Cybersecurity

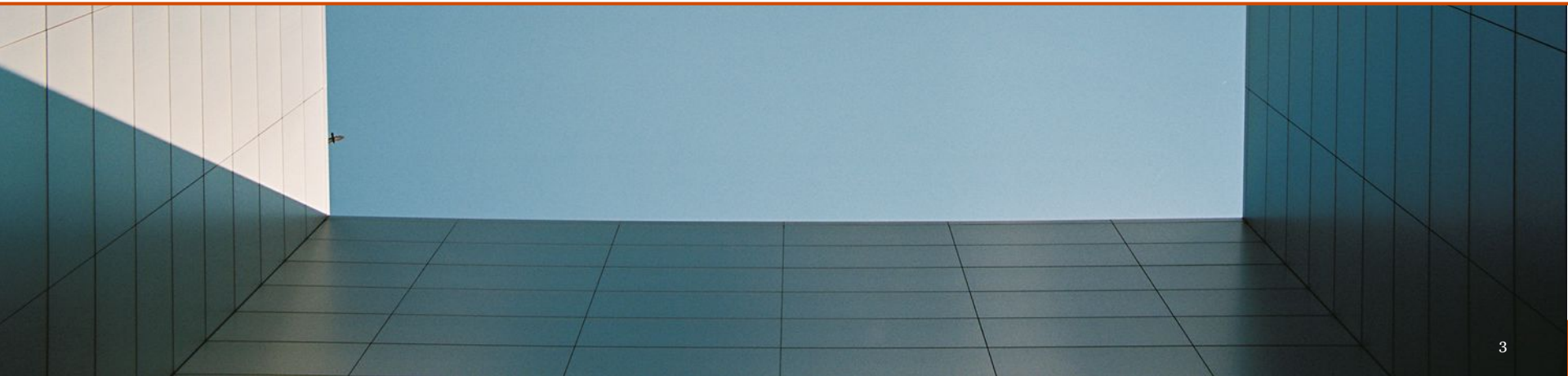
Incident Response References and Capabilities

PwC Consulting 2020

We exist to help build a secure digital society

Everything we do aligns to that

Table of contents

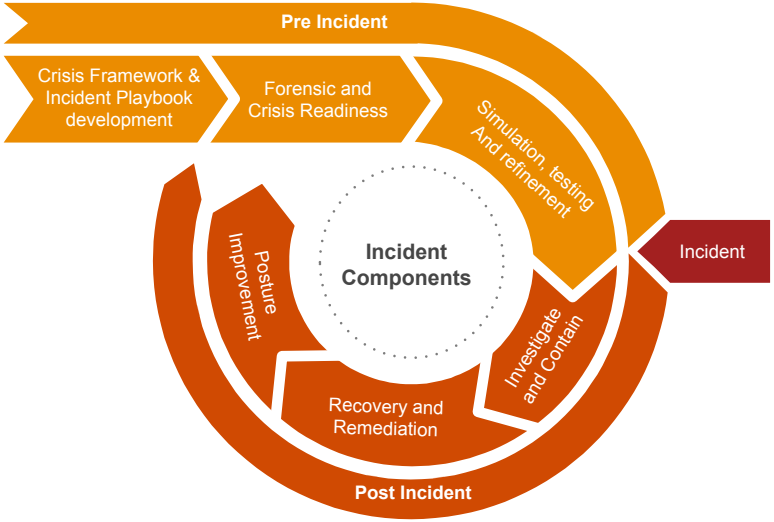


1

Cybersecurity Incident Preparation Model

PwC CyberSecurity Incident Preparation Model

Cybersecurity incidents have become inevitable; the result of our increasingly interconnected and technology-enabled world. As the increasing frequency of high-profile breaches shows, no organisation is immune. It's important to be prepared and be able to respond effectively.



PwC understands the Incident Management and Response as a continuous improvement process, where results, sources and TTP's (Tools, Tactics and Procedures) of an incident **serve as an input for the security state** of the organization, Forensic Readiness and training for the involved actors and parties.
PwC considers three differentiated stages during the process:

Pre-Incident, Live incident, Post-Incident

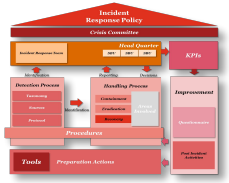
Incident Impact, involves the support of technical, legal, business and image assistance, among others.

Pre Incident - Readiness and Preparation

Based on our **experience**...

