www.pwc.ch

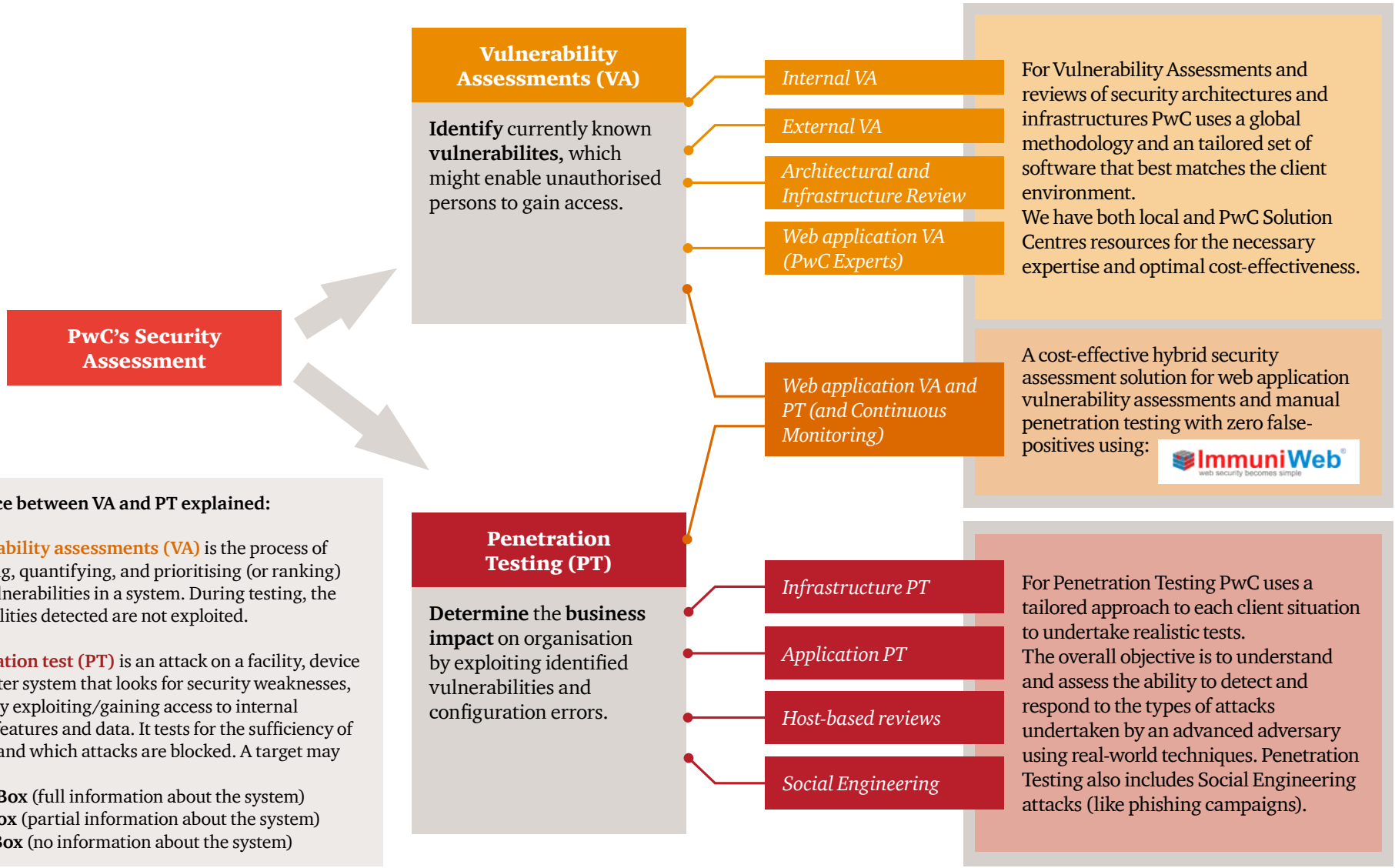
PwC's Advanced Threat and Vulnerability Management Services

Our comprehensive approach

pwc

PwC's security assessment services

A joint business relationship provides clients with access to High-Tech Bridge's innovative web security platform ImmuniWeb® for external web application assessments together with PwC's market leading **Threat and Vulnerability Management** services.



Difference between VA and PT explained:

A **Vulnerability assessments (VA)** is the process of identifying, quantifying, and prioritising (or ranking) all the vulnerabilities in a system. During testing, the vulnerabilities detected are not exploited.

