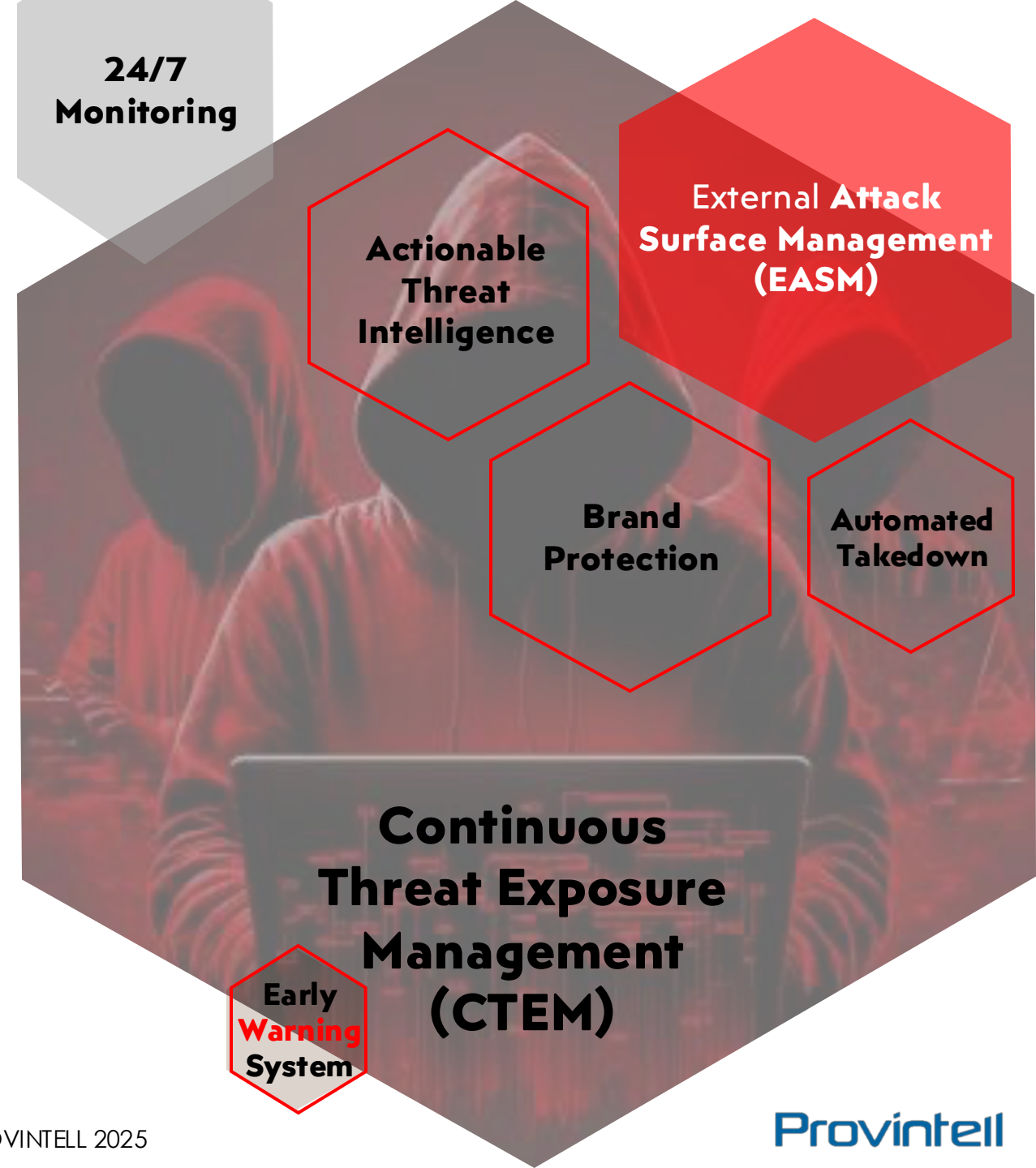
CODERED ASM®

STAYING AHEAD OF CYBER THREATS

PROVINTELL Cyber Security
www.linkedin.com/company/provintell-technologies-sb/
www.provintell.com
info@provintell.com

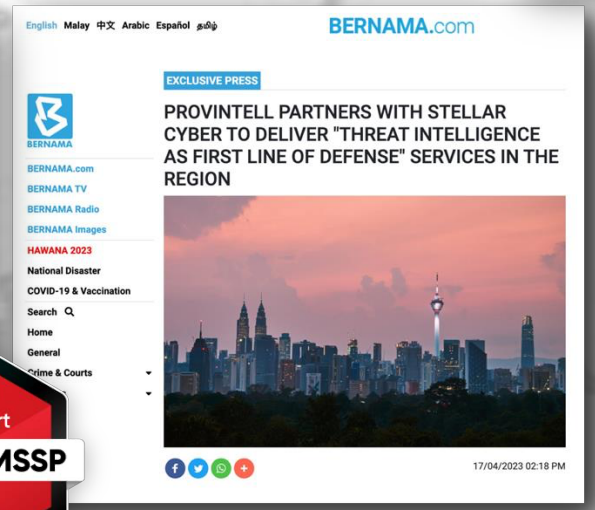


CODERED CYBER

Provintell

THREAT INTELLIGENCE AS FIRST LINE OF DEFENSE

Actionable Threat Intelligence For Digital Risk Protection



CODEREDASM

*Trademark registration

Provintell

SOLUTION OBJECTIVES

Focus Area

Challenges

Compliance Risk

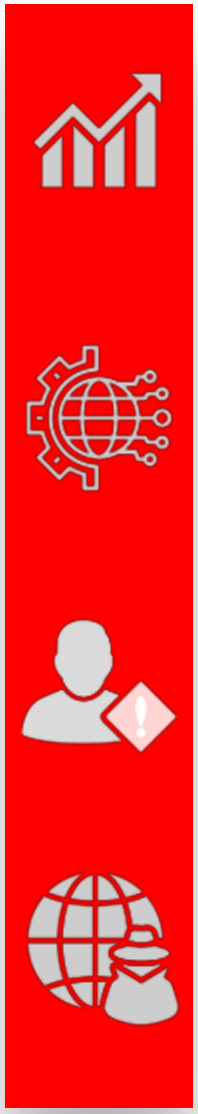
Cyber Threat Exposure Risk

Data Breaches, Privacy Threat and System Compromise

System Vulnerability, Security Misconfiguration and Shadow IT

Evolving Threat Landscape

Are you aware of your current EXPOSURE RISK and ATTACK SURFACE?



