



*Enabling Cyber Resilience in Asia*

# Cybercrime is a Major Risk for any organization



Overlooking cybercrime eventually leads to reputational damage, financial loss and legal liability

Top 3 Cyber Threats  
in **ASIA**

**Phishing**  
**Ransomware**  
**Insider Threat**

Source: Kaspersky, "Kaspersky  
Security Bulletin 2022"

**62min**

Time to access  
**Sensitive Data** from a  
Phished Victim

Source: CrowdStrike,  
"2023 Threat Report"

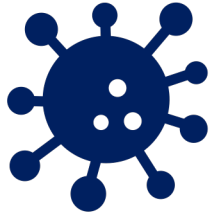
The **annual cost** of  
**cybercrime** is set to  
increase from 2022 to  
2025

**+300%**

Source: Cybersecurity Ventures,  
"Cybersecurity Market Report", 2022

# Why is it hard for organizations to manage cyber risk ?

Cyber risk is harder to reduce due to aggravating factors in **Asia**



## Threat Landscape

Asia is home to some of the world's fastest-growing economies, and this growth has been accompanied by a **rapidly evolving threat landscape**. **How do you keep up with and prevent the latest threat?**



## Cloud Security

The adoption of cloud-based services and the shift to remote work has resulted in an increased risk of data breaches due to an **expanded and dynamic attack surface**. **Do you understand your attack surface? How do you identify and remediate potential gaps?**



## Scarce Security Expertise

Cyber expertise is **hard to attract and retain**. Asia Pacific lacks nearly 2.1M cyber security professionals. This results in **not knowing what to do, or being unable to do it**.

# Partner with a leading cyber security team in Asia



Cybersecurity is what we do. Focus on your business, we take care of your security



We fight  
cybercrime **24/7**

We investigate thousands of  
alerts per year

Our team understands the threat  
landscape and adapts to it



We have  
**Expertise**

We know how other organizations  
tackle their security

Our experts hold the highest  
security certifications



We Have  
**Talent**

Top cyber talent wants to work  
with top cyber talent.

**Our entire company is built  
around cyber:** leadership,  
culture, work

## The cyber service Partner that actually delivers

Cyber delivery is hard. We don't just advise, we actually do the work for you.

Deep **Expertise** and **Experience** across both Cyber Defense and Offense  
Strong understanding of the latest threats and attack techniques

**Synergies** between our capabilities

**Responsive** and **Flexible** working model

Ability to respond quickly to the evolving threat landscape

**Proactive Advice** because it is the right thing to do

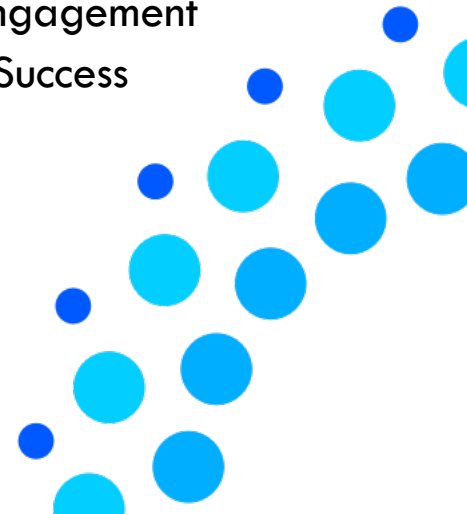
**Transparency & Trust**

We say what we do and we do what we say

Clear and Concise metrics showing the effectiveness of our solutions

**Collaborative** Engagement led by our Customer Success Team

➤ Enabling your cyber resilience



You are in good company !



## What they say about Theos

Overall Customer Rating: **8.6/10**

### CISO

*“Thank you Theos Team for your flexibility and **expertise**.”*

### Head of Cyber

*“One of a few vendors that **works closely with us**”*

### CISO

*“Very responsive, **SLA is quite impressive**, **Flexibility** and Resources Management are very good”*

### Director – Information Security

*“it’s a **pleasant experience** this year for the Annual Program. Thank you Theos”*