A **Penetration test (PT)** is an attack on a facility, device or computer system that looks for security weaknesses, potentially exploiting/gaining access to internal systems, features and data. It tests for the sufficiency of defences and which attacks are blocked. A target may be a:

- **White Box** (full information about the system)
- **Grey Box** (partial information about the system)
- **Black Box** (no information about the system)

Case study – combined PwC cyber risk assessment with ImmuniWeb® hybrid security assessment

PwC delivered a IT Security Risk assessment based on the ISO27001 standard for a Swiss luxury company illustrating the combination of our cyber-risk assessment approach and utilising **High-Tech Bridge's ImmuniWeb® web security testing platform**. Our approach consisted of the following three phases:

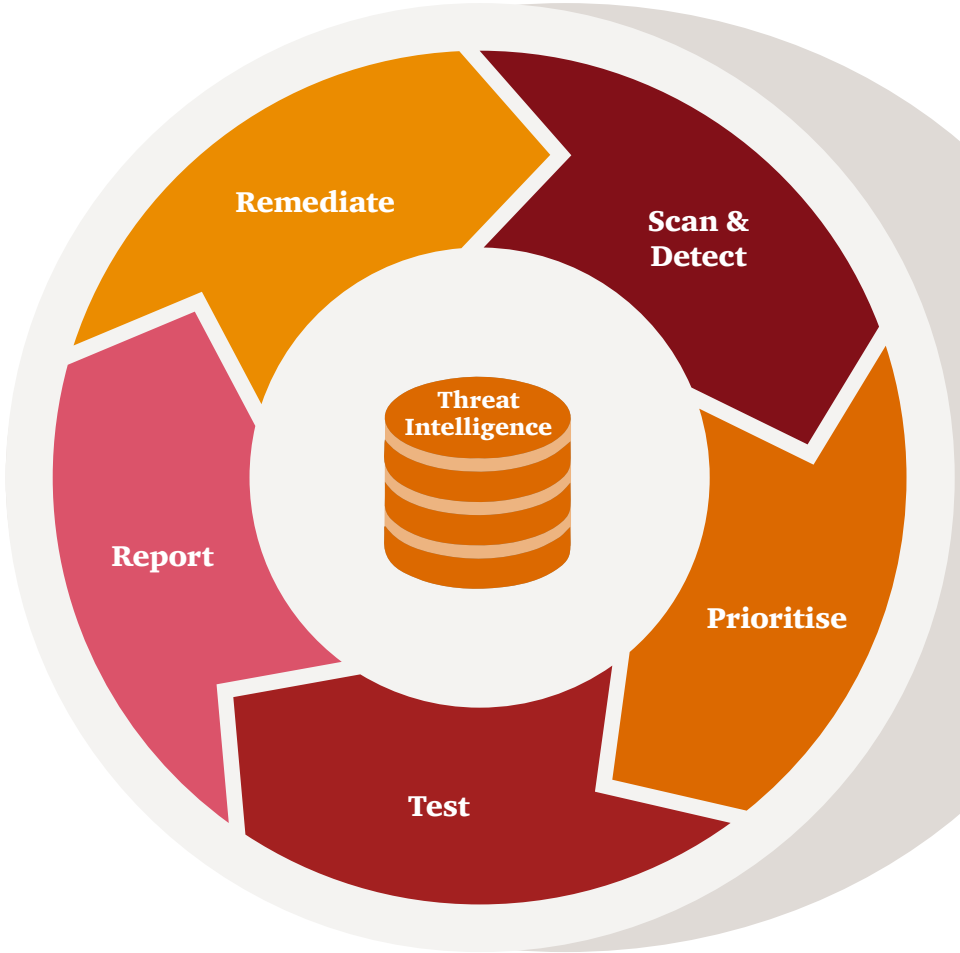
1. **A cybersecurity risk assessment was completed** covering all the client's main information assets and data, to identify the key risks to the client's information systems and to achieve a maturity benchmark based on international standards. We identified the key information assets that were prioritised first, for the implementation of new security controls within the organisation, and we performed a review of the client's information security risk management processes and activities.

2. **An assessment of the client's information security controls was completed** to evaluate both the design and the operational effectiveness of the internal controls. We identified the key controls and activities within the following domains: access control, human resources security, asset management, operations and communications security, supplier management, change management and compliance. In addition, to the internal controls testing, we used ImmuniWeb® to conduct a comprehensive vulnerability assessment and to perform manual application logic and authentication testing over the client's web application. Based on this vulnerability assessment and our own testing, we reported all the observations and made recommendations for improvement to the client.

3. **An information security roadmap was then developed** to plan and organise the remediation of the information security controls, based on the results of all the tests performed.

PwC's Threat and Vulnerability Management (TVM) Framework

PwC provides a holistic, cost effective and business focused Threat and Vulnerability Management (TVM) service, enabling our clients to focus on the key risks to business operations and the information assets that matter.



Tailored Risk Profile: Our Threat and Vulnerability Management (TVM) service approach is based on a tailored risk profile.

Scan & Detect: To detect vulnerabilities we scan our clients networks and systems both internally and externally.

Prioritise: We prioritise the detected findings in order to focus our efforts on the most severe vulnerabilities.

Test: Based on the prioritised list of findings we create both test strategy and plan and execute the agreed tests.

