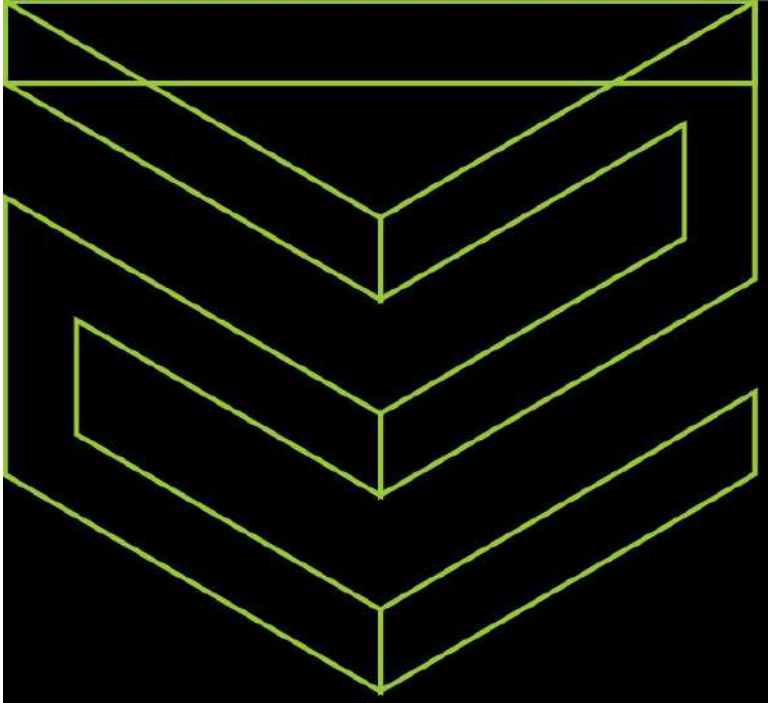
ESTABLISHED / YEAR 2016



TJAKRABIRAWA

INTELLIGENT SECURITY SERVICES

COMPANY PROFILE
ver. 2022

CYBER ATTACK IN NUMBERS

COMPANY OVERVIEW

OUR SERVICES

“

There are only two
types of companies:
those that have been hacked,
and those that will be.

Robert Mueller
FBI Director,2021

01/ BACKGROUND STORIES

Cyber attacks have been rated the fifth top rated risk in 2020 and become the new norm across public and private sectors. This risky industry continues to grow in 2022 as IoT cyber attacks alone are expected to double by 2025.

Nearly every industry has had to embrace new solutions and to forced companies to adapt, quickly.

Source: https://www.embroker.com/blog/cost-of-data-breach

Consequences of the cyber security incident may still impact your business weeks, if not months, later. Below are five areas where your business may suffer:

- Financial losses
- Loss of productivity
- Reputation damage
- Legal liability
- Business continuity
- Business continuity problem

02/ CYBER ATTACK IN NUMBER

92% Of **malware** is delivered by email.

25% Of businesses are estimated to have been victims of **cryptojacking**

98% Of cyber attacks rely on **social engineering**

63% Recent data breach statistic found that 63% of successful attacks come from internal sources, either control, errors, or fraud

43% Of cyber attacks target small business

60% Of small companies go out of business within six months of syver attack.

79% Of financial institutions said **Cybercriminals ave become more sophisticated**, leveraging highly targeted social engineering attacks.

67% Of financial institutions reported an increase in **home equity loan fraud**


WHAT
ABOUT
INDONESIA?

Data of 2 million of the BRI life insurance's customers were sold online for

US$ 7,000

Based on the account's image post, exposed data include electronics ID card information, birth certificate, and health track records.

In May 2020, millions of personal data was non-consensually stolen from the popular e-commerce, Tokopedia. Some even claimed the exposed 91 million personal data was sold for

US$ 5,000

An internet user claimed to have information of the breach of 2.3 million Indonesians from the General Elections Commission (KPU) website back in May 2021. This user believed the data breach took place since 2013 and claimed that the hackers threaten to leak

200 million

“

Cyber security is **not a cost center**, but reliable investment to support business and **generate profit.**

Green
Tjakrabirawa
Director
2022

CYBER SECURITY IS AN INVESTMENT

Cyber crime will cost companies worldwide an estimated $10.5 trillion annually by 2021, up from $3 trillion in 2015.

