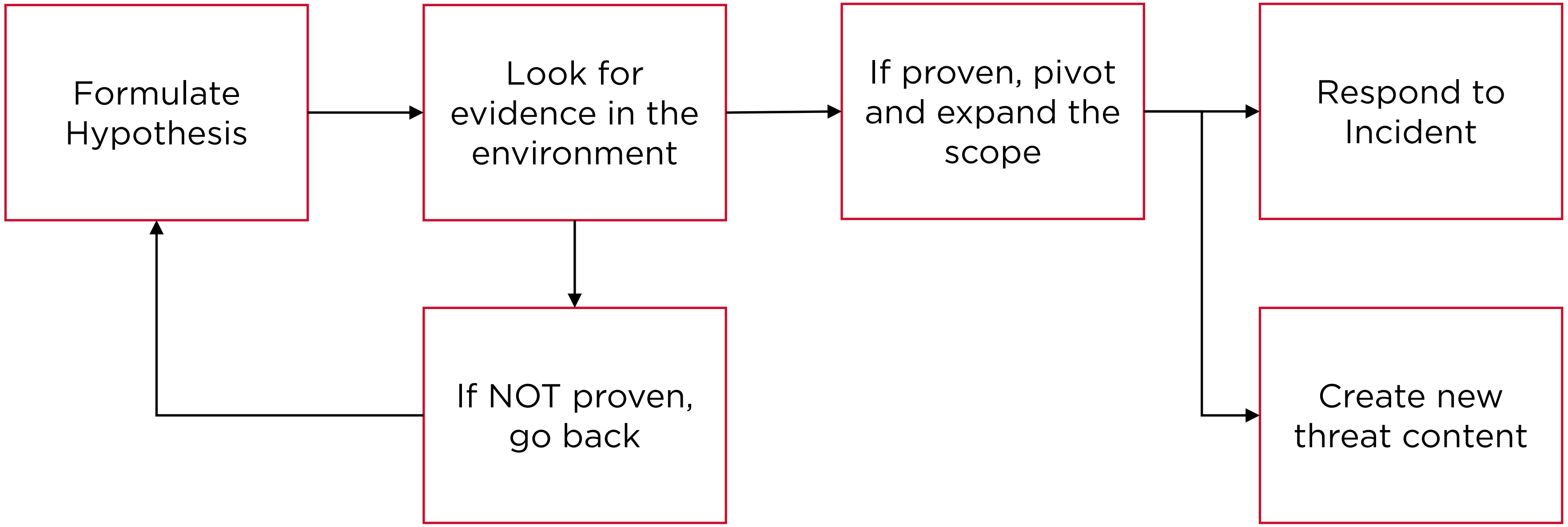
- Threat Intel Reporting
- Inform Detection Engineering

Detection Engineering



Threat Hunting

Threat Hunting is a manual process. Automated Threat Hunting is just Threat Detection!


Formulate Hypothesis
Look for evidence in the environment
If proven, pivot and expand the scope
Respond to Incident
Create new threat content
If NOT proven, go back

Example Threat Hunting Triggers

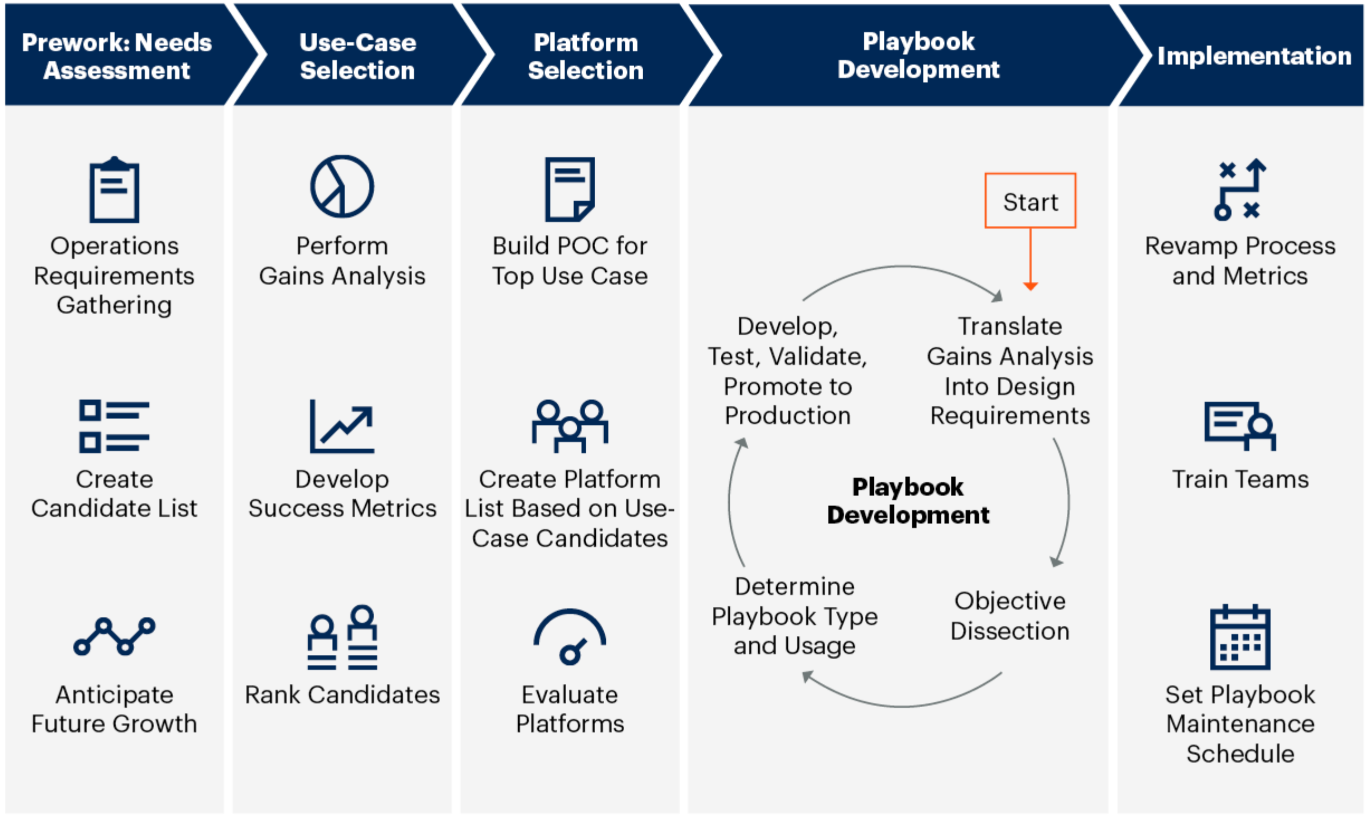
- **Indicators of Attack/TTPs (Structured Hunt)**
- **Abnormal/Spike in activity (Unstructured Hunt)**

Not discovering a threat is not a failure. Typical byproducts of threat hunting:

- Discover misconfiguration
- Incorrect Logging
- Misaligned security policies
- Poor Security Practices

Automation

Security Automation Guidance Framework



Prework: Needs Assessment
- Operations Requirements Gathering
- Create Candidate List
- Anticipate Future Growth

Use-Case Selection
- Perform Gains Analysis
- Develop Success Metrics
- Rank Candidates

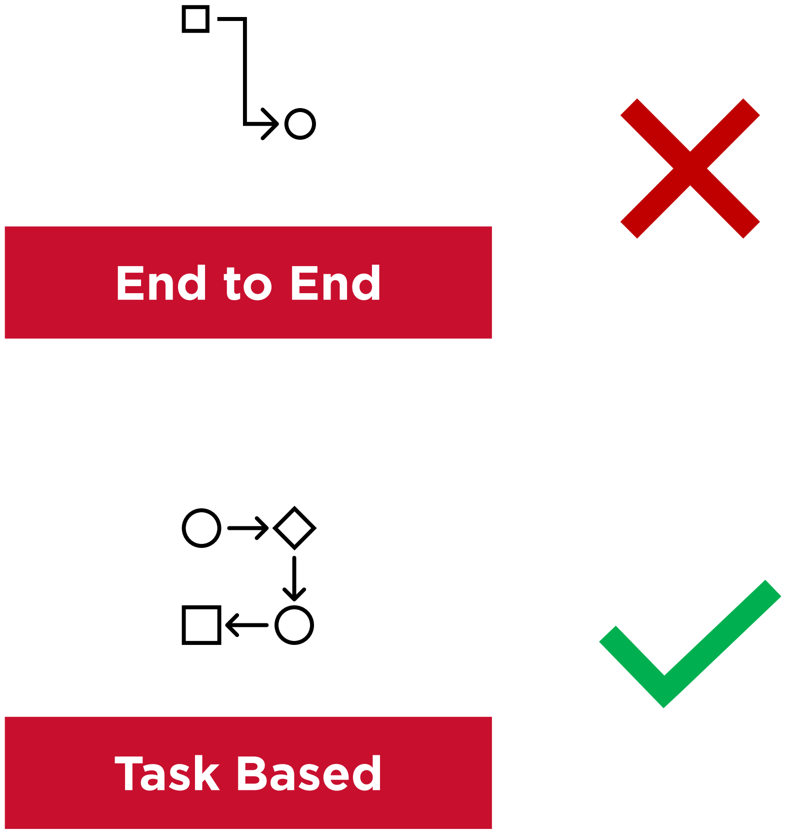
Platform Selection
- Build POC for Top Use Case
- Create Platform List Based on Use-Case Candidates
- Evaluate Platforms

Playbook Development
- Start
- Translate Gains Analysis Into Design Requirements
- Objective Dissection
- Determine Playbook Type and Usage
- Develop, Test, Validate, Promote to Production

Playbook Development

Implementation
- Revamp Process and Metrics
- Train Teams
- Set Playbook Maintenance Schedule

Automation Approach



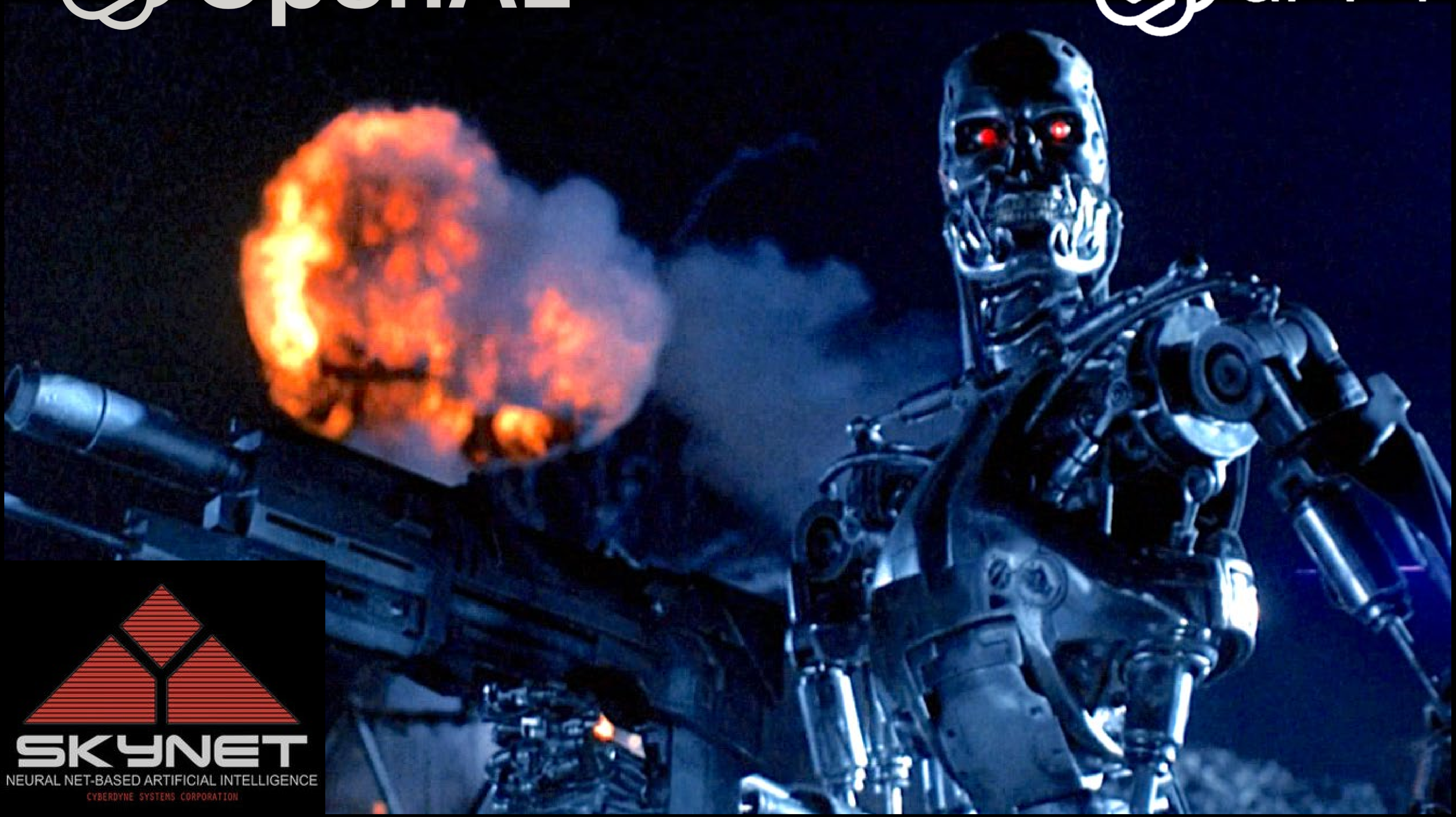
End to End ✗

Task Based ✓

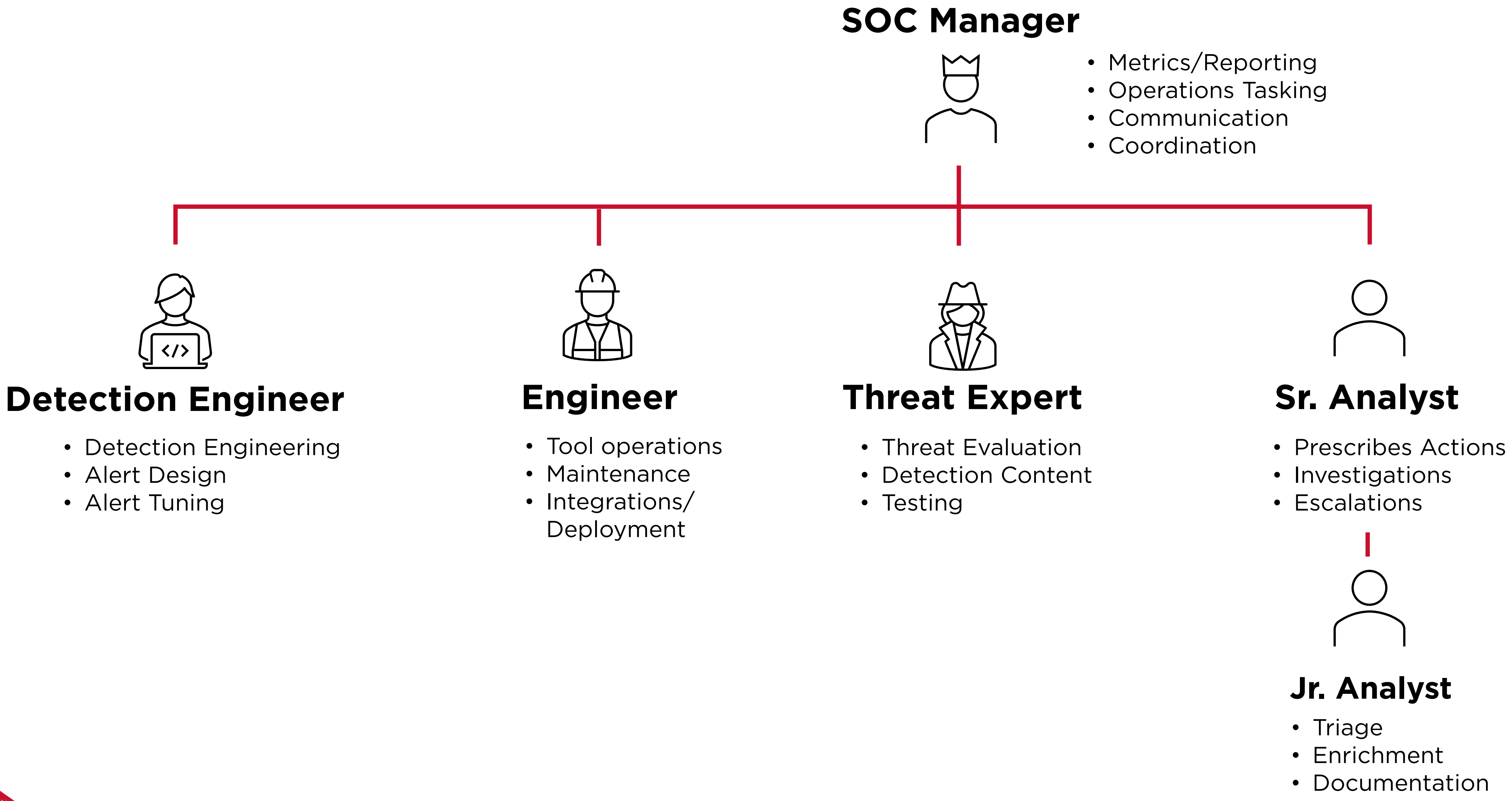
Do we have the right People?

OpenAI

GPT-4


SKYNET
NEURAL NET-BASED ARTIFICIAL INTELLIGENCE
CYBERDYNE SYSTEMS CORPORATION

SOC Roles



SOC Manager

- Metrics/Reporting
- Operations Tasking
- Communication
- Coordination

Detection Engineer

- Detection Engineering
- Alert Design
- Alert Tuning

Engineer

- Tool operations
- Maintenance
- Integrations/ Deployment

Threat Expert

- Threat Evaluation
- Detection Content
- Testing

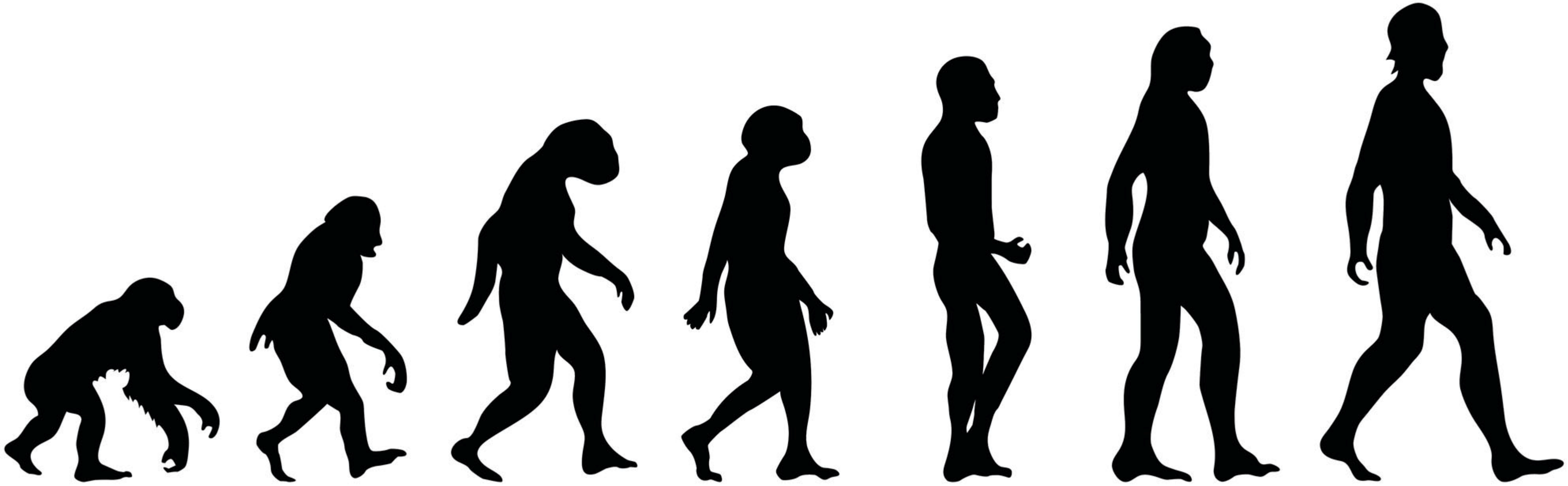
Sr. Analyst

- Prescribes Actions
- Investigations
- Escalations

Jr. Analyst

- Triage
- Enrichment
- Documentation

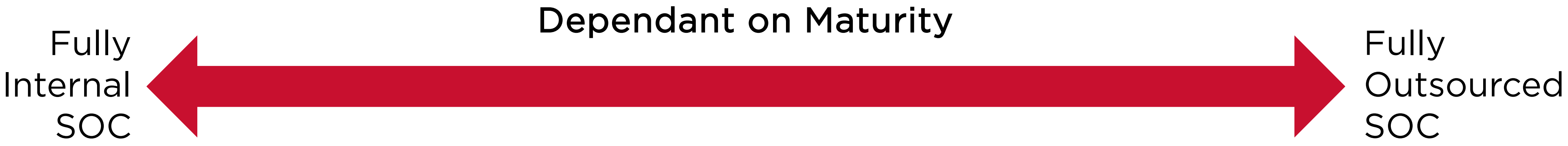
Evolution of Security Analysts



Network Security → SysAdmin → Software Engineer

Hybrid SOC?

Reality: Every SOC is a Hybrid SOC



Dependant on Maturity

Fully Internal SOC

Fully Outsourced SOC

Outsource tactical, repeatable common activities

Ensure 24x7 Security Monitoring & Response

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Controls Effectiveness

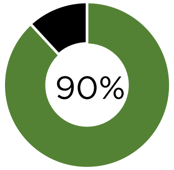
Effective Security Management: Measurement & KRI’s

Key Risk Indicators are key performance indicators or drivers that allow you to assess the overall health of your security operation.

Example Hygiene Dashboard

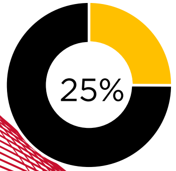
Vulnerabilities

4 Successful Scans Run in Period



% of Systems with VM Agent installed

358 Critical Vulnerabilities over 60 days old

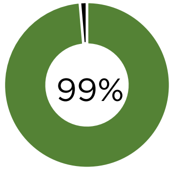


% of Critical Assets with Vulnerabilities

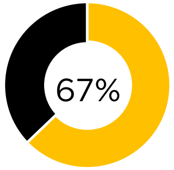
Endpoints

26 Systems without Endpoint Agent Installed

15 Malware Events Detected in Period



% of Critical Systems Reporting into SIEM



% of Systems Reporting into SIEM

Users

27 Users with Outstanding Security Training Modules

0 Users failing phishing exercises

15 Phishing Emails Reported during period

Effective Security Management: Control Validation

Proactively validate the effectiveness of your security controls

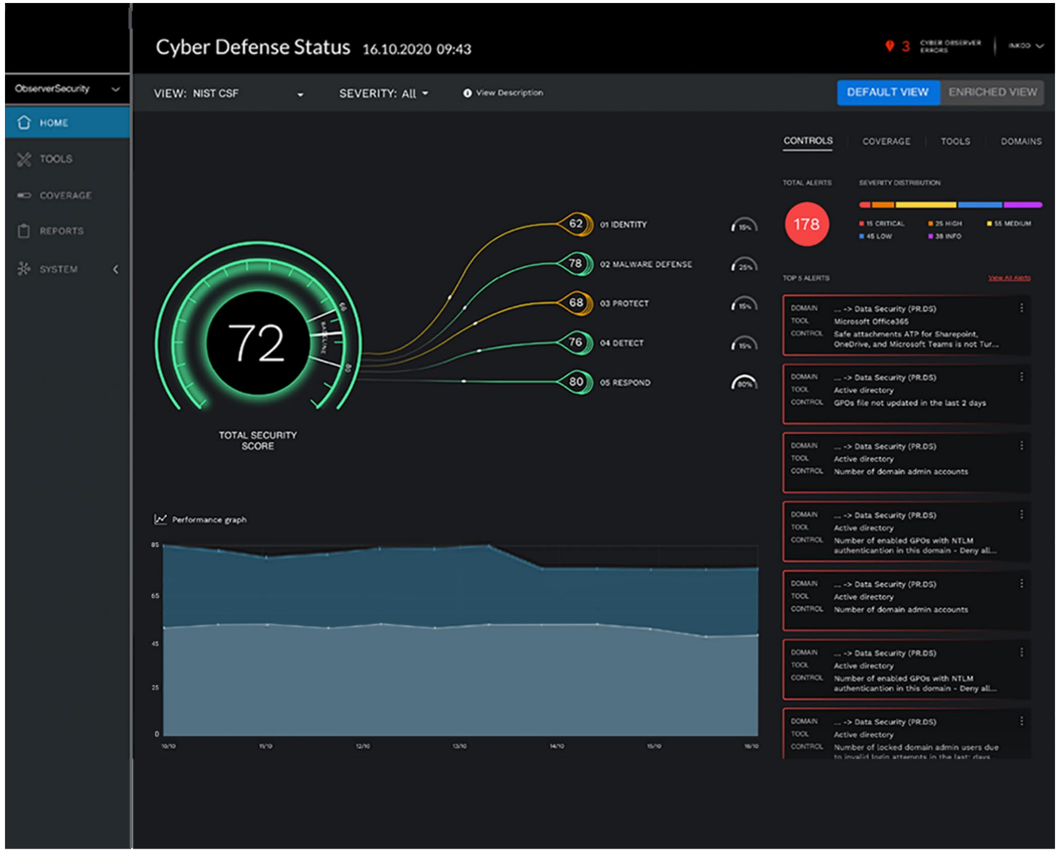
Cyber Security Testing

- Internal & External Penetration testing
- Red Teaming Exercises
- Purple Teaming Exercises

Automated Tools

- Breach & Attack Simulation
- Attack Path Management

Continuous Control Monitoring



DOMAIN ... -> Data Security (PR.DS)
TOOL Microsoft Office365
CONTROL Safe attachments ATP for Sharepoint, OneDrive, and Microsoft Teams is not Tur...

