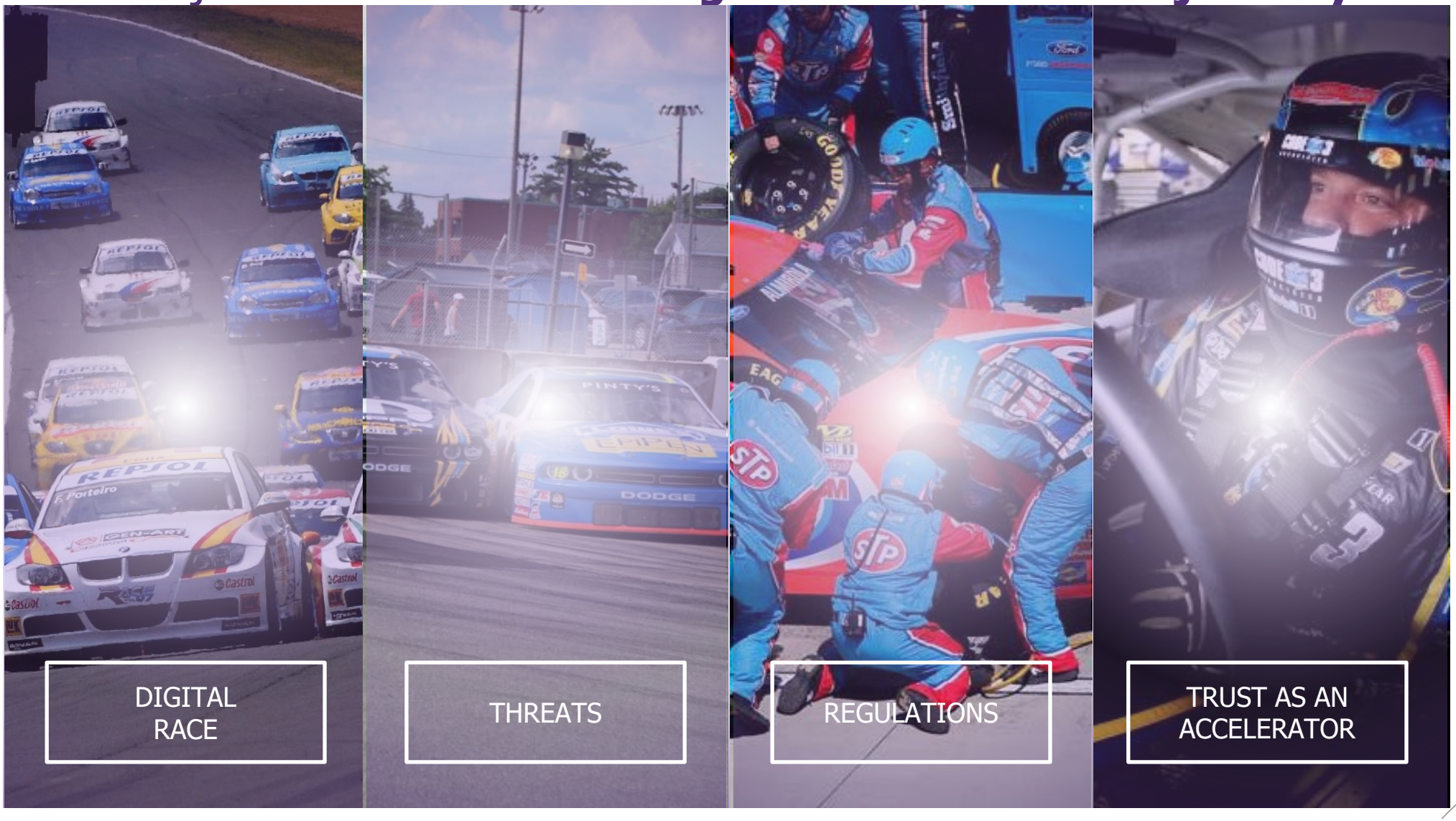
WAVESTONE

Cyber Security Transformation and Optimisation

G-Cloud 13

April 2022

Our objective: ensure **a safe digital transformation journey**



*In the light of constantly changing **cyber threats** and risks introduced as a result of **digital transformation**, we work with complex organisations to help them identify, protect, detect, respond and recover from cyber-related events.*

