

# Incident Response Services

January 2024



# Table of Content

1. Incident Response Services
  2. Incident Response Retainer
  3. Pricing
  4. Example engagements
- A. Attachments

# Key Contacts



## Michal Wojnar

*Cyber & Privacy Lead*  
M: + 420 724 726 166  
E: [michal.wojnar@pwc.com](mailto:michal.wojnar@pwc.com)



## Marek Nejedly

*Threat Management lead*  
M: +420 735 701 525  
E: [marek.nejedly@pwc.com](mailto:marek.nejedly@pwc.com)

**Hot Line: +420 251 151 050**



# Incident Response Services

# PwC Cybersecurity Incident Response Services

## Pre-Incident Services

### Readiness Assessment

- Structured evaluation of the current status of the preparations
- Analysis of existing playbooks and incident management
- Analysis of past incident reports
- Recording of the IT architecture

### Readiness Services

- Continuous coordination on disruptions and incidents
- Onsite team training (cyber arena, blue team, red team training)
- Ongoing adaptation and updating of the threat situation
- Ongoing optimization of incident management
- Creating playbooks
- Deceptions & purple teaming

## Post-Incident Services

### Live Incident Response and Crisis Management

- Incident coordinator & (crisis) communication
- Intrusion Assessment & Containment
- Analysis & malware analysis support
- Evidence Preservation & Computer Forensics
- Recommendations for action – information security & data protection
- Legal Support

### Post Incident Review

- Research into causes and recommendations for action prevention
- Identification of improvement needs in Incident & Crisis Management
- Preparation of expert opinions for cyber insurance & assessment of the extent of damage
- Derivation of Lessons-Learned
- (Preparation of) reporting to stakeholders

## Incident Response Retainer

# Incident Response Retainer Features

**Our retainers provide global, on-demand, 24 x 7 x 365 access to a specialist cyber incident response team in the event of a cyber incident.**

**Key benefits include:**

- A rapid and effective response to reduce the impact of an incident, with no need to onboard a provider whilst under duress, which could delay your response.
- Preparation of relevant plans, documentation and a maturity roadmap for IR maturity.
- Customisable service agreements to suit your specific business requirements.
- Availability of relevant reporting and data to demonstrate compliance to stakeholders and regulators
- Access to a wide-range of cyber security, forensic, business advisory and legal counsel – all of whom are experienced in working closely together in times of crisis.

**Our incident response retainers include:**

- 1 Initial and ongoing workshops** to understand your business, IT infrastructure, and existing incident response policies and procedures, and ensure an effective response.
- 2 On-site and remote response SLAs.**
- 3 Multiple escalation channels** including a 24/7 emergency response telephone hotline.
- 4 Real-time virtual communication** with our incident response team to ensure we are an extension of your team, and not just another service provider.
- 5 Crisis preparedness and management support** where it is needed, from board-level to first-responder teams.
- 6 Access to our customised incident reporting** templates, and a range of other resources.
- 7 Unused retainer hours can be used** on readiness exercises and select set of cybersecurity advisory services, to maximise your return on investment.
- 8 Rapid access to a range of additional cyber security services** (including threat intelligence and threat detection) to inform wider security strategy.

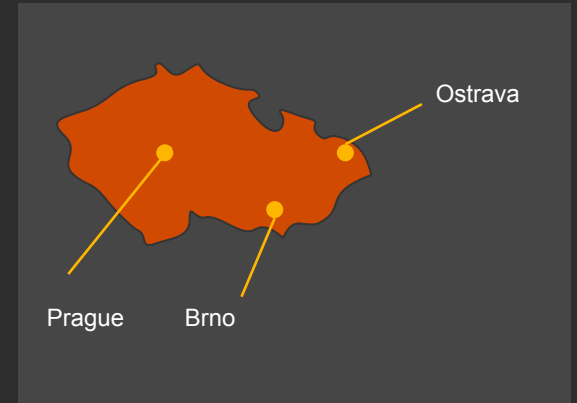
# Global PwC capabilities driven by the local team

We are structured to bring our global expertise, deep technical experience, industry specializations and technology partnerships to every incident response case. We offer this service through our local and easily accessible team in Prague, Brno, Ostrava & Warsaw, who can be contacted with a single phone call, email or chat message via the defined communication platform.

Local PwC contacts will work with your local teams to understand the specific challenges. In this way, we ensure that security incidents can be adequately dealt with at each individual location. In preparation, methods for cooperation are coordinated and incident response processes are tested.

Our colleagues respond to every security incident request promptly. Our IR call center takes your inquiries 24x7. Our incident response experts will be at your site as quickly as possible. Specific SLAs can be customized based on your requirements.