DOMAIN ... -> Data Security (PR.DS)
TOOL Active directory
CONTROL GPOs file not updated in the last 2 days

DOMAIN ... -> Data Security (PR.DS)
TOOL Active directory
CONTROL Number of domain admin accounts

DOMAIN ... -> Data Security (PR.DS)
TOOL Active directory
CONTROL Number of enabled GPOs with NTLM authenticantion in this domain - Deny all...

DOMAIN ... -> Data Security (PR.DS)
TOOL Active directory
CONTROL Number of domain admin accounts

DOMAIN ... -> Data Security (PR.DS)
TOOL Active directory
CONTROL Number of enabled GPOs with NTLM authenticantion in this domain - Deny all...

DOMAIN ... -> Data Security (PR.DS)
TOOL Active directory
CONTROL Number of locked domain admin users due to invalid login attempts in the last: days

Summary

Ensure your visibility is not limited in scope and extends across the modern IT landscape

Gain visibility across the **Attack Surface** to minimise exposure, **Threat Activity** to confidently detect threats, and **Control Effectiveness** to ensure your investments deliver when required

Don't leave Data out of the equation, and prepare for GenAI/Microsoft Co-Pilot....It's coming!

Detection & Response needs to cover the expanded attack surface, and be specific to your environment

If you're starting out on your D&R journey, focus on tactical rather than strategic detection. Mature into Strategic

Don't go it alone

Validate your controls – don't leave it to chance!

Integrity360
your **security** in mind

Thank you

Richard Ford
rford@integrity360.com

© 2009 Sony Pictures Digital

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Brian Martin

Director of Product Management,

Integrity360

#securityfirst2023

FLDSMDFR

Flint Lockwood Diatonic Super Mutating Dynamic Food Replicator

On-Prem Application

- Good visibility
- Controlled access
- Confined behind perimeter
- Secure

= Good understanding of exposures to compromise

But

- Lacks scalability
- Requires own hardware
- Limited accessibility

CBFLDSMDFR

Cloud Based Flint Lockwood Diatonic Super Mutating Dynamic Food Replicator

Cloud-Based Application

- Massive scalability
- No hardware management overhead
- Wide accessibility
- Flexibility in units of production

But

- Poor visibility
- Wide attack surface
- Greater accessibility
- No longer hidden within perimeter

= New Exposures to Compromise

Cloud [klaud]

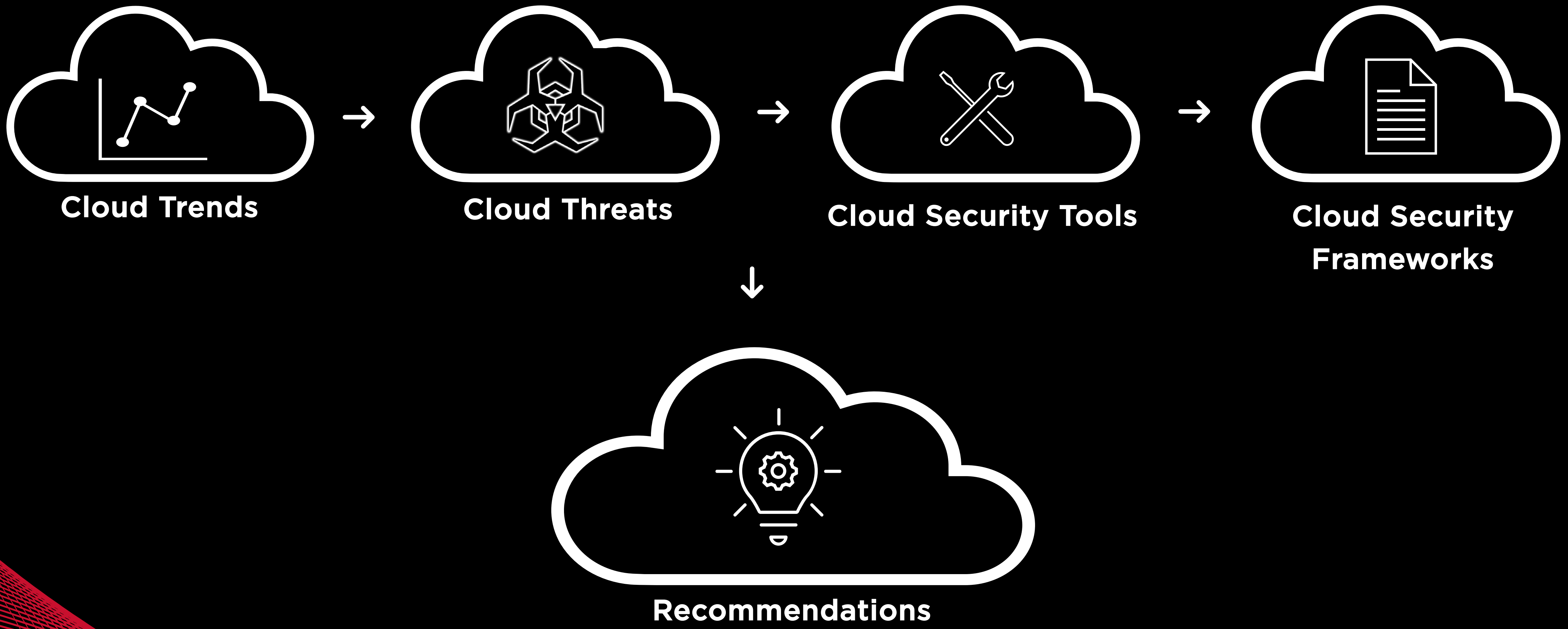
noun

- anything that obscures or darkens something, or causes gloom, trouble, suspicion, disgrace, etc.

Source: Dictionary.com

To understand Cloud Security, we must
first understand what we mean by Cloud...

Cloudy Contents



Cloud Trends

Cloud Threats

Cloud Security Tools

Cloud Security Frameworks

Recommendations

Cloud Trends

The Shift to Cloud Continues apace

Just because it's pervasive doesn't mean we understand it!

- ○ Is Evolving
- ○ Is Multi-faceted
- ○ Means different things to different people
- ○ Is not always uniformly understood
- ○ Requires technical understanding
- ○ Involves full Dev to Ops Lifecycle

To get cloud security right, we must understand cloud

SaaS Applications - Cloud connected systems -
Public/Private Hybrid Clouds - Web APIs - Cloud Native
Development – IaaS – Containers – Serverless - IaC

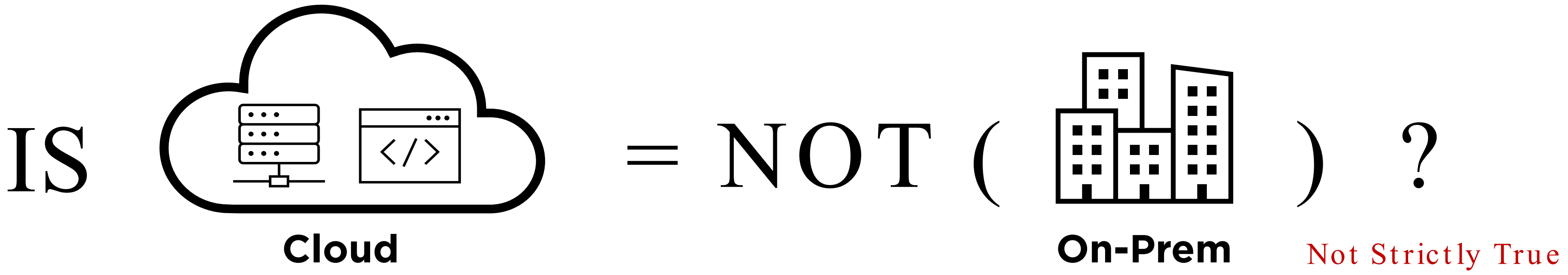
Definitions can be confusing

> “Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies.”

Gartner

We think of Cloud defined as one or more of IaaS, PaaS, and SaaS

Cloud is integral to IT, not separate from it



IS Cloud = NOT (On-Prem) ?

Not Strictly True

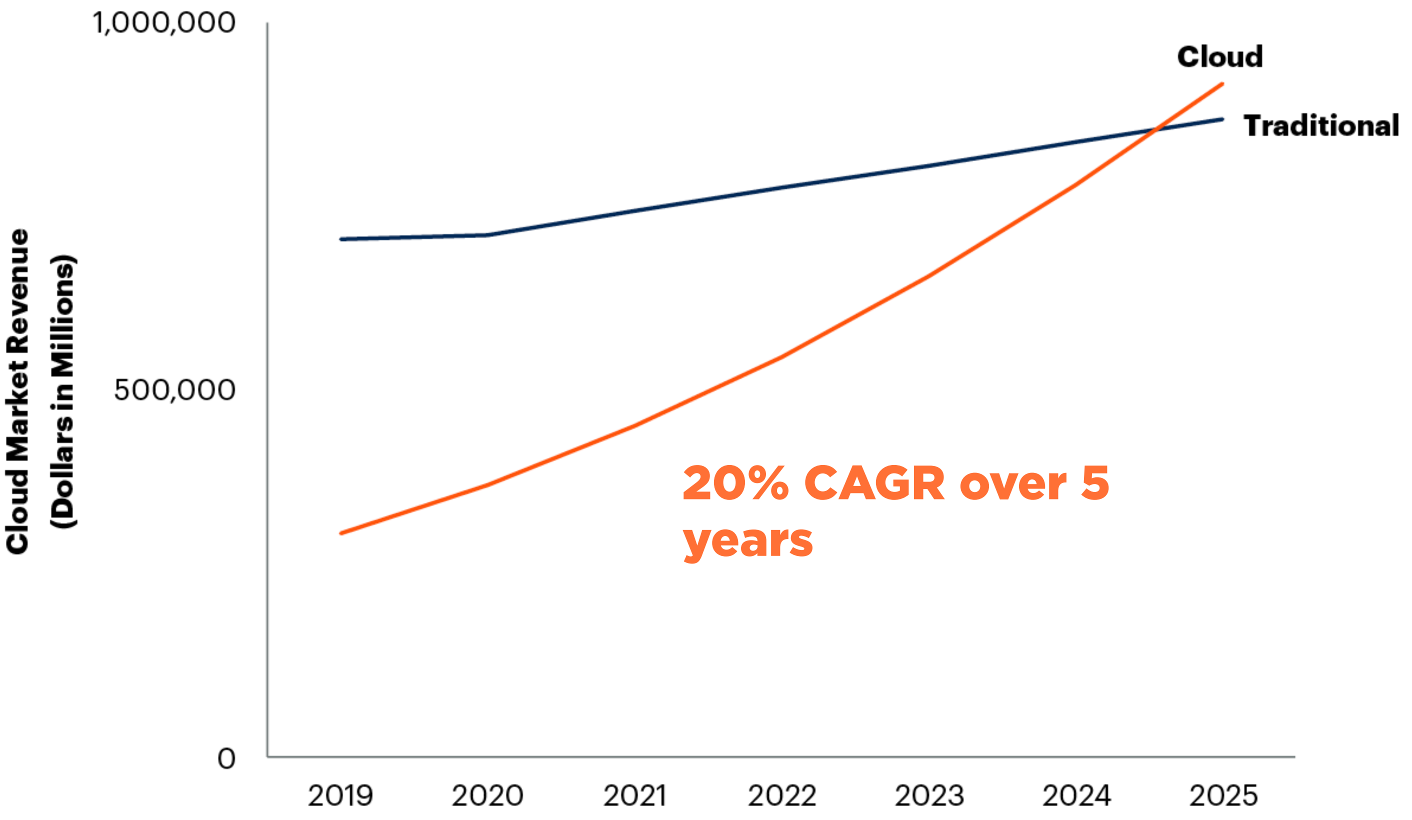
"Private cloud computing is a form of cloud computing that is used by only one organization, or that ensures that an organization is completely isolated from others"

⇒ On-prem = Private Cloud also, e.g. providing compute and applications remotely from a private or rented datacentre

Cloud refers more to the means of access to central, scalable resources than the ownership model per se

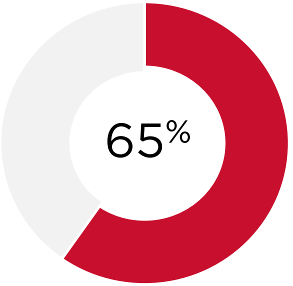
PUBLIC CLOUD + PRIVATE CLOUD + SaaS = IT

Cloud spending to overtake traditional within 2 years

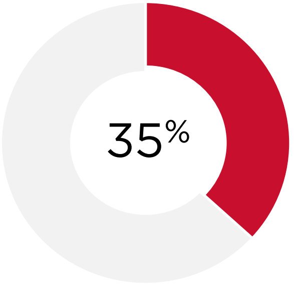


Source: Gartner, 2022

But “Traditional” also includes private cloud infrastructure spending in private and 3rd party datacentres!



of organisations are heavy users of cloud

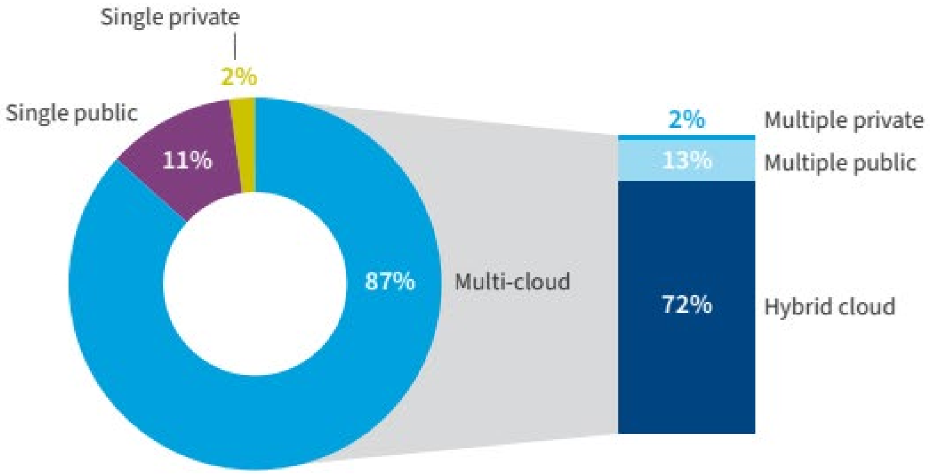


of organisations are moderate to light users of cloud

Source: Flexera State of the Cloud report, 2023

It’s mostly not single cloud either

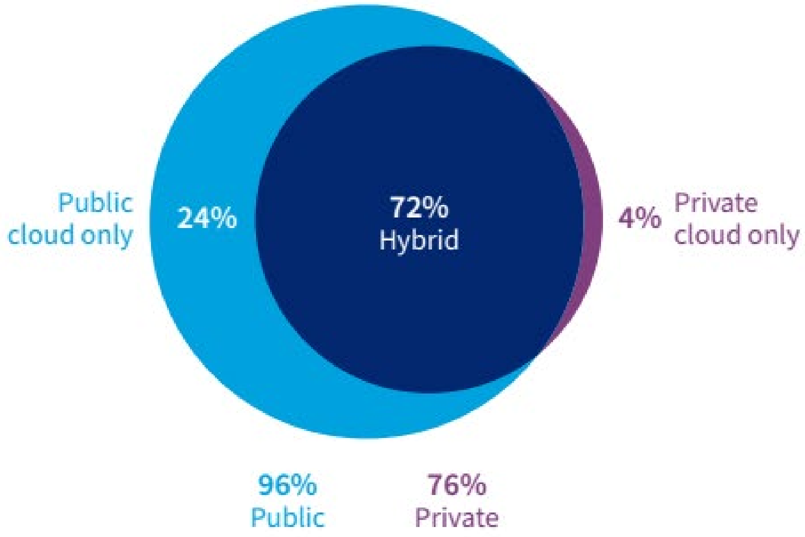
Organisations embrace multi-cloud



87% Multi-cloud

Source: Flexera State of the Cloud report, 2023

Public vs. private Cloud usage



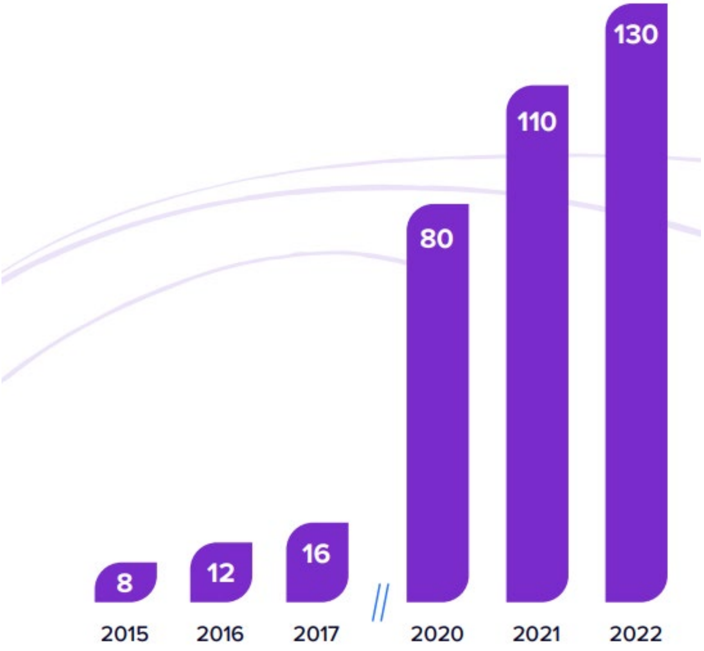
72% Hybrid public/private

By 2025, 80% of enterprises will have adopted multiple public cloud infrastructure as a service (IaaS) offerings

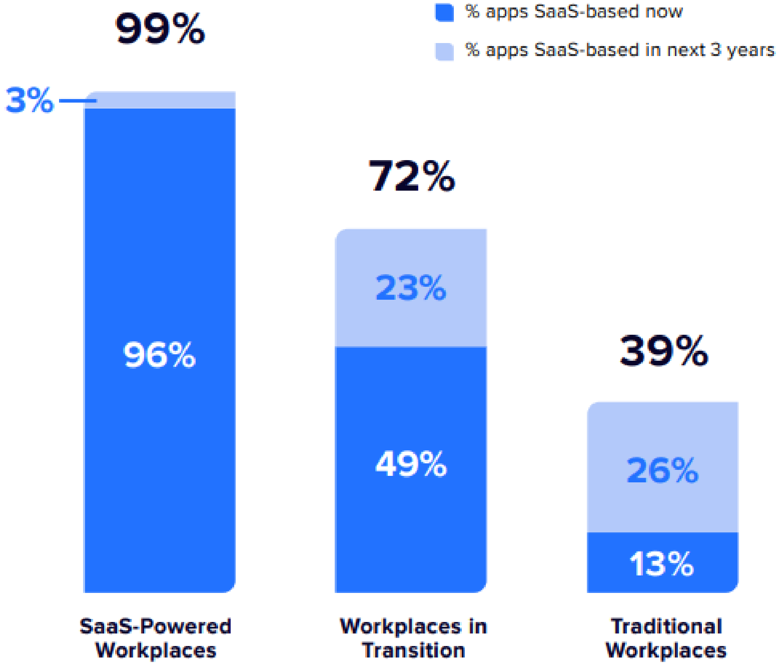
Source: Gartner, 2022

SaaS spend continues to grow by 15-20%

SaaS Apps used per organisation



% SaaS Apps by 2023-2026



IT typically is aware of only a third of SaaS Apps due to decentralised ownership and sourcing.

Source: BetterCloud state of SaaSOps 2023

Cloud Risks

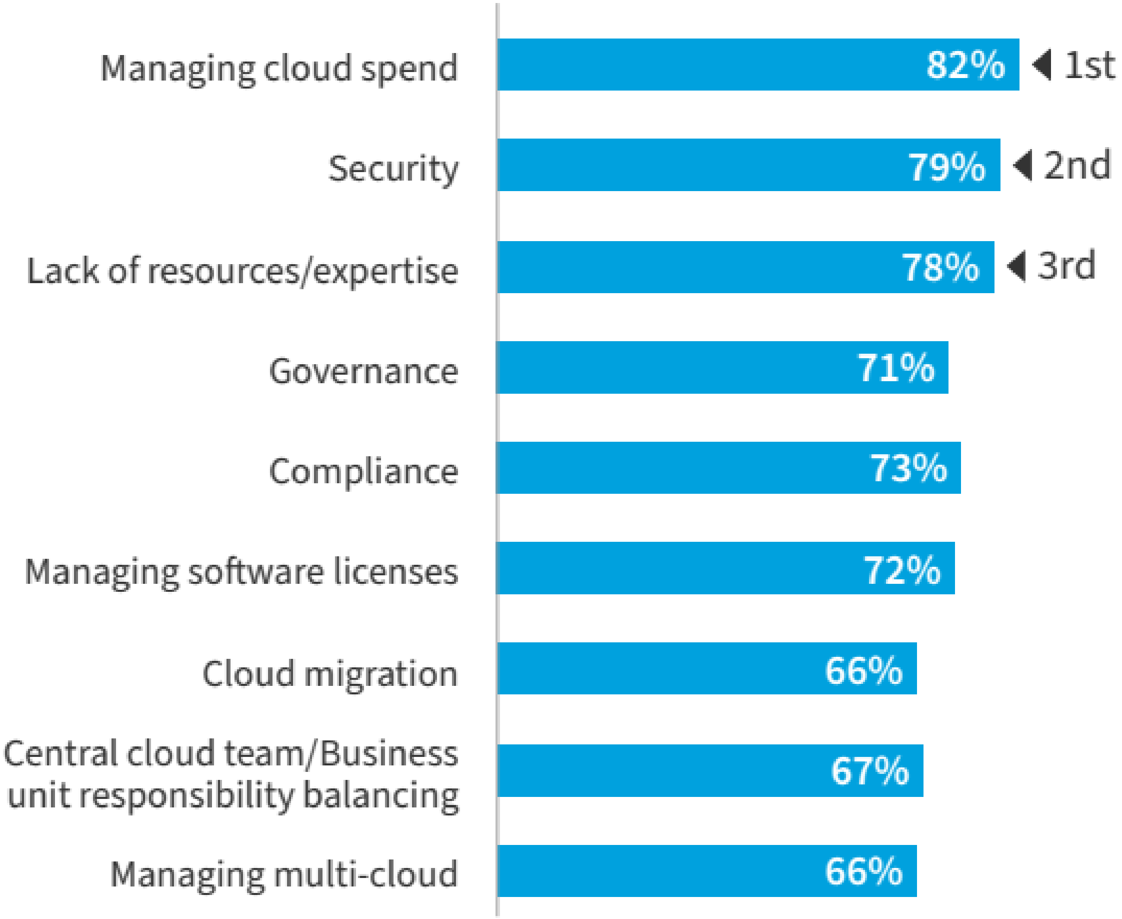
Cloud Security Grows as a Challenge

RELAX

Cloud security is no longer the top cloud challenge!!

Top Cloud Challenges

Well maybe not...