An independent leader in cybersecurity & resilience

Building Digital Trust in your organisation is an **essential business enabler** for success in the race for **digital transformation**

700+
Consultants & Experts

1,000+
clients in **20+** countries

Our clients
ExCom, Business, CDO, CIO, CISO, BCM

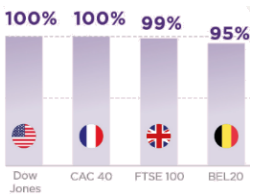
PROVEN EXPERTISE

- Risk management and Compliance
- Cloud & next-gen security
- Program management and C-level
- Digital Identity & eFraud
- Ethical Hacking and Incident Response
- Business Continuity and Cyber-Resilience

FORRESTER®
European Cyber Consulting Provider (MidSize)

Sectorial benchmarks

CISO & Start-ups radars



CyberLab

CERT-W

Our latest topic of engagement with our clients

ASSURANCE

Build a **practical framework** and **automate evidence collection**

RESILIENCE

Reduce business impact when hit by operational threats with practical measures

CLOUD

Fully **integrate Cloud assets in your security model**

IDENTITY & ACCESS MANAGEMENT

Leverage new solutions to enable **dynamic and transparent** security model (zero trust)

CRISIS EXERCISES

Improve **board and business preparedness** with **realistic exercise**

3rd PARTY SECURITY

Increase oversight and **on-going control** on your supply chain

SOC & FUSION CENTRE

Mature your Security Operations Centre (SOC) service toward integrated **Fusion Centre**

Preparing for a cyber-crisis - Here is a challenge.

1. It is no surprise: companies are under pressure, cyber-attacks are growing harder and trickier *(ransomware, supply-chain… 60 attacks managed by Wavestone in 2020)*
2. Cyber-crisis governance is often set-up… but shortcomings appear on real crisis *(24/7, third-parties onboarding, logistics…)*
3. Cyber-crisis is a race against the clock – preparation is key, especially on investigation & defense *(have logs – lots of logs, DC rebuilding automation, business apps restarting priorities…)*
4. Most importantly: you better be working together *(partners, CxO, operations, communication, authorities…)*

Our Capabilities

Define your cyber-crisis governance

- Adapt your current crisis organization to cybersecurity
- Define major incidents playbooks (ransomware, leak…)
- Onboard crisis stakeholders: training, tooling, templates…

Simulate attacks and test your response

- Design relevant scenarios inspired by recent attacks
- Create a storyboard and build realistic stimuli
- Roll-out the exercise and identify lessons learnt

Help you deal with cyber-attacks

- Technical expertise: forensics, malware analysis, Threat Hunting…
- Help crisis directors handle with crisis management
- Defense plan definition: AD recovery, security…

Our Boosters

Cyber-crisis assessment Framework

Playbooks for major incidents

Off-the-shelf exercise scenarios & chronograms

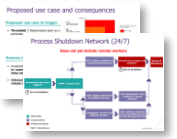
Exercise assessment grids

AUTHORIZED TO USE CERT

TF-CSIRT Trusted Introducer

CERT-W, with a 24/7 incident response service

Incident Response toolkit



Third Party Security – An Overlooked High-Priority Threat

1. Many organisations are under-prepared to defend against growing threats from their supply chain *(SolarWinds, Accellion, etc.)*

2. Multiple Governments have highlighted supply chains as 'an area for urgent attention'. *(FCA/PRA stressed exit, EU DORA)*
What about fourth party threats?

3. Third Party management is often weighed down by manual and inefficient processes
(High FTE count for limited added value)

4. COVID has brought to light multiple failures in third party management and the need for tools/automation *(ServiceNow, CyberVadis, RiskSense, etc.)*

Our Capabilities

Adopt a 'Know Your Supplier' approach

- **Unify and integrate** processes with legal, procurement, finance etc.
- **Extend** process to cover **pre-contract** light touch, up to **exit** strategy
- Define **triage and assessment** framework based on sensitivity

Automate

- **Automate the evaluation** (ratings/questionnaires)
- **Automate governance,** and integrate evaluation with orchestration
- Design and produce **MI/Dashboard**

Make it happen

- **Set up and steer a change programme** based on the above
- Deploy a **task force to remediate** a backlog of under-assessed or 'risky' suppliers

Our Boosters

Vendor categorisation and sensitivity-based assessment approach

Lifecycle key steps and checklists

Market benchmark for automation of evaluation and governance

Toolchain end to end blueprint and integration points

MI & Dashboards

Off the shelves templates of questionnaires, contract clauses, IT integration scenarios. Etc.