Our professionals, handpicked from the military, law enforcement, and security services, have years of experience identifying and responding to a range of incidents on some of the world's most sensitive networks. Our security experts were part of NATO Locked Shield exercise where they achieved 3rd place across NATO countries.



The PwC network is present almost worldwide: Our 721 locations are spread over 158 countries with over 250,000 people.



PwC has more than 650 IT forensic, incident response and threat intelligence professionals and more than 60 IT forensic labs worldwide.



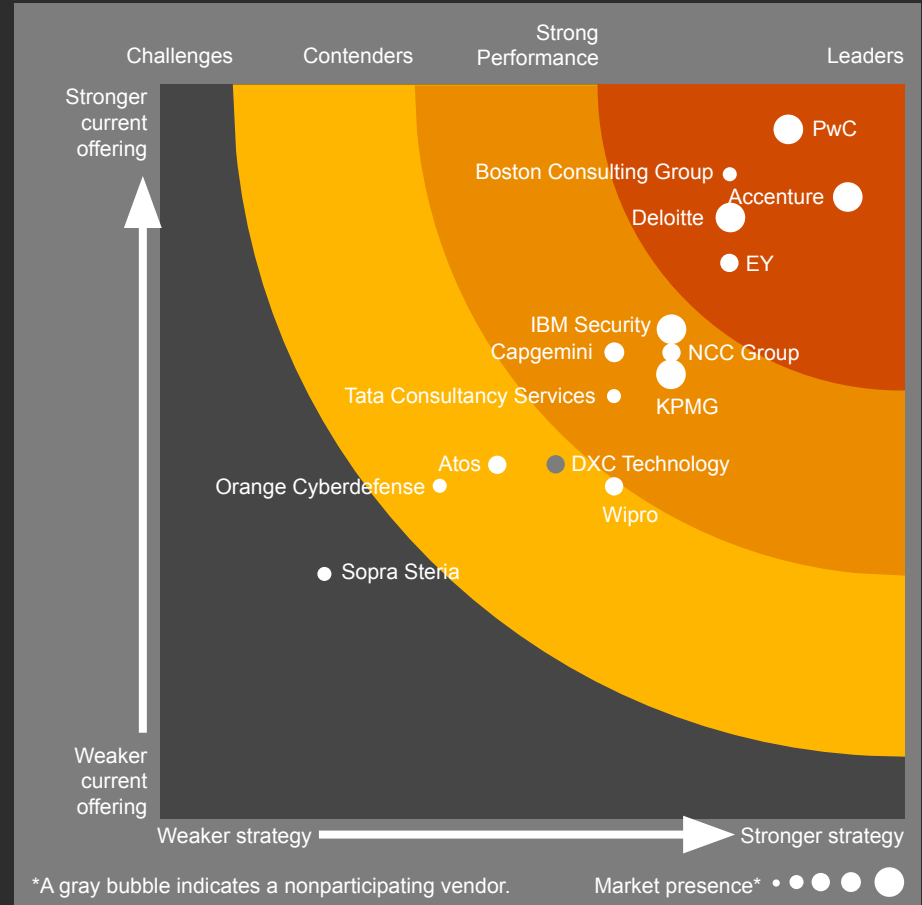
PwC IR team is certified for ISO 9001, TISAX and ISO 27001.

Members of our team hold various cybersecurity certifications (SANS, CISSP, OSCP, CEH) and members of GIAC Advisory Board.

# Top European Cybersecurity Consulting Providers Q3 2021

## According to Forrester, what distinguishes PwC?

- PwC convinces with highly qualified and targeted support for executives for cybersecurity: With the exclusive CISO Masterclass program, PwC supports your CISO in growing into his new leadership role.
- PwC invests in the development of tools and applications in the areas of DevSecOps, Cyber Threat Intelligence and Incident Response, which are made available via a SaaS platform.
- PwC promotes the technical development of its consultants efficiently and practically, thereby ensuring an experienced pool of consultants.
- Clients who rely on both strategic executive-level support and highly qualified technical skills are well served with PwC.



# PwC CEE – Digital Forensics & Incident Response

## Our team

Our incident response team includes cybersecurity incident experts and computer forensics experts. As part of our Incident Response Retainer, PwC offers support in preparing for a security incident, dealing with an emerging security incident and conducting IT forensic evidence preservation and analysis. Below is a representation of our Incident Response Retainer core team. If necessary, this is supported by other experts from the areas of IT security, information security, data protection and forensics as well as our lawyers.