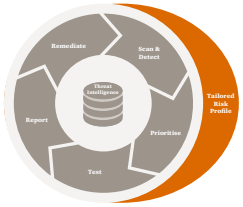
Report: A report summarises our activities and the most essential test results and makes them tangible for a management audience.

Remediate: In cooperation with our clients our team of experts remediates the detected vulnerabilities.

Threat and Vulnerability Management Services

"We have approximately 6,000 vulnerabilities in our applications. Every year we fix about 1,000 and we find another 1,000. The question is: are we finding and fixing the right ones?"

CIO, large financial services organisation



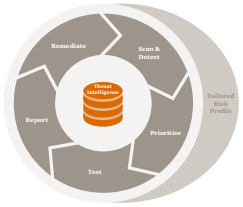
Tailored risk profile

Every organisation has to identify and then protect its own information assets and also has to cope with specific cyber risks depending upon the industry in which it operates and the types of data it collects, processes and stores. For example, this could cover all or any of the following: intellectual property, personal customer/business customer records or credit/debit card data and manufacturing and production systems using industrial control systems.

Therefore, a “one size fits all” cybersecurity assessment will inevitably fail to address the real “value at risk” to the organisation. A Cybersecurity Assessment has to take these differences between organisations and industries into account.

To cope with the characteristics of each organisation and in order to provide the most value, our approach includes tailoring the approach over threat and vulnerability management to be focused on the specific higher risk information assets. This tailoring consists of the following phases:

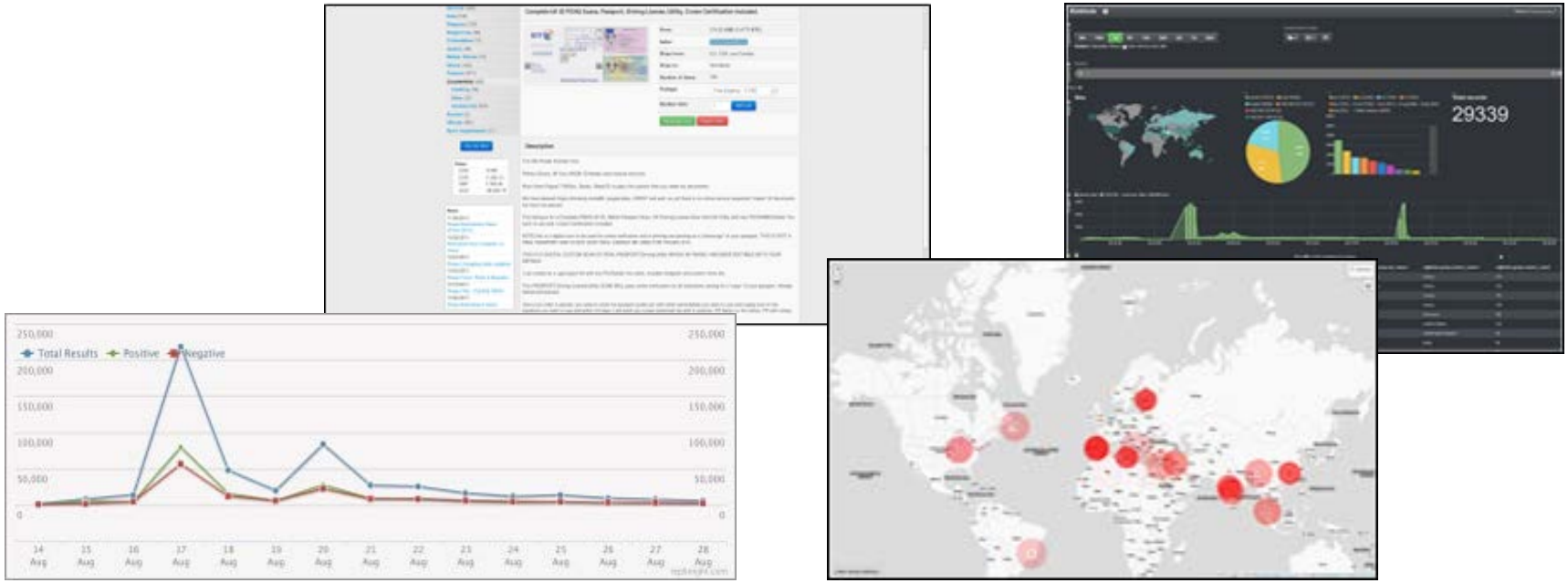
Scoping	Business impact assessment	Threat Profile
• Develop an understanding of the characteristics of the organisation as a whole and of the environment to be assessed • Define and agree the scope of the environment to be assessed	• Assess potential business impact to an organisation should information assets be compromised	• Profile and prioritise all threats that are relevant to the environment being assessed • Identify the potential ways that the highest priority threats could manifest to cause harm to the environment being assessed

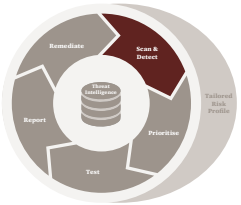


Threat intelligence

At the heart of our TVM Framework is our Threat Intelligence Fusion Centre (TIFC). Many companies are challenged to understand which threat actors might be targeting their resources, personnel, data, facilities, partners, and other crown jewels. Our proactive, threat actor-focused approach can enable organisations to increase their understanding of the threats they face and help them to rate their findings and prioritise their TVM activities.