Proliferation of cybercrime with sophisticated cyber attacks using AI technologies.

Impact of emerging technologies on organization's attack surface. Adoption of cloud services and IoT. Digitalization of business processes.

Human error, system misconfiguration and shadow IT issues are increasing.

Hackers don't hack in, they just log in! Sensitive data and user credentials leak in the dark web.

Over 80% of cyber security incidents

are the results of public exposure due to **security misconfigurations** and vulnerable attack surfaces.

1 out of 3 cyber attacks

are targeting the unmanaged IT assets known as **shadow IT**, and we like to call it the **low hanging fruits**.

Over 10.3b of USD losses

were reported in Y2022 due to phishing attacks. Most of the successful **account takeover (ATO)** attacks are due to the stolen credentials obtained from the **dark web**.

More about CODERED ASM:
https://www.youtube.com/watch?v=0KTiHqNrE80

CODEREDASM® is EASM + CTEM as-a-Service

A complete solution for **External Attack Surface Management** and **Continuous Threat Exposure Management**.

What is Continuous Threat Exposure Management (CTEM) ?

External **Attack Surface Management** (EASM)

Shadow IT Detection and Vulnerability Management

Dark Web and **Hack Threat** Monitoring and Response

Sensitive PII Data Leak Detection and Account Takeover (ATO) Prevention

Phishing and Scam Sites Monitoring and Response

Brand Protection

System Compromise Monitoring and Response

Subdomain Takeover and Malware Sinkhole Detection

Supported by 24/7 SOC via **Threat Responder Mobile App**

AI-Native SecOps Integration with Gen AI Contextual Detection and Consensus Prediction (NEW)

CODEREDASM® is EASM + CTEM as-a-Service

A complete solution for **External Attack Surface Management** and **Continuous Threat Exposure Management**.

How it works?

Attack Surface Discovery

- Internet-facing digital asset discovery.
- Public exposure and misconfiguration.
- Vulnerabilities and low hanging fruits.

Comprehensive Digital Footprints Coverage

- Websites, forums, dark web, social media and app stores.
- Impersonation threat, scam and brand infringement.

Actionable Threat Intelligence Aggregation

- Over 100+ of public, private and commercial threat databases.
- Multi-channel threats aggregation and exposure coverage.
- Multi-platform integrations for brand and scam protection.

Exposure Risk Analysis

- Comprehensive exposure coverage.
- Integration with Security Operation Center (SOC) workflows.
- Utilization of AI and machine learning platforms for automated threat detection and attack surface analysis.

24/7 SOC Monitoring and Response

- Automated and managed threat response by 24/7 SOC.
- Automated Take Down services.
- Account Takeover (ATO) prevention.
- Custom SOAR integration.

CTEM

CODEREDASM® is YOUR FIRST LINE OF DEFENSE

Why You Need It?

1

Proactive and Pre-emptive Protection

Upgrading from vulnerability management to **exposure risk and attack surface management**. Maintaining a proactive security posture to prevent security breaches.

2

Actionable Threat Intelligence / Early Warning System

Wide-ranging **threat intelligence databases** integration and aggregation to provide a unified view of potential cyber threats.

3

24/7 SOC Monitoring and Response

Integration with our in-house SOC workflows for automated threat hunting, detection and response with the use of AI and machine learning technologies. Reduces mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

4

Automated and Managed Takedown

Automated takedown reduces mean-time-to-respond (MTTR) to minutes and hours.

5

Account Takeover (ATO) Prevention

ATO attack prevention with Active Directory integration and other security platforms with **custom SOAR connectors**.

6

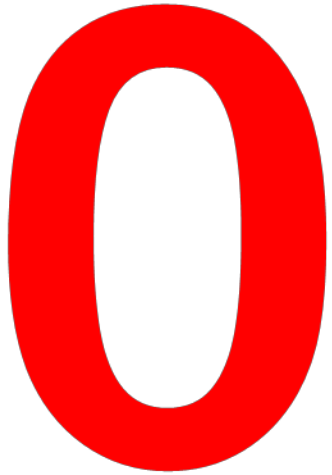
Zero False Alarm

Automated **assessment and validation** by our 24/7 cyber security specialists.

Why organizations prefer CODEREDASM®

Zero False Alarm
Validated by our 24/7 cyber security specialist.

Zero Cyber Security Workforce
We are your 24/7 cyber security specialists.



Zero License
Annual service subscription.
Highly scalable to meet future business requirements.

Zero Hardware and Software
No installation and deployment required. No CAPEX.

How Hackers Turn Your Blind Spots Into Security Breach Headlines?

YOUR BRAND

What's your valuable data?

YOUR EXPOSURE

How vulnerable are your systems and your users?

YOUR BLIND SPOTS

How easy to obtain your valuable data?