Mature SOC capabilities enable organisations to effectively detect and respond to threats

1. Advanced organisations are bringing together security teams under the Cyber Fusion Centre (CFC) umbrella.
2. 56%[1] of cyber leaders say that cyber security staff shortages are putting their organisations at risk.
3. Larger threat attack surface caused by the shift to remote working has attracted the attention of cyber criminals worldwide.
4. Existing SOC teams lack the expertise across People, Process, Service and Technology , required to successfully deliver transformation.

Our Capabilities

Establish your SOC maturity baseline

- Demonstrate **why** change is needed; targeted investment
- Use results as input to strategy, TOM and **business case**
- Measure **current-state** and define **target-state** using SOC-CMM

Develop your strategy

- Articulate **what** you need to achieve across **all domains**
- Create a **workforce strategy**; right skills, right locations, MSSP vs in-house and Outline career paths to **retain knowledge**
- Define your tooling strategy; SIEM, UEBA, SOAR

Define and implement your TOM

- Specify **how** you are going to operate in order to realise your strategy and achieve business objectives
- Exploit opportunities to **automate** common tasks
- Preserve **compliance** with x-border data requirements

Our Boosters

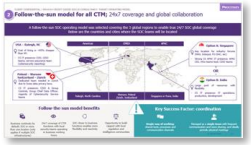
Our digital facilitation tools ensure interactive workshops for geographically disparate teams

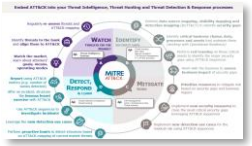
Our industry benchmark allows direct peer comparison

Our research & knowledge centre provides industry insights

Our templates and industry analysis accelerates the production of your strategy

Our stakeholder-friendly content ensures your change is supported and adopted





Our collaborative and cross discipline approach gives your initiative the best chance of success

Identity & Access Management is front and centre of security and digital strategies

1. IAM is an asset for **Cybersecurity**: move from perimetric toward Zero Trust approach
   (unique ID traceability, secure authentication, secure on any device)

2. IAM is a **Business Enabler,** bringing agility & shorter time-to-market, at scale
   (efficient processes, consumed as a commodity, as a service (API))

3. IAM streamlines the **user experience,** delivering on user expectations of an effortless, simple UX, as at home
   (easy onboarding, risk-based decisions to simplify, omni-channel)

4. 63% of organisations **lack the holistic vision** to reap these benefits
   (unbalanced investment in tech vs. people and processes, little end to end vision)

Our Capabilities

Positively transform your IAM estate

- Migrate from **legacy IAM** platform and processes
- Adapt **IAM to the Cloud – secure APIs**
- **Consolidate** mixed environments (e.g. post-merger): TOM, Strategy, Architecture

Simplify compliance and access rights

- **Overlay Id Analytics** on top of IAG to restore control over accesses
- **Automate recertification** processes for compliance
- Leverage tools to **identify roles** and create a RBAC model

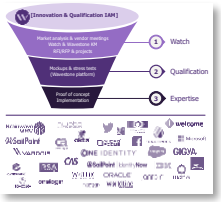
Streamline user/customer experience with innovation

- Deploy **state of the art authentication means** (password less, risk-based auth etc.)
- Implement a single UX on all channels with **CIAM**

Our Boosters

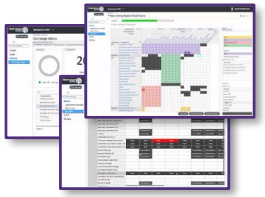
IAM Maturity assessment Framework

Vendor market vision



Migration scenarios, programme structure and governance…

Rights review methodology



Ready to use toolset to accelerate review and role building

Demo assets and environments to work with non-tech users

Something cool on CIAM

Cloud Security is a must for today's digital enterprises

1. Moving to the cloud should be seen as an opportunity to simplify and standardise security
(service model, templates, automation…)

2. Still… cyber attacks against misconfigured cloud services are on the rise and so are the fines for data breaches
(Capital One, Docker Hub, Facebook…)

3. Understanding the boundaries of the shared responsibility model with your providers is crucial – don't assume!
(consider service type: IaaS, PaaS, SaaS…)

4. And… monitoring in the cloud continues to be a key priority to detect attacks and manage vulnerabilities in your cloud estate
(native capabilities, UEBA, SOAR…)

Our Capabilities

Assess & secure your cloud services

- Review the risk position of your cloud estate
- Define strategy and deliver remediation programme
- Define target operating model and repeatable controls
(IAM, automated misconfiguration reviews, etc.)