Through our incident response engagements, full time research team, participation in invite-only trust groups and private information sharing arrangements with select third parties, we collect, enrich and distil a significant volume of technical data associated with targeted threat actors. In addition, we have the ability to identify the victims associated with specific command and control domains via our sinkholing infrastructure.





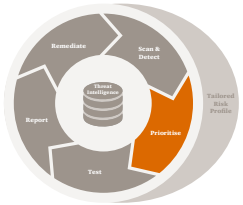
Scan & detect vulnerabilities

By using different vulnerability scanning approaches we help our clients to identify currently known vulnerability and configuration errors on network, operating system, database, and application level which might enable unauthorized persons to gain access.

We can perform an internal network vulnerability assessment of internal IP ranges provided by a client with different tools and scanning applications. All internal based vulnerability assessment activity will be performed from the point of the view of an unauthenticated user with the aim to only identify network level vulnerabilities and issues. Such an assessment can also be completed from an external, and internal (DMZ, Intranet) point of view as well as on applications, a WASA (a web application security assessment). We can do this with tools that PwC has acquired, or help you to acquire and configure the tool you have selected.

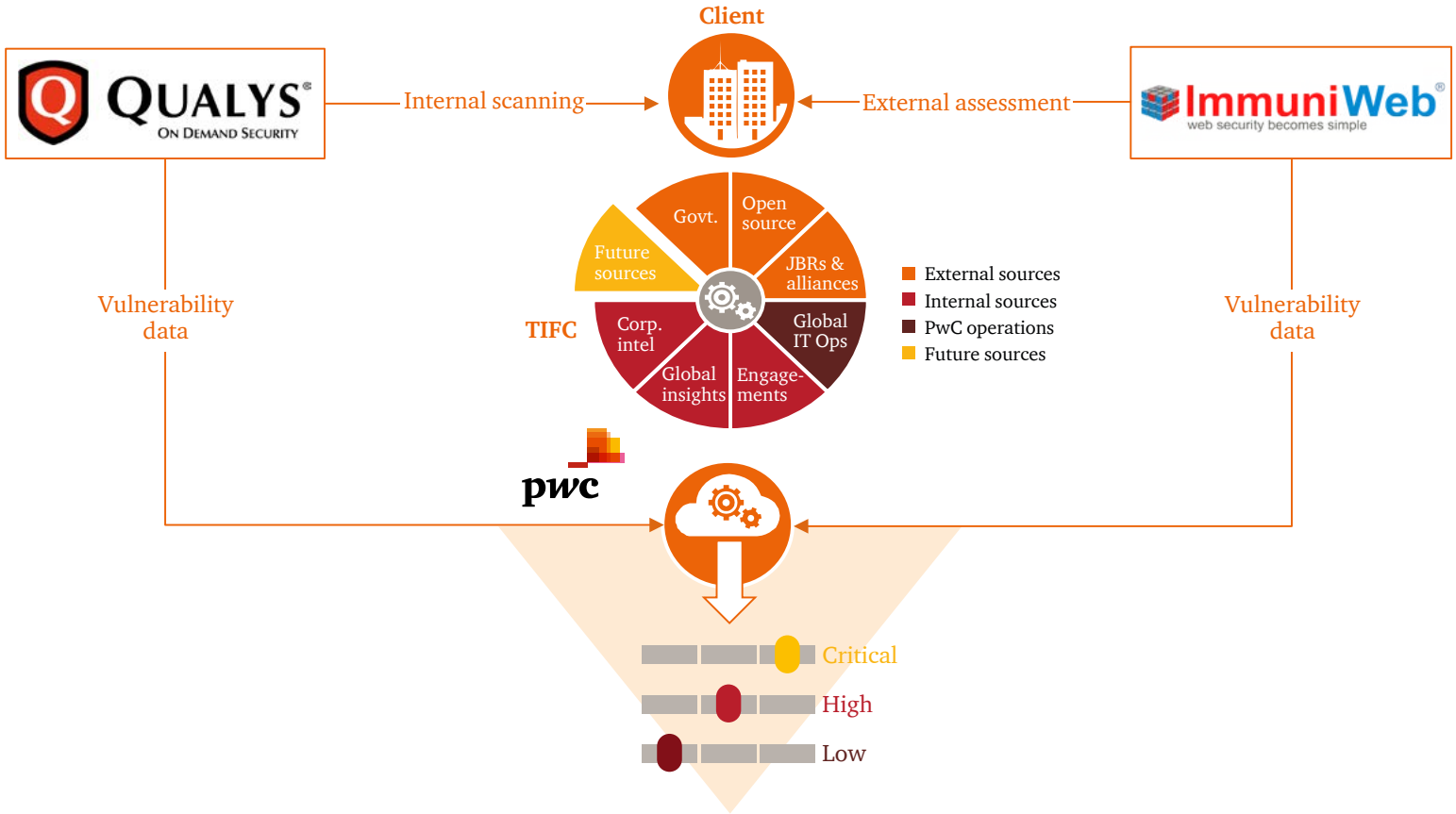
To minimise the risks of vulnerable systems being compromised, vulnerability assessments should be run regularly. Good practice is to deploy vulnerability scanning software and scan for vulnerabilities on a continuous basis. To help our clients achieve this we can deploy the appropriate technology, processes and training to enable our clients to perform ongoing vulnerability assessments.