1. Governance Framework

Establish a governance model that allows proper communication control and coordination against any type of scenario.

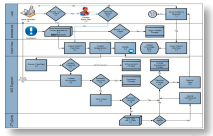


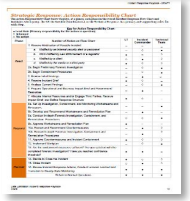
2. Crisis Framework

Develop a set of guidelines to enable an appropriate response to crisis events with minimum disruption to business.

3. Threat Modelling

Identification of real world threats to face in order to properly adapt and prepare efforts.



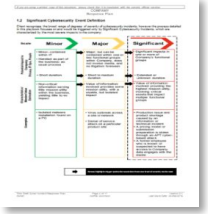


4. Playbook development

Step by step technical and management guidelines for specific incident types.

5. Forensic Readiness

We help you to have the right data available and accessible to thoroughly investigate an incident and inform a containment strategy.

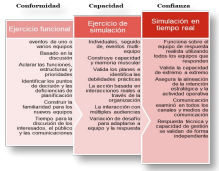


6. First Responder training

Preparing your technical teams to make critical decisions within the first 48 hours of an incident, including monitor and containment.

7. Crisis Simulation

A tailored exercising programme to ensure all teams in your response structure are ready to put your crisis framework and playbooks into action.



… we provide an **approach focused on the constant evolution** of organizational processes.

Pre Incident - Readiness and Preparation

We provide a range of services to help businesses improve their readiness and ability to respond to all types of cyber threats:

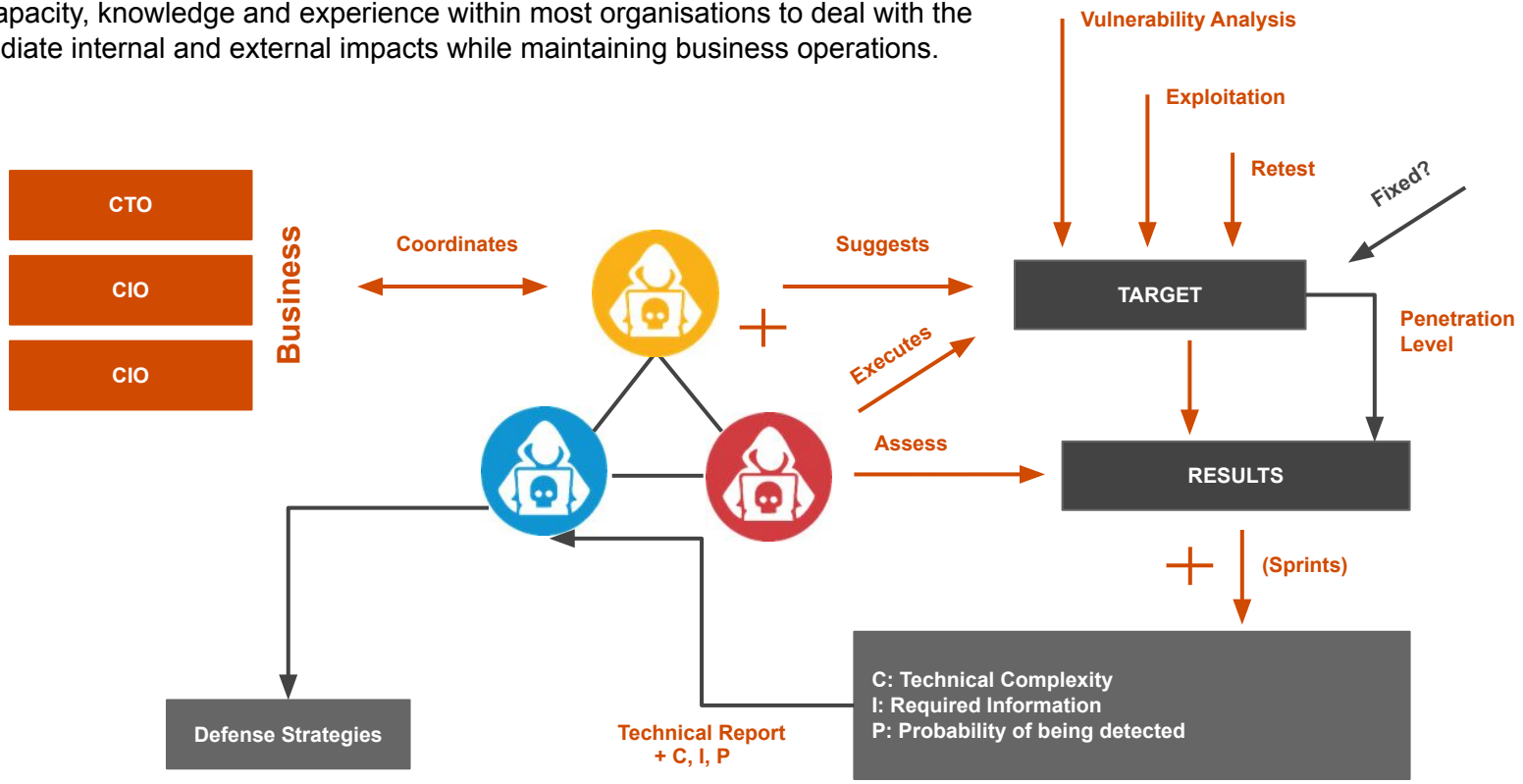
- **Playbook Development** - Step by step technical and management guidelines for specific incident types, including workflows, roles of key personnel and action plans.
- **Forensic Readiness** - We help you to have the right data available and accessible to thoroughly investigate an incident and inform a containment strategy.
- **First Responder Training** - Preparing your technical teams to make critical decisions within the first 48 hours of an incident, including how to monitor and contain an incident
- **Crisis Simulation** - A tailored exercising programme to ensure all teams in your response structure are ready to put your crisis framework and playbooks into action.
- **Crisis Framework** - After evaluating your existing crisis management procedures, we help you develop a set of guidelines to enable an appropriate response to crisis events with minimum disruption to business.
- **Threat Modelling** - Assessing the security of your information assets to help you identify vulnerabilities and understand how relevant threats would navigate your infrastructure to achieve their objective.
- **Breach Readiness Assessment** - Helping you to understand your level of legal preparedness to respond to a data breach.
- **Threat Profiling** - Identifying the real-world threats you face, enabling you to tailor your preparation efforts appropriately.