Transform cloud security capabilities

- Secure AWS, Azure and GCP through service centres
- Enhance cloud security monitoring and automate incident response *(Sentinel, Unified Audit logs, MCAS, etc.)*
- Manage secure cloud migration and adoption projects

Prepare for tomorrow's challenges

- Leverage the cloud to enable a NextGen security model
(IAM in the cloud, homomorphic encryption, innovation start-ups, etc.)
- Prepare for a "stressed" exit from your cloud providers
(exit plans, containerisation, etc.)

Our Boosters

Wavestone's cloud security assessment framework

Cloud controls matrix based on CSA

Integration blueprints with native cloud provider capabilities

Configuration & hardening guidelines for major providers

Airline model

Security solution benchmarks

Operational Resilience is becoming a top priority in the UK

1. Traditional business continuity and crisis management measures cannot cope with major disruptions
   (OVH, Sodinokibi, COVID-19)
2. Regulators worldwide, with the UK as a leader, are setting new requirements that can be seen as great opportunity
   (FCA, PRA, DORA)
3. Companies are setting up operational resilience programmes with high budgets
   (£500k -£1m one-off costs, 3-4% of IT budget for remediation)
4. To achieve true operational resilience, companies must change their mindset
   (SMF accountability, silo-breaking, training and awareness)

Our Capabilities

Run an Operational Resilience Programme

- Structure an Operational Resilience target
- Identify Important Business Services and impact tolerance
- Map the IBS value chain and underlying assets

Challenge existing capabilities

- Qualify threats and scenarios
- Understand existing resilience capabilities and controls
- Test resilience, identify gaps and mitigate risks

Accelerate transition to *Business as usual*

- Define governance to maintain Operational Resilience
- Produce high-quality MI dashboards to monitor resilience
- Set up tooling to increase efficiency and accuracy

Our Boosters

FCA/PRA Maturity assessment and compliance framework

IBS identification, impact tolerance and mapping methodology

List of top core resilience capabilities to be deployed

Testing plan methodology

Tooling Radar

MI & Dashboards

Security Assurance is the keystone of any cybersecurity function

1. With more and more threats, regulations, innovation... companies rethink their cybersecurity strategy *(ransomware, FCA/PRA, cloud)*
2. Companies shift from a unique strategy to risk-based strategies for their different business entities, leveraging security frameworks *(NIST, CIS20, ISO27001)*
3. Transformation is done through a reorganisation of the cybersecurity function and the delivery of large programmes, with high investments *(up to £100-150m/year and 1 security FTE/200 employees for Financial Services)*
4. 4 types of projects stand out: security foundations, protection of sensitive environments, zero-trust convergence, and cyber-resilience *(patching, AD security, IAM, BCP/DRP)*

Our Capabilities

Define your cybersecurity strategy

- Conduct a cyber benchmark to compare against peers
- Define a cybersecurity assurance framework and agree on a target profile to be reached
- Devise a cybersecurity strategy and associated roadmap

Build and assure your cyber programme

- Define project scoping, as well as programme assurance approach and toolkit
- Manage or assure a cybersecurity programme
- Produce MI dashboards to report to C-level

Reorganise your cybersecurity function

- Define a new Target Operating Model (TOM), considering offshore and cost optimisation strategies
- Coach cybersecurity stakeholders
- Outline job profiles and career paths

Our Boosters

Wavestone cyber-benchmark tool
(already used for ~50 companies)

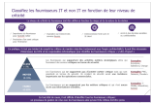
Wavestone CISO Radar on CISO priorities for 2021

Programme Assurance toolkit
(planning, budget, progress, risk, etc.)