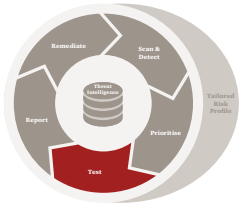
ImmuniWeb® web security testing platform, from our business partner High-Tech Bridge, is an example of a hybrid solution to carry out managed vulnerability scanning in parallel with advanced manual testing on continuous or on-demand basis.



Prioritise vulnerabilities

The prioritisation of vulnerabilities and elimination of false-positives is a critical step to focus further testing activities on vulnerabilities that are substantial and might represent a considerable risk for the business. The illustration below shows an example architecture using **Qualys** for internal scanning and ImmuniWeb® for external penetration testing and managed vulnerability scanning. The incorporation of our **Threat Intelligence Fusion Centre (TIFC)** service is essential for the prioritisation of the obtained vulnerability data and means we can enrich your vulnerability exposure picture by basing the findings on risk, not just severity.





Security testing

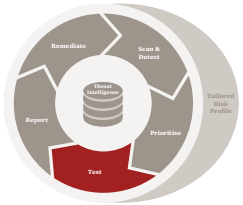
Traditional penetration tests “attack the front door” – by scanning and attacking your public internet addresses. This could provide an acceptable comfort level against ‘traditional’ attacks, but will not assess your vulnerability to more sophisticated attacks (known as Advanced Persistent Threats or APT).

Our penetration testing solutions are tailored to your specific needs. We use intelligence and experience from previous attacks to simulate what happens during a real cyber-attack. We take into account specific situations as well as environmental variables to build up a threat scenario. Outlined below is a schematic of the penetration testing services offered by our Swiss Penetration Testing team.

Security testing strategy

Security testing plan

Infrastructure penetration testing	Application penetration testing	Host based reviews	Social engineering
• External • Internal • Red Teaming • CREST Star* - Threat – Intelligence led testing • Scenario based testing • SCADA / ICS / OT testing • Wireless testing	• Grey/white box web application security testing • Black box application testing • Web application testing • XSS (Cross-Site-Scripting) • Source code reviews • ERP Testing	• Desktops and laptops • Servers • Virtualisation • Firewalls • Networks devices • SAN • Encryption devices • Databases • Mobile devices	• Physical access • Telephone tests • Behavioral, including phishing and spear-phishing



Security testing – case studies

Can a user (authenticated or unauthenticated) perform functions that they should not be able to, in order to escalate their assigned level of privilege?

Real life example: While performing penetration testing on an e-Banking application, we identified several weaknesses allowing to transfer money from an account to another account without authentication controls.

Application penetration testing

Are your staff aware of security and related threats?

Could they be easily tricked into handing out sensitive information or access credentials?

Real life example: While performing a penetration testing by using social engineering methods, we were able to obtain sufficient credential allowing us to access the internal network and sensitive strategy data.

Social engineering

Is your main financial planning system and its supporting infrastructure vulnerable to manipulation?

Can it be easily exploited to make fraudulent payments or misrepresent your financial position?

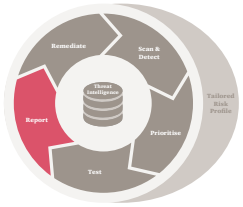
Real life example: While performing penetration testing on a SAP environment, several vulnerabilities related to the Operating system and the database were identified. A full control over the SAP application (SAP_ALL) was obtained by exploiting identified vulnerabilities.

ERP penetration testing (SAP and Oracle)

Is the access to your financial planning system and information technology infrastructure adequately secured? Are you storing sensitive data on mobile devices?