What are the benefits?

- ➔ Helps organisations to minimise the financial, reputational and operational impact of the breach.
- ➔ Teams involved are able to confidently and effectively respond to an incident.
- ➔ Security and risk teams have the information and documentation needed to notify regulators and stakeholders in a timely but controlled manner.
- ➔ You have a clear understanding of threats facing your business so preparedness efforts can be tailored accordingly.

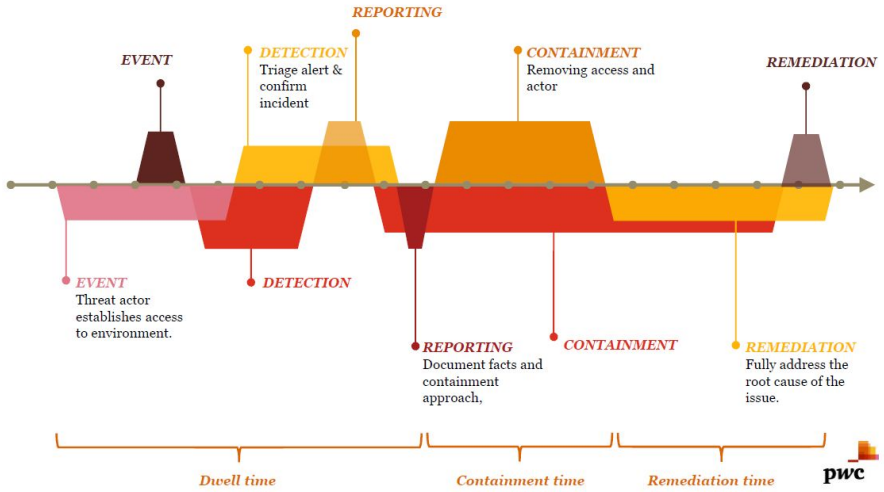
Live Incident: Deployment and Coordination Schema