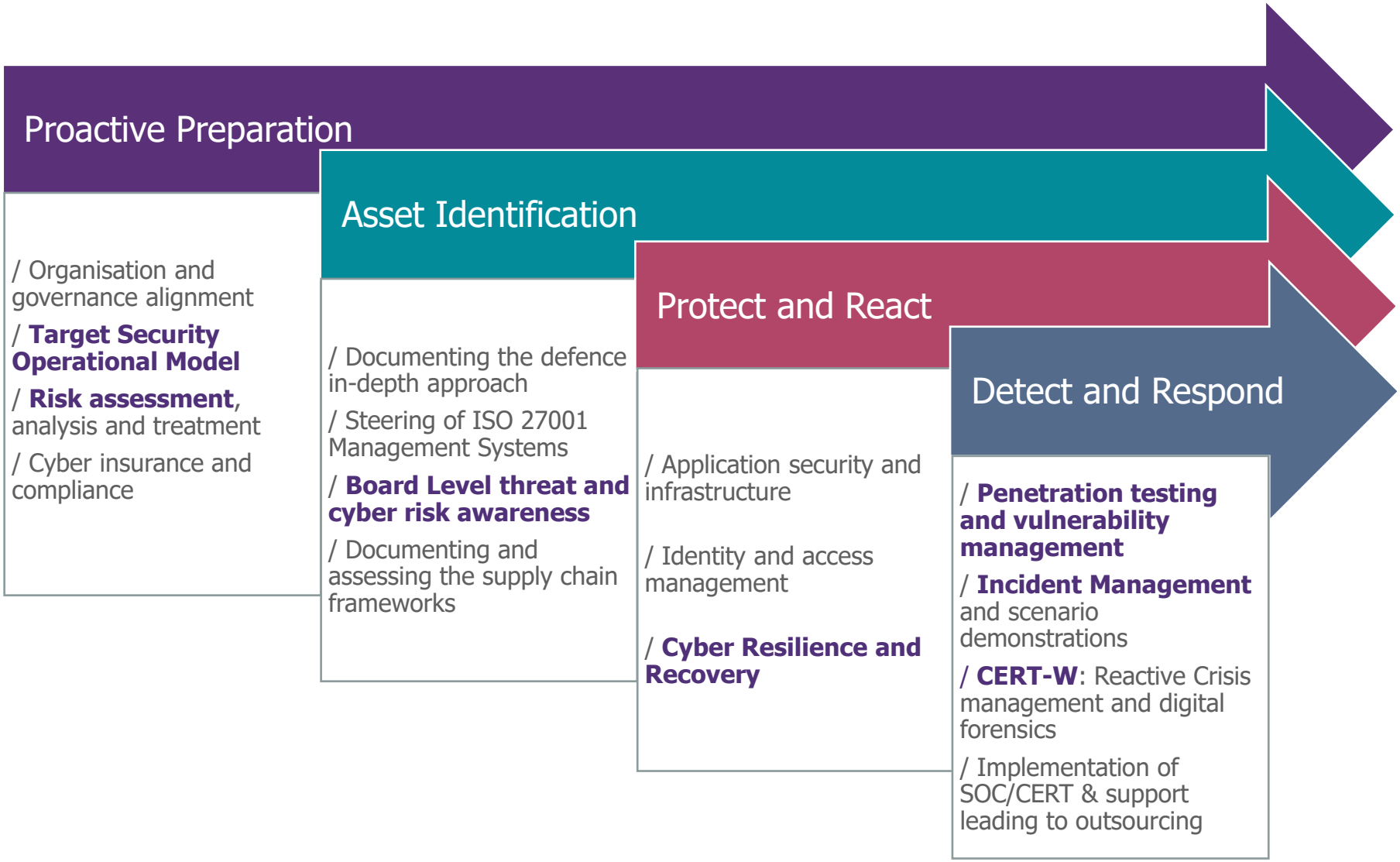
C-level MI dashboard templates
(risk coverage, protection against major attacks, etc.)