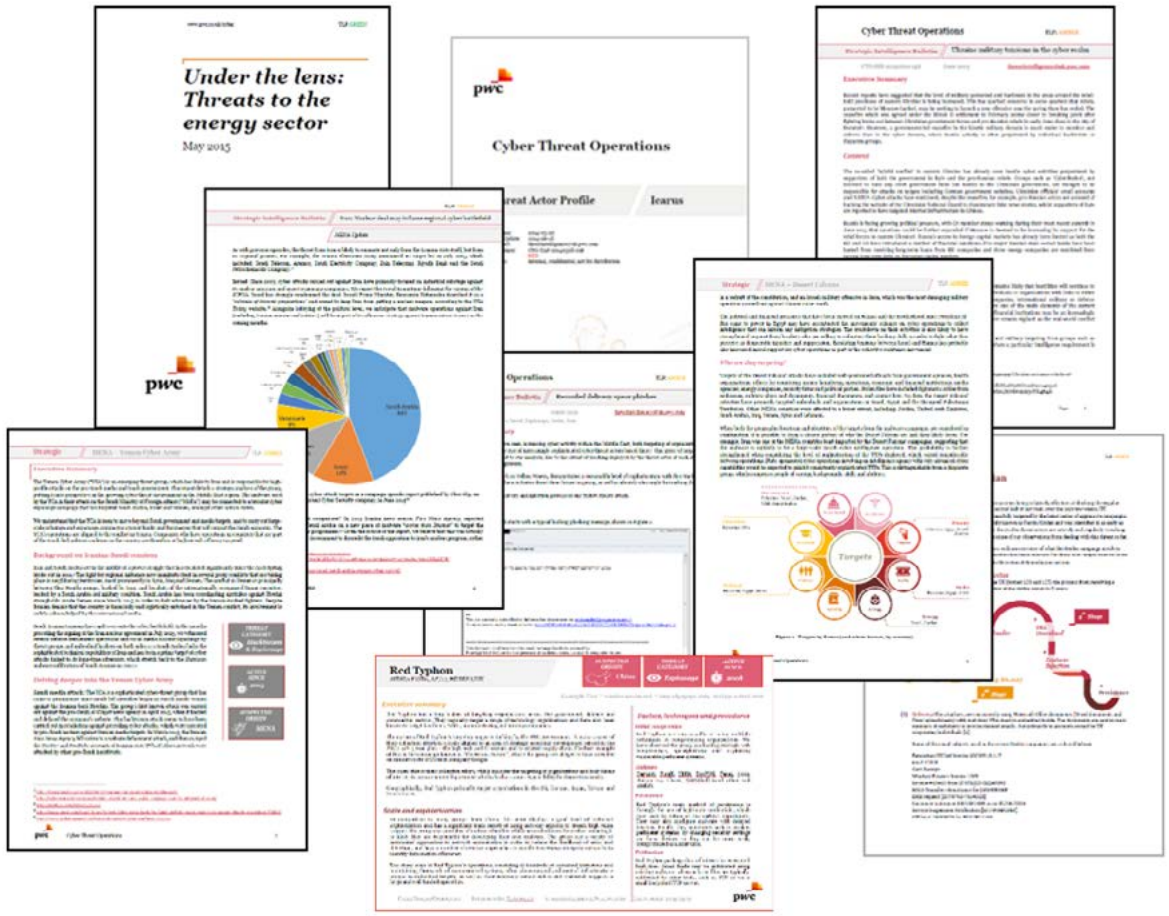
Real life example: While performing a penetration testing on a mobile device, we were able to access sensitive data stored on the mobile, which included business strategic data as well as user personal passwords.

Mobile security

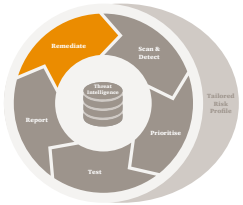


Reporting

Our high quality business focused reports provide you with market leading, tailored, and valuable information that will meet your unique requirement of improving the overall control environment through implementing and sustaining cost effective, programmatic and relevant solutions to address risks. Crucially, we will understand the root cause of issues, allowing you to implement solutions and embed robust controls throughout the business.



- The testing service is only as good as the data it produces. The ability for a provider to understand that data, its value and how it can be analysed further to provide additional insight into what caused the weakness is paramount in the ongoing improvement cycle.
- The definition of what reports you need, how that data should be analysed, and what is relevant about it is determined at the inception of the contract so as to ensure you get exactly what you need from day one.



Remediation of vulnerabilities

From vulnerability assessments and penetration testing, organisations identify many hundreds and thousands of vulnerabilities. Many organisations struggle to drive remediation of the vulnerabilities. We have considerable experience assisting organisations implement and drive vulnerability remediation using the 4 stage process outlined below:

0 Vulnerability Remediation Team Mobilisation

- Analyse the current vulnerability data and create a vulnerability remediation plan
- Define the required processes to implement a remediation program
- Implement / update the solution to identify vulnerabilities

1 Drive the remediation programme

- Coordinate the vulnerability remediation programme across the organisation
- Asses the risk to the business of vulnerabilities
- Root cause analysis
- Prioritise vulnerability remediation activities
- Promote and publicise successful remediation efforts/behaviours