All organisations

Source: Flexera State of the Cloud report, 2023

Cloud vastly increases the attack surface

FlexBooker
3.7m Users' Data
Unsecured AWS S3 bucket

FlexBooker
19m Users' Data
Misconfigured AWS S3 bucket

Microsoft
2.4TB Customer Data
Misconfigured Azure Blob Storage Bucket

SHANGHAI CHINA
Data of 1Bn citizens
Cloud management console on internet

Microsoft
37GB source code
Compromised source code repository

medibank
9m customers' data
Cloud-based network compromised

PEGASUS AIRLINES
22M files – 6.5TBs
Misconfigured AWS S3 bucket

MANGATOON
23m users' data
Unsecured Elasticsearch DB

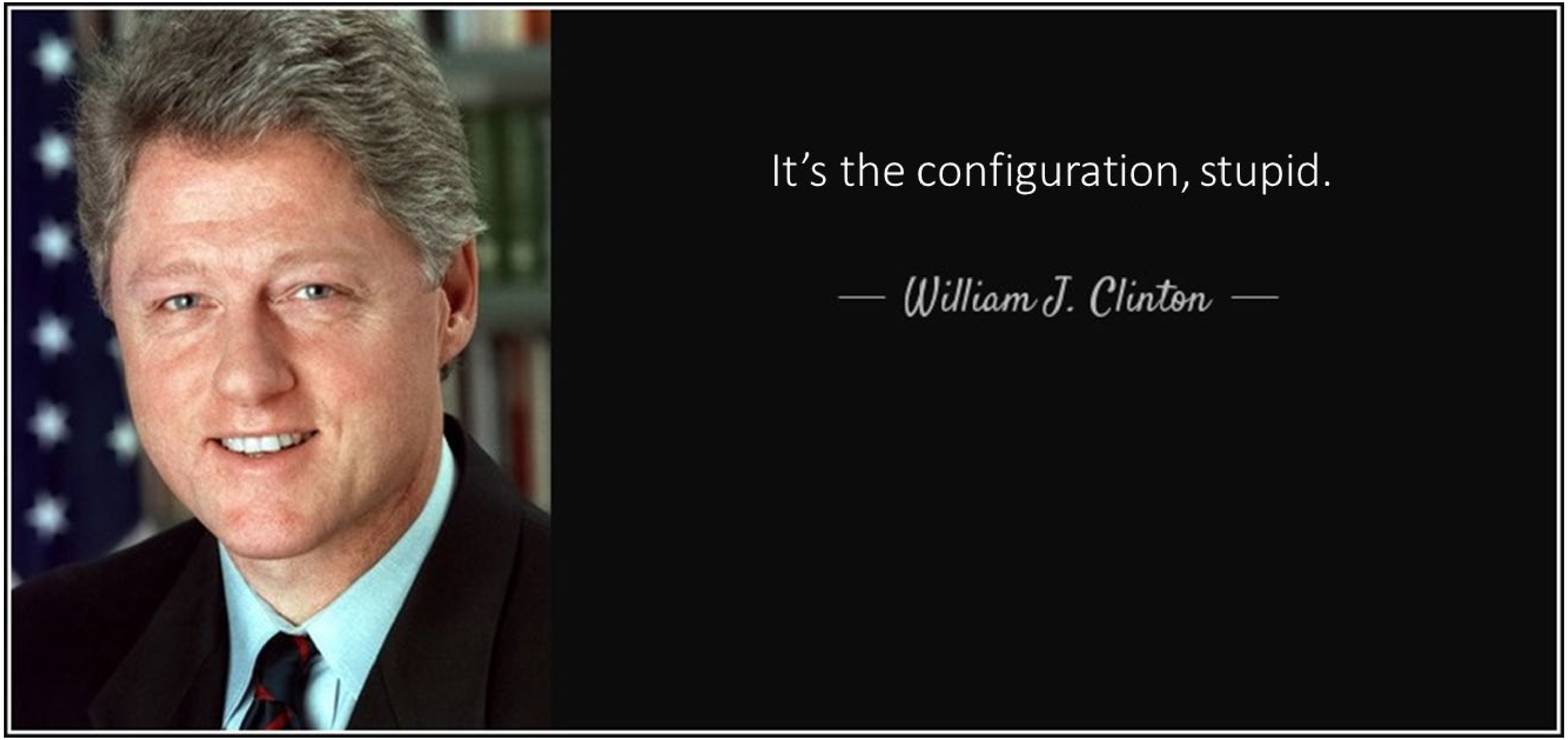
PUMA
6K Employee Records
Compromised 3rd party cloud-HR system

prime video
215m User Records
Deployment error on Prime Video database

Civicom
>100K files incl aud/vid
Misconfigured S3 bucket

LastPass•••|
30m users' data
Dev credentials stolen to access cloud storage

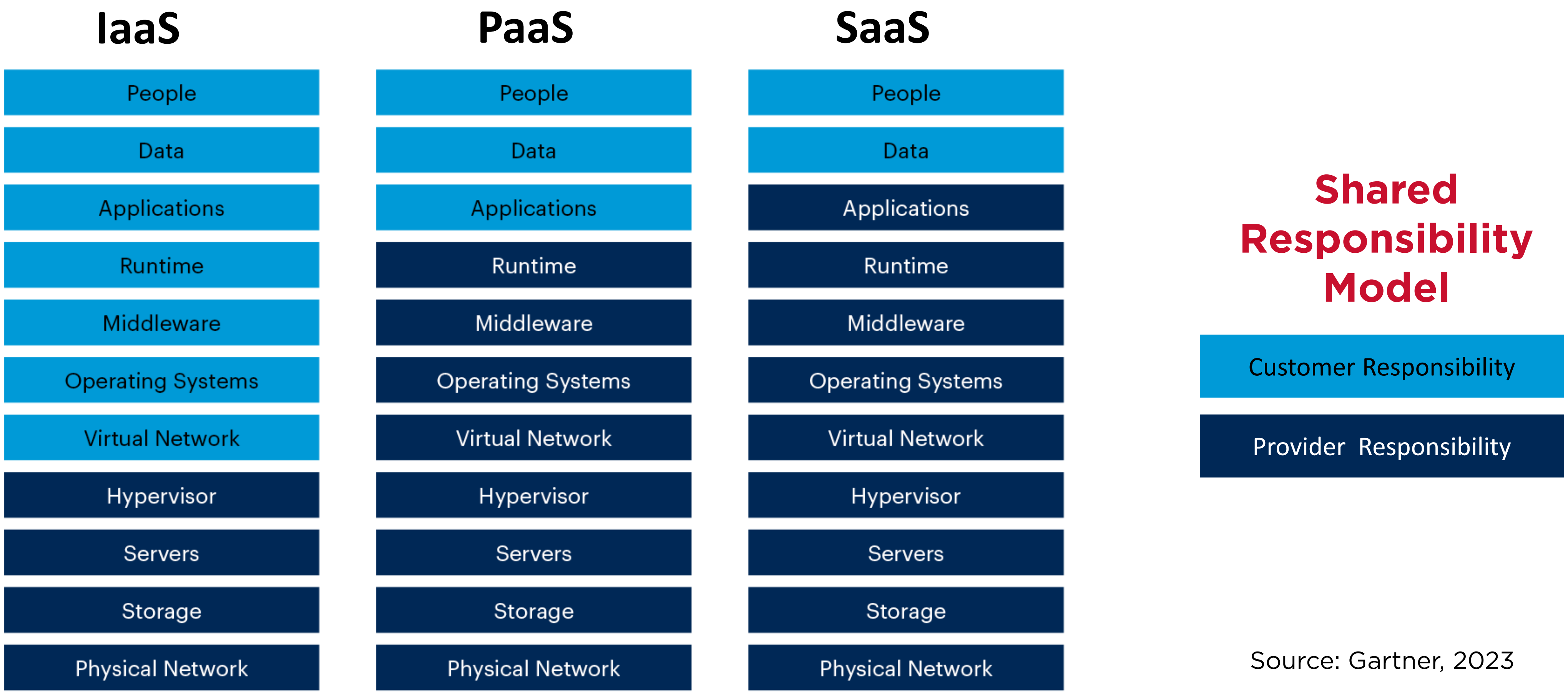
If Bill was in charge of Cloud Security...



It’s the configuration, stupid.

— William J. Clinton —

"Through 2025, over 99% of cloud breaches will have a root cause of a customer misconfiguration or mistake."



IaaS	PaaS	SaaS
🟦 People	🟦 People	🟦 People
🟦 Data	🟦 Data	🟦 Data
🟦 Applications	🟦 Applications	■ Applications
🟦 Runtime	■ Runtime	■ Runtime
🟦 Middleware	■ Middleware	■ Middleware
🟦 Operating Systems	■ Operating Systems	■ Operating Systems
🟦 Virtual Network	■ Virtual Network	■ Virtual Network
■ Hypervisor	■ Hypervisor	■ Hypervisor
■ Servers	■ Servers	■ Servers
■ Storage	■ Storage	■ Storage
■ Physical Network	■ Physical Network	■ Physical Network

Shared Responsibility Model

🟦 Customer Responsibility

■ Provider Responsibility

Source: Gartner, 2023

Categories of Cloud Risk

Provider Risk – will they
- Maintain security?
- Maintain service levels
- Maintain price and business terms
- Stay in business?

Failure is Rare

Usage Risk – will we
- Maintain security?
- Configure it appropriately?
- Govern employee activity?

Frequent Failure

Implications for Cloud Risk Management

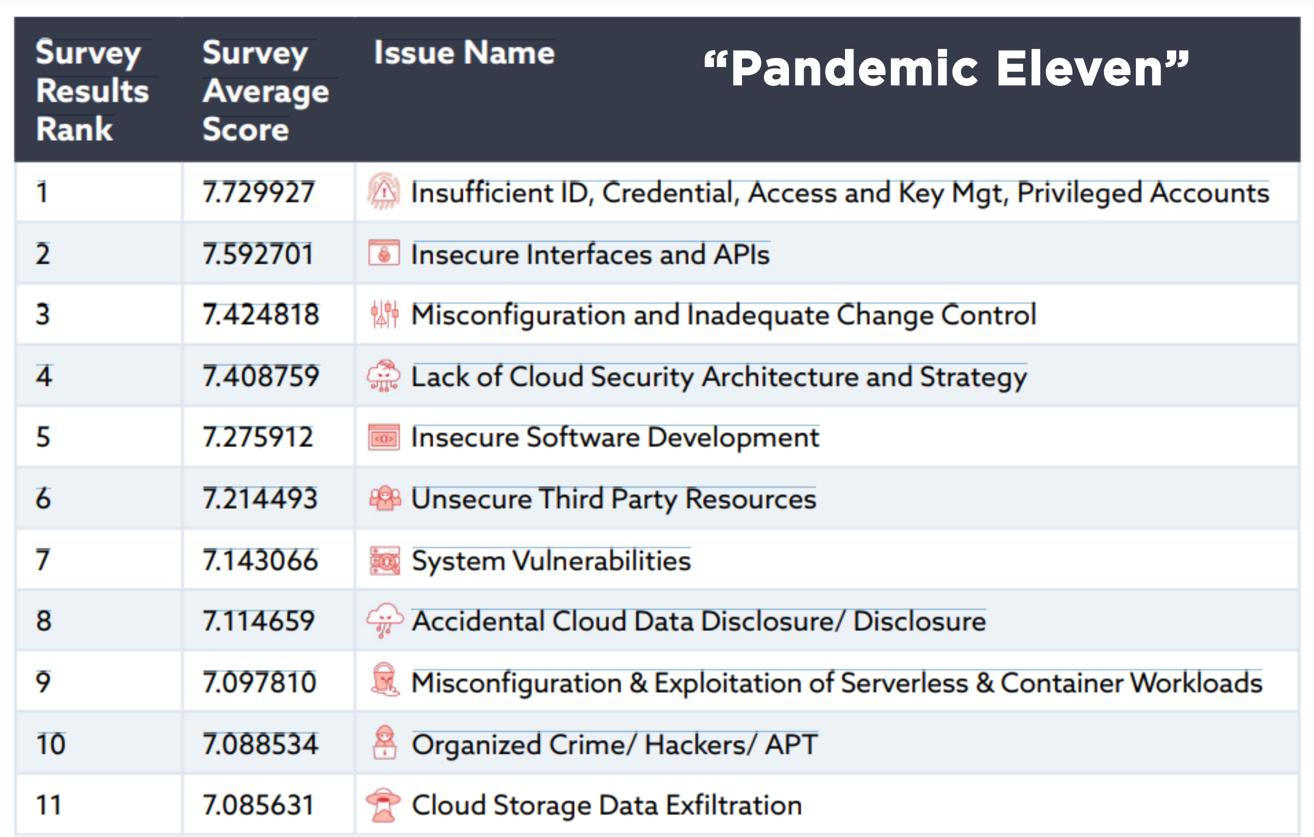
Provider Risk
- Hard to assess
- Difficult to influence vendor
- Vendor circumstances can change

Mostly outside of your control

Usage Risk
- You can choose which services to use
- You control how organisation uses and configures the services

Within your control

Top Threats to Cloud Computing – Cloud Security Alliance, 2022



“Pandemic Eleven”

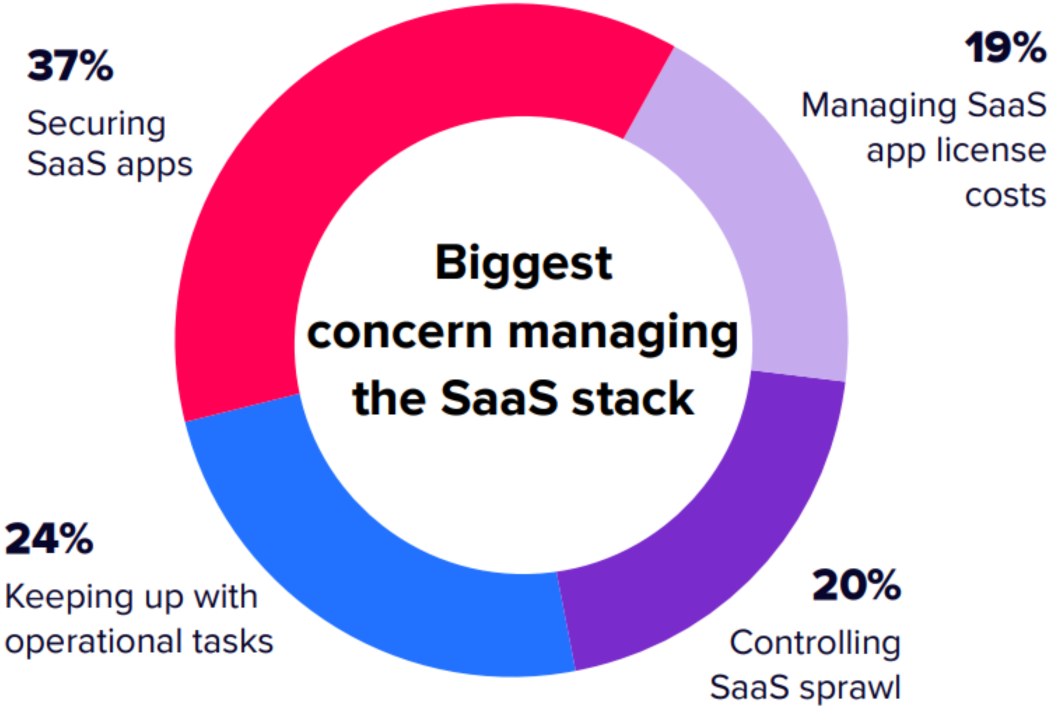
Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	Insecure Interfaces and APIs
3	7.424818	Misconfiguration and Inadequate Change Control
4	7.408759	Lack of Cloud Security Architecture and Strategy
5	7.275912	Insecure Software Development
6	7.214493	Unsecure Third Party Resources
7	7.143066	System Vulnerabilities
8	7.114659	Accidental Cloud Data Disclosure/ Disclosure
9	7.097810	Misconfiguration & Exploitation of Serverless & Container Workloads
10	7.088534	Organized Crime/ Hackers/ APT
11	7.085631	Cloud Storage Data Exfiltration

Source: Cloud Security Alliance, 2022

Key Themes

- Misconfiguration, accidents
- Managing identities, credentials, keys, accounts
- Insecure Interfaces, APIs
- Insecure development
- Internal and 3rd P. Vulnerabilities
- Security architecture and strategy

Securing apps is the leading SaaS-related concern for most organisations



Source: BetterCloud state of SaaSOps 2023

Top Themes

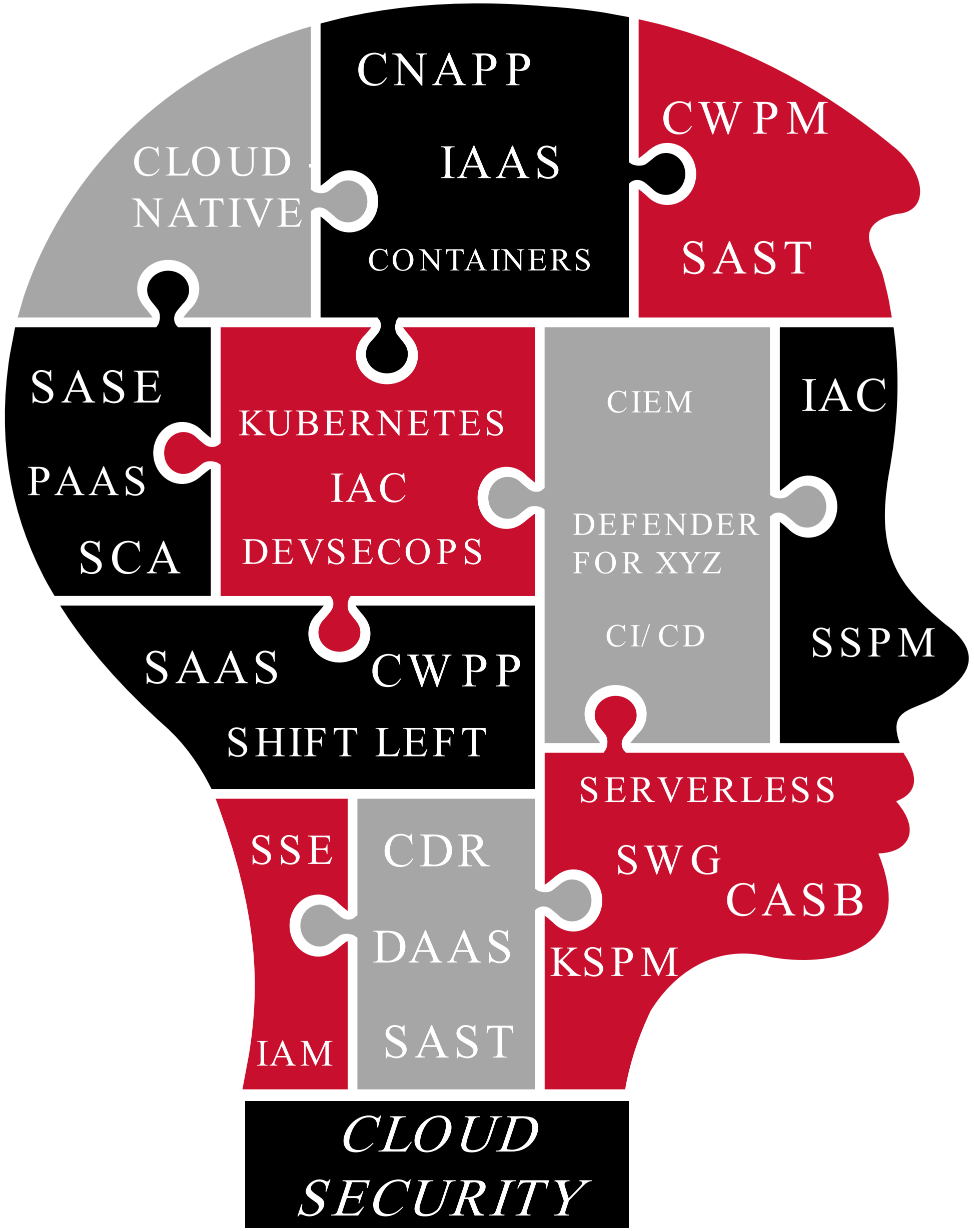
- New/unauthorised SaaS apps
- User misuse, policy violations
- Sharing of sensitive data publicly

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Cloud Security Tools

Making sense of the shifting landscape

Confusing, right?



Making sense of Cloud Security Tools

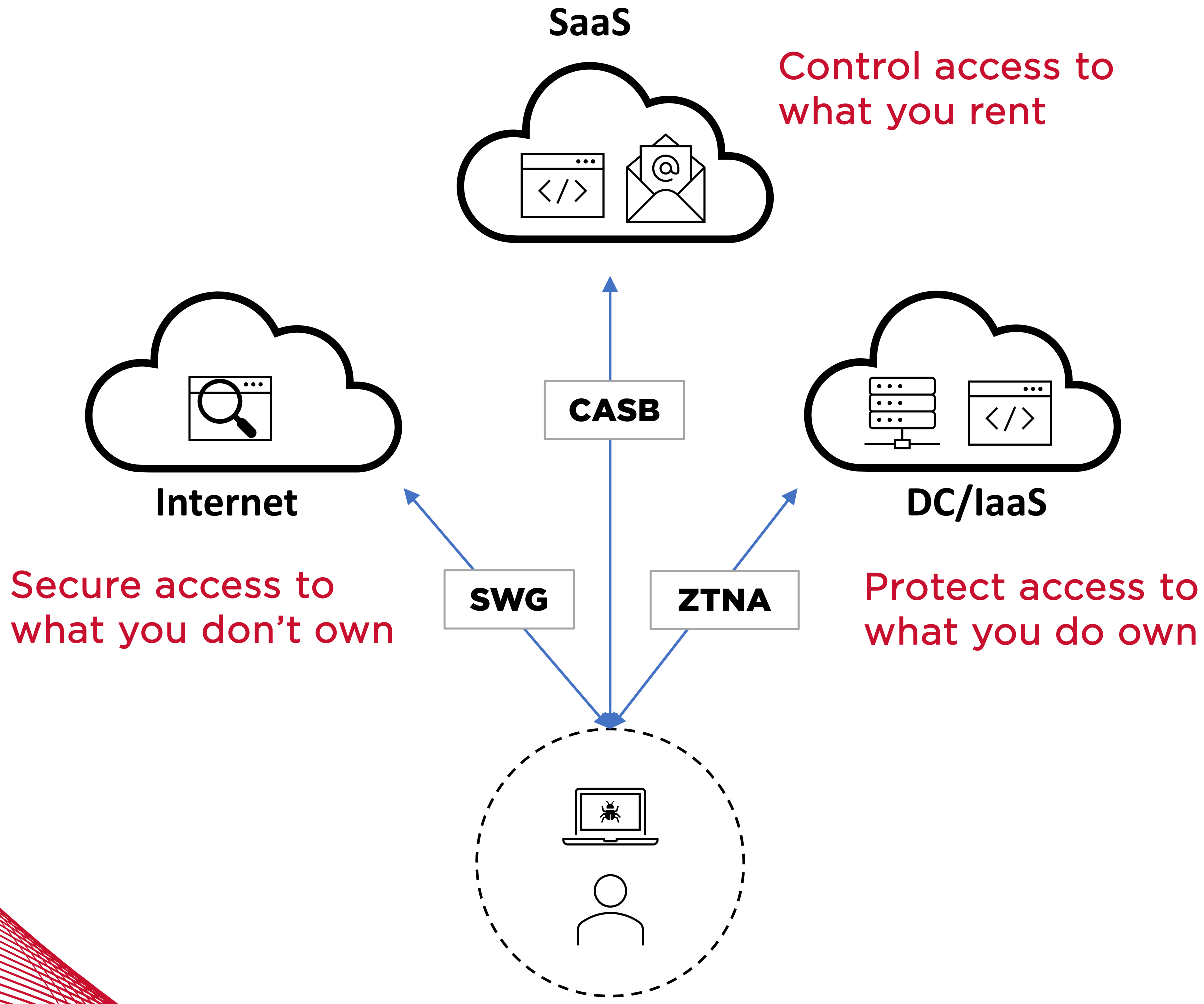
1. Secure Cloud Access

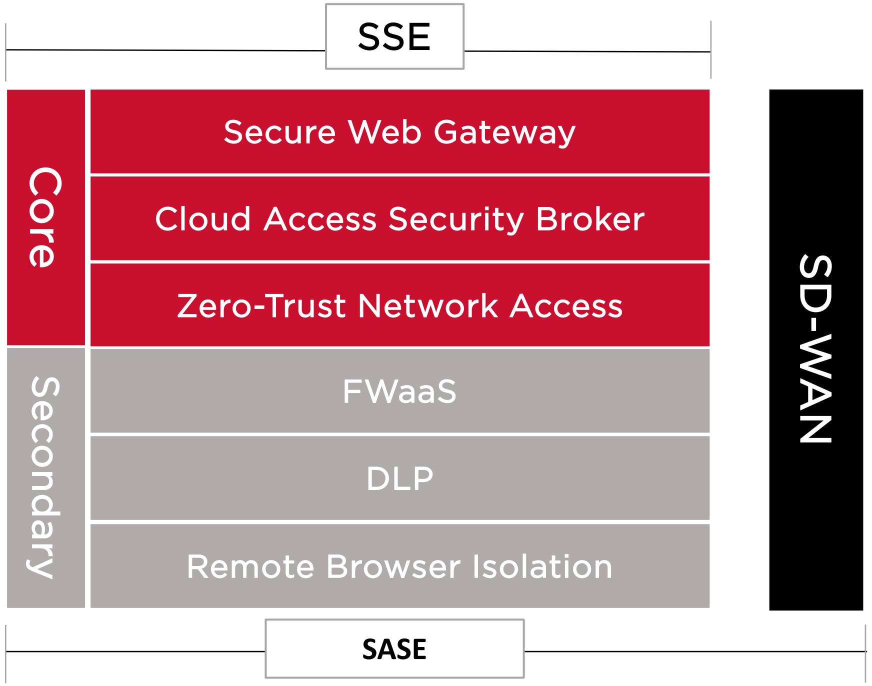
2. Secure Cloud Configuration

3. Secure Cloud Workloads

4. Secure Cloud App Development

1. Secure Cloud Access


SaaS
Control access to what you rent
CASB
Internet
DC/IaaS
Secure access to what you don't own
SWG
ZTNA
Protect access to what you do own



SSE

Core
- Secure Web Gateway
- Cloud Access Security Broker
- Zero-Trust Network Access

Secondary
- FWaaS
- DLP
- Remote Browser Isolation

SD-WAN

SASE

Continued drive towards consolidation will see single vendor deployments

SSE recommended starting point for both SASE & Zero-Trust

Security Service Edge: Enabling Secure "Work from Anywhere"

2a. Securing Cloud Configuration – IaaS/PaaS

Cloud Security Posture Management (CSPM)