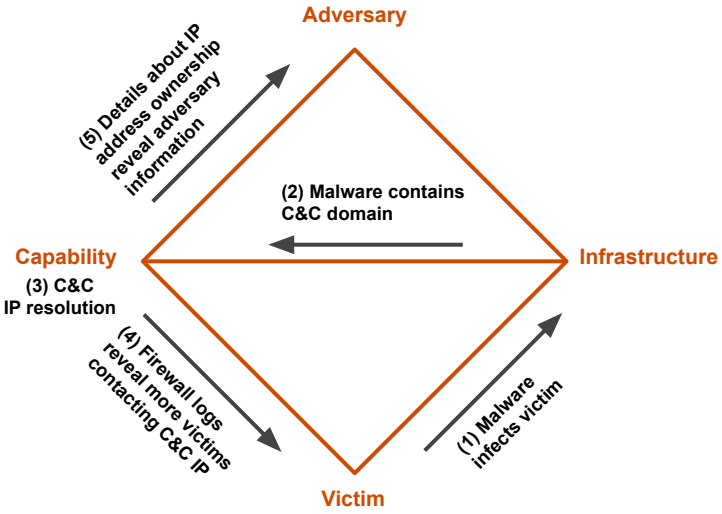
When a disaster arises or a major incident is discovered there is little time and rarely the capacity, knowledge and experience within most organisations to deal with the immediate internal and external impacts while maintaining business operations.



Post Incident - Coordination and Support

The timeline of an incident and its management is complex, even with a very experienced, trained and documented team. In the very first moments, the main challenge is how to correlate the different details available and link them together to support the decision making.



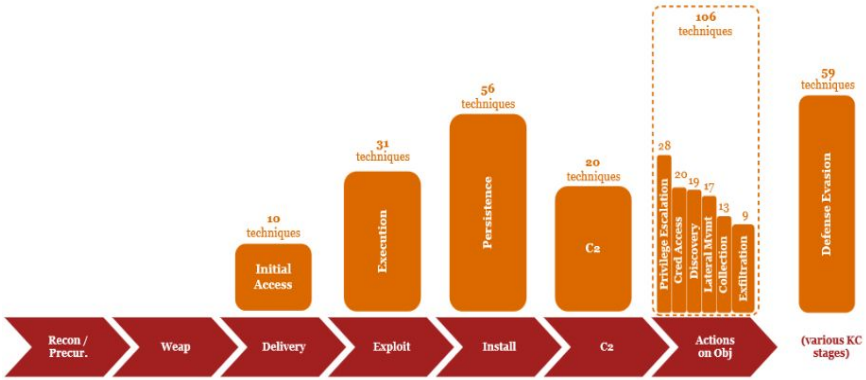


The "Diamond Model" is a systematic approach which allows us to map the different steps an adversary is taking to compromise the environment so we can take further actions. It is usually documented based on the kill chain model to understand the Tool, Tactics and procedures of the attacker.

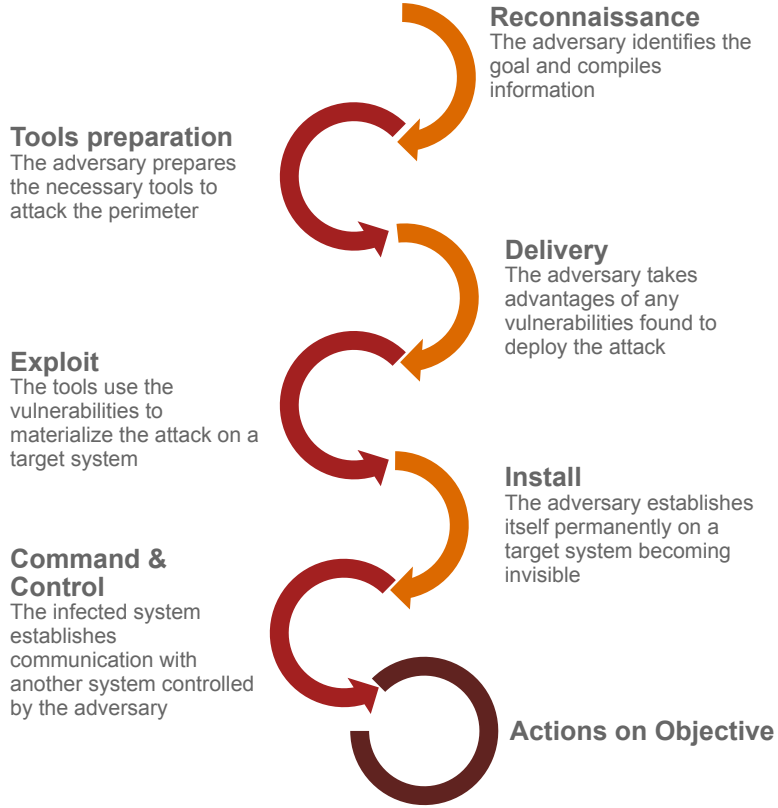
Post Incident - Coordination and Support

How we approach detecting intrusions

- ➔ Start with **known attack behaviors** (Killchain and Mitre ATT&CK pictured)
- ➔ Establish **baselines** for “normal” and alert outside these norms
- ➔ **Hunt for threats**, create new detections, and constantly improve



Cyber Kill Chain (CKC)



Post Incident - Review and Lessons Learned

An independent end-to-end evaluation of an organisation's response to an incident, from root-cause analysis to evaluating the effectiveness of stakeholder and legal management.