# Recognized and Accredited for our innovation and service excellence



2023 Asia-Pacific  
Cybersecurity Entrepreneurial Company of the  
Year



2022 Circle of Excellence  
-  
SMB of the Year



Top 10 Enterprise Security  
-  
Startups in APAC 2019



CREST Accredited Asia  
-  
Penetration Testing



Singapore CSRO License  
-  
Penetration Testing  
SOC Monitoring Services



Philippines DICT Accredited  
-  
VAPT & ISMS Assessor



# Continuously investing in the technical development of our Team



SOC-200



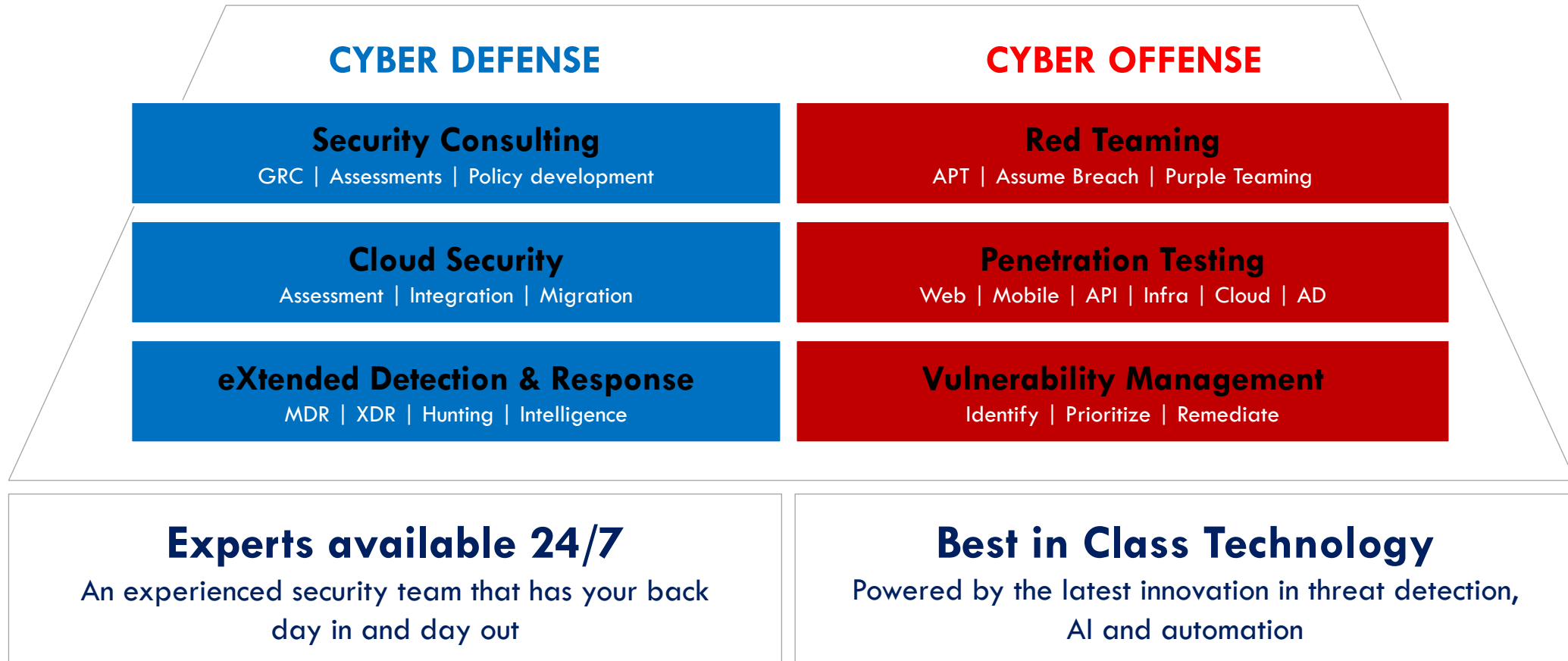
CERTO



**How do we do it ?**

# Tackling cyber security from both angles: Defense and Offense

End-to-end cyber services with collaboration between **blue** team and **red** team, powered by best-in-class technology, delivered by industry experts



# Case Studies

1. Threat Detection & Response: Insurance in Asia
2. Penetration Testing: Stock Exchange in SEA
3. Red Teaming: Technology Company in Asia
4. Security Transformation Program: Global Manufacturing

# Case Study - Protecting 8000+ assets for one of the largest insurances in Asia



## Customer's profile:

One of the largest insurance company in Asia, which has **6200+ employees** across eight offices within the APAC region. The company offers life and medical insurance, general insurance, employees benefits.



8000  
Endpoints



Standard  
Operating  
Procedures

## Customer's challenge:

- Looking for a partner to implement the solution covering their entire endpoint estate.
- Required product expertise as well as strong technical investigation and troubleshooting skills to ensure a smooth and fast deployment.
- Full technical documentation was also a requirement.

## Solution delivered:

- Theos completed the full policy and configuration implementation within a week, and worked with the client as agents were rolled out. Deliverables included a Technical Design and a Troubleshooting Procedure.
- The following deliverables were completed: Technical Design, Policy Implementation, Design and Handling of Upgrade Process, Troubleshooting of deployment and compatibility issues, Defining the Standard Operating Procedures, Defining the Response Playbooks, Integration with third party tools and applications.

## Values delivered to the customer:

- **Our experience & expertise:** Our **experience** and **expertise** in defining an effective security programme that is relevant to the customer by leveraging on their current investment and complementing their old architecture with market leading security technologies.
- **On-time delivery:** During the implementation, Theos identified a compatibility issue and worked with the product vendor to overcome this issue and proceed with the deployment, which was successfully delivered in 2-months of time.

# Case Study - Delivering VAPT programme for a stock exchange in SEA



## Customer's profile:

One of the **largest stock exchanges in South East Asia**, with 200+ listed companies as of 2021, and a **market capitalisation of USD200+ million** as of 2021.