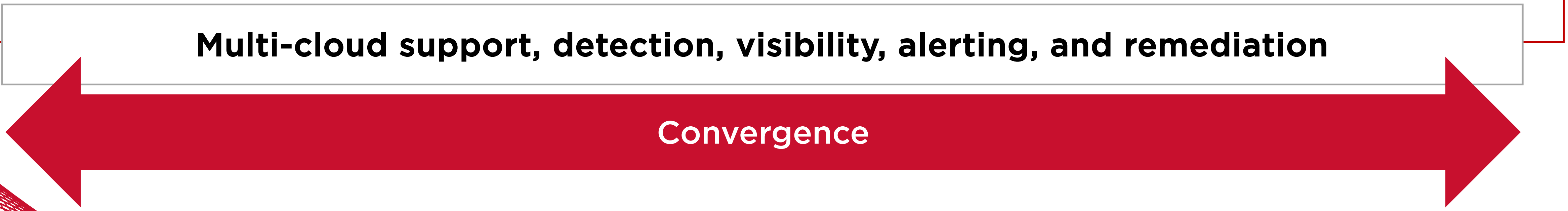
- Visibility of assets
- Security and compliance assessment of configuration
- IAC Scanning
- Policies and frameworks

Kubernetes Security Posture Management (KSPM)

- Automate security scans across K8s clusters
- Detect K8s misconfigurations
- Define security policies
- Assess and categorise threats

Cloud Identity Entitlements Management (CIEM)

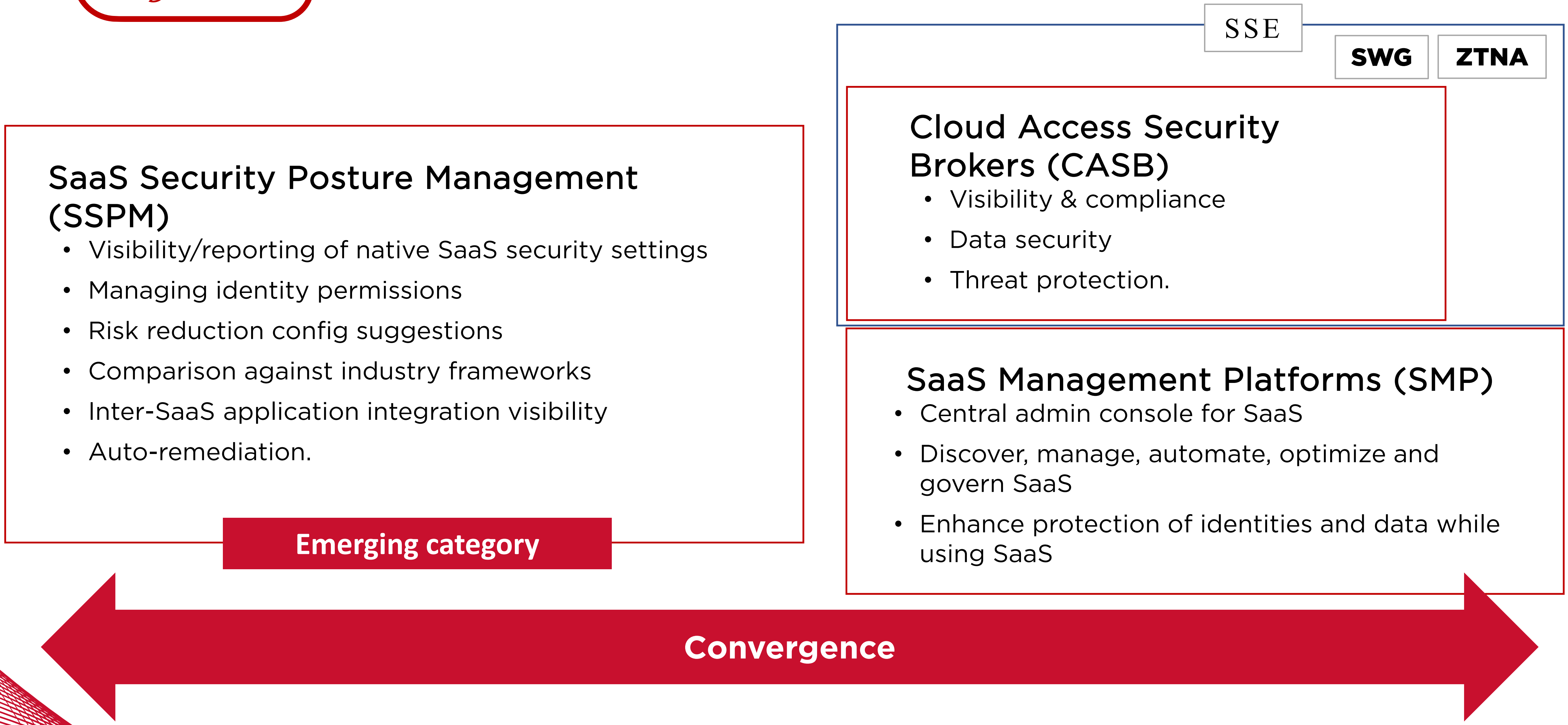
- Governance of entitlements in hybrid and multicloud IaaS
- Detect anomalies in entitlements
- Spots dormant and unnecessary privileges



Multi-cloud support, detection, visibility, alerting, and remediation

Convergence

2b. Securing Cloud Configuration - SaaS



SaaS Security Posture Management (SSPM)

- Visibility/reporting of native SaaS security settings
- Managing identity permissions
- Risk reduction config suggestions
- Comparison against industry frameworks
- Inter-SaaS application integration visibility
- Auto-remediation.

Emerging category

SSE

SWG

ZTNA

Cloud Access Security Brokers (CASB)

- Visibility & compliance
- Data security
- Threat protection.

SaaS Management Platforms (SMP)

- Central admin console for SaaS
- Discover, manage, automate, optimize and govern SaaS
- Enhance protection of identities and data while using SaaS

Convergence

3. Securing Cloud Workloads

Cloud Workload Protection Platforms (CWPP)

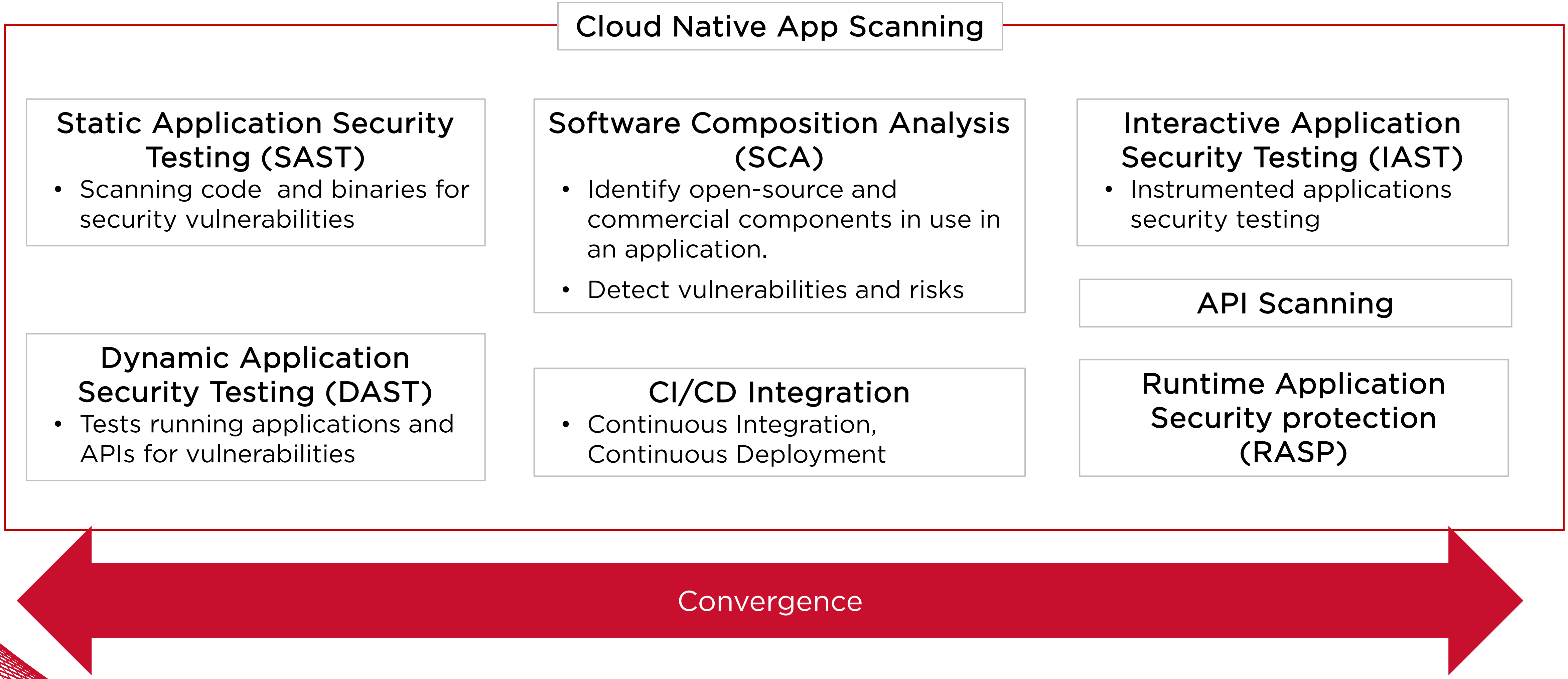
- Workload-centric security offerings
- Protect server workloads in hybrid and cloud deployments.
- Consistent visibility and control for physical machines, virtual machines, containers and serverless workloads
- System integrity protection
- Application control
- Behavioral monitoring
- Intrusion prevention
- Anti-malware protection

Cloud Configuration Security

- Cloud Security Posture Management (CSPM)
- Kubernetes Security Posture Management (KSPM)
- Cloud Identity Entitlements Management (CIEM)

Convergence

4. Securing Cloud App Development



Cloud Native App Scanning

Static Application Security Testing (SAST)

- Scanning code and binaries for security vulnerabilities

Dynamic Application Security Testing (DAST)

- Tests running applications and APIs for vulnerabilities

Software Composition Analysis (SCA)

- Identify open-source and commercial components in use in an application.
- Detect vulnerabilities and risks

CI/CD Integration

- Continuous Integration, Continuous Deployment

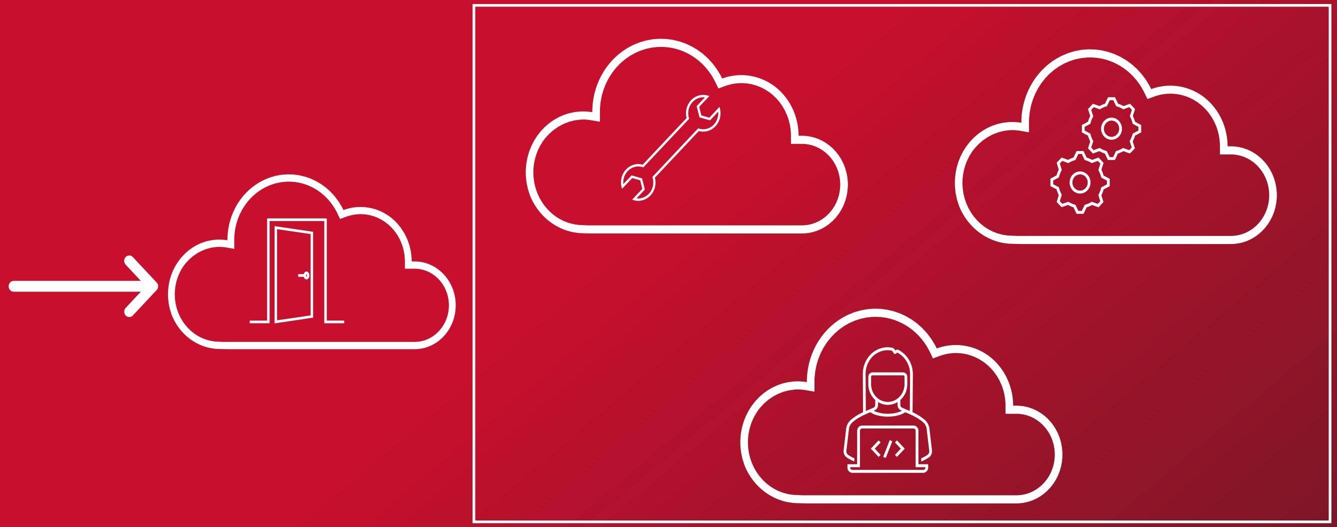
Interactive Application Security Testing (IAST)

- Instrumented applications security testing

API Scanning

Runtime Application Security protection (RASP)

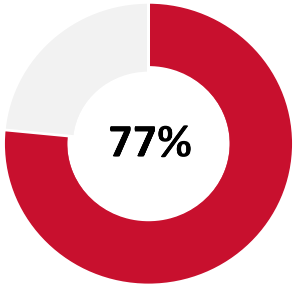
Convergence



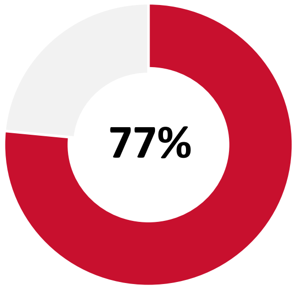
Bringing it all together

Convergence is what it’s about

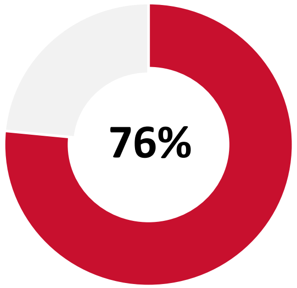
Too many tools...too little time



of organisations are pushing new code to production at least weekly, 48% daily



of organisations struggle to identify what tools they need to meet their objectives



of organisations say the number of security tools they are using create blind spots

- Source: Palo Alto Networks The State of Cloud-Native Security | 2023

Now you only have to remember one acronym!

CNAPP – Cloud Native Application Protection Platforms

Full Lifecycle

Artifact Scanning

- SAST/DAST
- API Scanning
- Software composition, 3rd party libraries
- Exposure scanning
- Known security loopholes
- Secrets, data
- Attack Path analysis

Cloud Configuration

- CSPM
- IaC Scanning
- CIEM
- KSPM
- Network config & security policy

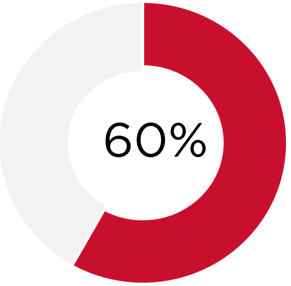
Runtime

- Web Application & API protection
- Application monitoring
- Workload visibility
- Network visibility
- Vulnerabilities Detection

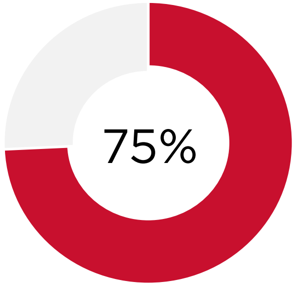
Detection & Response

Predictions

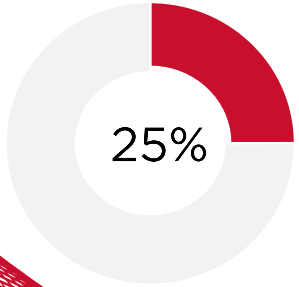
By 2025



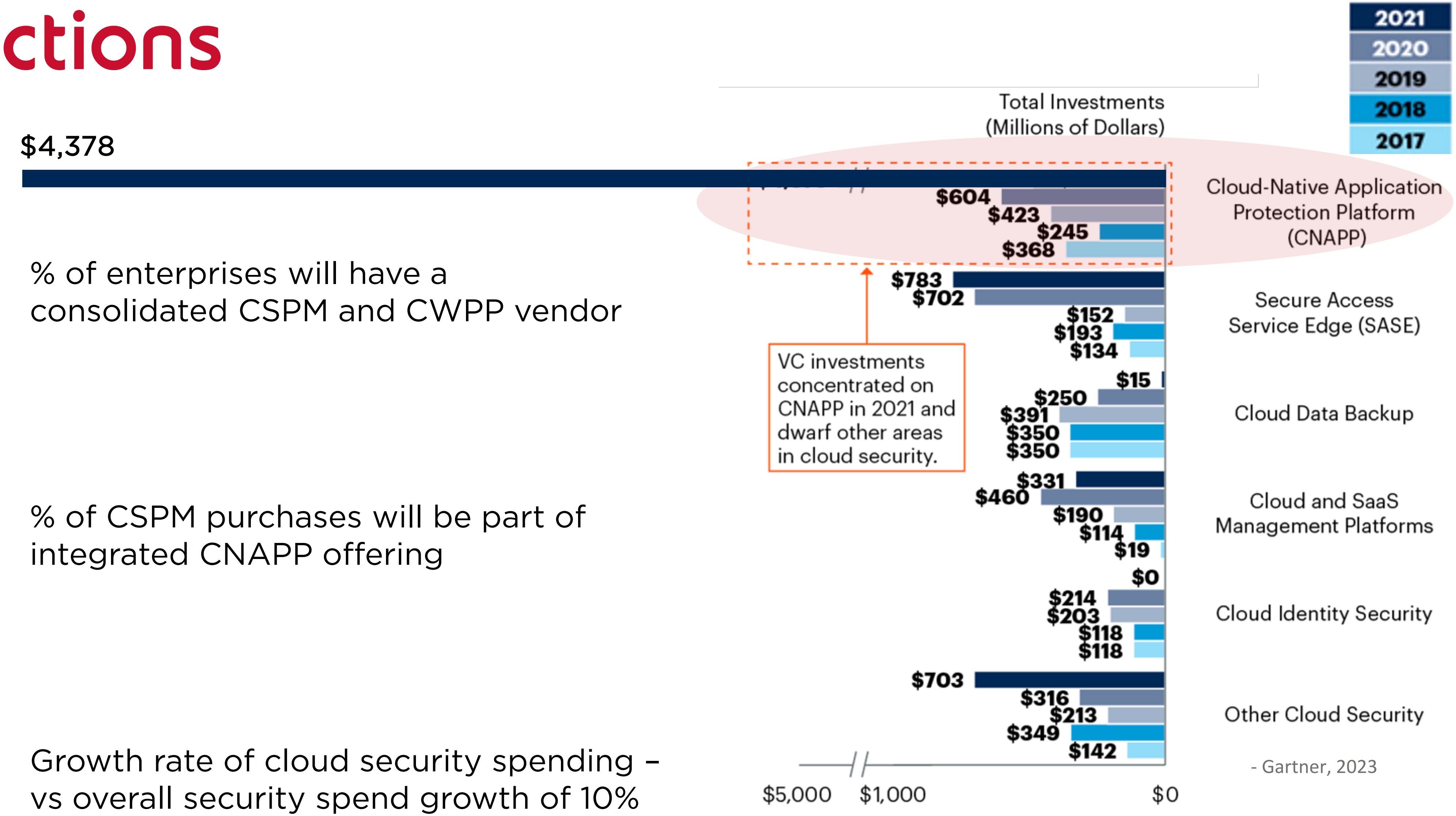
% of enterprises will have a consolidated CSPM and CWPP vendor



% of CSPM purchases will be part of integrated CNAPP offering



Growth rate of cloud security spending – vs overall security spend growth of 10%



VC investments concentrated on CNAPP in 2021 and dwarf other areas in cloud security.

- Gartner, 2023

CNAPP is where most investment is going

Choosing a Security Framework

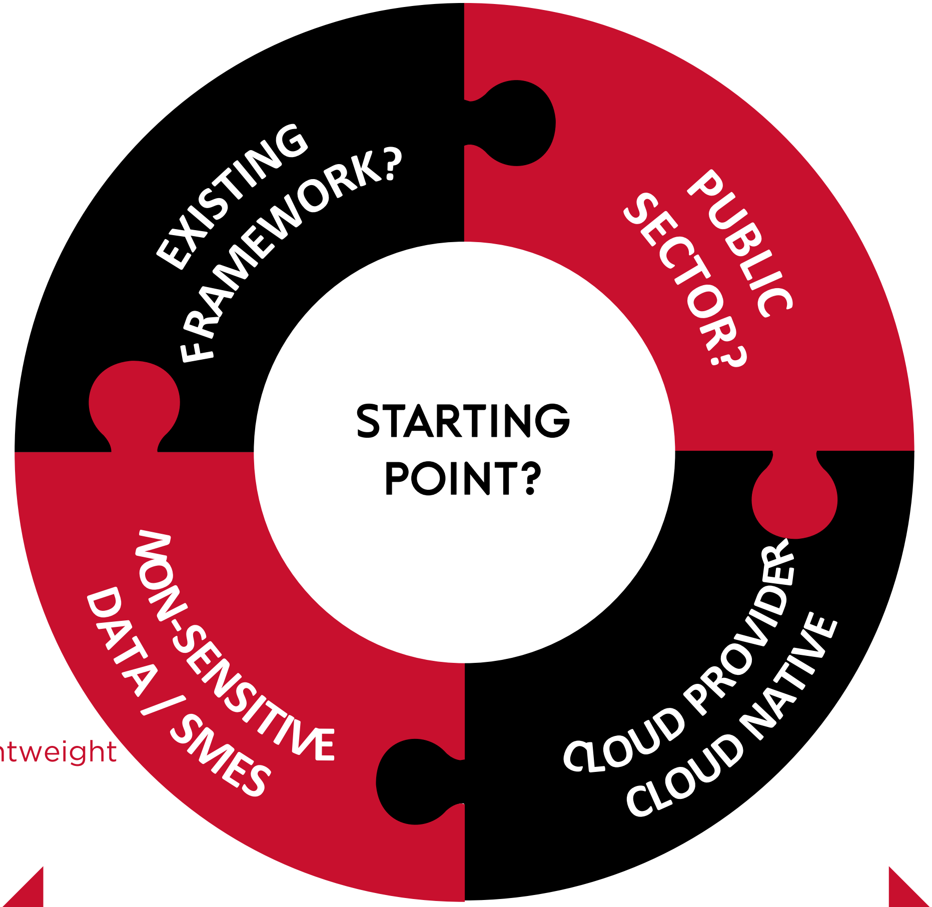
General Security Frameworks are equally applicable to cloud

USE CLOUD OVERLAYS ON EXISTING FRAMEWORKS

- ISO 27001/2 -> ISO 27017
- CIS TOP 18 CONTROLS -> Cloud Companion guide
- CIS benchmarks
- NIST CSF FRAMEWORK
- CYBER ESSENTIALS (/Plus)

ESSENTIALS / LIGHTWEIGHT FRAMEWORKS

- Cyber Essentials
- UK NCSC – Cloud Security Principles – Lightweight
- CSA CCM Lite



STARTING POINT?

EXISTING FRAMEWORK?

PUBLIC SECTOR?

CLOUD PROVIDER CLOUD NATIVE

NON-SENSITIVE DATA / SMES

NCSC / GOV-BACKED FRAMEWORKS

- Ireland - NCSC Public Sector Cyber Security Baseline standards
- UK - NCSC Cloud Security Principles, Cyber Essentials Plus
- See local NCSC guidance

FRAMEWORK FOR CLOUD PROVIDERS

- CLOUD SECURITY ALLIANCE - Cloud Controls Matrix v4.0

CSP-Specific Frameworks as req'd

- Azure/AWS Well-architected Framework
- GCP Google Cloud Framework
- CIS benchmarks for Azure, AWS, GCP, etc.

Cloud Security =
IT Security

Summary Recommendations

Assess, define scope and leverage 3rd party expertise

Cloud Security Assessment

Understand Full Cloud Security Scope

Utilise a controls framework

Regular pen testing and controls testing

- Public/private, IaaS, PaaS and SaaS
- Securing cloud access – SSE
- Get a grip on SaaS usage, visibility, configuration, security
- Control cloud configuration - Cloud Security Posture Management
- Monitor and protect cloud workloads with CWPP
- Shift left with security into the development cycle
- Move towards integrated full-lifecycle tooling with CNAPP

Consider all aspects of securing cloud

Integrity360
your security in mind

Questions?

Brian Martin
brian.martin@integrity360.com

SECURITY
FIRST
CYBER SECURITY CONFERENCE 2023

Unlocking Security Insights: External Pentesting & Mastering Your Attack Surface

Måns Blacker

Cyber Security Testing Team Leader
Integrity360 Sweden

#securityfirst2023

- SOC
- EDR
- PKI
- Brandväggar
- Nätverkssegmentering
- Ej localadmin
- Enhetskryptering
- IDS/IPS
- Dot1x
- …

Vanliga misstag

- Bortglömda servar och tjänster
- Öppna filytor
- Opatchade system
- Felkonfigurationer
- Standardlösenord
- Lösenord hårdkodat i skript, konfigurationer eller källkod

Orsaker

- Stress
- Produktivitet
- Bekvämlighet
- Oförutsedda händelser

Att undvika

- Verktyg
- Rutiner

- Penetrationstester

Integrity360
your **security** in mind

Frågor?

SECURITY
FIRST
CYBER SECURITY CONFERENCE 2023

Security that drives your business forward

Marie Berner Moberg, Regional Director Nordics, Rapid7

Magnus Jansson, Senior Security Solutions Engineer, Rapid7

#securityfirst2023

RAPID7 + Integrity360
your **security** in mind

17 oktober 2023

Security that drives your business forward.