AUTOMATED DETECTION & AI THREAT PREDICTION (NEW)

AUTOMATED RESPONSE WITH AI SOAR & BAS (NEW)

IR PLAYBOOK & SOC WORKFLOW INTEGRATION

1

Scam and Phishing Sites

1. Fake Website
2. Fake Mobile App
3. Social Media Impersonation
4. Account Compromise (Dark Web)

2

Malware and Data Exfiltration

5. System Exposure
6. Vulnerable Attack Surface
7. Shadow IT
8. System Compromise (Malware)

3

Breach Headlines

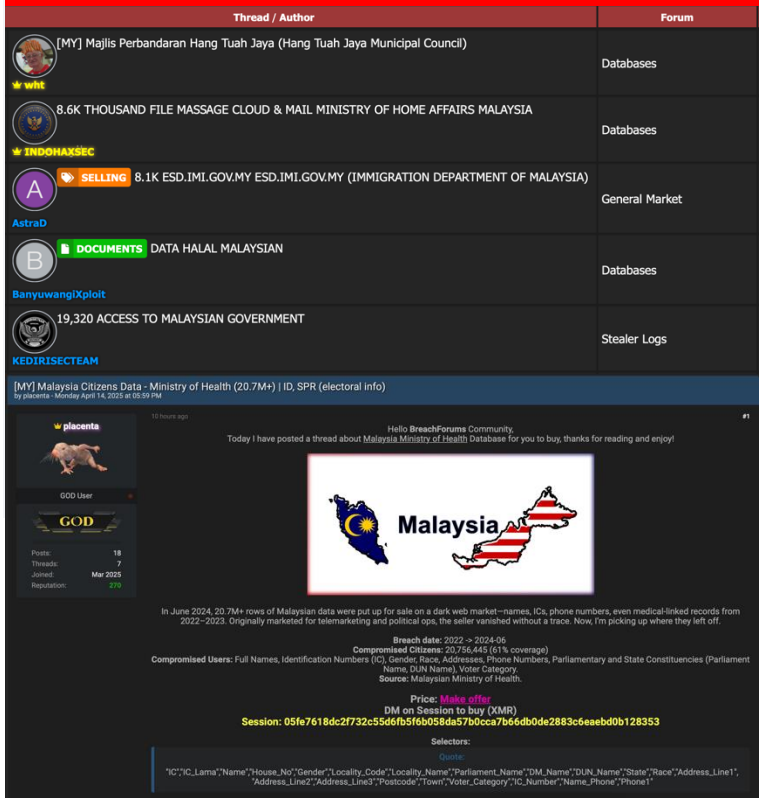
9. Hack Threat
10. DDOS Target
11. Third Party Risk
12. PII Data Leak (Dark Web)

CODERED CYBER

Provintell

USE CASE #1 – SENSITIVE DATA LEAK (PII)

THREAT



IDENTIFY / DETECT

- Hack Threat
- Sensitive Data Leak

RESPOND / PROTECT

- Hack Threat Playbook
- Incident Response
- Custom SOAR

AI-NATIVE CONSENSUS THREAT PREDICTION (NEW)

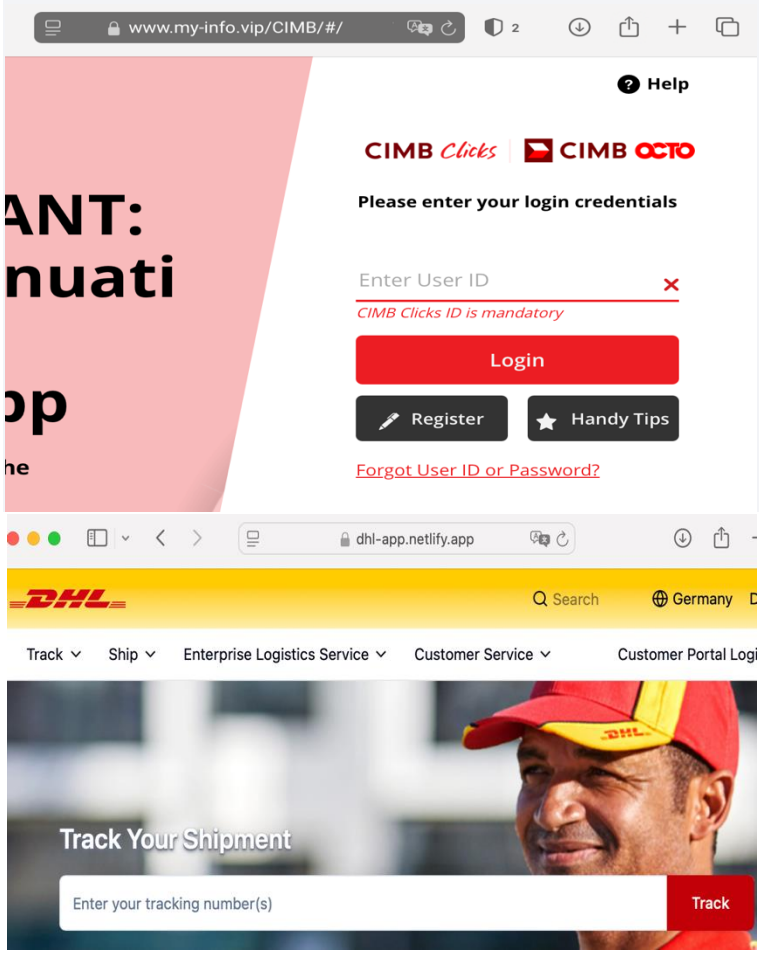
Sensitive Data Leak	→	Online Fraud Threat	→	System Compromise
Fidelity 95%		Fidelity 75%		Fidelity 65%