The Incident Response Retainer core team has skills in **Incident Response Services, Crisis Management, and IT Forensics.**

### Cyber & Privacy Team



**Michal Wojnar**  
Cyber & Privacy  
Director



**Marek Nejedlý**  
Threat  
Management  
lead



**Jan Banasiak**  
L3  
Prague

Incident Response  
Services



**Martin Ročák**  
L2  
Prague



**Ivana Mišová**  
L2  
Brno



**Josef Pindřák**  
L2  
Prague

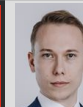


**Stanislav  
Mogilevtsvev**  
L2  
Prague

### Forensic Services Team



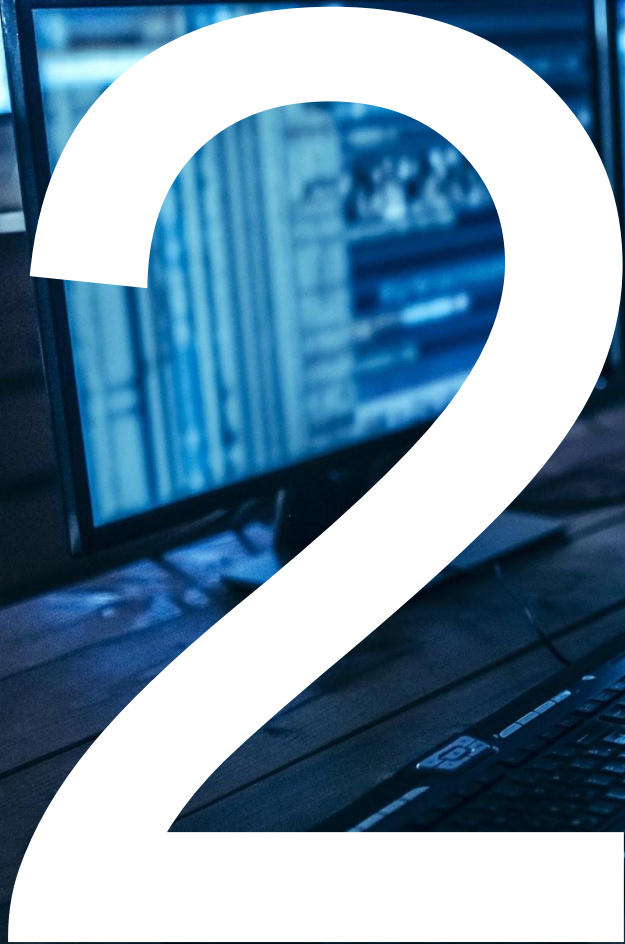
**Jakub Javorský**  
Head of  
Forensics



**Oliver Waczulík**  
L3  
Praha

Forensic Technology  
Services



A large, white, stylized number '2' is positioned on the left side of the image. The background is a dark, blue-toned photograph of a person working at a desk with multiple computer monitors. The person's hands are visible on a keyboard. The overall atmosphere is professional and tech-oriented.

# 2

## Incident Response Services

Rapid access to expertise  
when you need it most



# Incident Response Retainer | Readiness and Rapid Model

|  |   |   |   |
|--|---|---|---|
| <p><b>EUR 99,- / 120,- / call</b><br/>for basic*</p> <p><b>EUR 999,- / Month</b><br/>for Readiness</p> <p><b>EUR 2,499,- / Month</b><br/>for Rapid</p> | <p><b>Incident Readiness</b></p> <ul style="list-style-type: none"> <li>Annual incident management workshop</li> <li>Annual architecture workshop</li> <li>5 (readiness) -15 (rapid) of days of specialized resources in a retainer format</li> <li>Annual management report with recommendations based on incidents</li> </ul>   |   |   |
|  | <p><b>First Response - Remote Support</b></p> <ul style="list-style-type: none"> <li>24/7 on-call service from Czech Republic as SPOC (single point of contact)*</li> <li>Recording of the incident</li> <li>Allocation to specialists (second level)</li> <li>Initial analysis of the incident together with the customer &amp; presentation of the next steps</li> <li>Readiness: reaction time within 4 hours (Monday-Friday 9am-5pm)</li> <li>Rapid: reaction time within 1.5 hours (Monday-Sunday 0-24)</li> </ul> | <p><b>Incident Handling &amp; Coordination</b></p> <ul style="list-style-type: none"> <li>Assessment of the impact</li> <li>Task distribution and coordination with the customer's specialists and our experts</li> <li>Reporting to stakeholders</li> <li>Support of involved departments</li> <li>On-site the next working day (Monday-Friday) within the Czech Republic</li> <li>On-site the next working day (Monday-Friday) within the Czech Republic</li> </ul> | <p><b>Computer Forensics &amp; Security Expertise</b></p> <ul style="list-style-type: none"> <li>Performs forensic data backup and analysis</li> <li>EDR-based threat hunting capability</li> <li>Cause research and reconstruction of the incident.</li> <li>Security testing of measures</li> <li>Specialists for specific systems</li> <li>Access to PwC Threat Intelligence and OT Security Competence Center</li> <li>Log file analysis</li> <li>Malware analysis</li> </ul> |
|  | <p>*Only if the call is outside of Monday – Friday 9am-5pm. Otherwise it's free.</p> <p><b>Reduced readiness fee rates in incident response cases, external communication and data exchange platform, detection techniques and sandbox technology on demand</b></p>   |   |   |