Annual PT  
retainer contract



30+ applications  
tested per year

## Customer's challenge:

The client is one of the Stock Exchanges in Asia. Being a prime target for malicious actors, they need to constantly test the strength of their applications and systems to **minimise the risk of compromise**. They were looking for a partner to engage in the long term to deeply understand their architecture and applications while providing a flexible commercial framework.

## Solution delivered

- An annual retainer for Vulnerability Assessments and Penetration Testing across the entire application estate of the Stock Exchange with **a minimum of 30 tests per year**.
- Ethical Hackers are deployed within the stock exchange as well as remotely to look for flaws and vulnerabilities that an attacker could exploit. Recommendations and remediation services are provided on an on-demand basis.

## Values delivered to the customer:

- Local and remote Ethical Hackers available on-demand.
- Leverage on our past learnings on delivering to large FSI customers in Asia, as all projects are delivered in-house and not outsource to contractors.



# Case Study - Adversary Emulation for a Technology Business in Asia



## Customer's profile:

A technology company headquartered in Hong Kong providing IT services to enterprises globally



Annual Red Team Exercise



Custom Objective and Scenario

## Customer's challenge:

- Rise in recent supply chain attacks where IT management companies are targeted to attack their customers resulting in significant legal and financial liabilities.
- The leadership of the company decided to execute a red team exercise to assess the likelihood that an initial compromise leads to liabilities that could threaten the very existence of the business.

## Solution delivered

- Theos designed a custom objective consisting of the Red Team Operators focusing their efforts on **escalating their initial access** to platforms and tools allowing access to client environments.
- In order to address this specific risk, the scenario selected was **Assume Breach**. Red Team operators were provided with remote access to a standard end-user laptop with regular end-user privileges and accesses..

## Security Value delivered

- The Red Team Operators uncovered several attack vectors that could be conducted from an end-user device with low privilege accounts escalated to an access to client environments.
- The customer was provided with detailed remediations recommendations and successfully mitigated the attack vectors during the re-run of the attack

# Case Study - Private Equity Acquisition leads to a Security Transformation Programme



## Customer's profile:

A **cosmetic manufacturer** company, headquartered in US, which has **300 employees** across seven offices globally. The company designs and manufactures exclusive brands and private labels for mass, drug and specialty retailers and provide outsourcing solutions to leading beauty companies operating worldwide.



3 years managed service contract



1000+ Threats identified within the first 2 months



350 Endpoints Hardened and Protected

## Customer's challenge:

- The business was recently acquired by a Private Equity firm with a mandate to **uplift the entire security posture of the company**. The requirements covered all aspects of information security with a global footprint and a need to provide ongoing security management over several years.
- The customer was seeking a security partner who could implement and run a **breath of security services globally**, at a commercial point commensurable with a mid-size enterprise.

## Solution delivered:

Theos provided an end-to-end **Security Transformation** Programme spanning Security Architecture, VAPT and Managed Detection and Response:

- Define **5 InfoSec Policies** (1) Information Protection Policy (2) Acceptable Use Policy (3) IT Systems Security Policy (4) Risk Management Policy (5) Third Party Security Policy.
- Performed **Vulnerability Discovery & Penetration Testing**: initially perform a vulnerability discovery on all its Internet facing systems, and conduct penetration testing on up to 3 external-facing applications or systems.
- **Deliver Vulnerability Management**: scanning the entire estate for vulnerabilities, which will then be validated and remediated by Theos. Theos does validate findings and dismiss false positives to facilitate the remediation process and ensure a quicker time to fix issues.
- **Implementation of advanced Endpoint Detection and Response (EDR) solution**: Monitoring and provide technical support with response of NBD. Support is provided online.