WHY CYBER SECURITY IS AN INVESTMENT?

Cyber security is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry systems.

03/ WE ARE TJAKRABIRAWA

Established in 2016 to help our client gained access to professional cybersecurity services. Create a better business with our security services.

WHY US ?

Our security export has deep knowledge in wide range of security services, such as penetration testing. Digital forensic and fraud analysis, but not also it, we align our technical specialities with business mindset, so we can help your business mindset, help your business to grow.

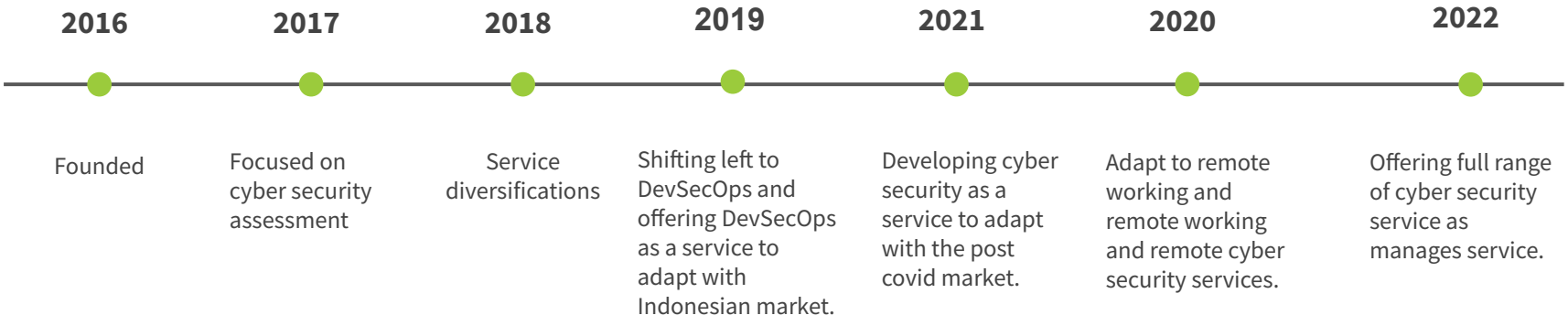
Our value and beliefs, as a dedicated security consulting company, we committed :

To insist on **excellent** in every task

To give highest standards of ethics, integrity, trust, and confidence

To pay attention **very detail in every project**

04/ COMPANY MILESTONES



WHY US ?

WIDE RANGE OF CYBER SECURITY SOLUTION

We offered a complete spectrum of cybersecurity services which include technical and compliance services.

REAL LIFE ATTACK SIMULATION

We can simulate real life attacks and give a deeper insight how targeted attack can occur and how can damage your business

ENSURING YOUR COMPANY COVERED

We constantly utilize our research and development so we can dig a new vulnerability and attack vector to ensure your company covered.

INTERNATIONALLY RECOGNIZED CERTIFICATION

Our team competence are backed up with certification from international certification body such as OffSec & CompTIA

STANDARDIZE METHODOLOGY

Standardized methodology which benchmark our works with OSSTM, ISSAF, OWASP, PTES plus our experience and creativity.

TAILORED BASED ON CLIENT NEEDS

Our expertise are customizable by client requirement to ensure the best delivery while maintain flexibility.

We respect our client confidentiality, privacy, and secrecy, through NDA and our team integrity.