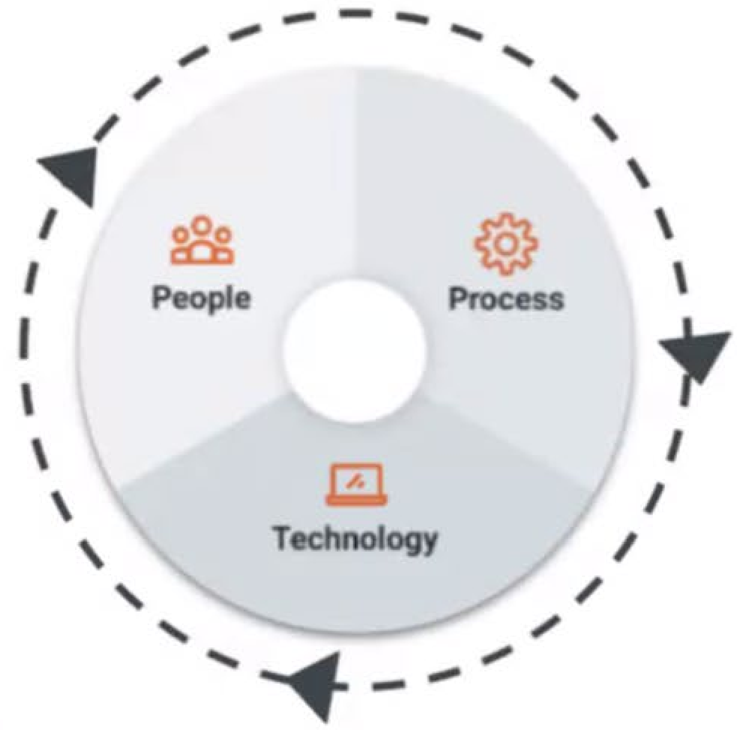
Marie Berner Moberg
Regional Director Nordics

Magnus Jansson
Senior Security Solutions Engineer

You Protect Our Future. We’ve Got Your Back!

Operationalising Cybersecurity

Aligning an Organization's **People**, with those **Processes** and **Technology**



Prevention

Detection

Response

People

Process

Technology

Rapid7 Global Threat Intelligence Community

Security expertise infused into everything we do

Insight Customers

11k+ Global Customers

Service Engagements

Field Insights from Leading Global MDR and Services Organization

Metasploit

Industry Leading Penetration Testing Tool

Attacker KB

Vulnerability Database & Community

Project Heisenberg

Global Honeypot Network

Project Sonar

Global Internet Scanning

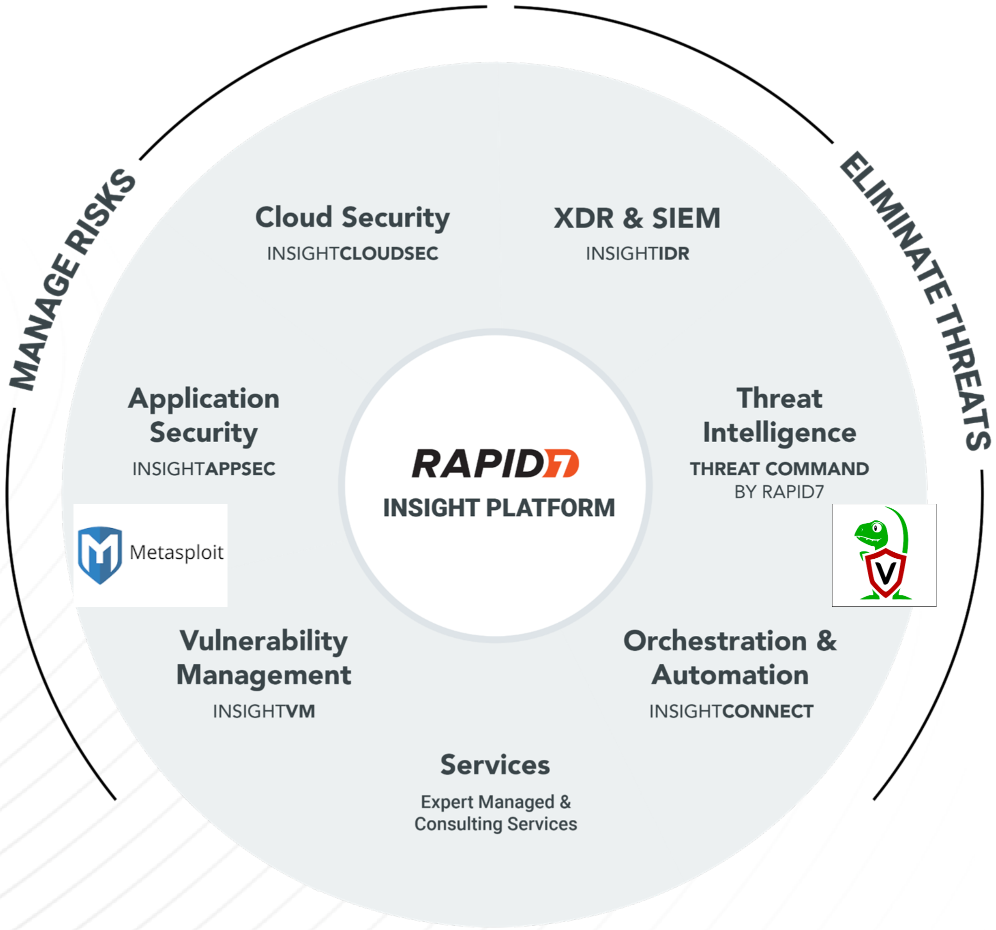
Velociraptor

Digital Forensics & Incident Response

Threat Command

Attack Surface Expertise

Unite risk and threat detection.



Rapid7 Benefits

Proactively mitigate risk across your cloud environment with up-to-the minute insights

Extinguish threats early and completely with expertly vetted detections

Respond quickly and confidently with guided playbooks and SOAR workflows

Global SOC expertise infused into products and available via leading MDR service

Rapid7 Advantage

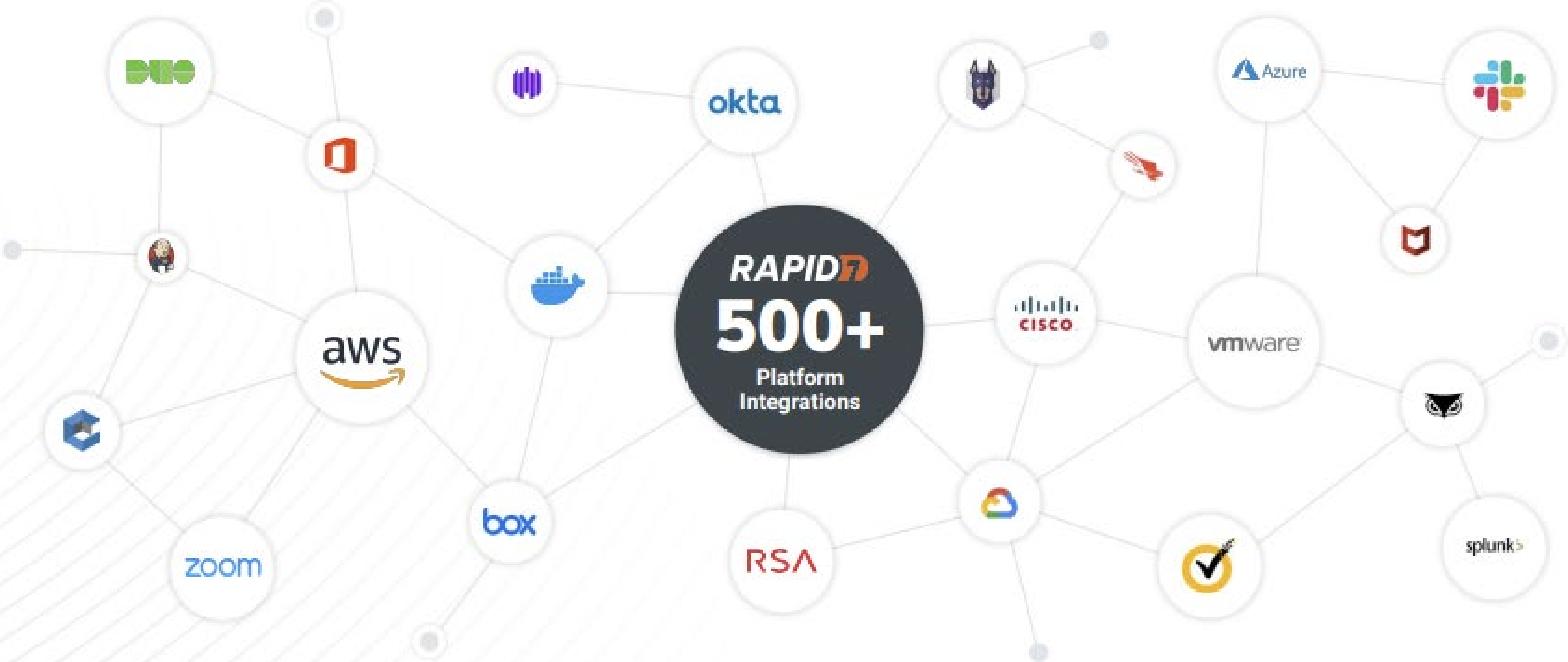
Unmatched Time-to-Value

Consolidation without Sacrifice

Unique Intel from Open Source Community

Access to Expertise Where and When You Need It

Extensive Partner Ecosystem



RAPID7

Best-in-Class Technology

Security Services

Research and Community

Global Ecosystem

300+ Platform Integrations

12,000+ Customers

49% of Fortune 100
NASDAQ: RPD

270+ Nordic Customers

Global Footprint

144 Countries
21 Offices

EMEA 850 + Employees
SOC Ireland & Prague

Leader of Innovation

56 Patents
Open Source Communities

350+ Development & Support in EMEA

You Protect Our Future. We’ve Got Your Back!

72 Tools and we’re still Drowning in Breaches

Control - Contain - Communicate

Detection is Complex

Gathering Data - Indexing - Context

Response is Crucial

Contain - Remediate - Mitigate

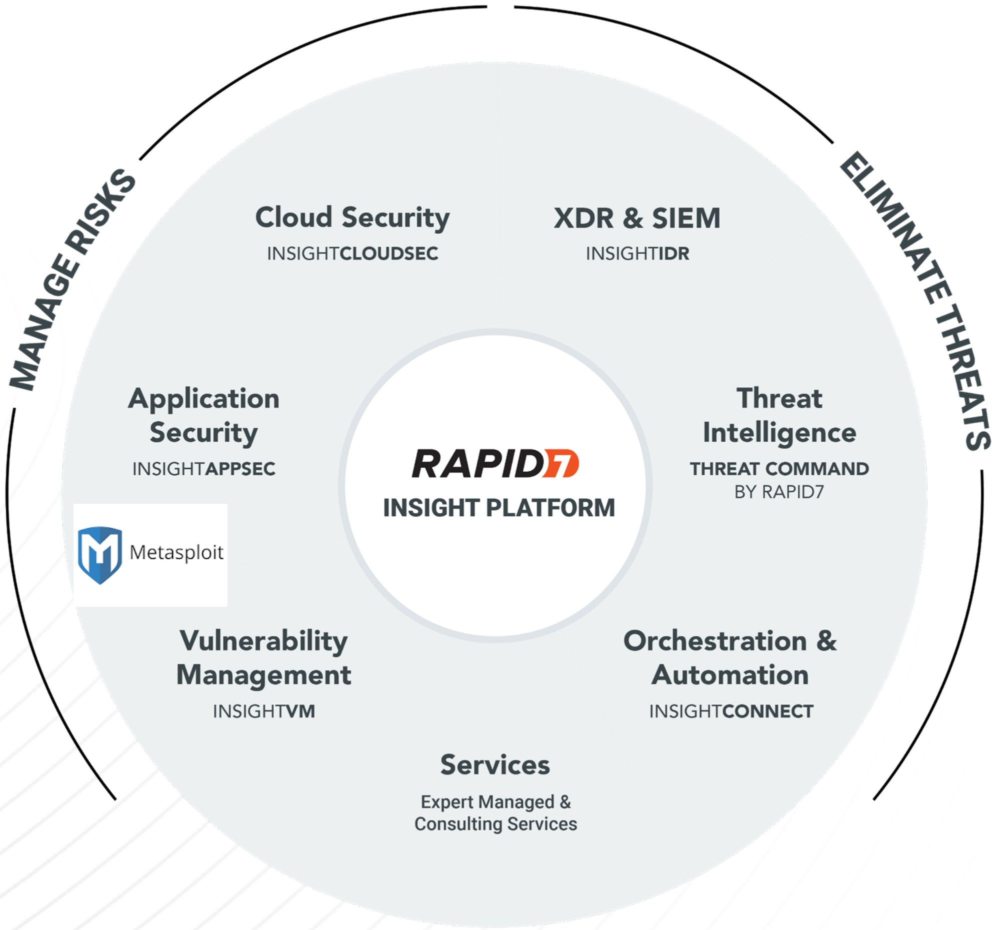
Actions are not equal

Learn - Weaponise - Build

Two disciplines, one aim

Advance - Securely - Together

Unite risk and threat detection.



RAPID7

Rapid7 Benefits

Proactively mitigate risk across your cloud environment with up-to-the minute insights

Extinguish threats early and completely with expertly vetted detections

Respond quickly and confidently with guided playbooks and SOAR workflows

Global SOC expertise infused into products and available via leading MDR service

Rapid7 Advantage

Unmatched Time-to-Value

Consolidation without Sacrifice

Unique Intel from Open Source Community

Access to Expertise Where and When You Need It

RAPID7

Say goodbye to chaos and drive your business forward.

Visit: **www.rapid7.com**

Contact: **info@rapid7.com**

SECURITY
FIRST
CYBER SECURITY CONFERENCE 2023

Clearing the fog of the unknown in your environment: An incident response approach

Patrick Wragg
Head of Incident Response, Integrity360

#securityfirst2023

Agenda

- What do I mean by the “unknown”?
- What I’ve witnessed
- Case studies
- My recommendations

What I am not here to talk about today:

- Phishing
- DDoS

What I‘ve witnessed..

- Most recent types of initial access: *External exploits*
- On the rise: *insider abuse*
- Unusual attack methods: *hardware backdoors*
- Most common threat actor motivation: *financial*
- On the rise: *hacktivism*

- Time before a company realises it's compromised:
  - Shortest: 45 minutes
  - Average: 2 weeks
  - Longest: 8 years
- Average threat actor extortion: *10% of annual revenue*
- Average cost to business for a breach: *over £1m*
- Average amount of data exfiltrated from a victim: *500GB but rising*
- Average time for a business to resume continuity after ransomware: *1 month*

Supply chain attacks

> ”
>
> Why spend effort infecting individual companies when I can just infect one that gives me access to all of them!
>
> *Attacker’s thought*

solarwinds

3CX®

Case Study 1

Company Profile

Industry: Bank

Employees: 250

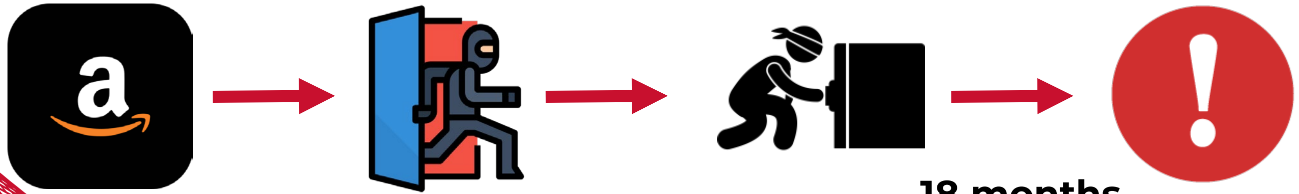
Annual Revenue: £800m

Customers: 1.4m

Impact

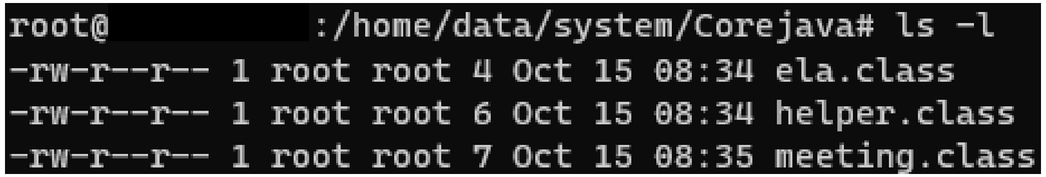
- 18 months-worth financial PII data stolen
- Suspended from VISA/Mastercard
- FCA fine of £20m

Compromise Kill Chain

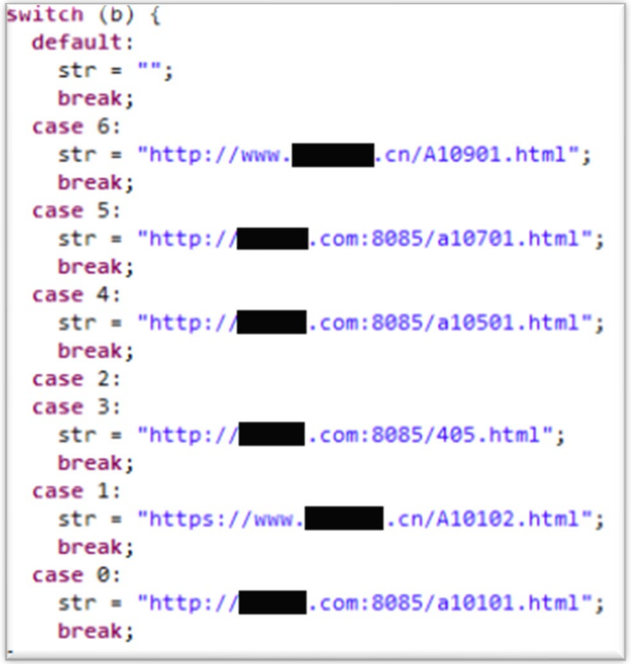


18 months

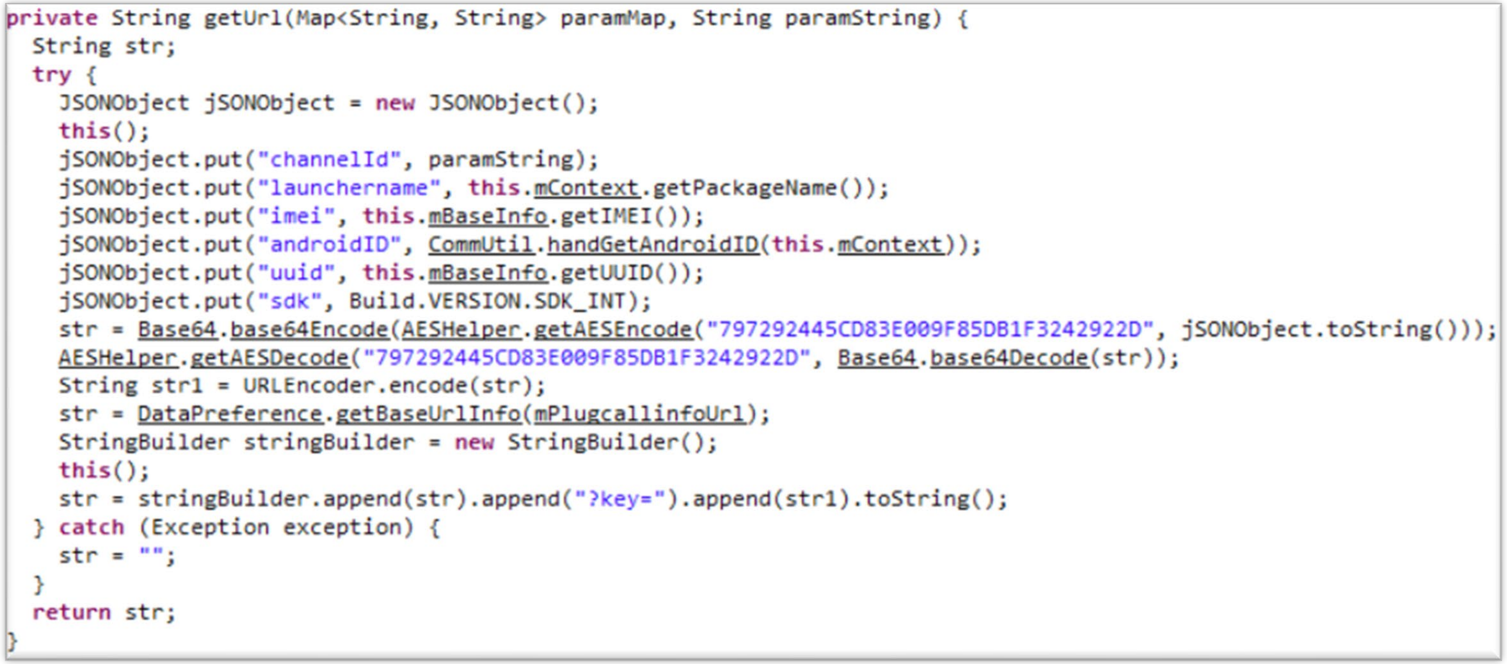
Case Study 1



```
root@[redacted]:/home/data/system/Corejava# ls -l
-rw-r--r-- 1 root root 4 Oct 15 08:34 ela.class
-rw-r--r-- 1 root root 6 Oct 15 08:34 helper.class
-rw-r--r-- 1 root root 7 Oct 15 08:35 meeting.class
```



```
switch (b) {
  default:
    str = "";
    break;
  case 6:
    str = "http://www.[redacted].cn/A10901.html";
    break;
  case 5:
    str = "http://[redacted].com:8085/a10701.html";
    break;
  case 4:
    str = "http://[redacted].com:8085/a10501.html";
    break;
  case 2:
  case 3:
    str = "http://[redacted].com:8085/405.html";
    break;
  case 1:
    str = "https://www.[redacted].cn/A10102.html";
    break;
  case 0:
    str = "http://[redacted].com:8085/a10101.html";
    break;
```



```
private String getUrl(Map<String, String> paramMap, String paramString) {
  String str;
  try {
    JSONObject jSONObject = new JSONObject();
    this();
    jSONObject.put("channelId", paramString);
    jSONObject.put("launchername", this.mContext.getPackageName());
    jSONObject.put("imei", this.mBaseInfo.getIMEI());
    jSONObject.put("androidID", CommUtil.handGetAndroidID(this.mContext));
    jSONObject.put("uuid", this.mBaseInfo.getUUID());
    jSONObject.put("sdk", Build.VERSION.SDK_INT);
    str = Base64.base64Encode(AESHelper.getAESEncode("797292445CD83E009F85DB1F3242922D", jSONObject.toString()));
    AESHelper.getAESDecode("797292445CD83E009F85DB1F3242922D", Base64.base64Decode(str));
    String str1 = URLEncoder.encode(str);
    str = DataPreference.getBaseUrlInfo(mPlugcallinfoUrl);
    StringBuilder stringBuilder = new StringBuilder();
    this();
    str = stringBuilder.append(str).append("?key=").append(str1).toString();
  } catch (Exception exception) {
    str = "";
  }
  return str;
}
```

VPN Attacks

- You have an externally facing device connected to your domain…
  - Add a set of default credentials
  - Add no multi-factor authentication..
- You might as well say “please breach me!”

Case Study 2

Company Profile

Industry: Law-firm

Employees: 400

Customers: 4k

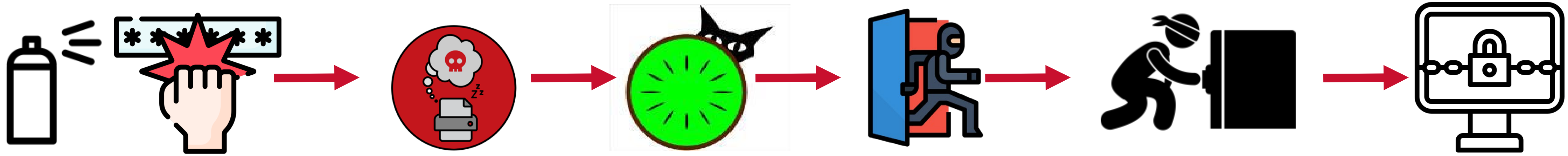
Annual Revenue: £200m

Ransomware: BlackCat

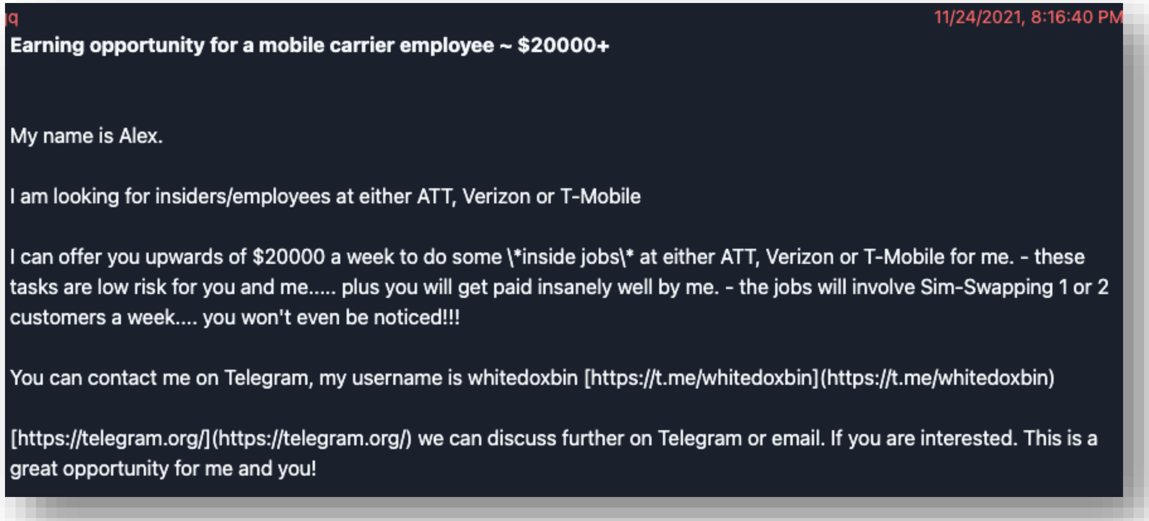
Impact

- 26 days business outage
- Law cases made public
- Fines of £11m
- Real losses were £m's per day

Compromise Kill Chain



Insider Abuse



q 11/24/2021, 8:16:40 PM

Earning opportunity for a mobile carrier employee ~ $20000+

My name is Alex.