Root-cause analysis – Understanding why this happened

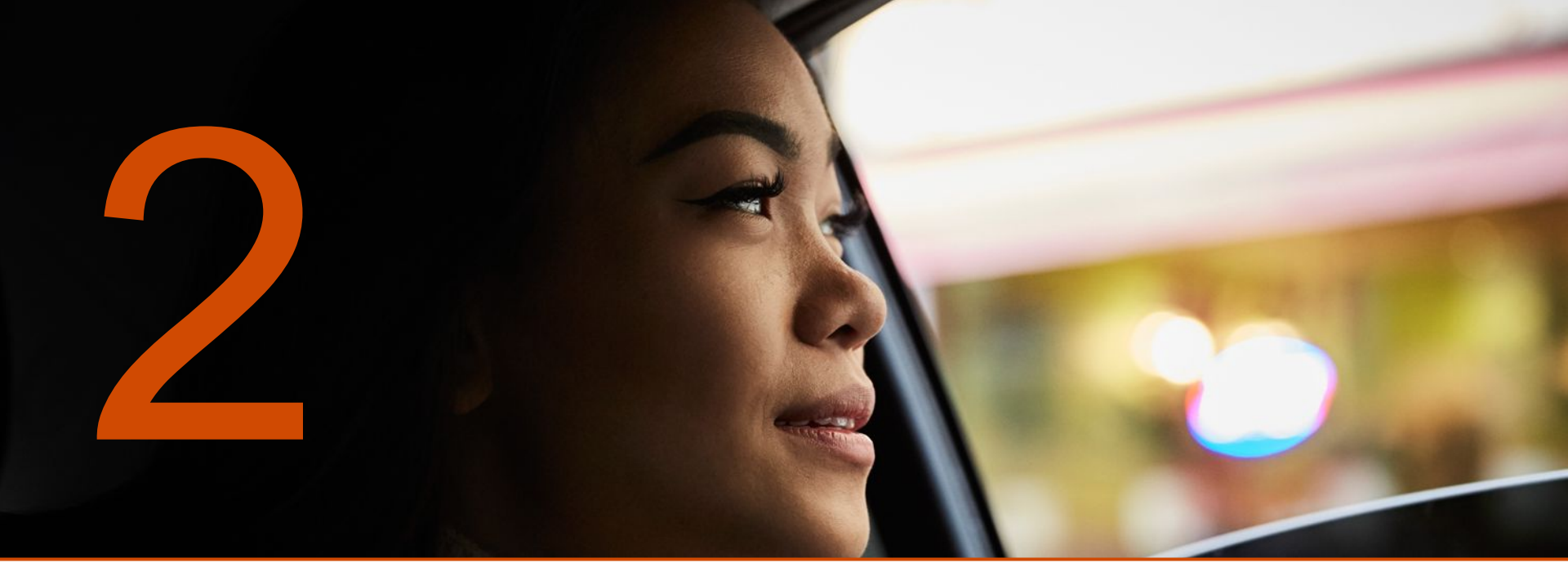
- An analysis of an organisation's network environment and infrastructure.
- Interviews with key IT stakeholders to document the facts of the incident.
- Preservation and analysis of forensic images or 'snapshots' of relevant systems and any log or firewall data.
- Interrogation of log files, system data and incident tickets or logs to establish all of the facts and timelines of the incident.

Incident response and management review

- Evaluating the effectiveness of the response to and management of the incident from both a technical and business perspective and plans, procedures and tools used to respond to the incident.
- Evaluation of the effectiveness of stakeholder and legal management.

What are the benefits?

- Allows organisations to understand why an incident happened and how they can be better prepared in the future.
- Lessons learned from post-incident reviews act as significant catalysts for change in the organisation's security culture, behaviours and processes.
- Provides an opportunity to assess the efficacy of both organisational and security controls in place to prevent, detect, mitigate, contain and recover from incidents.
- Provides concrete lessons and recommendations for improving incident management.