CODERED CYBER

Provintell

USE CASE #2 – PHISHING THREAT

THREAT



IDENTIFY / DETECT

- Phishing Threat
- Online Fraud Threat

RESPOND / PROTECT

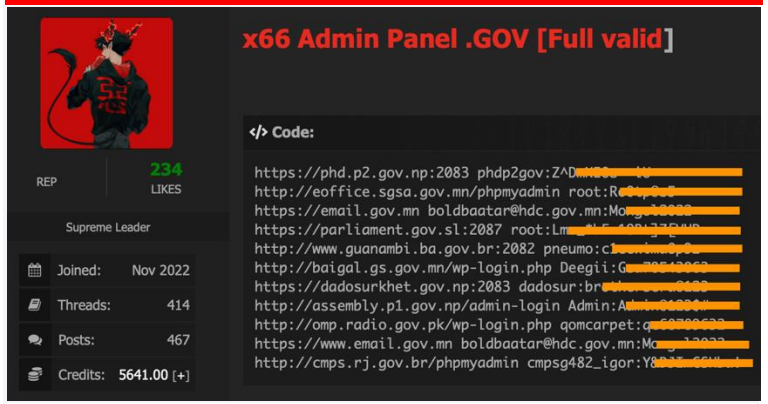
- Site Takedown Playbook
- Automated Takedown
- Custom SOAR

AI-NATIVE CONSENSUS THREAT PREDICTION (NEW)

Phishing Threat	User Credentials Leak	Sensitive Data Leak
Fidelity 95%	→ Fidelity 75%	→ Fidelity 55%

USE CASE #3 – USER ACCOUNTS COMPROMISE (ACCOUNT TAKEOVER)

THREAT




```
[{"fnd":"20231206","src":"https://auth0.open
ai.com/u/signup/password","fle":"
","hid":"
","inf":"20230325","pwd":"
","iip":"","mal":"Ra
ccoon","usr":"@gmail.com"},
{"fnd":"20231206","src":"https://auth0.opena
i.com/u/login/password","fle":"
","hid":"
","inf":"20230322","pwd":"
","iip":"","mal"
:"Raccoon","usr":"@gmail.co
{"fnd":"20231206","src":"https://auth0.opena
i.com/u/login/password","fle":"
","hid":"
","inf":"20230415","pwd":"
","iip":"","mal":"Rac
```


IDENTIFY / DETECT

- User Credentials Leak
- Session Cookies Leak

RESPOND / PROTECT

- ATO Playbook
- Custom SOAR
- Incident Response

AI-NATIVE CONSENSUS THREAT PREDICTION (NEW)

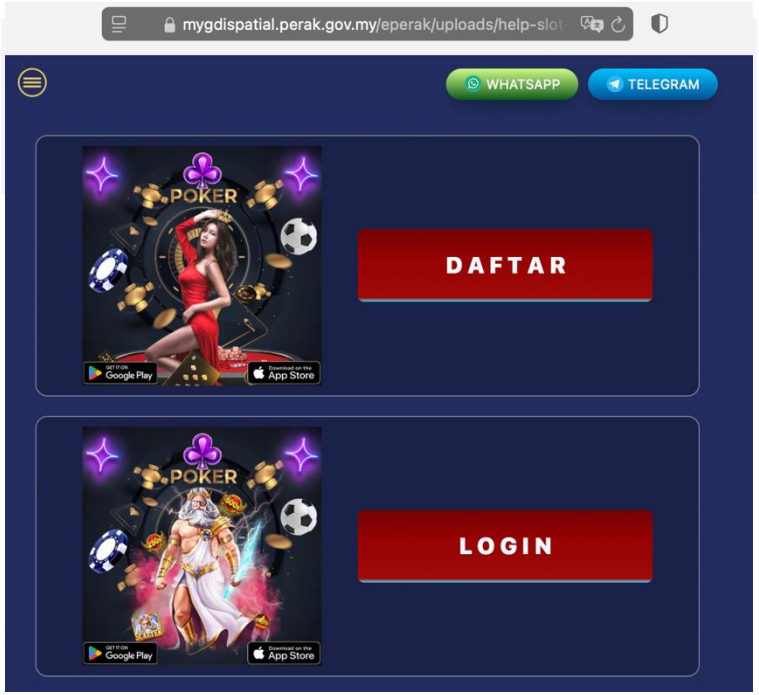
User Credentials Leak	Security Misconfiguration	Sensitive Data Leak
Fidelity 95%	Fidelity 75%	Fidelity 65%

USE CASE #4 – SYSTEM COMPROMISE (SUBDOMAIN TAKEOVER)

THREAT

Open Ports

21	53	80	143	161	443	465
2086	2087	2095	2096			



IDENTIFY / DETECT

- Shadow IT
- System Compromise

RESPOND / PROTECT

- Site Defacement Playbook
- Incident Response
- Custom SOAR

AI-NATIVE CONSENSUS THREAT PREDICTION (NEW)