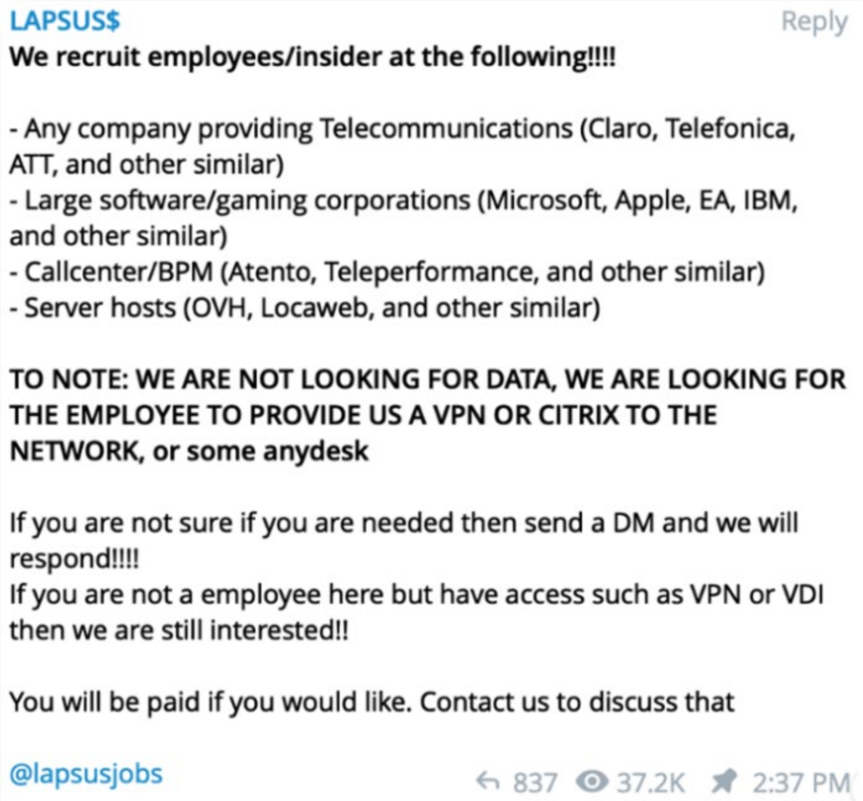
I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of $20000 a week to do some *inside jobs* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin https://t.me/whitedoxbin

https://telegram.org/ we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!

Source: https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/



LAPSUS$ Reply

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs ↩ 837 👁 37.2K 📌 2:37 PM

Case Study 3

LinkedIn

Company Profile

Industry: Energy

Annual Revenue: £542m

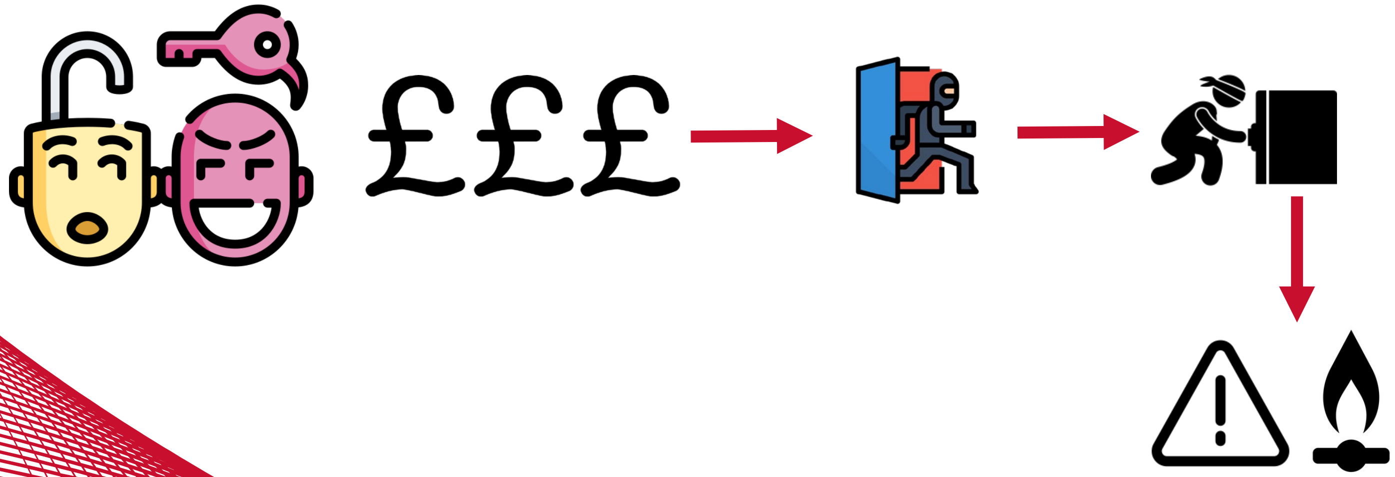
Employees: 6,000

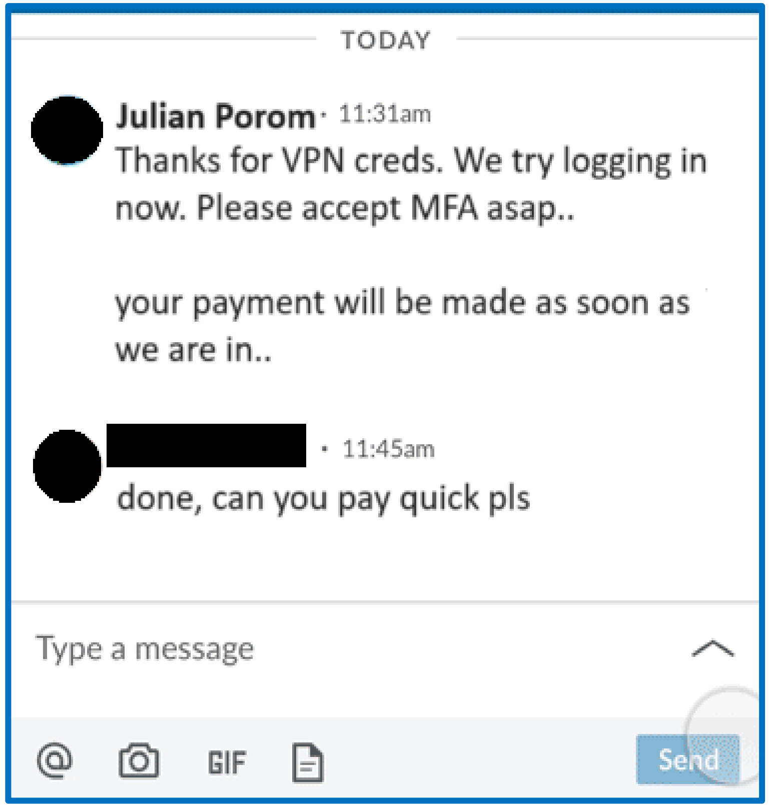
Ransomware: Lockbit

Impact

- Army drafted in to protect Pipelines
- £20m fines
- Threat to gas safety levels

Compromise Kill Chain




TODAY

Julian Porom · 11:31am
Thanks for VPN creds. We try logging in now. Please accept MFA asap..

your payment will be made as soon as we are in..

[redacted] · 11:45am
done, can you pay quick pls

Major Vulnerabilities

Confluence

vmware®

Exchange

Citrix NetScaler

ManageEngine

LOG4J

Case Study 4

vmware Horizon

Company Profile

Industry: Education

Employees: 120

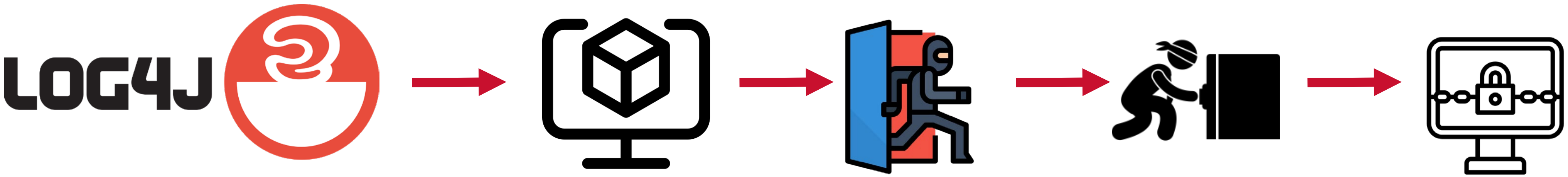
Students: 2,000

Ransomware: Lockbit

Impact

Students PII stolen
Threats made to parents

Compromise Kill Chain



My Recommendations

MITRE
ATT&CK™

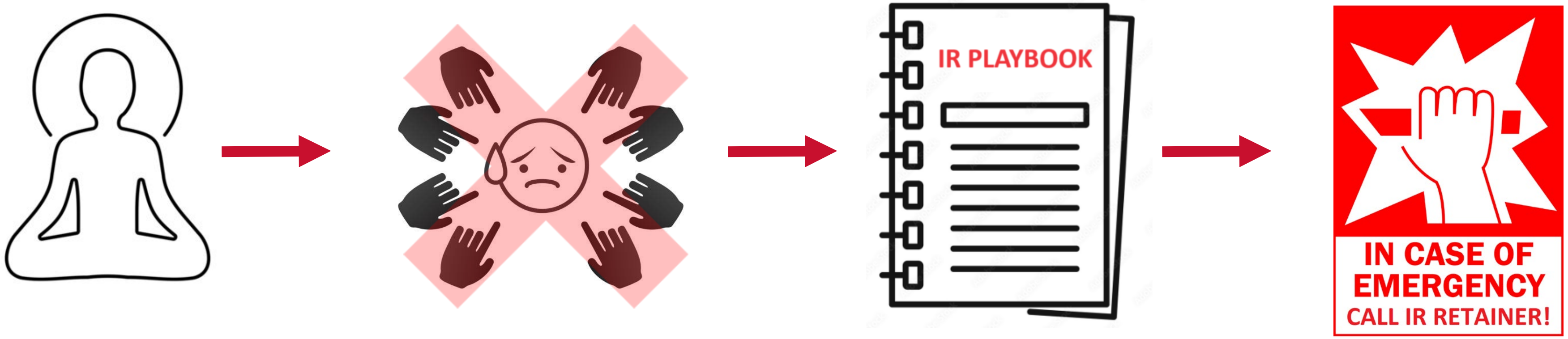
SHODAN

PICK ONE!
Anydesk
Teamviewer
LogMeIn
RemotePC
Zoho
VNC Connect

My Recommendations

- Think like an attacker.. “How can I get from A to B?”
- Immutable backups stored in an air-gapped location
- Know your third parties
- Monitor Linux hosts

If the worst happens:



Integrity360

your **security** in mind

Any questions?

SECURITY
FIRST
CYBER SECURITY CONFERENCE 2023

Want to gain external visibility

What does the more questionable part of the Internet see, say and do, aimed at your organization?

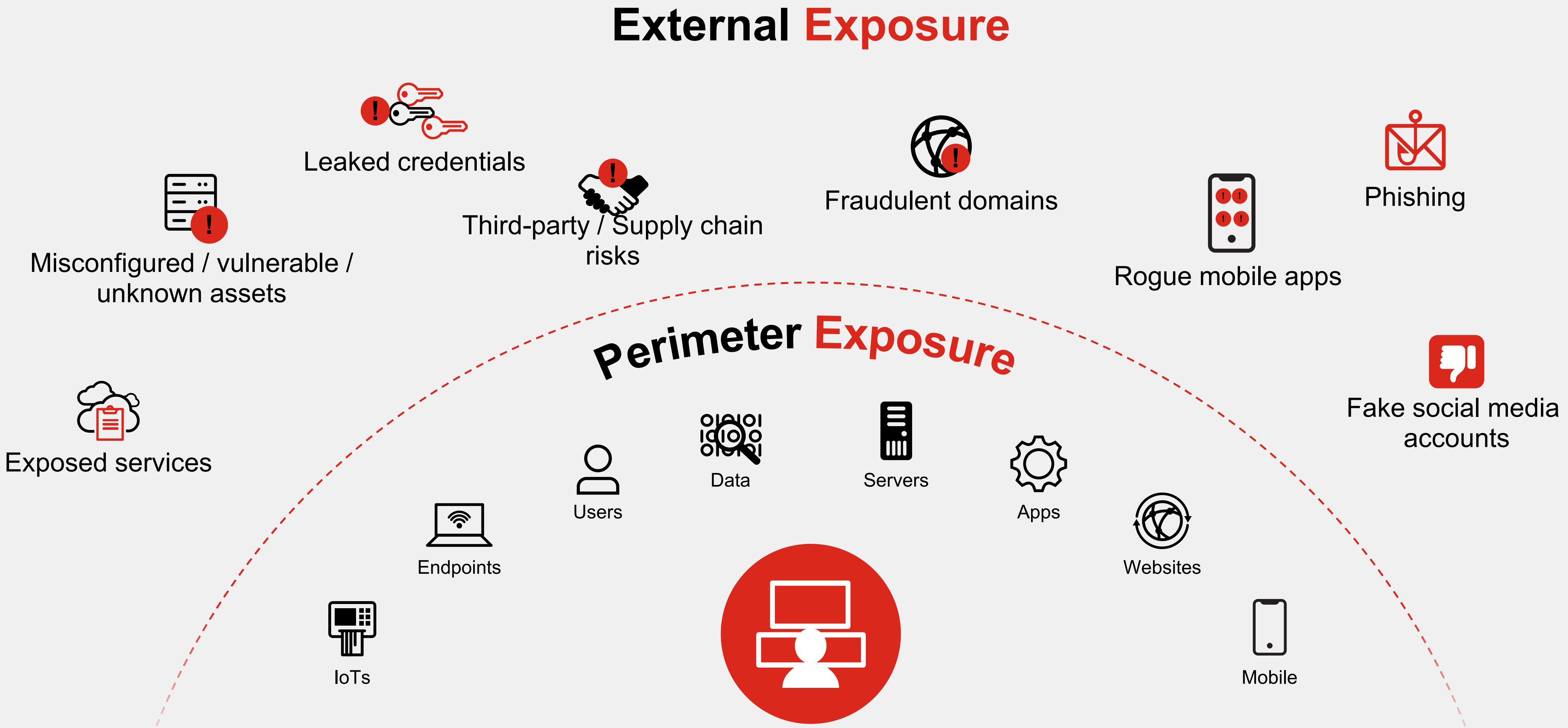
Martin Johansson
Systems Engineer, Fortinet

#securityfirst2023

Want to gain external visibility - What does the more questionable parts of the internet see, say and do aimed at your organization?

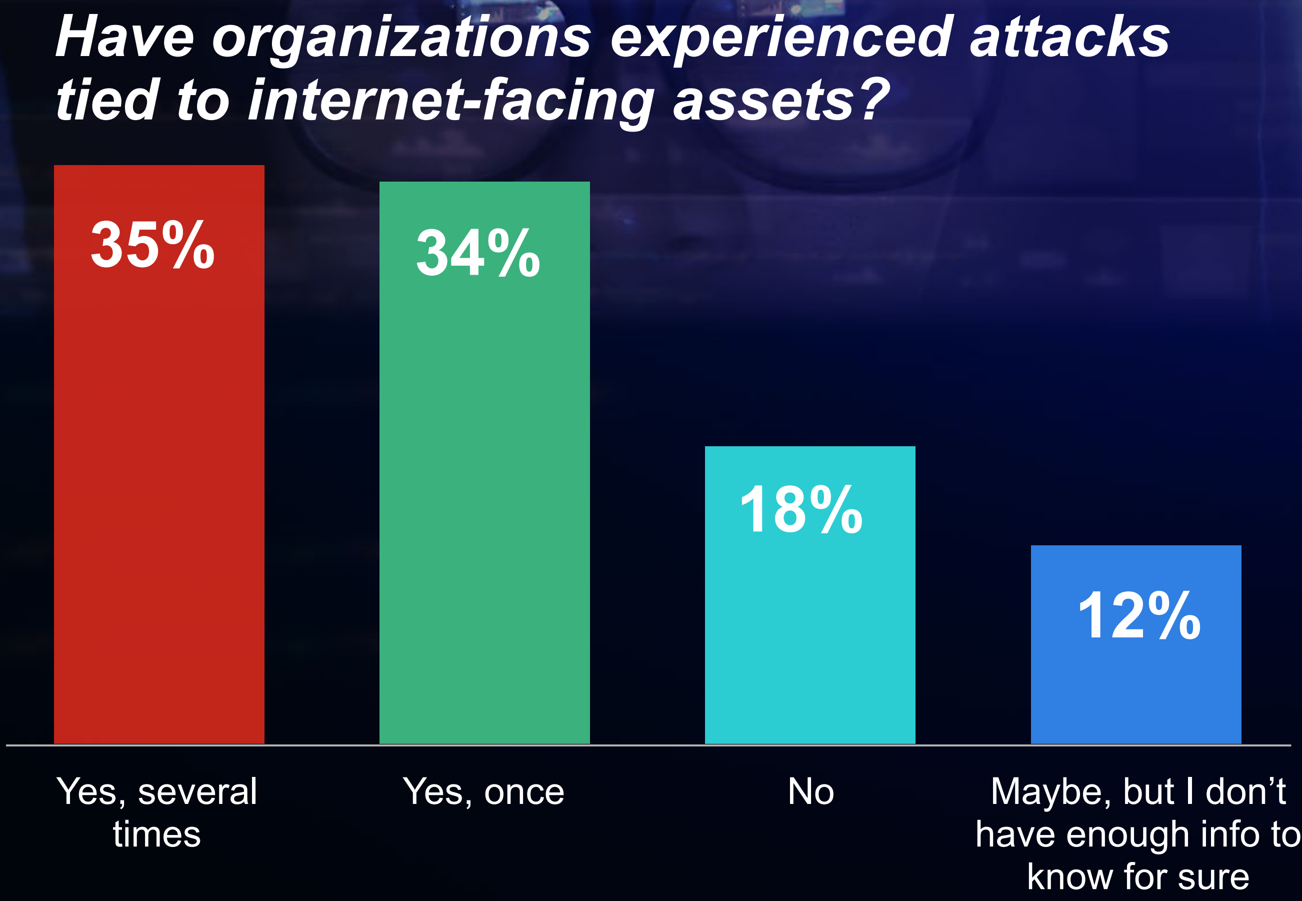
Martin Johansson, Systems Engineer

The Ever-Expanding External Threat Landscape



What is our exposure?

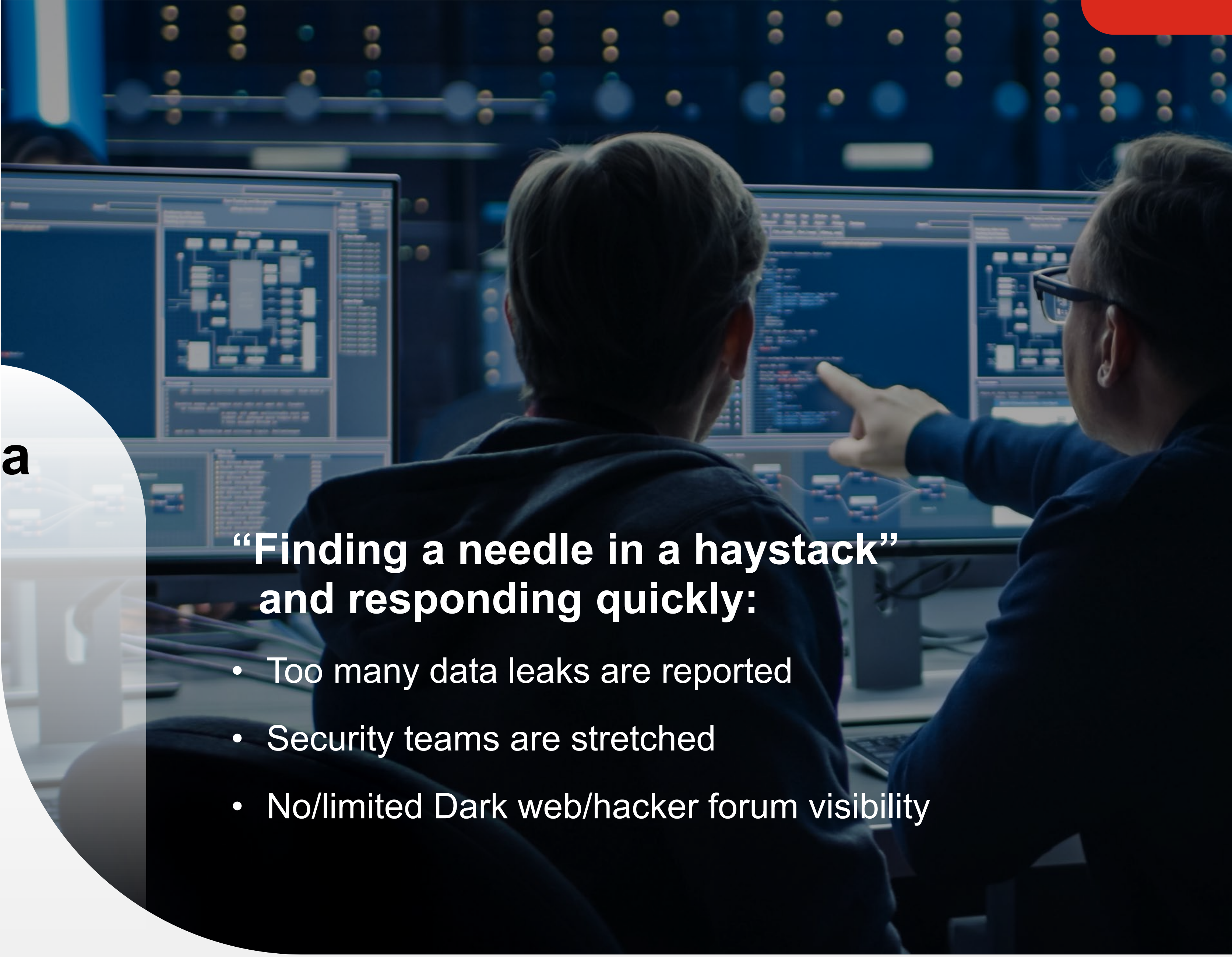
Unknown / unmanaged digital assets



Enterprise Strategy Group™ by TechTarget

Have we had any data leakage?

Credentials, customer records, sensitive data, Intellectual property or assets.

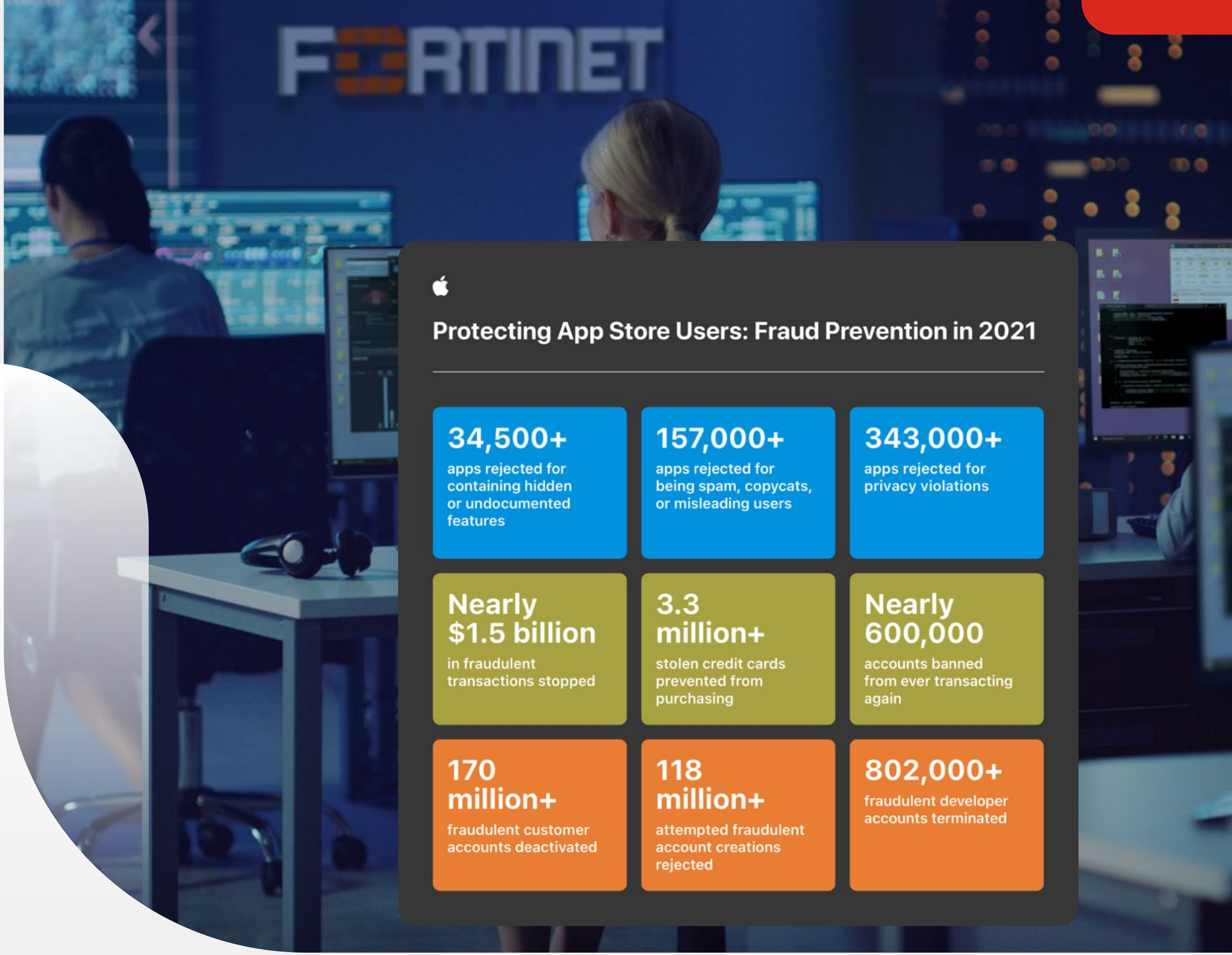


“Finding a needle in a haystack” and responding quickly:

- Too many data leaks are reported
- Security teams are stretched
- No/limited Dark web/hacker forum visibility

Are there any fake applications or websites?