05/OUR CLIENTS

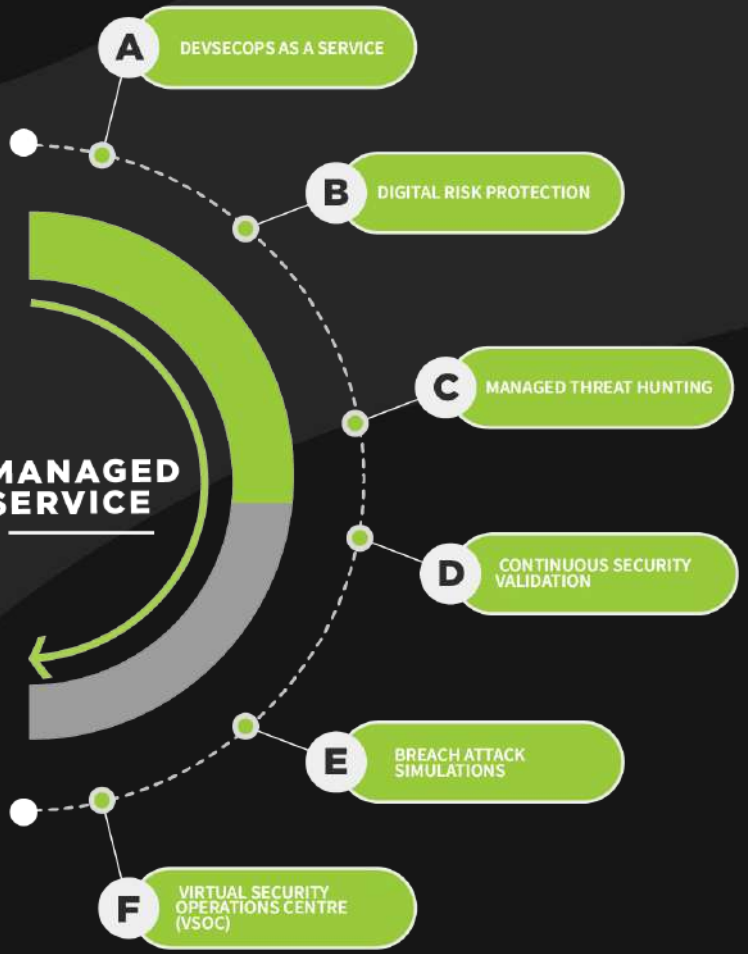
05/OUR CLIENTS

COMPANY PROFILE / YEAR 2022

FUTURE PROOF CYBER SECURITY SOLUTIONS

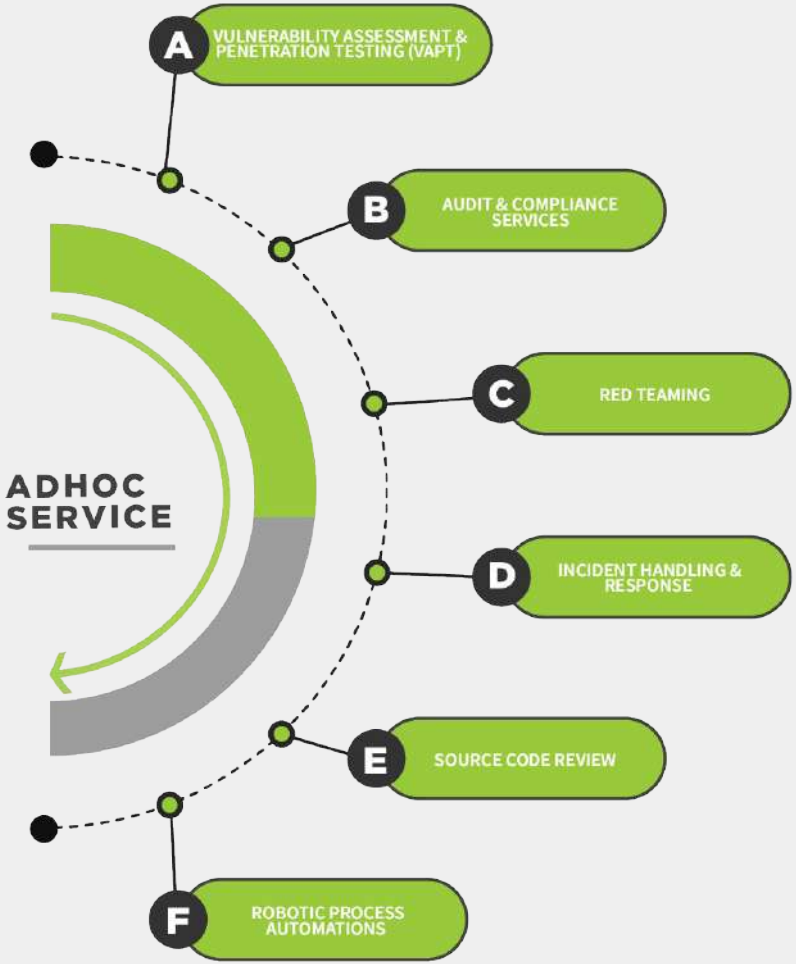
TJAKRABIRAWA
INTELLIGENT SECURITY SERVICES


1
MANAGED SERVICE
PRODUCT
ADHOC SERVICE
2



Continuous Cyber Security Service

1



Ala Carte Cybersecurity Service.