The prices and services shown are merely a structured representation of typical Security Incident Response services and not a binding offer. Despite the monthly flat rates, this is an annual service (12 months). You can switch between the Readiness and Rapid models once a year.

# Incident Response Retainer Selections

We offer the three essential Incident Response characteristics of speed, effectiveness and expertise in different forms.

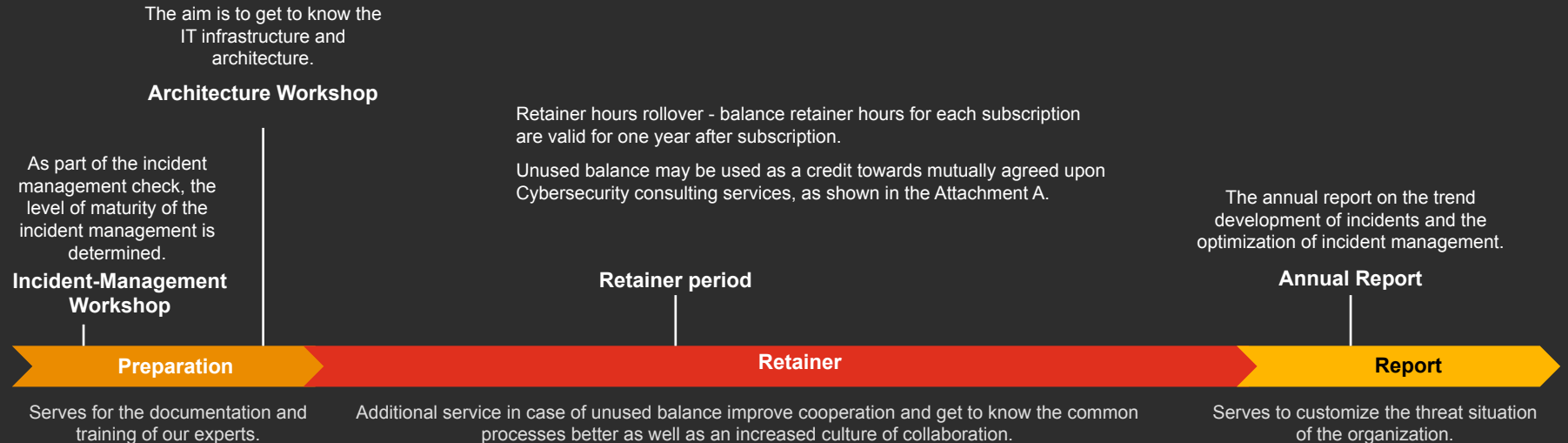
|           |                                 | 1 Speed  |  |                              | 2 Effectivity  |  |   | 3 Expertise  |
|-----------|---------------------------------|--|--|------------------------------|--|--|---|--|
|           |                                 | 24/7 Incident Response Hotline*                |  |                              | Incident Readiness & Annual Report                   | Collaboration                            | Retainer  |  |
|           |                                 | Remote Support                                 | Onsite Support   | Rate Card                    |  |  |   | Scalable number of SANS certified digital forensic and incident response experts (Malware Analysis, Threat Intelligence, OT, etc.) |
| Basic     | Free with framework agreement.* | Remote support within best effort              | On-site support based on best effort<br>Base by day rate | Standard                     | Not Included   | Not Included                             | Not Included  | Quality and security standards (ISO 9001, 27001, TISAX)  |
| Readiness | EUR 999 monthly                 | Remote support within 4h (Monday-Friday 9-17h) | Next business day onsite support (CZ+SK)                 | Reduced (retainer rate card) | Two workshops to review Incident Mgmt & Architecture | Communication and data exchange platform | Bank of 5 MDs used for first response or rollover for consulting  | Holistic expertise from a single source (legal, privacy, crisis management, business risks)  |
| Rapid     | EUR 2,499 monthly               | Remote Support within 1,5h (24x7 Operations)   | Emergency on-site support within 12 hours (CZ+SK)        | Reduced (retainer rate card) | Same as Readiness                                    | Same as Readiness                        | Bank of 15 MDs used for first response or rollover for consulting |  |

\*EUR 99 business hours / 120 EUR for a call outside of Monday – Friday 9am-5pm.