## Values delivered to the customer:

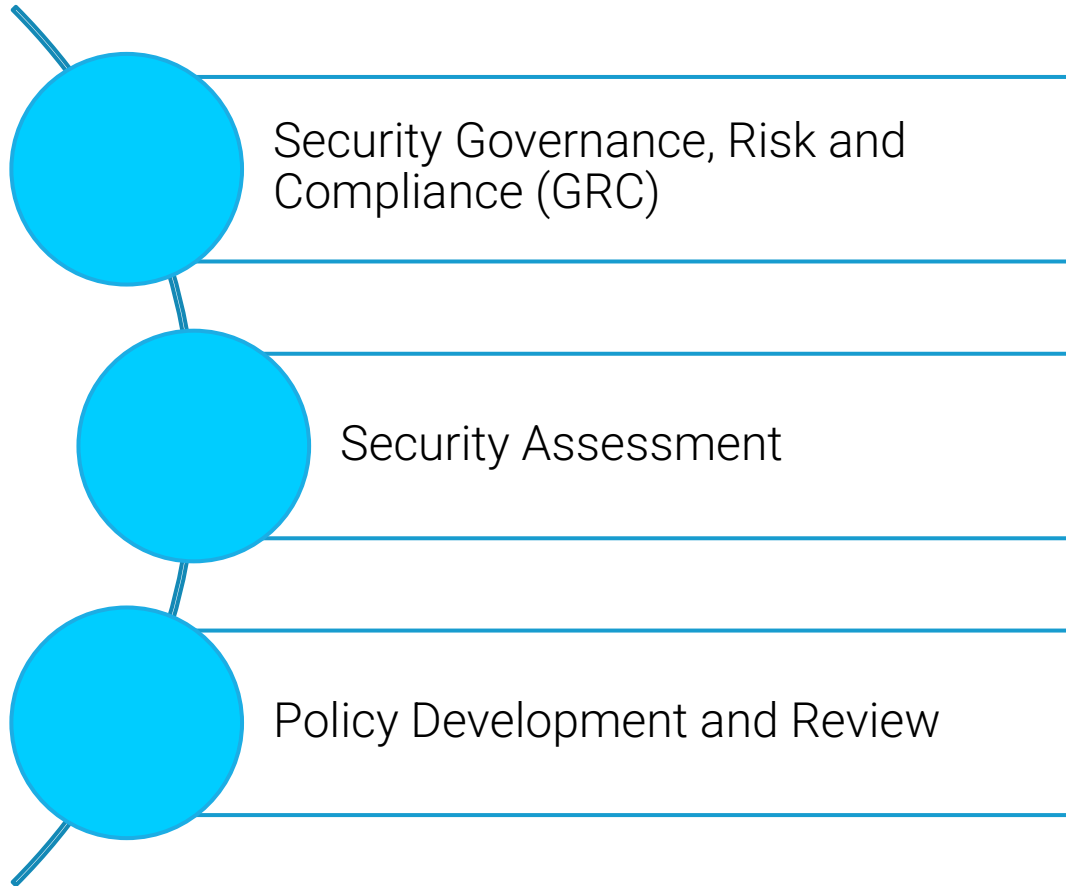
- **Our experience & expertise**: Our **experience** and **expertise** in defining an effective security programme that is relevant to the customer by leveraging on their current investment and complementing their old architecture with market leading security technologies.
- **On-time delivery**: The Programme was successfully delivered in less than 6 months (on time) and services are provided thereafter for several years.



# Cyber Security Services

# Gain insights with Security Consulting

Identify what needs to be protected and how, in line with your industry and regulatory requirements



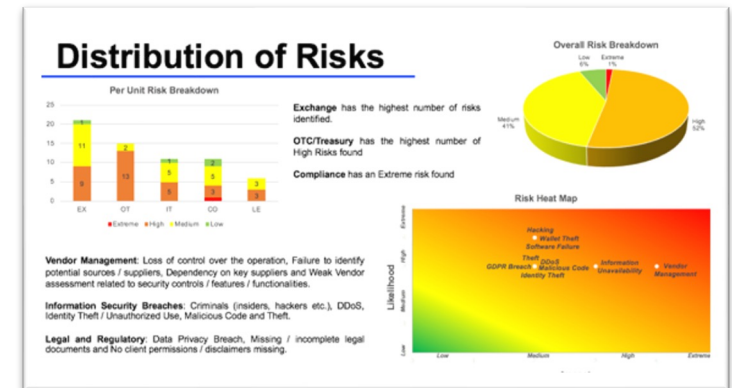
### Privacy Policy

**What information do we collect about you?**  
We collect information when you set up your account for the Services. In addition to our legal obligations, we also collect your birth certificate, passport, and other identification documents.

**How will we use the information about you?**  
We use your information to provide the Services to you. We use your information to verify your identity, for AML and KYC, and to support and improve the Services. [More]