Budget and TOM benchmark

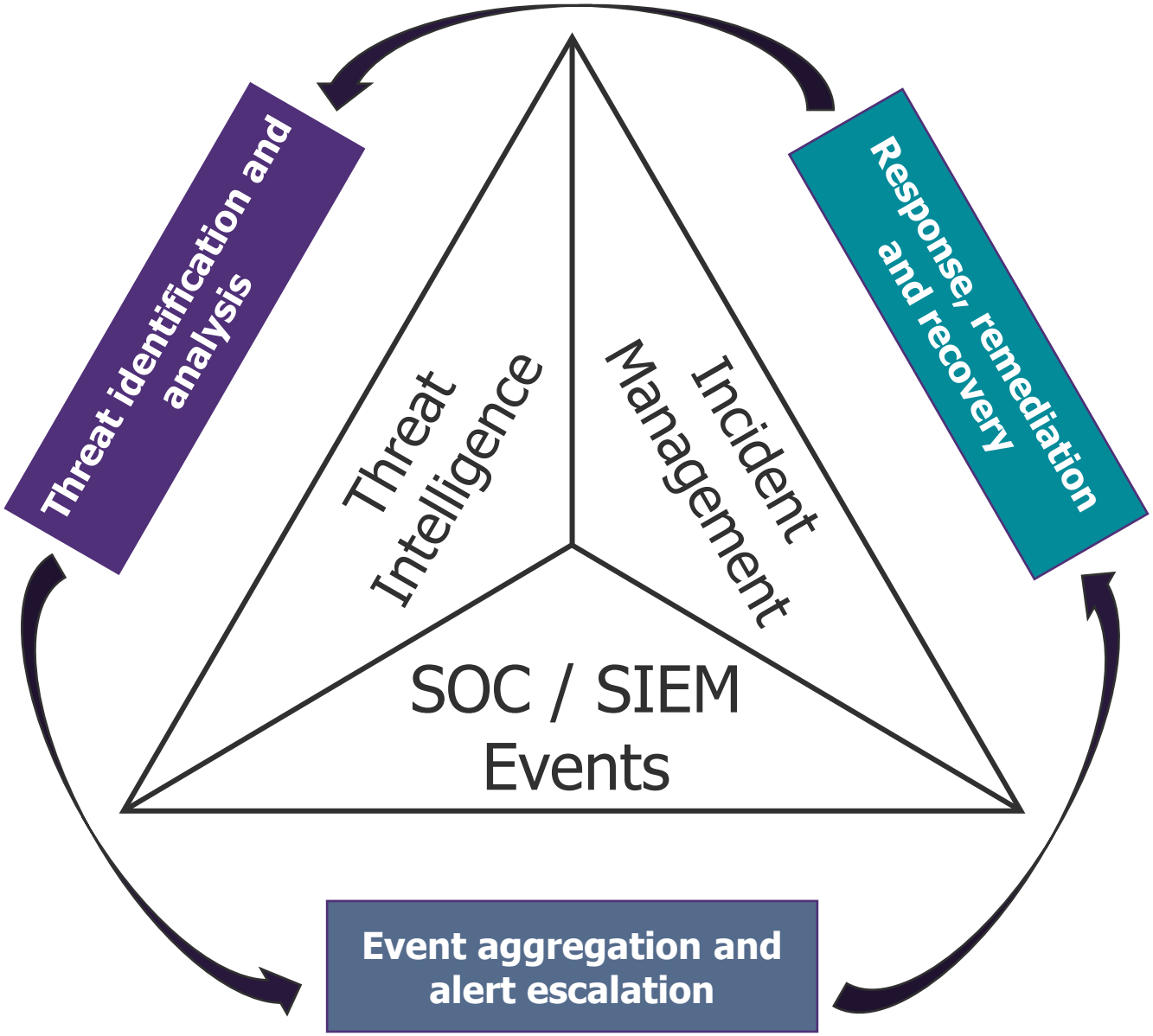
Cybersecurity job market benchmark



Our approach to Cyber Security Transformation and Optimisation

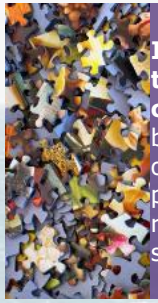


Proactive Cyber Security & Risk Mitigation



Wavestone brings a strong field experience on cybersecurity and resilience

RESILIENCE



Financial Regulator (confidential)

Increase of resilience to "cyber-catastrophes" through vital business outcomes identification, provision of recovery capabilities and stress-testing

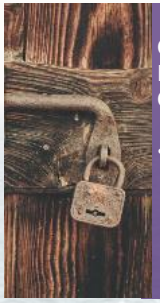
IDENTITY ACCESS MANAGEMENT

Public Broadcasting Group (confidential)

Identity Data Governance

- 35,000 users, extremely volatile population and strong business
- Streamlining of numerous Identity data sources and data quality control through an Identity Analytics approach, fine grain request provisioning w/ MDM source

3rd PARTY SECURITY



Manufacturing group (confidential)

CYBERSECURITY CLAUSES, PAQS AND PRIVACY COMPLIANCE

- Review and Position Analysis Questionnaires of policy, methodology and contracts, including data security measure.