2 Reduce the number vulnerabilities in existing systems

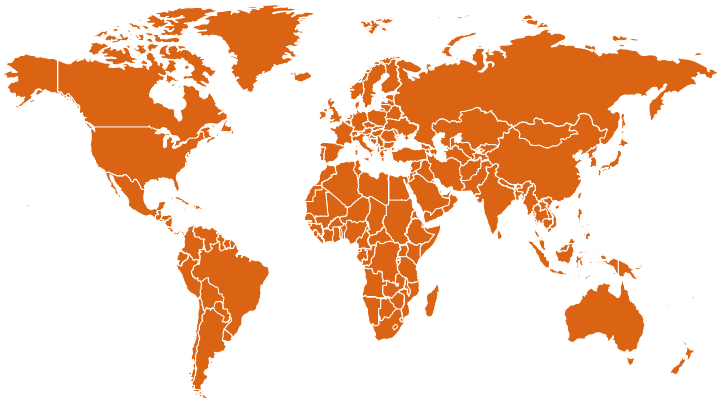
- Provide additional security SME's to support the IT teams in the development of remediation solutions

3 Ensure new systems do not have vulnerabilities

- Utilising knowledge of the vulnerabilities being identified - update Architecture principles and build documents to ensure that any new solution are designed, built and implemented in line with good security practices

Why PwC?

About PwC



PwC helps organizations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. PwC's member firms operate locally in countries around the world. By working together, member firms also comprise a vigorous global network similar in some respect to the IFRC. This provides our clients with the flexibility of **the most local and the most global of businesses.**

PwC Switzerland has offices in 15 of the country's largest cities with its main offices in Geneva and Zurich. On 30 June 2015, PwC Switzerland employed 2,676 people.

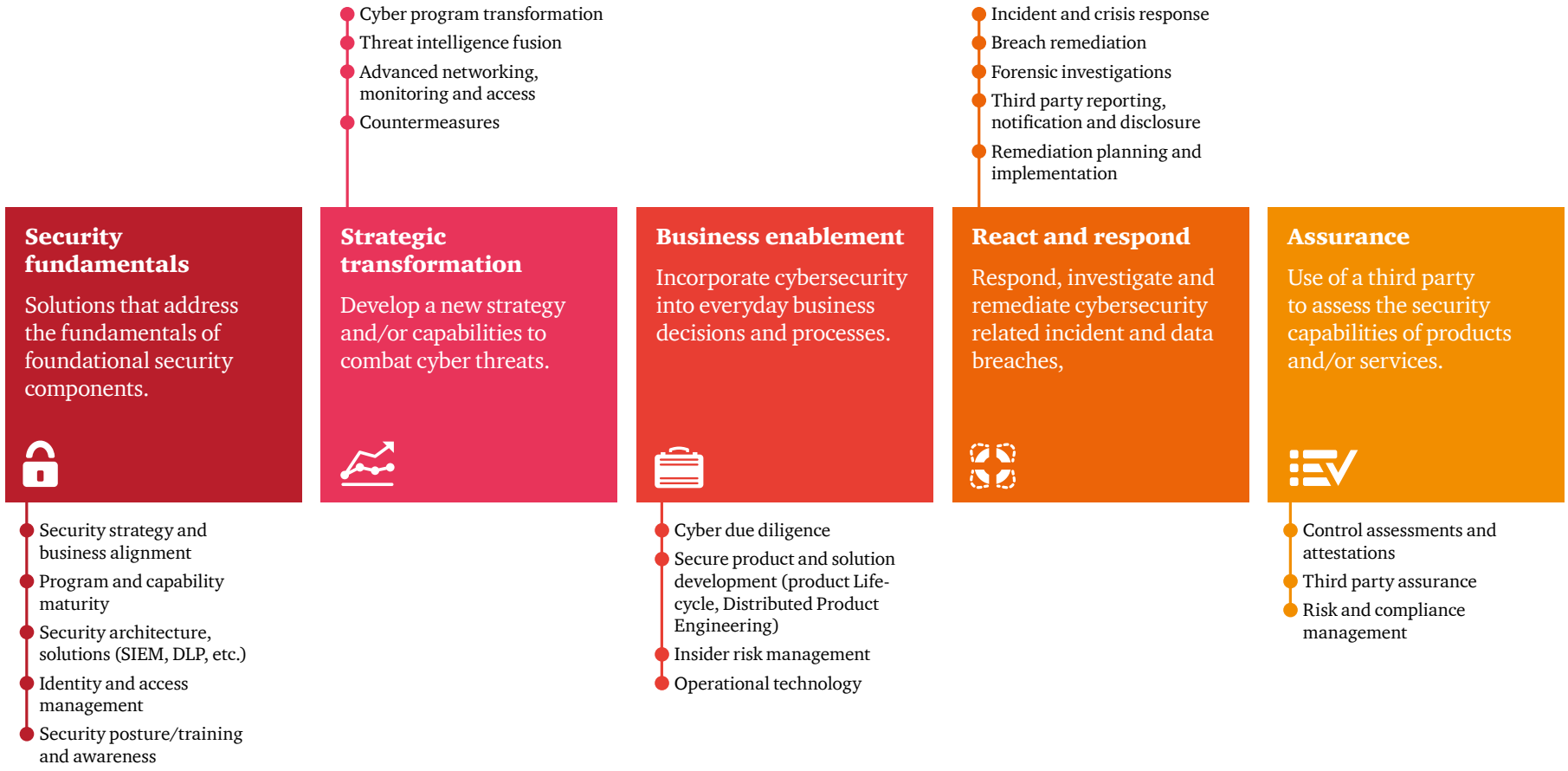
PwC brings a multi-disciplinary approach to information and cyber security, addressing the key components of strategy, governance, risk and compliance, and people, processes and technology. PwC's approach to information security blends business insight with a broader view of risk. We help clients to pursue opportunities by understanding their business drivers and threats and building in appropriate security enablers. We operate 55 forensic laboratories in 42 countries and support major incidents with a 'follow the sun' model.