Rogue mobile apps
Phishing websites



Protecting App Store Users: Fraud Prevention in 2021

34,500+ apps rejected for containing hidden or undocumented features

157,000+ apps rejected for being spam, copycats, or misleading users

343,000+ apps rejected for privacy violations

Nearly $1.5 billion in fraudulent transactions stopped

3.3 million+ stolen credit cards prevented from purchasing

Nearly 600,000 accounts banned from ever transacting again

170 million+ fraudulent customer accounts deactivated

118 million+ attempted fraudulent account creations rejected

802,000+ fraudulent developer accounts terminated

What about our Supply chain?

Supply chains and third-party vendors

Evaluates vendors, partners, and companies you are looking to partner with or acquire:

- Third-party, publicly-exposed digital assets
- Misconfigured/vulnerable assets
- Exposed services (e.g., APIs, exposed systems, open ports, storage)
- Leaked data/credentials for sales on hacker forums
- Ransomware risks

What about protecting our Brand?

Social media and news reporting on breaches

At risk:

- Market valuation
- Revenue and customer trust/loyalty
- Customer safety
- Business credibility

External Attack Surface: Challenges & Risks

More public-facing assets to monitor across multiple digital channels

Complex external attack surface, diverse assets, new attack vectors, limited or no visibility

Lack of security tools and skills to continuously monitor and respond

- Labor-intensive processes
- Require skilled resources to discover risks/leaked data and act quickly

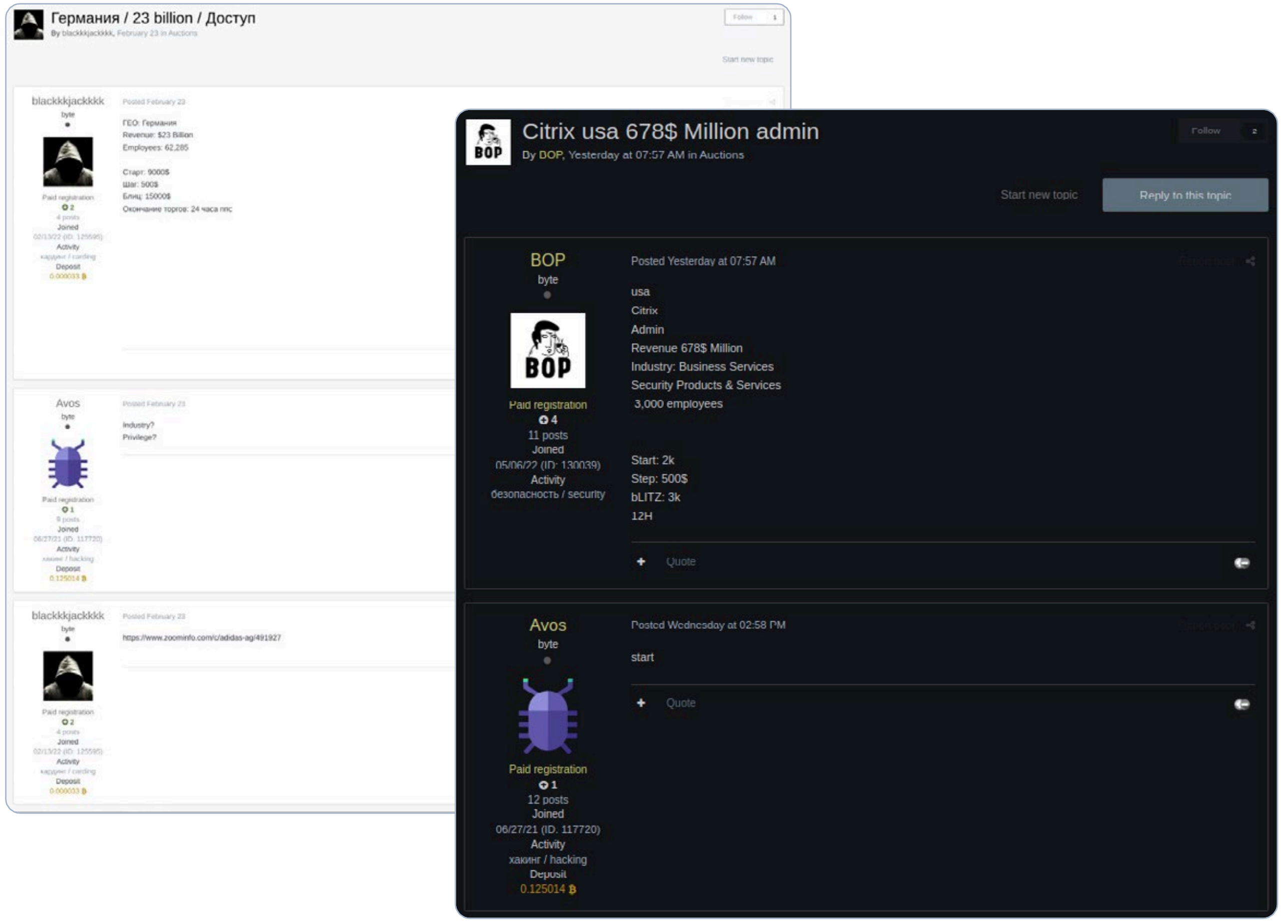
Increase in public-facing asset exploitation, brand impersonation, ransomware attacks and supply chain attacks

Website infringement is one of the easiest ways to impersonate a brand

Ransomware as-a-Service (RaaS)

RaaS is a business model where cybercriminals purchase ransomware software on the dark web and carry out ransomware attacks without any coding

RaaS operator purchases access from Initial Access Broker (IAB)



Германия / 23 billion / Доступ

By blackkkjackkkk, February 23 in Auctions

blackkkjackkkk
byte
Paid registration
2
4 posts
Joined
02/13/22 (ID: 125595)
Activity
кардинг / carding
Deposit
0.000033 ₿

Posted February 23

ГЕО: Германия
Revenue: $23 Billion
Employees: 62,285

Старт: 9000$
Шаг: 500$
Блиц: 15000$
Окончание торгов: 24 часа ппс

Avos
byte
Paid registration
1
9 posts
Joined
06/27/21 (ID: 117720)
Activity
хакинг / hacking
Deposit
0.125014 ₿

Posted February 23

Industry?
Privilege?

blackkkjackkkk
byte
Paid registration
2
4 posts
Joined
02/13/22 (ID: 125595)
Activity
кардинг / carding
Deposit
0.000033 ₿

Posted February 23

https://www.zoominfo.com/c/adidas-ag/491927

Citrix usa 678$ Million admin

By BOP, Yesterday at 07:57 AM in Auctions

BOP
byte
Paid registration
4
11 posts
Joined
05/06/22 (ID: 130039)
Activity
безопасность / security

Posted Yesterday at 07:57 AM

usa
Citrix
Admin
Revenue 678$ Million
Industry: Business Services
Security Products & Services
3,000 employees

Start: 2k
Step: 500$
bLITZ: 3k
12H

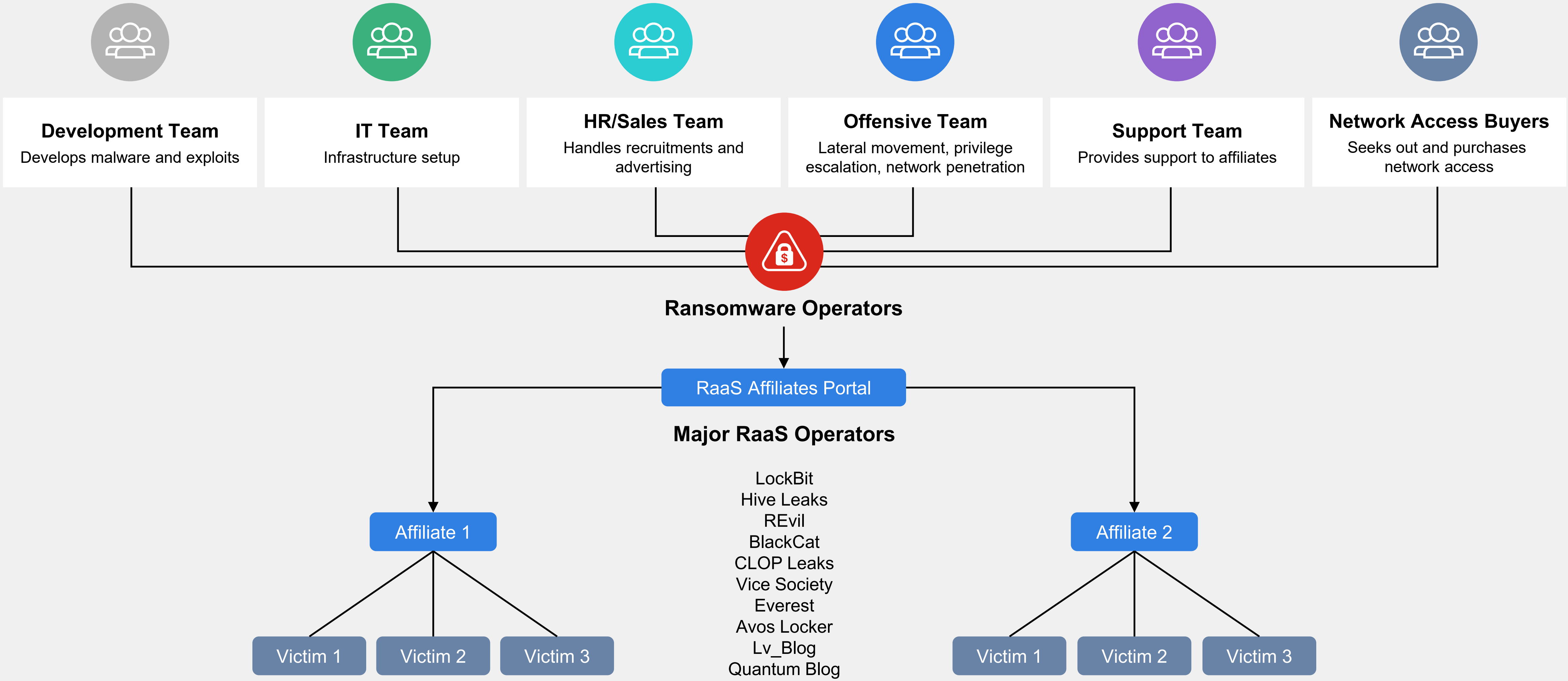
Avos
byte
Paid registration
1
12 posts
Joined
06/27/21 (ID. 117720)
Activity
хакинг / hacking
Deposit
0.125014 ₿

Posted Wednesday at 02:58 PM

start

Ransomware-as-a-Service (RaaS)

Ransomware Groups – Structural Overview



Major RaaS Operators

LockBit
Hive Leaks
REvil
BlackCat
CLOP Leaks
Vice Society
Everest
Avos Locker
Lv_Blog
Quantum Blog

How to Break the Attack Sequence — DRP Support

Pre-Attack: Recon, Weapon

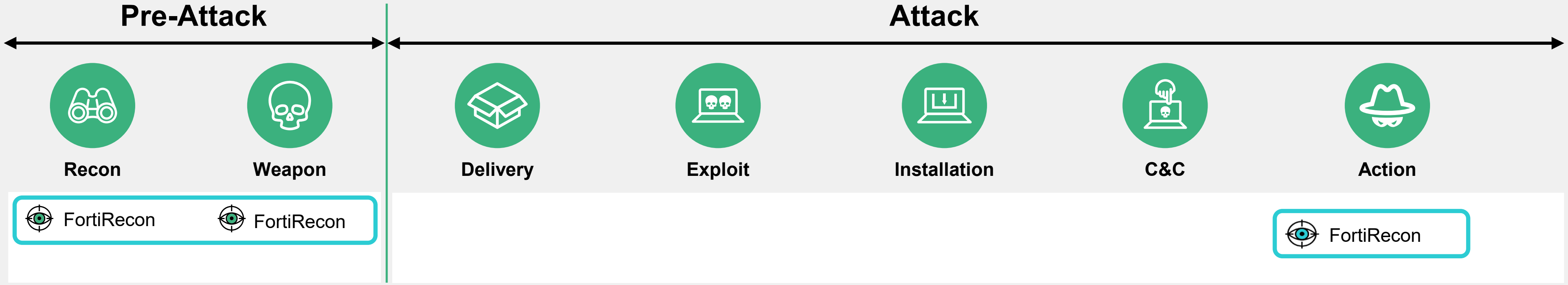
Attack: Delivery, Exploit, Installation, C&C, Action

	Recon	Weapon	Delivery	Exploit	Installation	C&C	Action
Products & Solutions	FortiRecon FortiDeceptor	FortiRecon FortiDeceptor	FortiGate (HW / VM / CN / SASE) FortiProxy FortiClient FortiEDR FortiADC FortiWeb FortiNDR AV+ANN FortiMail FortiCASB FortiCWP	FortiGate (HW / VM / CN / SASE) FortiProxy FortiClient FortiEDR Defuse compromised endpoint FortiADC FortiWeb Web application FortiDeceptor Threat detection, analysis, and response FortiSIEM UEBA	FortiGate (HW / VM / CN / SASE) FortiClient FortiEDR Defuse exploit FortiDeceptor Defuse Lateral Movement FortiCWP FortiSIEM UEBA	FortiGate (HW / VM / CN / SASE) FortiClient FortiEDR Defuse compromised endpoint FortiNDR FortiSIEM UEBA	FortiRecon FortiAnalyzer Event handlers & reports FortiSIEM Rules engine & threat hunting FortiSOAR Playbooks IOC Threat hunting Outbreak Detection ZTNA Auto tagging FortiClient Endpoint search FortiEDR|XDR FortiDeceptor Threat intelligence, & attack isolation
FGD AI-Powered Security		Credential Stuffing Prevention Service	Anti-malware, AV pre-Filter, SBX, Endpoint Vulnerability Protection, App Control, IL CASB, Credentials AV IL SBX IL CASB	IPS, Application, FW, IOT, OT IPS IoT OT	URL, AV URL AV	Botnet, C2, DNS BOT C2 DNS	

SOC Augmentation by FortiGuard

- Know Your Risks & Vulnerabilities — **Security Assessments**
- Train Your SOC — **IRR, Playbooks, Training**
- Managed Detection & Response — **MDR**
- Augment Your SOC — **SOC as a Service**
- Respond Faster and More Effectively — **Incident Response, FortiRecon**

How to Break the Attack Sequence — DRP Support



Digital Risk Protection

A digital risk protection (DRP) service

External Attack Surface Management

(EASM)

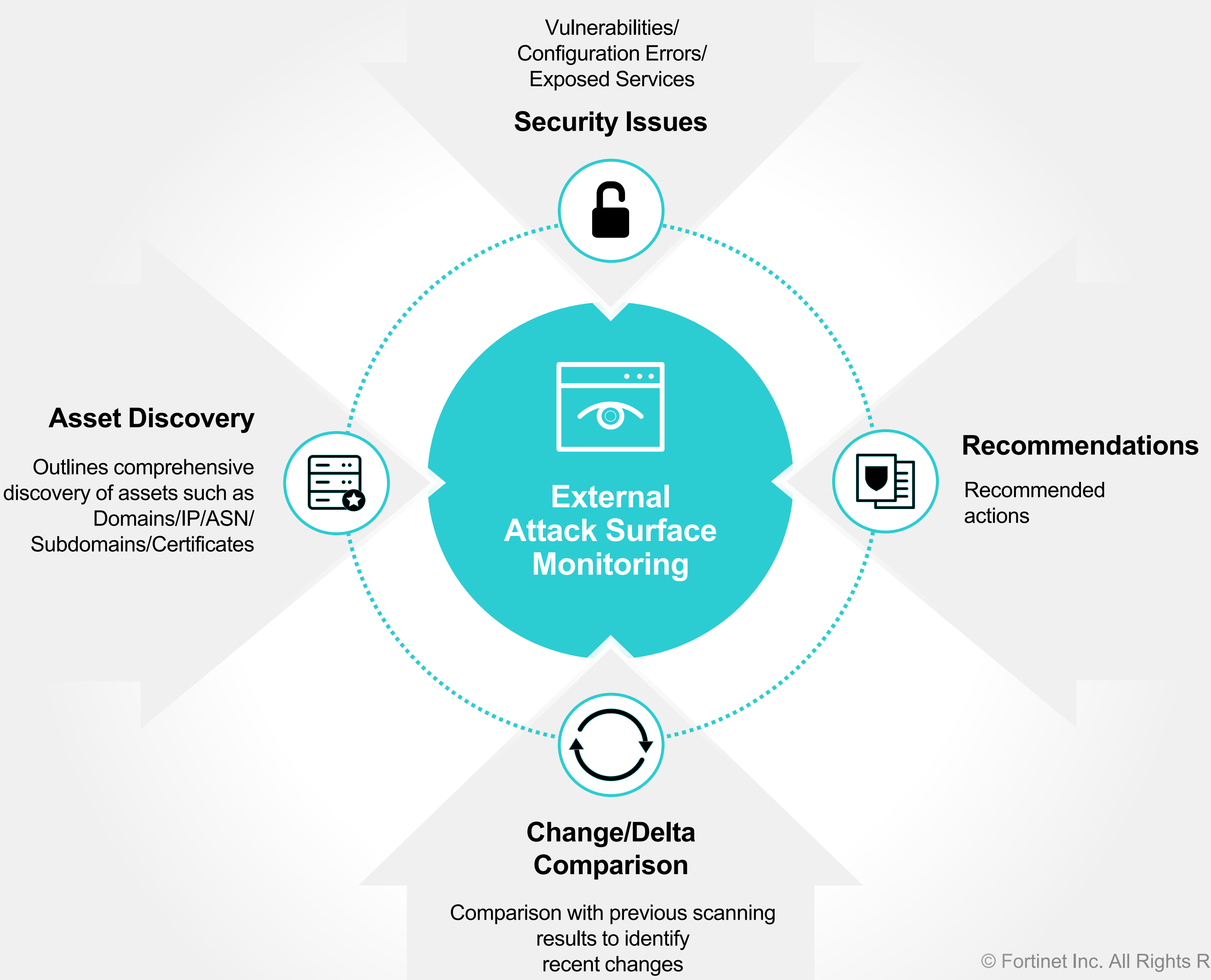
Brand Protection

Adversary Centric Intelligence

External Attack Surface Management

(EASM)

Zero-false positives, external risk prioritization and remediation



Vulnerabilities/
Configuration Errors/
Exposed Services

Outlines comprehensive discovery of assets such as Domains/IP/ASN/ Subdomains/Certificates

External Attack Surface Monitoring

Comparison with previous scanning results to identify recent changes

Brand Protection

Discover leaked credentials, Preserve customer trust and loyalty, and credibility with partners, suppliers, and investors

Brand Monitoring & Protection

Credentials Monitoring

Monitor leaked/ breached credentials

Typosquatting

Monitor similar-looking domain names

Rogue Apps Monitoring

Track rogue mobile applications

Social Media

Monitor discussions against brand in social media

Phishing Monitoring

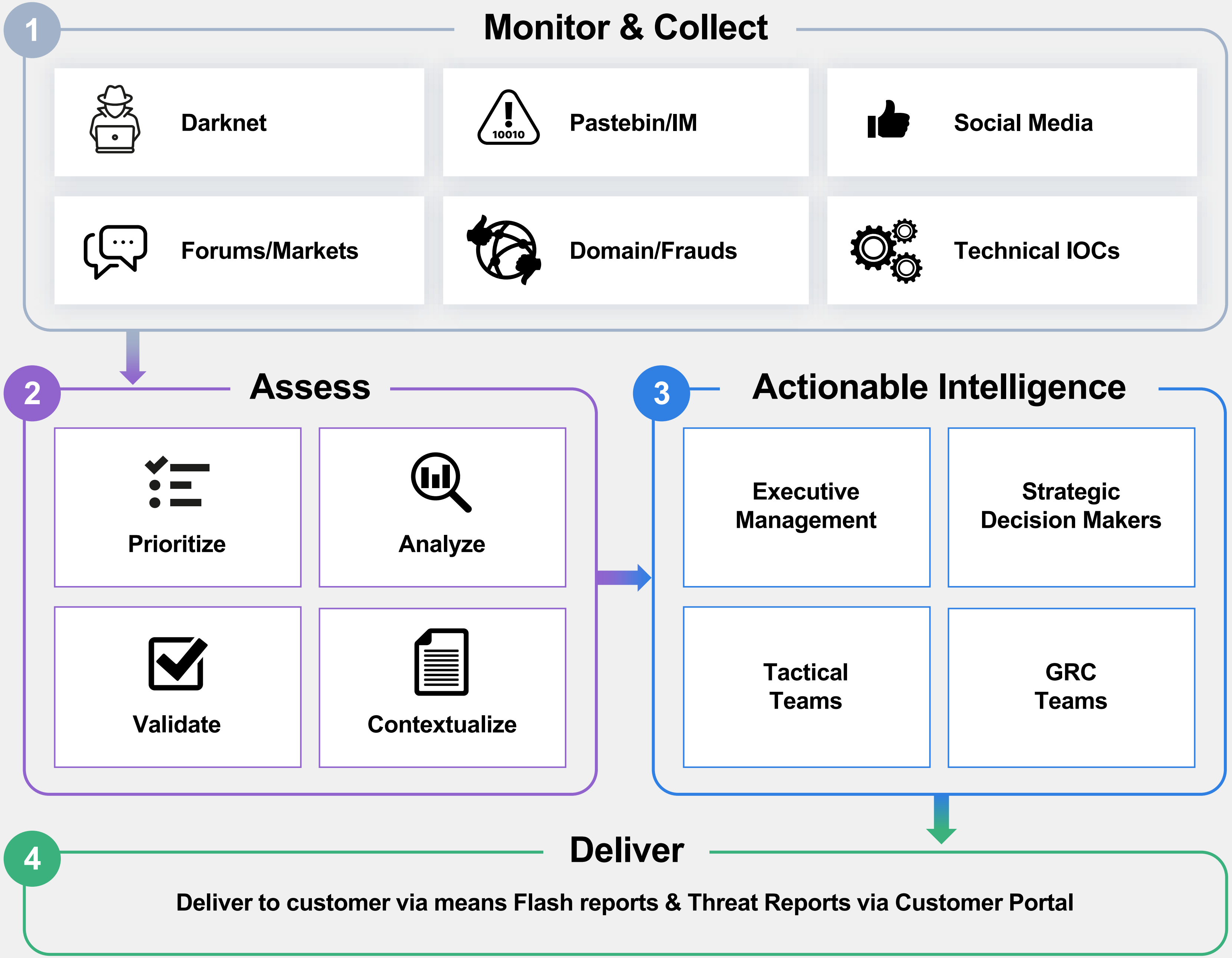
Track phishing campaigns against brands

Executive Protection

Monitor for exposed personal data / impersonations

Adversary Centric Intelligence (ACI)

Curated, actionable intel tailored to your attack surface



1 Monitor & Collect

- Darknet
- Pastebin/IM
- Social Media
- Forums/Markets
- Domain/Frauds
- Technical IOCs

2 Assess

- Prioritize
- Analyze
- Validate
- Contextualize

3 Actionable Intelligence

- Executive Management
- Strategic Decision Makers
- Tactical Teams
- GRC Teams

4 Deliver

Deliver to customer via means Flash reports & Threat Reports via Customer Portal

FortiRecon

A Fortinet DRP service

What are the key takeaways?