# Incident Response Retainer Model

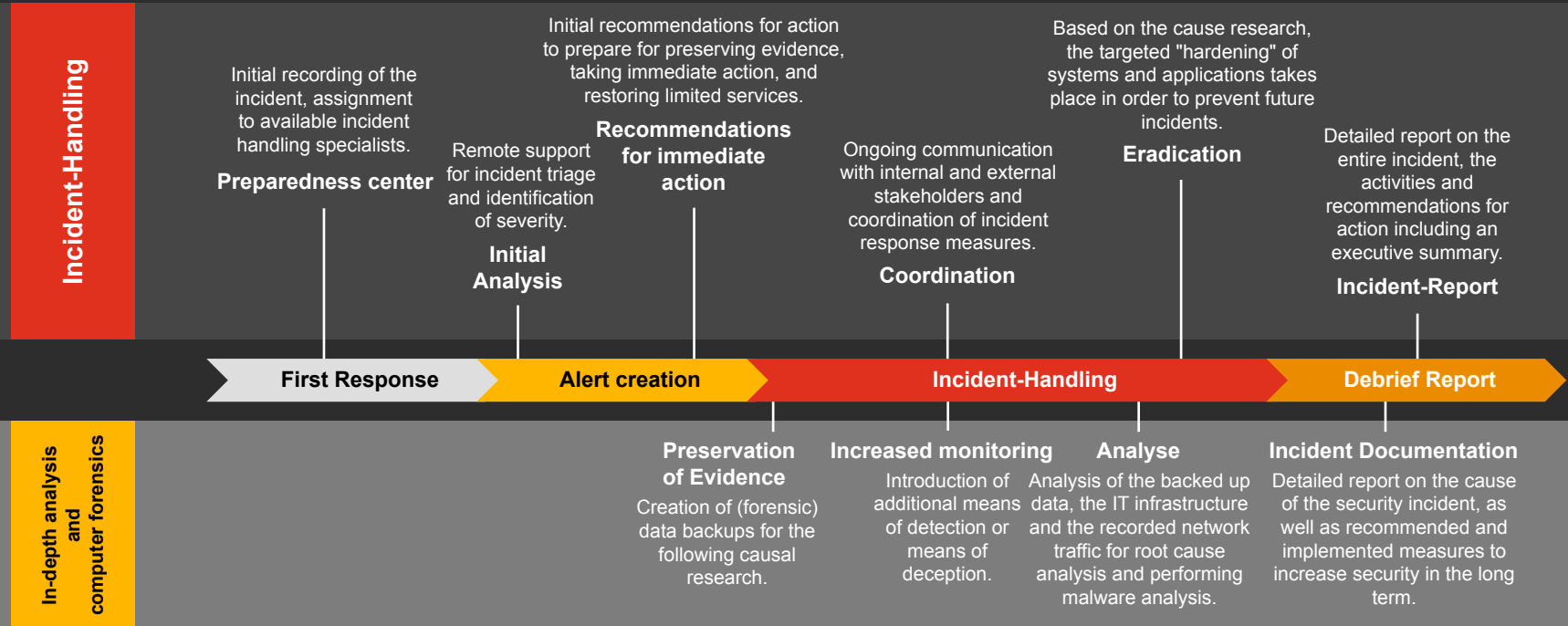
## A year without significant events

We support you in a sustainable and continuous improvement of your incident management in order to be able to react optimally to current threats.