Why PwC?

- **Technical resources that have a business focus:** we invest in our technical resources developing their technical and business skills, enabling them to relate technical findings to business risks and utilise business language in the reporting.
- **Consistency and quality in approach:** we adopt a consistent approach and tools for all penetration services performed globally, overseen by a central Quality Assurance and coordination team.
- **Tailored and tested methodology:** through our industry leading research and development and our extensive experience in the marketplace over at least 15 years, we have developed a proprietary penetration testing methodology.
- **Global reach:** we operate globally providing local language capabilities and understanding of culture with 50+ testers around the world, part of a security team of 3,200+ using a shared approach, methodology and knowledge. This allows us to provide both on-site and remote testing capabilities to deliver the most cost effective and flexible solution.
- **High quality and consistent reporting:** our reports will provide you with customised reporting and root cause analysis, including working closely with you to understand the impact of any findings identified in accordance with our clients risk management methodology. Crucially, we will understand the root cause of issues, allowing you to implement solutions and embed robust controls throughout the business.
- **Highly skilled consultants who are experienced operating at the CxO level:** Our consultants are used to working and communicating with CxO 's, translating technical findings into business language.
- **Research and Development:** our investment in research and development into emerging threats is one of the highest and most advanced in the industry.
- **Global automated portal solution:** we have developed a market leading, distinctive online portal solution for testing reporting and overall engagement management that we provide for global arrangements. Specifically, the 'portal' provides an integrated view of all penetration testing undertaken for your businesses globally providing customisable reports that can be tailored to address the varying needs of stakeholders.

Our strengths

We offer numerous solutions that help organisations understand their dynamic cyber challenges, adapt and respond to the risks inherent in their business ecosystem, and protect the assets most critical to their brand, competitive advantage and shareholder value.



Our service portfolio – breadth of services

We provide a comprehensive range of integrated cyber security services that help you assess, build and manage your cyber security capabilities, and respond to incidents and crises. Our services are designed to help you build confidence, understand your threats and vulnerabilities, and secure your environment. Our cyber security service delivery team includes incident response, legal, risk, technology and change management specialists.

Assess | Build | Manage | Respond

Understanding your capabilities and maturity will help you prioritise your investment

- Board-led maturity assessment
- Breach discovery assessment
- Cyber security diagnostic
- Cyber threat assessments and modelling
- Penetration testing
- Policy and contract review
- Privacy and cyber security legal assessment
- Standards compliance and certification
- Strategy and roadmap
- Third party assurance, including cloud
- Threat intelligence, detection and response maturity assessment

Assess | **Build** | Manage | Respond

Designing and delivering cyber security improvement programmes

Framework development

- Enterprise risk management
- Enterprise security architecture
- Information governance
- Privacy and cyber security legal strategy

Capability build

- Cyber security programme delivery
- Security technologies and SOC development
- Threat intelligence, detection and response capability development

Embedding security

- Awareness and training
- Contracting for security
- CSIRT and policy development
- Insider threat management
- Legal policy development
- Product development support
- Security intelligence and analytics

Assess | Build | **Manage** | Respond

Managing and maintaining control of your business, enabling you to focus on strategic priorities

- AAdvanced threat detection and monitoring
- Cyber defence team augmentation
- Data leakage monitoring
- Integrated managed security services
- Legal support to compliance officers and general counsel
- Managed vulnerability
- Retained incident response services
- Threat intelligence
- Security training

Assess | Build | Manage | **Respond**

Rapid, global access to leading cyber incident containment, investigation and crisis management expertise

- Breach notification
- Computer, network and malware forensics
- Crisis management
- Cyber incident legal advice including privilege
- Cyber incident response and forensic investigation
- e-Discovery and disclosure
- Fraud and eCrime data analytics
- Human resource advice – employee breaches
- Network intrusion containment and remediation
- Regulatory proceedings
- Third party litigations

Thank you

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers AG, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.