SOC & FUSION CENTRE

Investment bank (confidential)

Full Cyber Programme

- SOAR
- Threat detection
- EDR
- Threat intelligence
- Forensics
- Incident management

CRISIS EXERCISES

Government Regulator (confidential)

- Global financial crisis scenario caused by a major cyber attack
- 24 Financial Authorities involved
- 3 continuous days of exercise
- 1.000+ people involved
- 16 months to prepare the exercise

ASSURANCE

Investment Bank (confidential)

- Cybersecurity Programme Direction (3-year project, 8 FTEs involved)
- Assurance / Maturity assessment against Cyber Criminality

Latest publications

/ Organizing a cyber crisis exercise is not an easy task
/ Benchmark Incident Response 2020
/ Enhancing cyber-resilience and building a testing strategy
/ Cyber Crisis: how to handle communication
/ Choose the right tooling for your crisis management
/ Deep-dive into a real cyber-attack, field experience

Read more on wavestone.com/insights

Appendix

Stimulated by solving challenges and driven to succeed

Business
&
Technologies

Transformation

Positive Way

A unique ability to combine in-depth industry expertise, business functions know-how and technology mastering

BUSINESS FUNCTIONS

- Strategy
- Innovation management & funding
- Marketing, sales & customer experience
- People & change
- Finance, risk & procurement
- Operations & supply chain

INDUSTRIES

- Financial services
- Telecom, media & entertainment
- Consumer goods & retail
- Manufacturing
- Energies & utilities
- Transportation & travel
- Real estate
- Public sector & international institutions

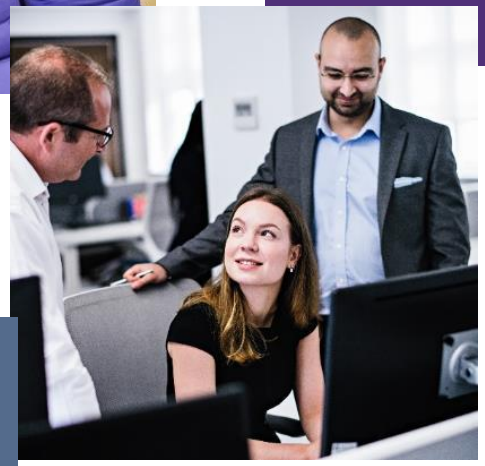
TECHNOLOGY

- Digital & IS strategy
- Digital & emerging technologies
- IT & data architecture
- Cybersecurity & digital trust

Wavestone, a fast-growing company

Pure-play
consultancy

€470m



3,500+
employees

15 offices
in 9 countries

Wavestone supports leading organisations shape and deliver their most critical transformations

In the UK we are the "go to" organisation for our senior executive clients for technology advisory. Our client focused approach allows us to bring deep business and technology expertise to add value to an organisation's agenda

- Cybersecurity
- Technology Advisory
- Operational Resilience

100+ UK Employees and growing

Deep subject matter capability and practical experience

Independent and impartial advice

Underpinned by our Attitude | Approach | Adaptability

Multidisciplinary approach

Collaborative consulting style

Blend different skillsets from breadth of expertise

One Global company, flat structure, no silos

Account Manager as single point of contact

How our culture drives the best outcomes for our clients

High Quality Delivery

Responsive

Outcome Focus

Based on **teamwork** and **enthusiasm**, which drives the mentality to succeed with our clients

Transparency drives **honesty** and **intimacy** to create an environment of trust. Leave a legacy.

Always bring the best capabilities, with **flexibility** to change, delivered from a single point of contact

Here's what our clients say....