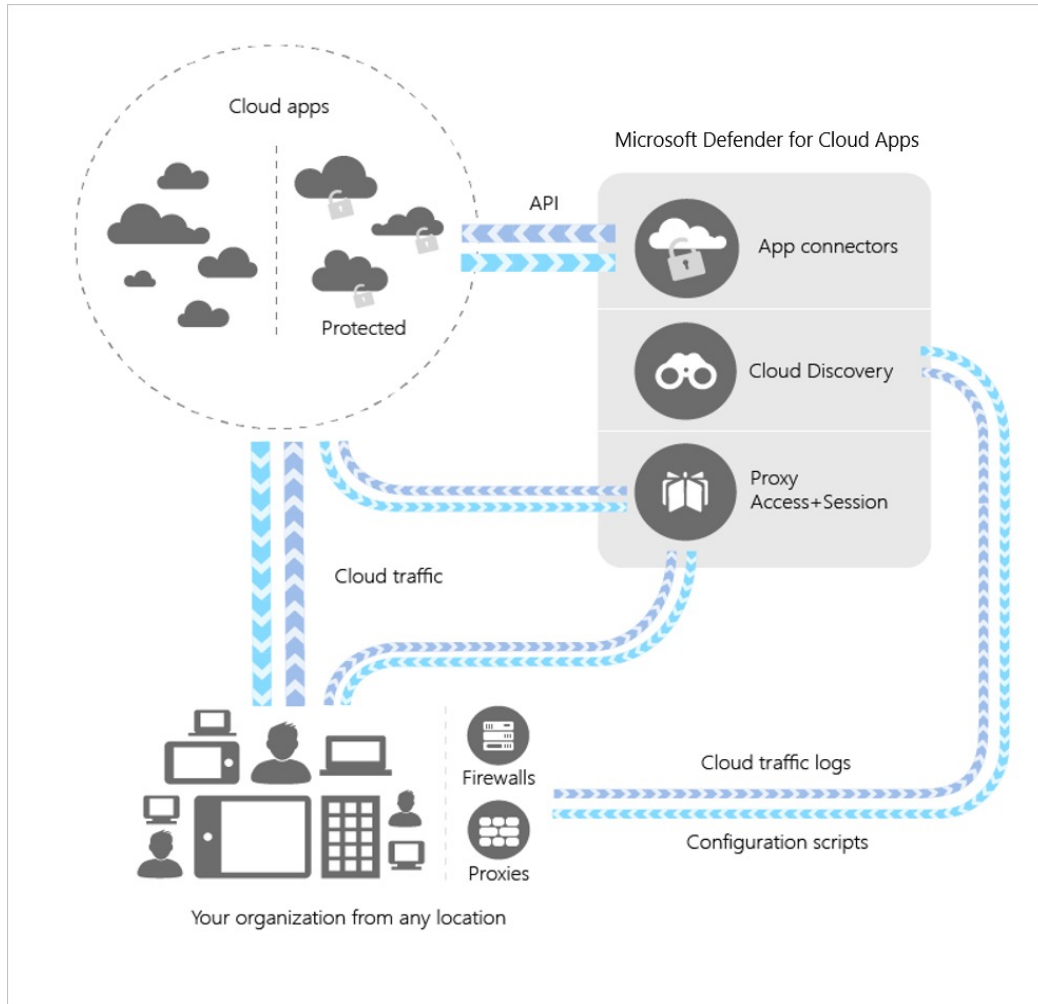
**Who do we share your information with?**  
We use third parties for support services, such as cloud service providers, payment processors, and other vendors. We use these third parties to provide the Services to you. We use these third parties to process your information with our related group companies and as required by law.

**Where do we process your information?**



# Enabling your Cloud Security journey

Assessing and protecting sensitive data and assets in the cloud



## Cloud Access Security Broker

- **Visibility** detect all cloud services; assign each a risk ranking; identify all users and third-party apps able to log in
- **Data security** identify and control sensitive information (DLP); respond to sensitivity labels on content
- **Threat protection** offer adaptive access control (AAC); provide user and entity behaviour analysis (UEBA); mitigate malware
- **Compliance** supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements



Microsoft



Defender for Cloud Apps

### SERVICES

Based on MS Defender for Cloud Apps

#### MDCA Setup

Conditional Access, Threat Detection, Data Loss Prevention, Reporting

#### Applications Onboarding

Integration of built-in and custom apps

**24/7 Monitoring & Response** of policy violations

#### SLA

- Acknowledge: 1 hour
- Respond: 4 hours
- Close: 16 hours

# XDR: Extended Threat Detection & Response

XDR is a service that uses advanced threat detection tools, real-time monitoring, and expert analysis to detect and respond to threats before they can cause damage.



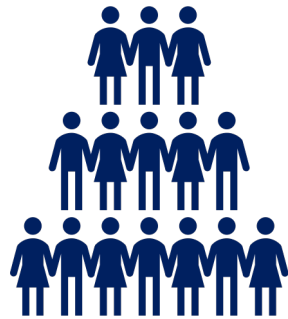
## 24/7 PROACTIVE SERVICE

- Turnkey Threat Detection, Investigation & Response
- Human-Led analysis and remediation
- Threat Intelligence and Hunting
- Active Containment and Disruption of Threats
- Visibility and Analytics