- *Gain the upper hand on your attacker*
- *Understand and monitor you attack surface*
- *Be proactive with your cybersecurity*
- *Protect your brand*

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Threat & Exposure Visibility

Magnus Jansson
Senior Security Solutions Engineer, Rapid7

Ellis Reed
Solution Architect
Integrity360

Martin Johansson
Systems Engineer
Fortinet

Richard Ford
CTO
Integrity360

#securityfirst2023

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Ur analytikerns ögon:
Utforska möjligheterna med 24/7 SOC

Emil Olofsson,

SOC Analyst, Integrity360 Sweden

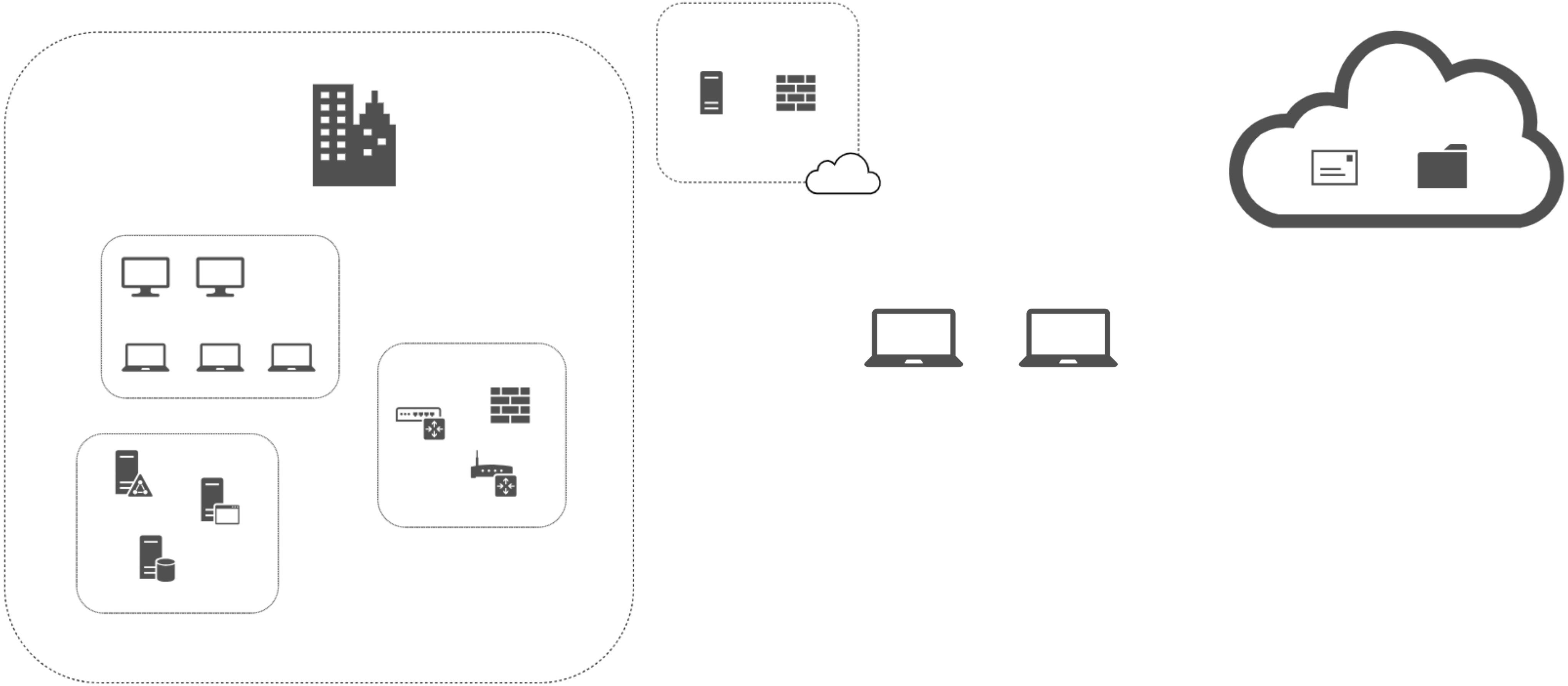
#securityfirst2023

Vad är behovet?

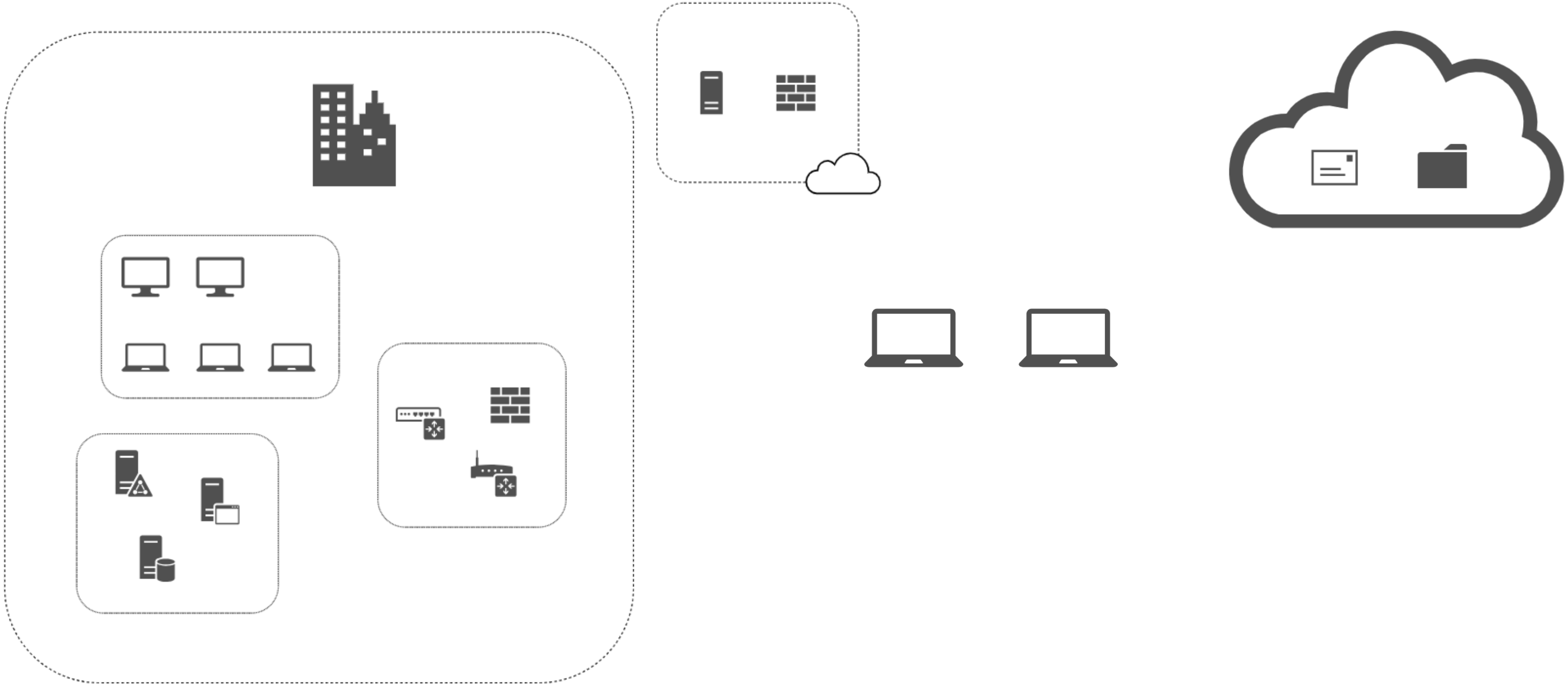
Förmågan att upptäcka och hantera

> “Förmågan att upptäcka och hantera eventuella intrång i vår IT-infrastruktur måste förstärkas

IT-infrastrukturen

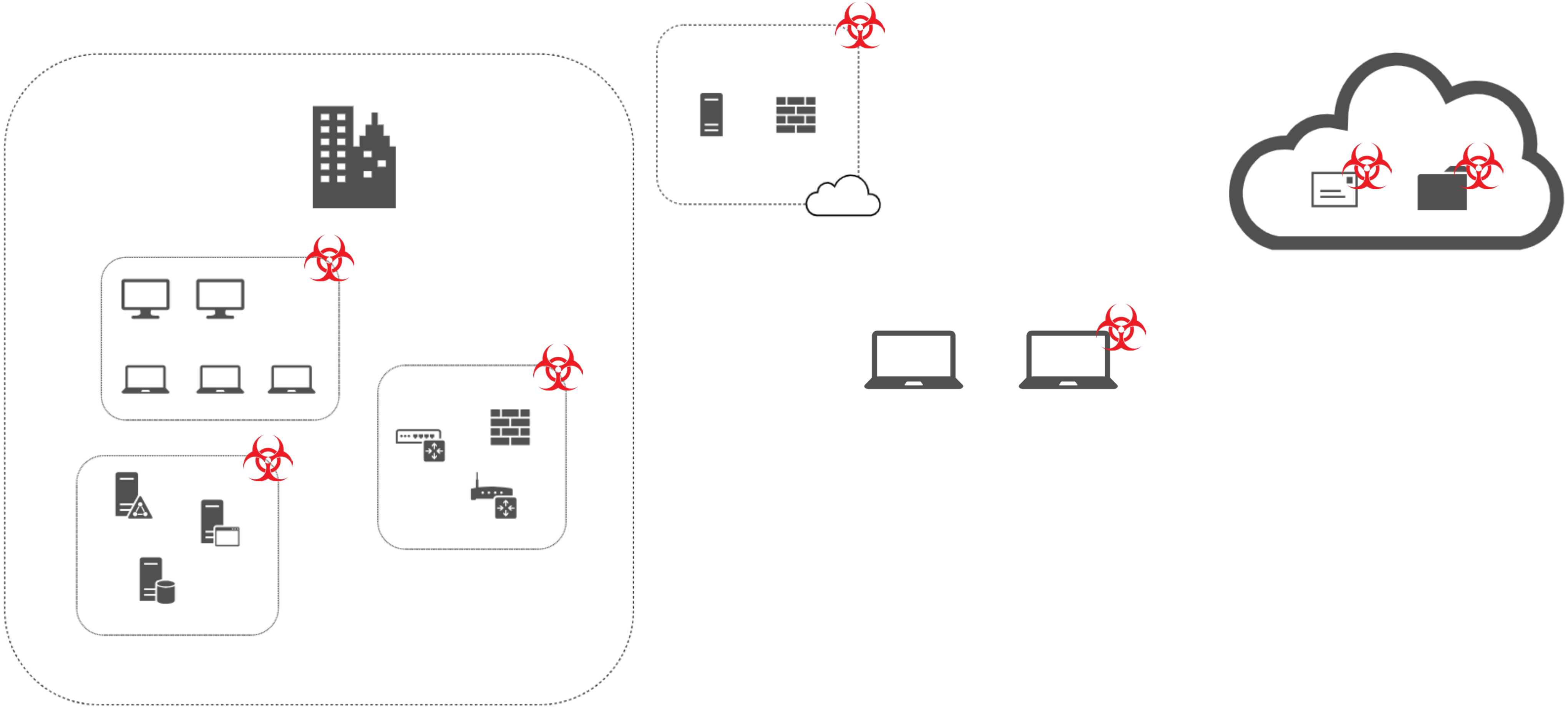


Spelplanen



Vägarna in och det skyddsvärda

Spelplanen



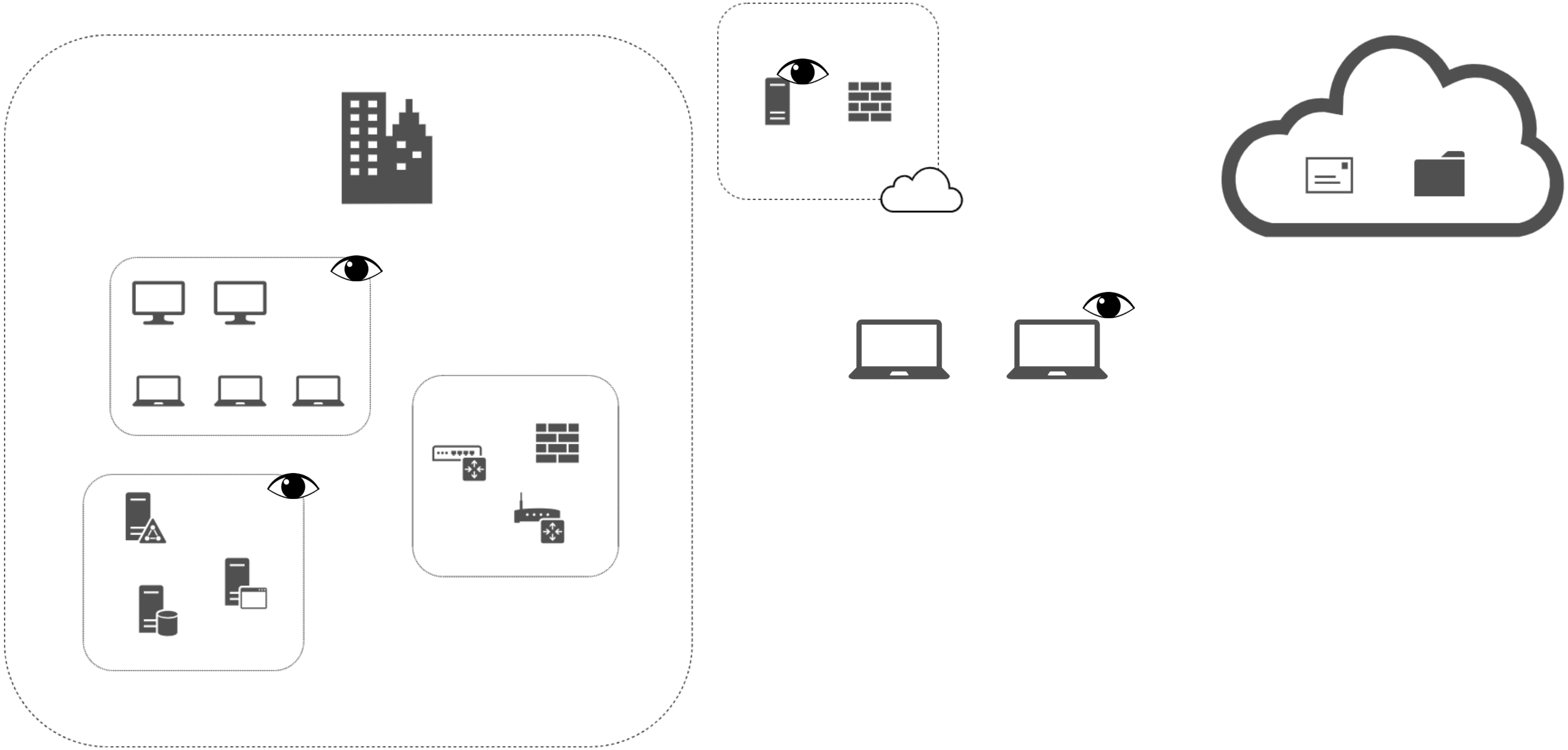
Steg för steg

EDR

Endpoint Detection & Response

- Skydda och förhindra
- Logga och larma
- Begränsa

Spelplanen

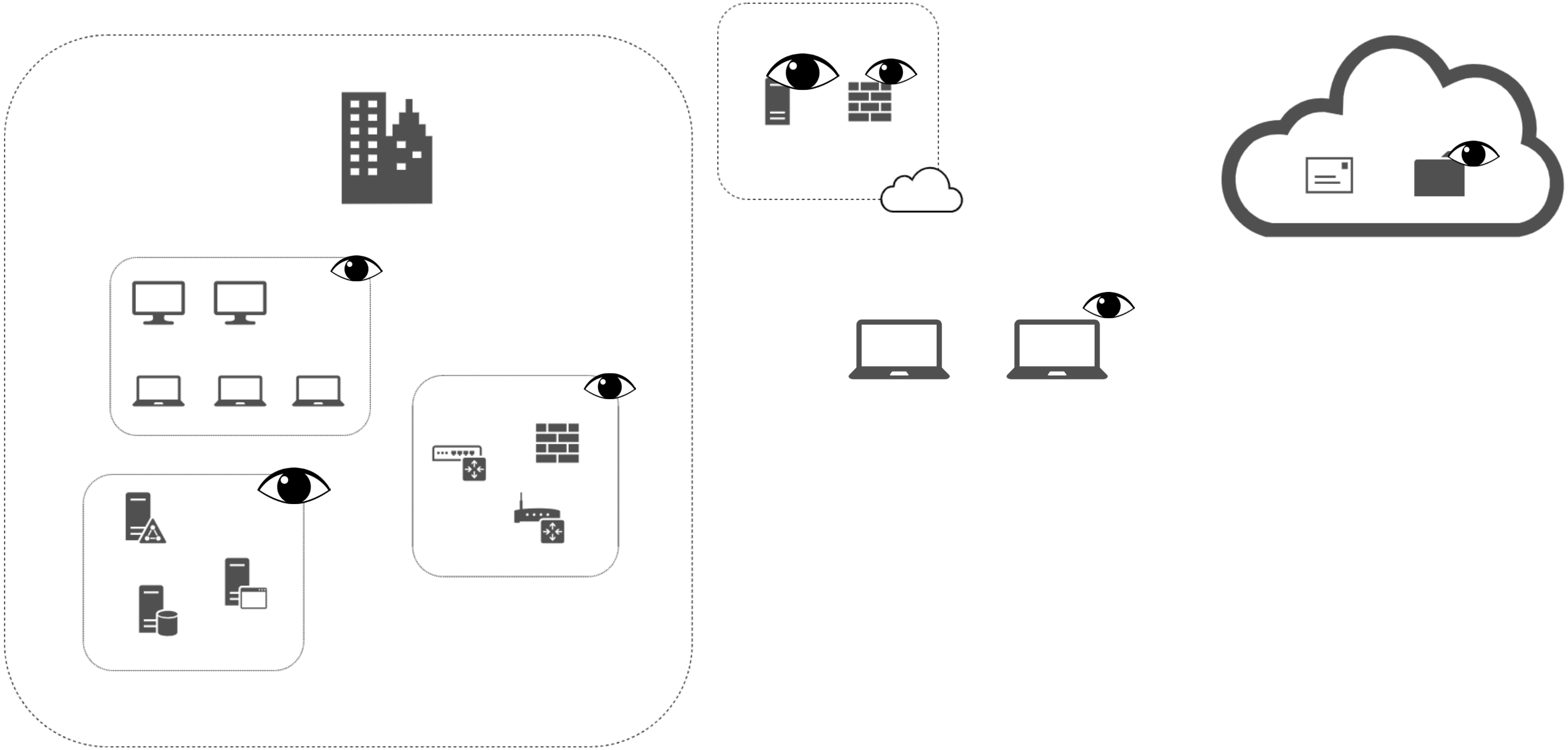


SIEM

Security Information and Event Management

- Spårbarhet
- Nätverksloggar – System och trafik
- Viktig infrastruktur
- Molnet

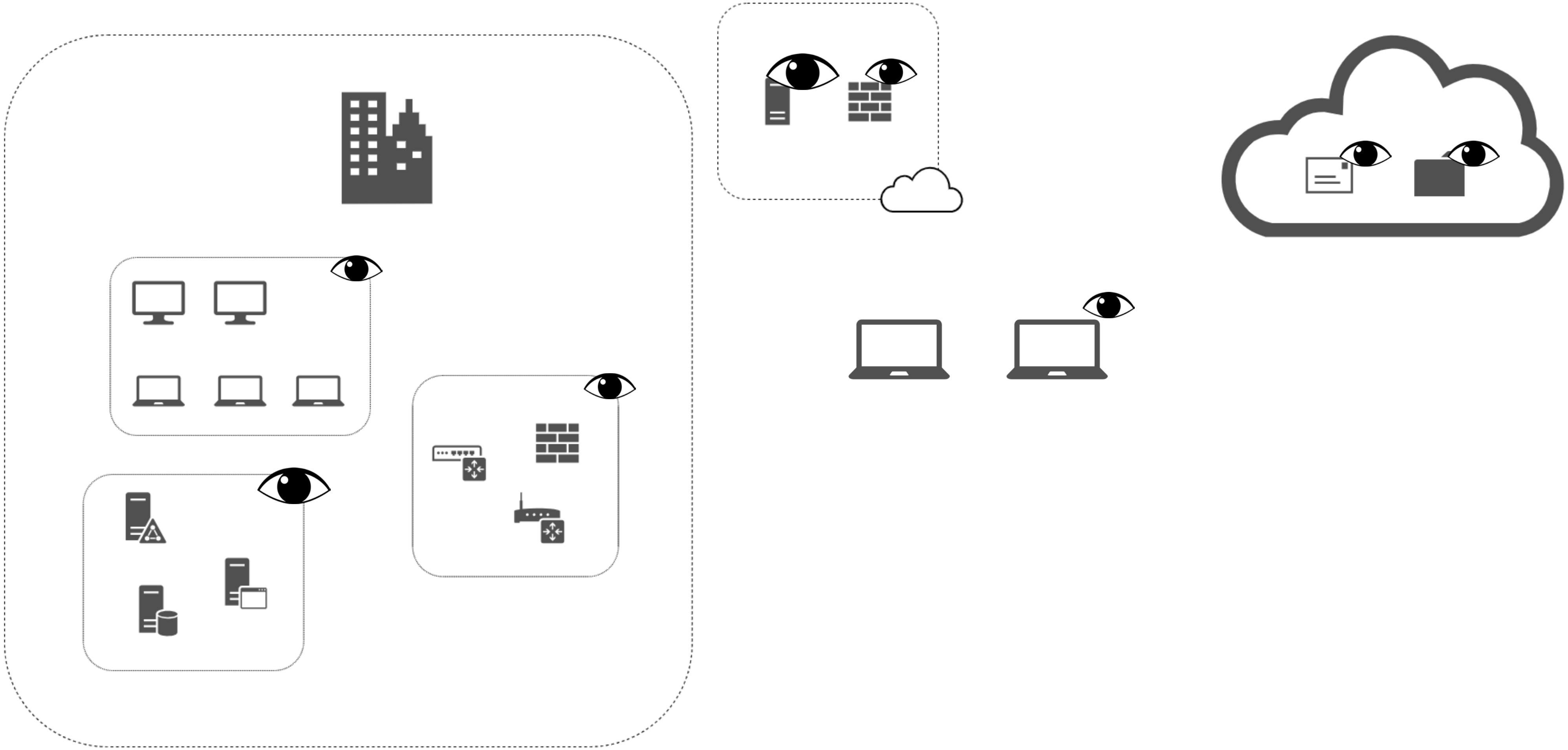
Spelplanen



Email Protection

- Skydda och förhindra
- Logga och larma
- Begränsa

Spelplanen



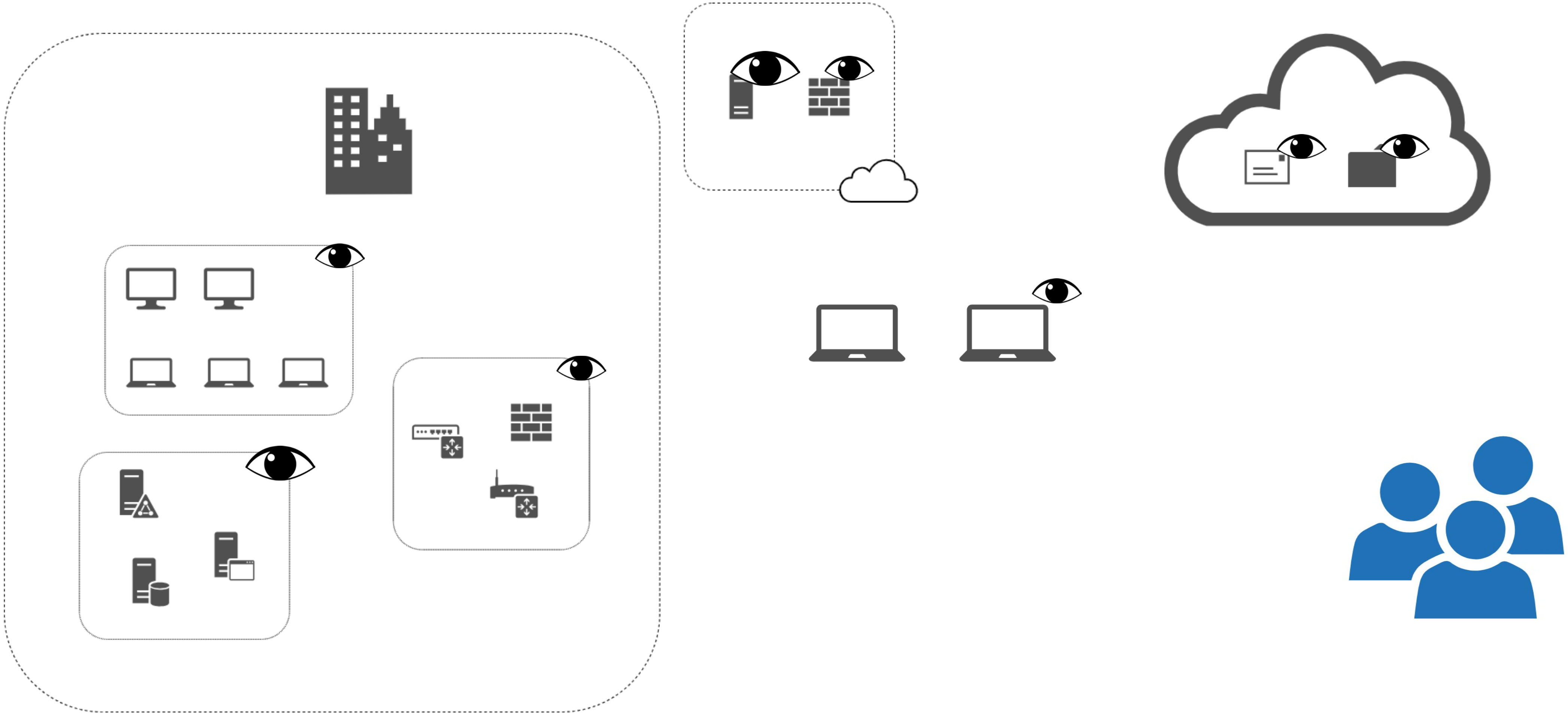
SOC

Security Operations Center

- Människor
- Övervaka, upptäcka och agera
- Korrelera
- Kommunicera
- 24/7

Upptäcka och hantera

Spelplanen



Integrity360
your **security** in mind

Thank you

Emil Olofsson
emil.olofsson@integrity360.com

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

SECURITY FIRST

CYBER SECURITY CONFERENCE 2023

Thank you

Integrity360

your **security** in mind