*I find there is masses of **energy and enthusiasm** and work alongside us effortlessly... through our partnership and **honesty,** we ended up in a position where we got the **outcome** we all wanted.*

COO | Global Investment Bank

*Wavestone provided programme management expertise at a very critical and sensitive time in the project. Your team was **always at our side** even through the toughest of times. Our engagement always felt like a **deep partnership.***

US COO | Global Bank

*It has been a pleasure with working Wavestone. You have brought some much needed **expertise** and thinking to the work we have undertaken and I appreciate both the **professionalism** and **collaborative nature**.*

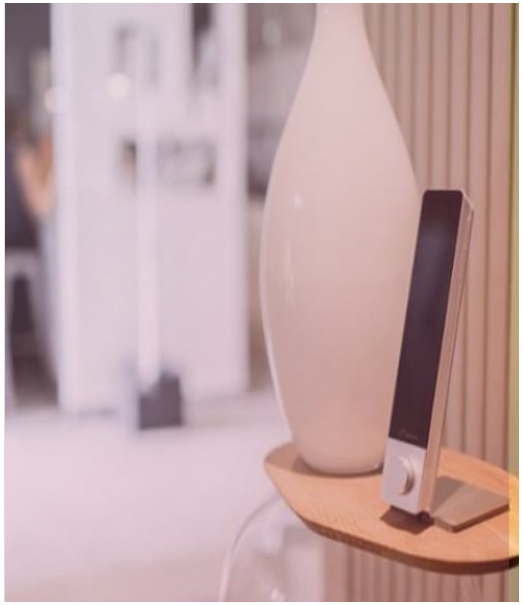
Head of Department |UK Regulator

Here's some of our recent work

Investment Bank

/

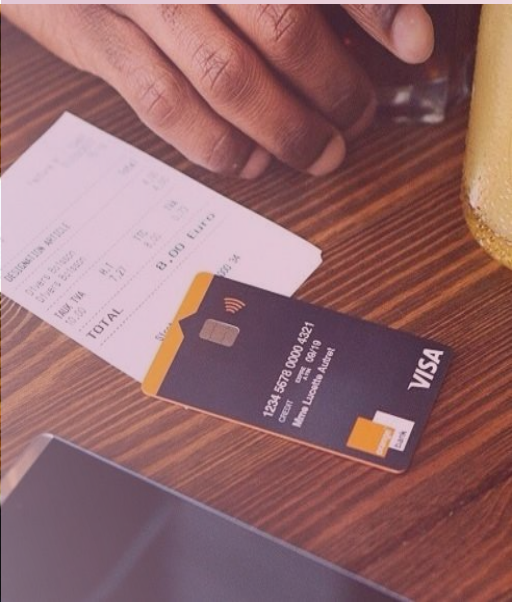
A Cloud Security review to recommend a unified cloud solutions in a secure way, with cost-effective approach



UK Government Entity

/

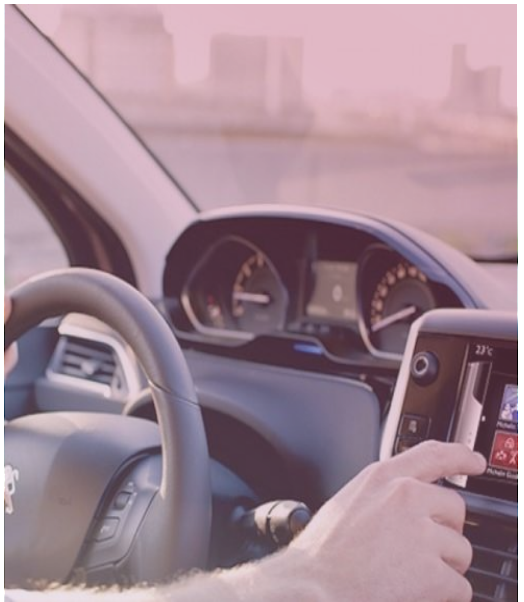
Established an effective go-to-market strategy for the future procurement of WAN services, with advisory on improving performance and reducing circuit costs



UK Regulator

/

Review of cyber recovery capability to ensure preparedness for recovery from a Cyber-Attack



Large Government Department

/

Technical Debt discovery exercise to help provide centralised view of IT Estate

The Positive Way

WAVESTONE

Mike Newlove
Partner

Jim Hennigan
Partner

uk.wavestone.com

@wavestone_UK