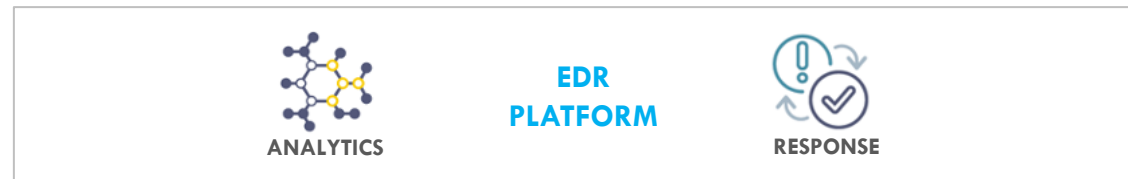


**SECURITY  
OPERATIONS  
CENTER**

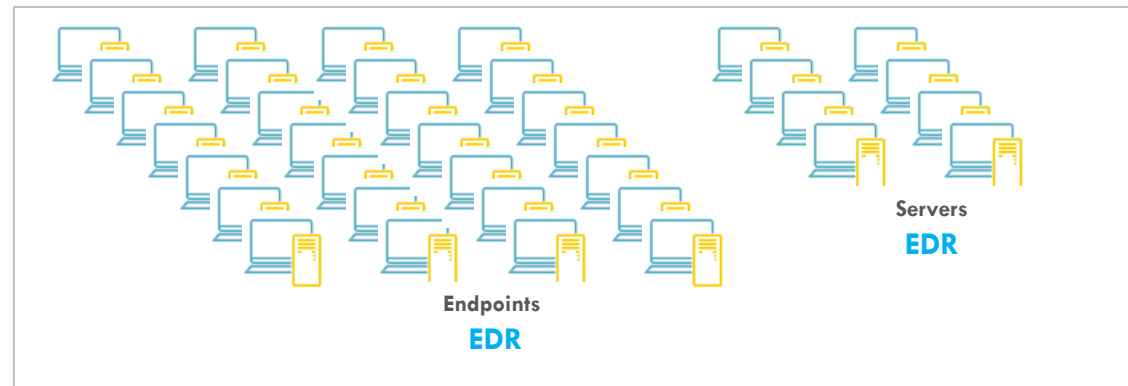
# Turnkey Threat Detection, Investigation & Response, 24x7x365



## 24/7 SOC



- Alert Monitoring
- Investigation
- Response
- Threat Hunting
- Fine-Tuning









ENDPOINTS & SERVERS LOG SOURCES



HIGH VALUE LOG SOURCES

# Flexible XDR deployment models with industry-leading SLAs

Service levels	MULTI-TENANT  Fully Managed Theos Platform	DEDICATED  Microsoft Environments Bring Your Own License Only	CUSTOM  Enterprise & Government Customers
<p><b>MDR: Managed</b> <b>Endpoint Detection &amp; Response</b></p> <p>Protect <b>Endpoints &amp; Servers</b> Enable Active Response</p>		 <p>Microsoft Defender For Endpoint</p>	<p>SUBJECT TO CUSTOMER REQUIREMENTS</p>
<p><b>XDR eXtended</b> <b>Detection &amp; Response</b></p> <p>Monitor &amp; Respond across <b>all sensitive channels</b>: Cloud, Email, Web, Identities, Data</p>		 <p>Microsoft Sentinel</p>	

Service Components	
<p><b>Customer portal</b> Self-Service</p>	
<p><b>Managed Deployment</b> Onboard in weeks</p>	
<p><b>Support &amp; Management</b> Hands-free technology</p>	
<p><b>Monitoring &amp; Response</b></p> <p><b>24/7 SLA</b></p> <ul style="list-style-type: none"> <li>- Acknowledge: 1 hour</li> <li>- Respond: 4 hours</li> <li>- Close: 16 hours</li> </ul>	
<p><b>Threat Hunting</b> Intel or customer-led</p>	
<p><b>Security Advisory</b> Cyber Posture Review</p>	
<p><b>Custom Use Case Dev</b> Up to 10 Rules</p>	<p>ADD-ON</p>

# Red Teaming: organization-wide Cyber Resilience Exercise

Assess the overall organization cyber resilience with a wide Red Teaming Exercise

- Emulate a Persistent Group of \*Real\* Hackers
- Test your Cyber Defenses
- Practice and refine your processes and capability
- 4 – 8 Weeks Exercise

### Red Team Scenarios

- ✓ **Advanced Persistent Threat**
- ✓ Assume Breach
- ✓ Third Party Compromise
- ✓ **Purple Teaming**

### Red Team Objectives

- ✓ **Data Theft**
- ✓ Data Integrity Compromise
- ✓ Establishing Access
- ✓ Operational Disruption