# Live Cybersecurity Incident Response and Crisis Management

## Typical example

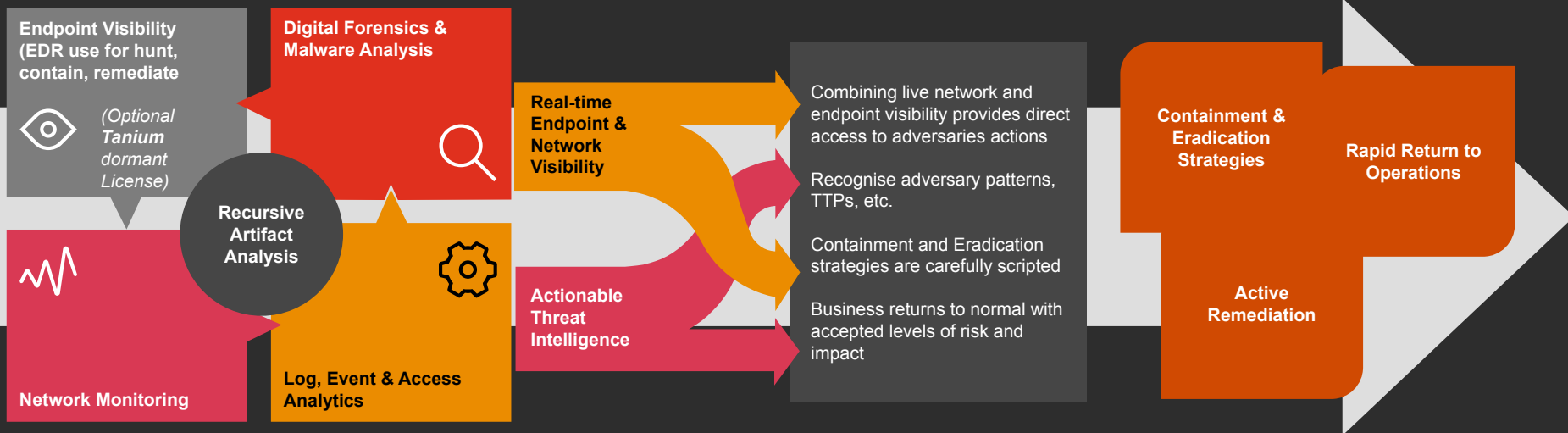


# Incident response technology

## Technical analysis, response and remediation

In the event of an incident we will **fully support you throughout response and recovery**, in order to **minimise and mitigate damage** to systems and data, and **minimise business risk**. Our **procedures are grounded in industry best practice**, and years of practical experience. For 'live' incident response investigations (e.g. network intrusions), our general practice is to follow the NIST Computer Security Incident Handling standard closely, deviating only when we know it is necessary.

Our technical analysis, response, and remediation activities are aligned with your processes and procedures (i.e. Cyber Security Incident Response Management and Cyber Security Crisis Management plans).



# 3

## Pricing and Assumptions



# Fee rates and expenses for incident response retainers

| Level                       | Incident Response Retainer Rate Card   |                | Incident Response Rate Card      |                  |
|-----------------------------|--|----------------|----------------------------------|------------------|
|                             | Reduced IR fee rates (readiness, rapid)  |                | Standard IR Fee Rates (basic)    |                  |
|                             | Hourly Rate  | Daily Rate(8h) | Hourly Rate                      | Daily Rate(8h)   |
| Head of IR / Forensics (SM) | EUR 225  | EUR 1,800      | EUR 325                          | EUR 2,600        |
| IR / Forensic Expert (M)    | EUR 181  | EUR 1,450      | EUR 280                          | EUR 2,235        |
| L3 - Senior S2.3            | EUR 125  | EUR 1,000      | EUR 163                          | <b>EUR 1,300</b> |
| L2 - Senior Associate       | EUR 94   | EUR 750        | EUR 119                          | EUR 950          |
| L1 - Associate              | EUR 69   | EUR 550        | EUR 88                           | EUR 700          |
|                             | <b>IR Hotline EUR 99 / call</b>  |                | <b>IR Hotline EUR 120 / call</b> |                  |
|                             | <b>EUR 999 / Month</b> <sup>for Readiness</sup><br><b>EUR 2,499 / Month</b> <sup>for Rapid</sup> |                |                                  |                  |

The prices and services shown are merely a structured representation of typical security incident response services on an annual basis and are not a binding offer. A 100% surcharge will be added to the rates shown for night hours (7:00 p.m. to 7:00 a.m.), public holidays and weekends.



# Assumptions



You warrant that you have all necessary rights or approvals to let us do the work and to use all such systems and information in connection with the performance of the Services.

You agree that to the extent you do not meet your obligations and this affects our ability to perform our obligations, we are relieved of such obligations.

## Your responsibilities

Our role is advisory only. You are responsible for all management functions and decisions relating to this engagement, including evaluating the scope of the Services and determining that it meets your needs. You are also responsible for the results of using the Services or Deliverables, and for establishing and maintaining your internal controls. You will designate a competent member of your management to oversee the Services.

Where you are using third parties in connection with the Services, you are responsible for contracting with them. You will be responsible for the management of those third parties and the quality of their input and work unless we agree otherwise.