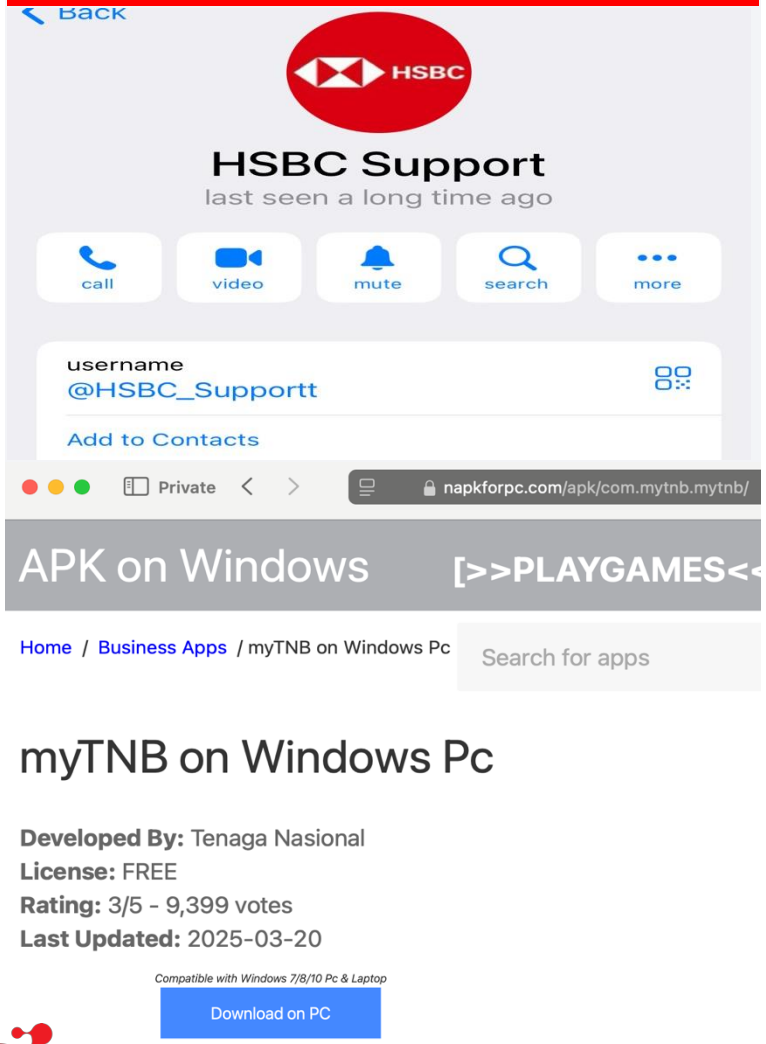
Security Misconfiguration — Fidelity 95% → Vulnerable Attack Surface — Fidelity 75% → System Compromise — Fidelity 70%

CODERED CYBER

Provintell

USE CASE #5 – IMPERSONATION THREAT AND FAKE APPS (SCAM)

THREAT



IDENTIFY / DETECT

- Online Fraud Threat
- Executive Impersonation
- Fake Apps Monitoring

RESPOND / PROTECT

- Social Media Takedown
- Fake App Takedown
- Automated Takedown
- Custom SOAR

AI-NATIVE CONSENSUS THREAT PREDICTION (NEW)

CODERED CYBER

Provintell

Comprehensive Exposure Coverage

INCIDENT RESPONSE / COMPROMISE ASSESSMENT	SECURITY TESTING AND RISK ASSESSMENT	CONFIGURATION MANAGEMENT	VULNERABILITY MANAGEMENT
1. System Compromise 2. Sensitive Data Leak 3. User Credentials Leak	4. Hack Threat 5. DDoS Target 6. Phishing Threat 7. Online Fraud Threat 8. Internet Reputation Risk	9. Shadow IT 10. Security Misconfiguration and Public Exposure	11. Vulnerable Attack Surface 12. Third Party Risk