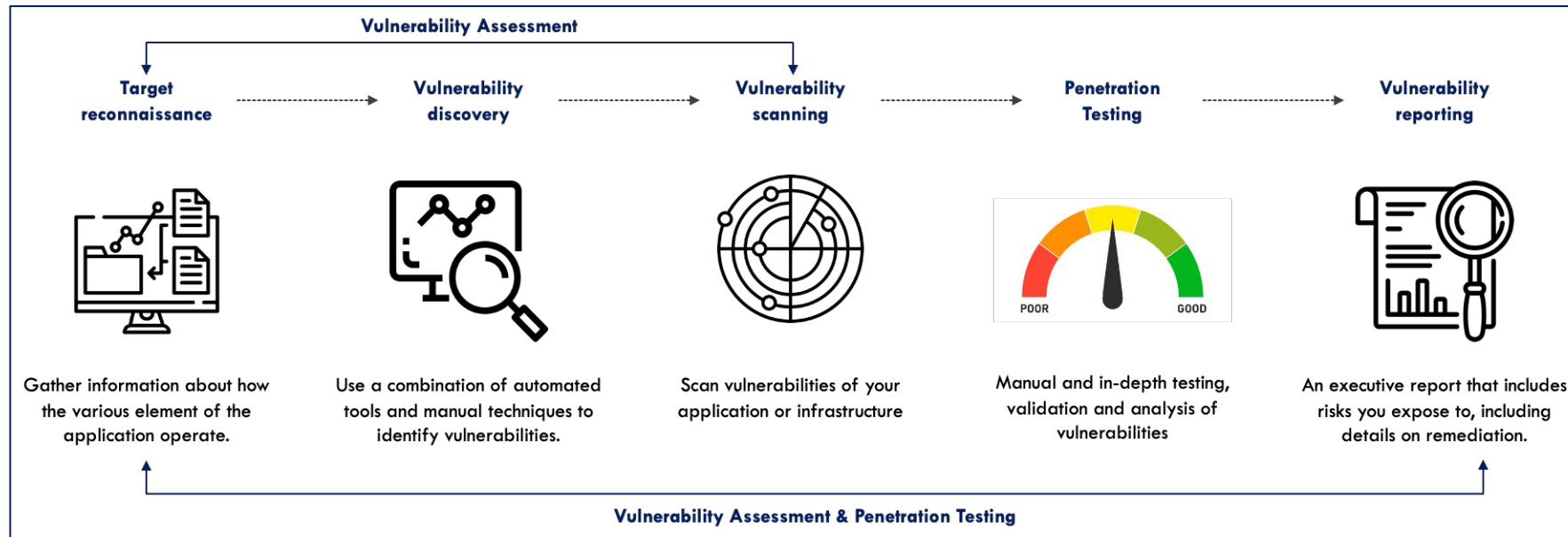




# Identify vulnerabilities with Penetration Testing

A team of expert white hat hackers use a combination of automated and manual techniques to simulate attacks and pinpoint flaws in your applications, systems and networks

## Methodology based on OWASP, CREST and PTES



- ✓ Web App
- ✓ Mobile App
- ✓ API
- ✓ Active Directory
- ✓ Internal Network
- ✓ External Network
- ✓ Wifi
- ✓ Cloud



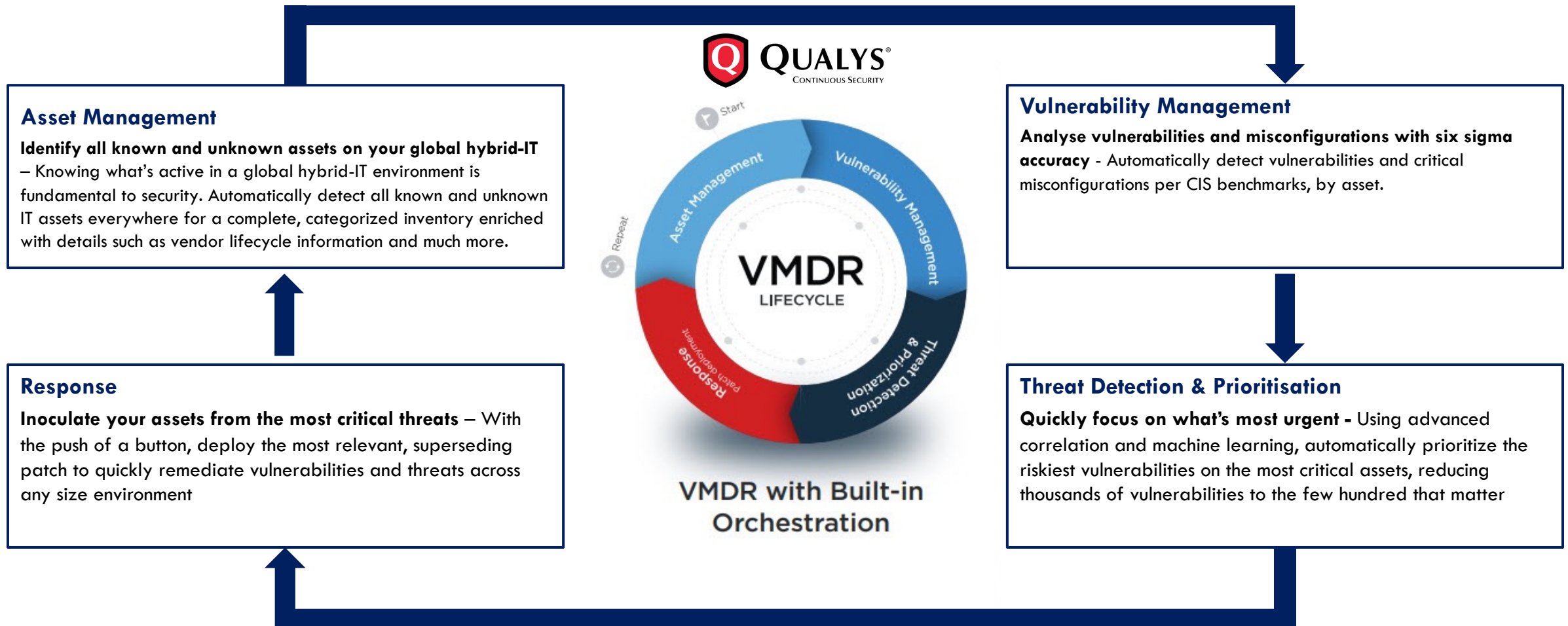
ID	Risk Level	Name
TFC001	Critical	Can Place Order for Other Users – Privilege Escalation
TFH001	High	Cross-site Request Forgery (CSRF) – Token Bypass
TFH002	High	Path Traversal
TFH003	High	Command Injection
TFH004	High	Cross-Site Scripting (XSS), Persistent
TFM001	Medium	Sensitive Data Transmitted Unencrypted
TFM002	Medium	Arbitrary Redirection
TFL001	Low	Insecure Password Policy
TFI001	Info	HTTP Strict Transport Security (HSTS) Not Enforced