## You will provide us with:

- Use of and access to all your systems and other necessary resources which we reasonably need to perform the Services;
- Access to and support of qualified staff members; and
- Accurate, reliable and timely information we may reasonably request about your systems required for us to perform the Services;
- You will be responsible for the provision of information relating to existing policies, plans or procedures, IT and security infrastructure and any other information we require to perform our tasks. This will also include access to your personnel who are able to advise on network and systems architecture. You will also be responsible for arranging any access required to third party systems or IT environments for us to perform our tasks;
- You recognize that delivery and execution of this service is upon a request, on-demand bases which
- will be determined by security event specifics; and
- Accept that remote or on-site execution will be upon an agreement reflecting current case confirmed by phone call & e-mail

# Assumptions

## Initial onboarding

We will conduct yearly onboarding and coordination sessions for the length of the contract.

### **Onboarding Sessions will involve the following activities:**

- A inventory of technologies, processes and solutions available for use in crisis management
- Discussion with you based on the provided inventory to define and provision access to required solutions to enable our incident response team
- Definition of Service Level Objectives for our incident response team, based on
- Alignment of our response plans and existing processes, to align with the following processes:
  - Cyber Security Incident Response Management
  - Cyber Security Crisis Management

## Third Party Access and Confidentiality Agreement

We will review and sign fortune entertainment group's Third Party Access and Confidentiality Agreement if selected, subject to our internal legal review and approval of the terms and conditions of the agreement

# Assumptions



You warrant that you have all necessary rights or approvals to let us do the work and to use all such systems and information in connection with the performance of the Services.

You agree that to the extent you do not meet your obligations and this affects our ability to perform our obligations, we are relieved of such obligations.

## Your responsibilities

Our role is advisory only. You are responsible for all management functions and decisions relating to this engagement, including evaluating the scope of the Services and determining that it meets your needs. You are also responsible for the results of using the Services or Deliverables, and for establishing and maintaining your internal controls. You will designate a competent member of your management to oversee the Services.

Where you are using third parties in connection with the Services, you are responsible for contracting with them. You will be responsible for the management of those third parties and the quality of their input and work unless we agree otherwise.

## You will provide us with:

- Use of and access to all your systems and other necessary resources which we reasonably need to perform the Services;
- Access to and support of qualified staff members; and
- Accurate, reliable and timely information we may reasonably request about your systems required for us to perform the Services;
- You will be responsible for the provision of information relating to existing policies, plans or procedures, IT and security infrastructure and any other information we require to perform our tasks. This will also include access to your personnel who are able to advise on network and systems architecture. You will also be responsible for arranging any access required to third party systems or IT environments for us to perform our tasks;
- You recognize that delivery and execution of this service is upon a request, on-demand bases which
- will be determined by security event specifics; and
- Accept that remote or on-site execution will be upon an agreement reflecting current case confirmed by phone call & e-mail



# Example of Incident Response Projects

| Type of engagement                | Client Anonymized Description              | Client Challenge   | What did we do   | Year |
|-----------------------------------|--|--|--|------|
| <b>Incident Response Retainer</b> | <b>International Logistics corporation</b> | Client had a major security incident and wanted to rebuild the environment and become security focused organization. | We rapidly deployed our TDR services after cybercriminal group encrypted 200 servers. PwC employed a powerful cybersecurity platform for security monitoring and threat hunting. Our service became a part of the Cyber Security program advisory focused on rebuilding the environment.           | 2023 |
| <b>Incident Response Retainer</b> | <b>International Retail Chain</b>          | Client had a security incident related to Ransomware from a threat actor DarkSide.                                   | We supported global PwC IR activity and together with forensics acquired the potential patient zeros. We performed security analysis which revealed root cause of the incident and helped with containment and remediation activities  | 2021 |
| <b>Global SOC</b>                 | <b>Global Fortune 500</b>                  | On-going monitoring of client environment and regular incident response activity                                     | We are providing Security Operation Center services for this client for over 3 years, and we were part of two major incidents involving human operated attackers. We were able to stop the attackers from achieving their objectives, find the root causes and assist with remediation activities. | 2023 |



# Attachments

```
    .parentNode.insertBefore(e,p)})(window.document,'script','@');
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
```