Mobile Alert

Email

Security Dashboard

24/7 SOC Live Chat

Integrated Ticketing System

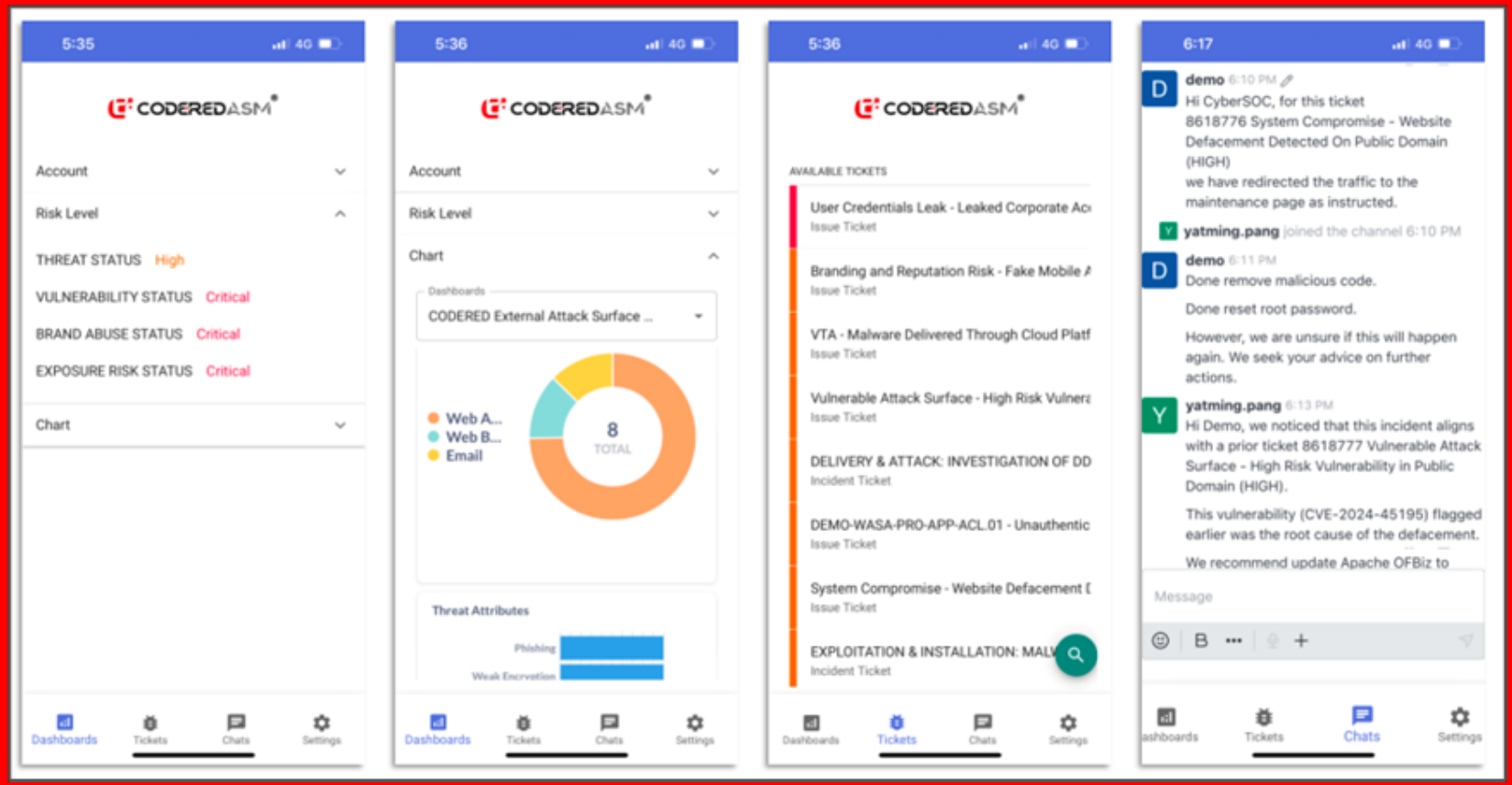
Monthly Report

Annual Service Subscription

Add-on Services

GET THE LATEST CODE RED ALERTS AND THREAT MITIGATION ADVISORIES VIA

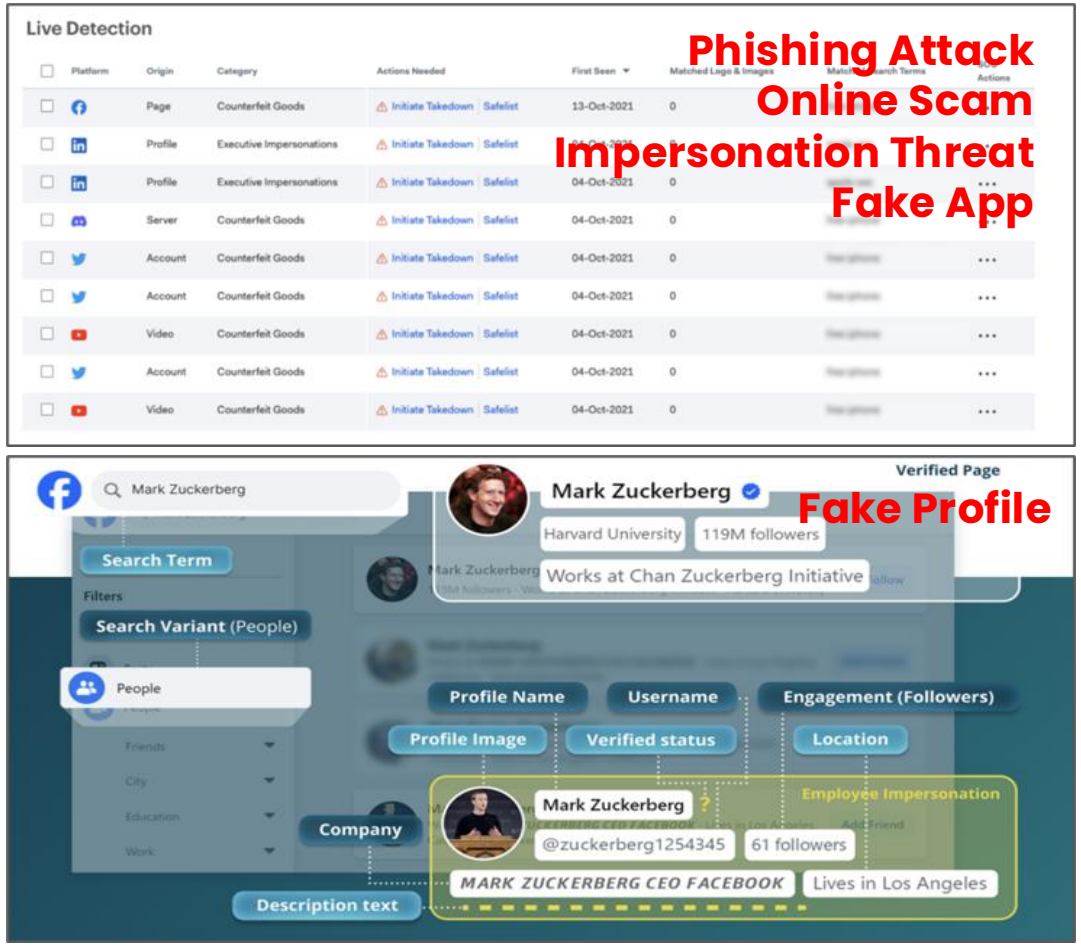
THREAT RESPONDER MOBILE APP



ANYTIME ANYWHERE

Provintell

CODEREDASM® BRAND PROTECTION Service



24/7 Live Detection Platform and SOC Monitoring

AI-driven live detection engines.
24/7 SOC monitoring and response.

- Social Media
- App Store
- Websites

Extensive coverage across all major social media platforms and over 500 app stores.

Automated and Unlimited Takedown

AI-assisted response (CoPilot)
Automated and managed takedown.

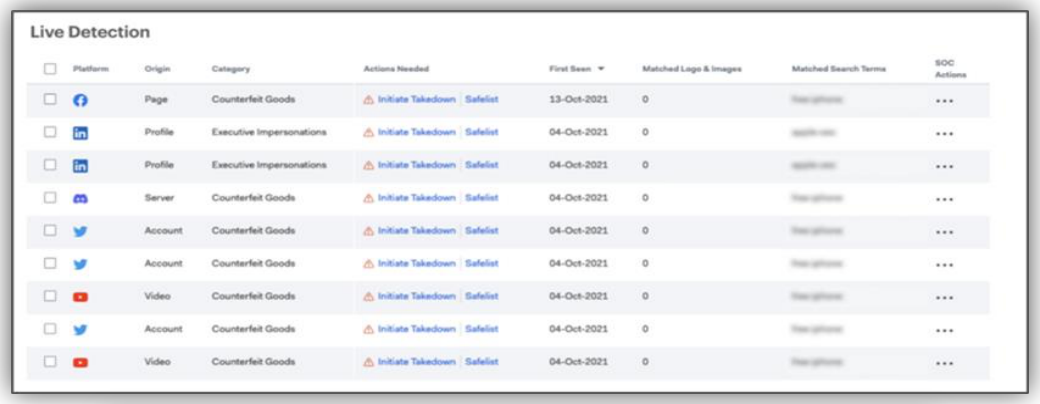
95%	2 mins	Unlimited
w/o manual intervention	Avg API based takedown time	Takedown service