# Vulnerability Management, powered by Qualys

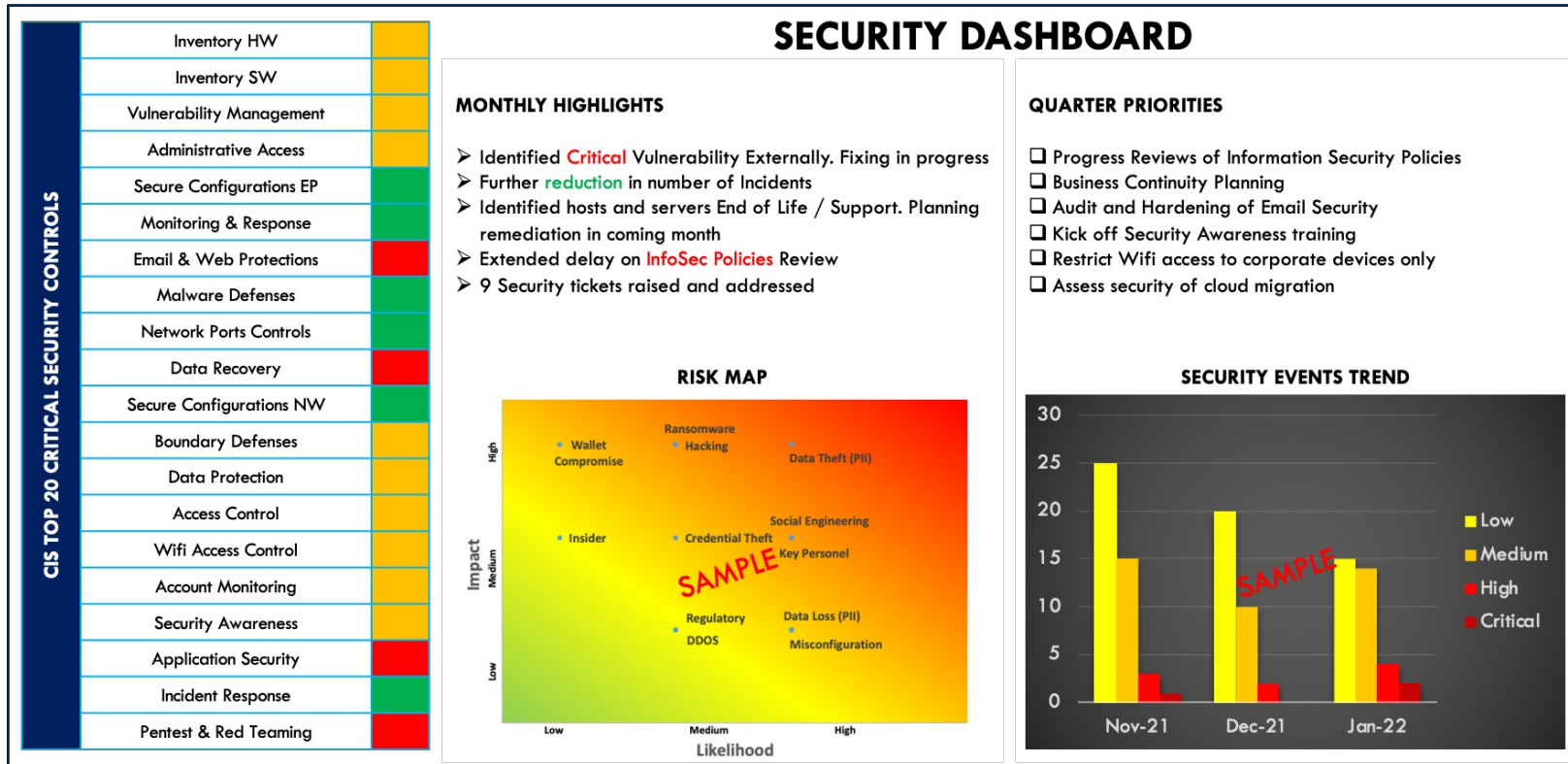
Vulnerability Management done the right way

- ✓ The VMDR programme enables you to **discover, assess, prioritize**, and **patch** critical vulnerabilities and misconfigurations in real time in one solution.
- ✓ Our joint solution with Qualys automates the entire process and significantly **accelerates an organization's ability to respond to threats**, thus **preventing possible exploitation**.



# Customer Success and Service Delivery

Monitor the progress of your security programme and ensure continuous buy-in from senior leadership



- Quarterly Security Steering Committee
- Risk Review
- Service Review
- Named Customer Success Manager

**“ Delivering cyber security outcomes,  
not silver bullets.”**

# THEOS

CYBER SOLUTIONS

Securing Modern Businesses