# Ransomware-specific Workshops

| Executive Workshop<br>incl. VR-Session   |                              | Ransomware<br>Experience Sharing  |                         | Ransomware Maturity<br>Assessment   |                              | Table-Top Exercise  |                         | Breach & Attack<br>Simulation   |                              |
|--|------------------------------|---|-------------------------|---|------------------------------|---|-------------------------|---|------------------------------|
| <p>We give your top executives an immediate cyber crisis experience using virtual reality.</p> <p>Workshops aimed directly at management have great advantages. In personal discussions, individual topics and questions regarding ransomware are given sufficient space and answers by our cybersecurity experts.</p> |                              | <p>We discuss hands-on lessons learned from ransomware attacks with your business stakeholders and technicians</p> <ul style="list-style-type: none"> <li>→ Pay or not pay?</li> <li>→ Legal restrictions</li> <li>→ How to communicate with the blackmailers</li> <li>→ Crypto payments</li> <li>→ Backup Lessons Learned</li> <li>→ Preparations for emergencies</li> </ul> |                         | <p>In order to find out in which areas of the company you are well prepared against ransomware attacks and where you still have to catch up, technical and organizational measures based on the NIST Cybersec Framework are checked.</p> <p>Specific and prioritized recommended measures help to increase resilience where it is most urgently needed.</p> |                              | <p>Simulating events allows the company to practice "Day X".</p> <p>Depending on the requirements, different levels in the organization are subjected to a business game.</p> <p>To practice precautions and subject them to a stress test.</p> |                         | <p>With the help of "MITRE CALDERA" &amp; our unique demo, we show you how quickly an attacker compromises domain and encrypts data.</p> <p>Breach &amp; Attack Simulations feature scripted and simulated attacks on our live infrastructure to show how to detect and respond to threats.</p> |                              |
| Preparation effort:<br>small amount  | time expenditure:<br>2h - 4h | Preparation effort:<br>small amount   | time expenditure:<br>4h | Preparation effort:<br>small amount   | time expenditure:<br>2d - 5d | Preparation effort:<br>small amount   | time expenditure:<br>6h | Preparation effort:<br>small amount   | time expenditure:<br>1d - 3d |
| Technical environment:<br>none   | Budget:<br>small amount      | Technical environment:<br>none  | Budget:<br>small amount | Technical environment:<br>none  | Budget:<br>medium            | Technical environment:<br>none  | Budget:<br>small amount | Technical environment:<br>Demo IT   | Budget:<br>medium            |

# Portfolio of related services

## 1. Cyber risk profile, key threats and critical assets

- Advice on **cyber risk profile** and potential **breach impact** (business operational risk, reputational risk, regulatory and compliance risk).
- Consult on **key cyber threats** relevant to client industry and **common techniques** adversaries use (insiders, nation-state, cybercriminals).
- Assist in identification and prioritization of **critical & high value assets (systems/data)** („*crowns jewels*“) and assessing value at risk.

## 2. Incident Response Plan

**Assess readiness, design and test incident response plan** („IR Playbook“) that will include step by step **technical and management guidelines** for specific incidents:

- roles and responsibilities
- incident handling process
- breach analysis and impact assessment
- communication plan (internal and external)
- cooperation with third-parties
- crisis management and regulatory aspects

## 3. Cyber Crisis Simulation

Run a **tabletop exercise** in which key client personnel (executive team and technical team) are gathered to **face a simulated but realistic cyber-attack scenario**.

The **cyber crisis simulation** is facilitated by PwC and is aimed to **rehearse client's response capability** to cyber-attack in a safe learning environment.

The exercise increases ability and agility in responding to incidents and effective recovery.

## 4. Compromise Discovery

Targeted threat actors often maintain remote access to client environment long time before being detected.

As part of **proactive threat detection** we will look for **indicators** of current and/or past **compromises** and **malicious activity** at clients' infrastructure.

The main client benefit is an **early detection of breach or threats that have not yet resulted in a data breach** but requires management action.

## 5. Threat Hunting

▪ Advice on client **practices for threat hunting** and suggesting improvements.

▪ **Co-source of experienced threat hunters** (L2/L3) searching proactively for threats and unusual patterns, performing structured threat hunting analyses.

▪ Performing **targeted hunting to analyze and respond to changes in threats** (e.g. driven by intelligence on new attack campaigns and techniques).

## 6. Incident Response

PwC incident response teams will help clients **to analyze, understand, contain and minimize the impact of a security breach**.

Our assistance will include **initial analysis** and triage, **assessment of the scope** of incident, advice on **mitigation and crisis management** activities (including forensics, legal, regulatory reporting and PR support) and helping with the recovery/remediation.



# PwC Cybersecurity und Privacy Portfolio

We build trust in a digital world



Information  
Security & Privacy



Cloud, PAM & OT Security



Awareness & Culture



Threat Management & Incident  
Response



# Thank you

We build trust in a digital world

[pwc.com](https://www.pwc.com)

© 2022 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.