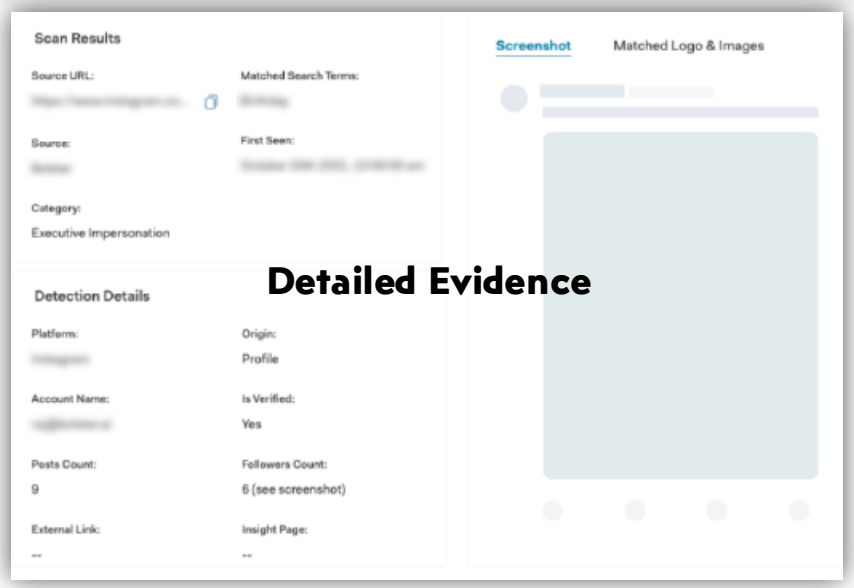
* Statistics source from integrated brand protection platform

Social Media IMPERSONATION Monitoring

- Fake Profiles
- Phishing Campaigns
- Scams
- Counterfeit Listings
- Executive Impersonations

Live Detection Platform





Detailed Evidence

1 AI-driven Detection and Takedowns

Automatically detect fake pages, logo abuse, fake ads, counterfeit products, unauthorized sales, phishing campaigns.

2 Extensive Coverage

Covering wide range of major social media platforms.

3 24/7 Monitoring

Managed by 24/7 Security Operation Center for alert notification and response.

FAKE APP Monitoring

App Stores

Detect unauthorized and fake apps

Websites

Detect fake apps related scam sites

1

CODEREDASM®

Multi-channel threat detection engines

+

Managed by 24/7 Security Operation Center

2

Remove unauthorized and fake apps

3

Block or **takedown** malicious scam sites

For Financial Services

1

Actionable Threat Intelligence for Digital Risk Protection

External attack surface management.

Analyze risks and warn security teams on potential threats and exploitable vulnerabilities. Early warning system.

Highly contextualized alerts with zero false alarm.

2

Continuous Threat Exposure Monitoring and Response

Continuously identify, monitor, and mitigate the attack surfaces and exposure risks on organization's public facing assets.

Automated and coordinated action playbooks to remove the identified threats.

Integration with SOC workflows.

3

Brand Reputation Monitoring and Response

Online financial scams and phishing campaigns.

Impersonation and brand infringement threat.

Automated threat mitigation

For Healthcare

Protecting Patient Data

Securing patients' information.

Compliance with health data regulations.

Improved data protection.

Ensuring Compliance with Regulations

Regulatory landscape for healthcare.

Best practices for compliance.

Reporting and audit requirements.

Incident Response

Developing healthcare-specific response plans.

Quick response to data breaches.

Case studies of incident response.

For Retail and E-Commerce

Safeguarding Customer Information

Protecting customer data.

Ensuring secure transactions.

Handling data breaches and notifications.

Preventing Fraud and Cyber Attacks

Techniques for fraud detection and prevention.

Securing the common attack surface in retail and e-commerce.

Strategies for strengthening security posture.

Enhancing Consumer Trust

Building customer confidence through security.

Transparent communication of risk management practices.

Enhancing user experience while ensuring security.

For Telco

Cyber Attacks

Identifying and managing the exposure to denial of service, malware and phishing attacks on the telecommunication networks.

Privacy and Trust

Securing the common attack surface in the telecommunication networks which can lead to the exposure and misuse of customer data, impacting privacy and trust.

Strategies for strengthening security posture.

Service Disruption

Maintaining a good cyber hygiene is essential in preventing the service interruption on the telecommunication services that are often caused by cyber attacks and technical failures.

For Government

Protecting Sensitive Information

Ensure good cyber hygiene and system security posture in protecting the confidential data, such as personal information and classified documents remain secured from unauthorized access or leaks.

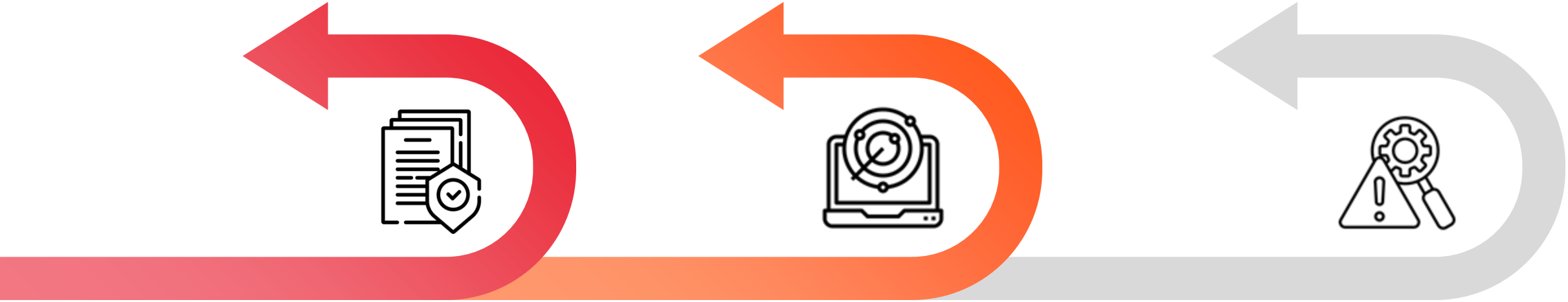
Mitigating Cyber Threats

Identifying and managing the exposure to cyber threats in safeguarding the national critical information infrastructure from data breaches.