2

Why PwC Cybersecurity?

Why PwC Cybersecurity?

PwC's Cybersecurity practice can help you think more broadly about security and move boldly toward new possibilities

A Winning Alliance

PwC Cyber Portugal, with the support of **PwC Cyber Spain**, consists of more than 300 professionals, leaders in the management of Technological Risks and Cyber Security.

Distributed across 6 different locations, the **PwC Cyber Security Area** is made up of more than 65 Qualified cyber security specialists, with a diverse range of industry experience and strong business acumen to provide business-focused high-quality service. Also, PwC has a Cyber security Lab in Madrid.

It is, moreover, connected and fully integrated into the global Cyber Security team to help the industry combat attacks against **IT and OT environments**.

Also, **PwC has more than 60 cyber-labs across 37 countries**, and our methods and processes stand up to be scrutinized by the courts and regulators. We can put together an integrated plan for information security, helping to secure your assets across different landscapes.

Among all the Cyber security labs mentioned, we have cyber-labs presence and specialists in security, investigation, incident response, and risk services workforce across the globe.

Also, our Clients are able to take advantage of our extensive global knowledge through our **network of experts**, as needed.

+4000 Professionals

Specialised Consultants, Ethical Hackers, Investigators, Technologists, OT Experts, Attorneys and industry Leaders in Cyber Security and privacy.

+60 Specialized Centers

Designed to investigate and analyze the latest trends in threats and Cyber Security technologies, as well as perform the necessary tests.

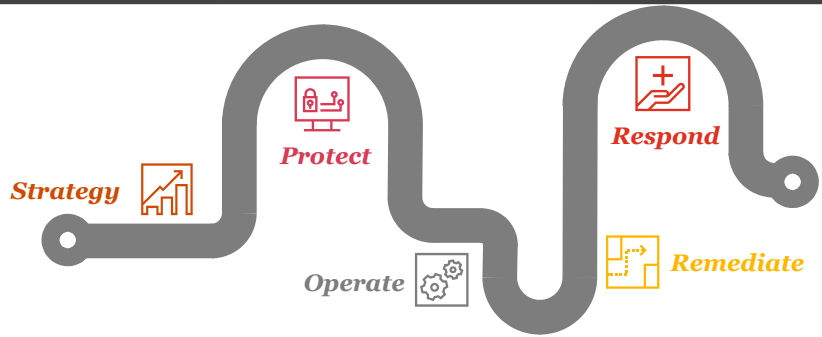
Professional accreditations

Our specialists have **top known Security Certifications** from Top-tier Information Security Associations and Agencies.

Focus on Cyber Security and privacy to achieve your goals

(ISC)² ISACA OFFENSIVE Security EC-Council SANS ISO

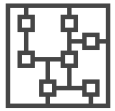
PwC's Cyber Security Approach



Why choose us as your cyber incident response partner?

FORRESTER®

Leader in the Forrester Wave™: Digital Forensics and Incident Response service providers, Q3 2017.
Strong performer in the Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019



As well as a depth of **technical knowledge**, we understand the **business, legal and regulatory context** that underpins your operations.

We have provided **digital forensics and incident response services** in global companies since 1998, among them, we have provided Incident Response and Crisis Management services in the past years.

pwc

We have the knowledge and support of our **global network**.

- PwC UK: Certified by CREST, the industry body for technical cyber security, to deliver cyber incident response services. Also, Certified by the National Cyber Security Centre' Cyber Incident Response (CIR) scheme to respond to sophisticated attacks on networks of national significance.
- PwC US: Awarded NSA's Certified Incident Response Assistance (CIRA) accreditation in 2016.

Thank you.

pwc

Contacts

Miguel Dias Fernandes

Partner
+351 965 354 475
miguel.dias.fernandes@pwc.com

Jorge Sacadura Costa

Senior Manager
+ 351 914 142 752
jorge.sacadura.costa@pwc.com

Rodrigo Perez Monteiro

Senior Consultant
+ 351 918 389 170
rodrigo.perez.monteiro@pwc.com

Cesar Táscon Alvarez

Partner Cybersecurity ES
+34 609 420 773
cesar.tascon.alvarez@pwc.com

Kris McConkey

Partner Cyber Threat Operations UK
+44 (0) 7725 707 360
kris.mcconkey@pwc.com

Yanir Laubshtein

Director Cybersecurity Strategy IL
+972 3 795 4479
yanir.laubshtein@pwc.com

pwc.com