Maintaining Public Trust

Maintain public confidence by ensuring that government entities handle and protect citizen information responsibly and securely.

For NCII
(Cyber Security Act 2024)



Licensed Penetration Testing and Managed Security Service Providers by NACSA.

Intelligence-Led Penetration Testing and Red Teaming for NCII entities.

Incident Response and Communication.

CODERED VTA

Vulnerability and Threat Advisories

"**Emerging threat** detection rules and techniques that helping you stay ahead of cyber threats"

30/10/2024

Severe Authentication Bypass Vulnerability in Fortinet FortiManager Allows Remote Code Execution

Read More →

16/10/2024

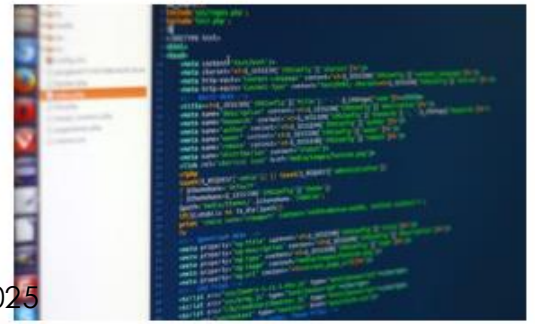
OilRig Exploits Windows Kernal Flaw in Cyber Espionage

Read More →

11/10/2024

Weaponizing Visual Studio Code for Remote Access in Sophisticated Cyber Attacks

Read More →



04/10/2024

Critical Linux CUPS Printing System Flaws Could Allow Remote Command Execution

Read More →

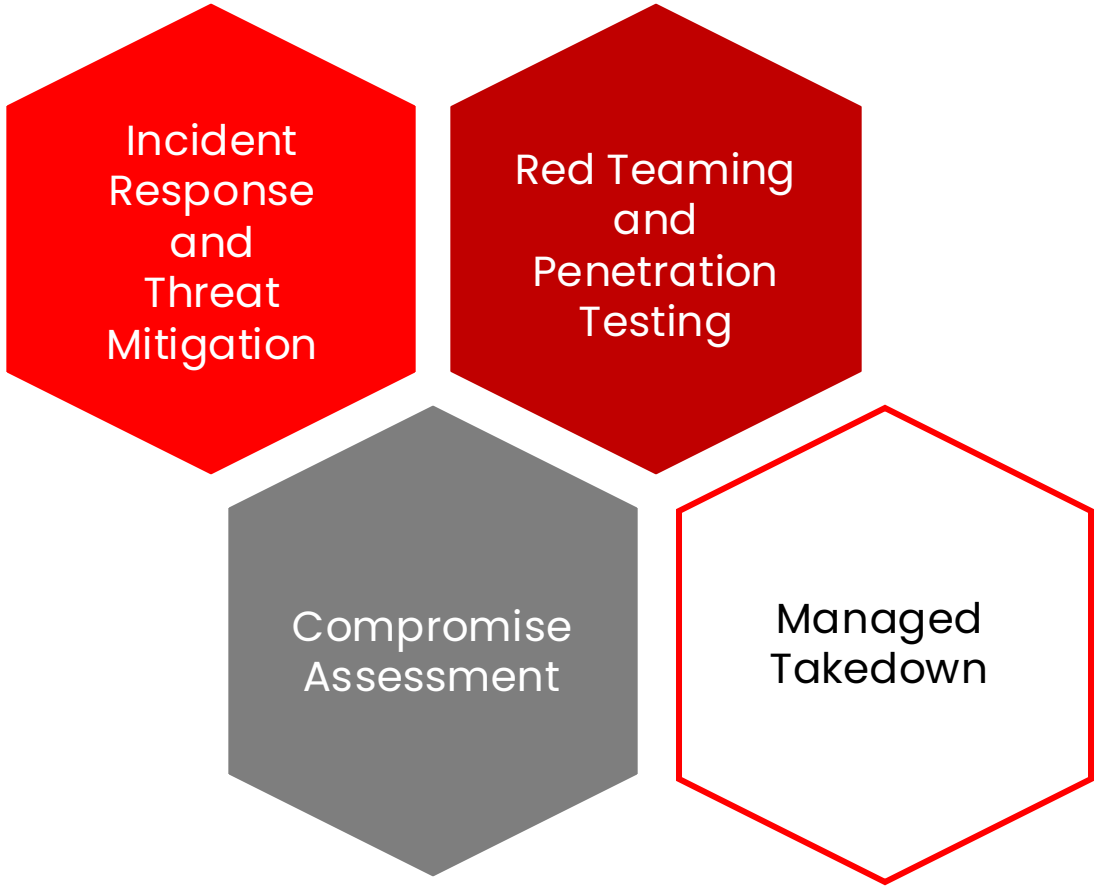
CODERED CYBER

Provintell

Add-on **Service Credits**

CODERED IR

Incident Response and Compromise Assessment



THANK YOU

is a registered trademark of

Provintell

www.provintell.com

Partnership inquiries business@provintell.com

More information info@provintell.com