2

Ala Carte Cybersecurity Service.

2

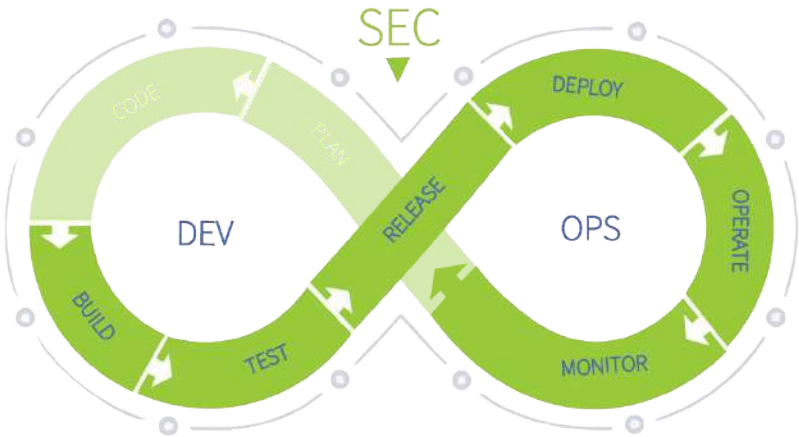

1
MANAGED SERVICE
PRODUCT
ADHOC SERVICE
2

A DEVSECOPS AS A SERVICE

Offering DevSecOps end to end services minus the time and resources as soon as possible.

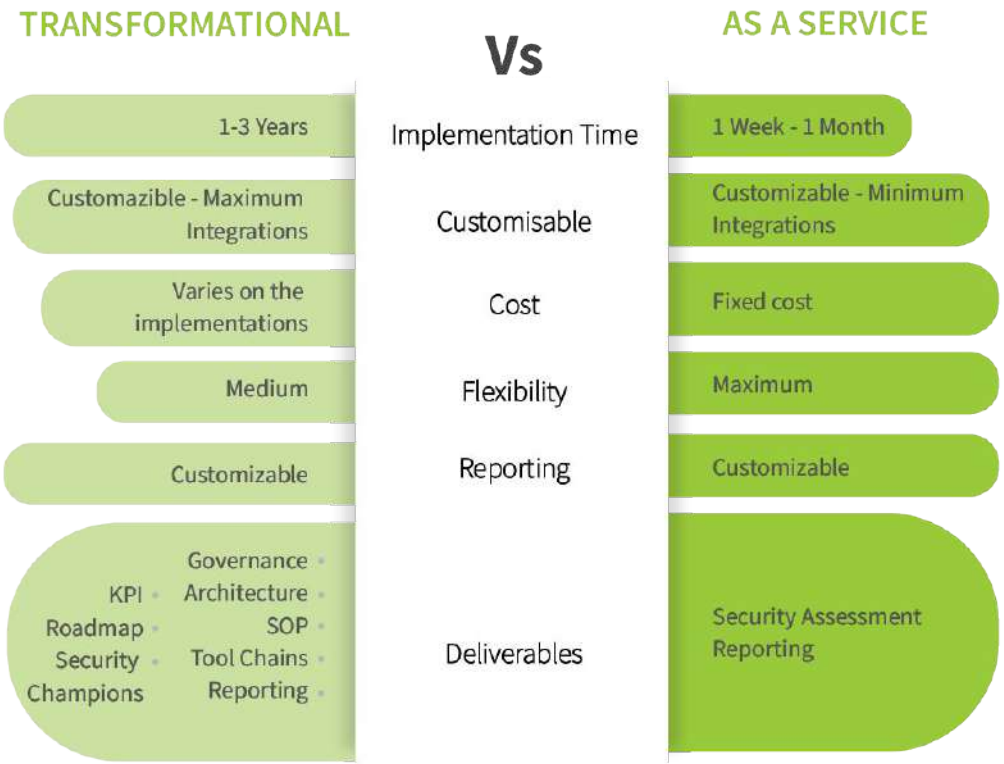
The main advantage of devsecops as a service:

- Integrate with current ci/cd pipeline
- End to end security services
- Easy integrations (days-weeks)
- Flexible tool chain options
- Fixed cost
- Include bug bounty services



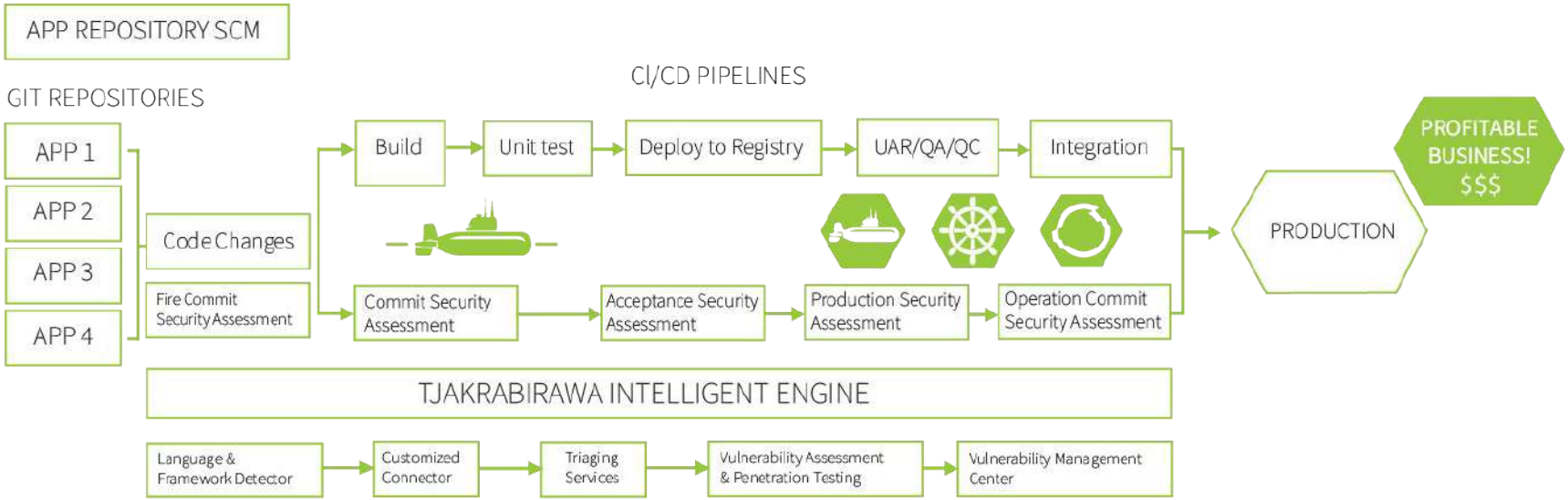
DEVSECOPS AS A SERVICE

COMPARISON TABLE



DEVSECOPS AS A SERVICE

ARCHITECTURE DIAGRAM



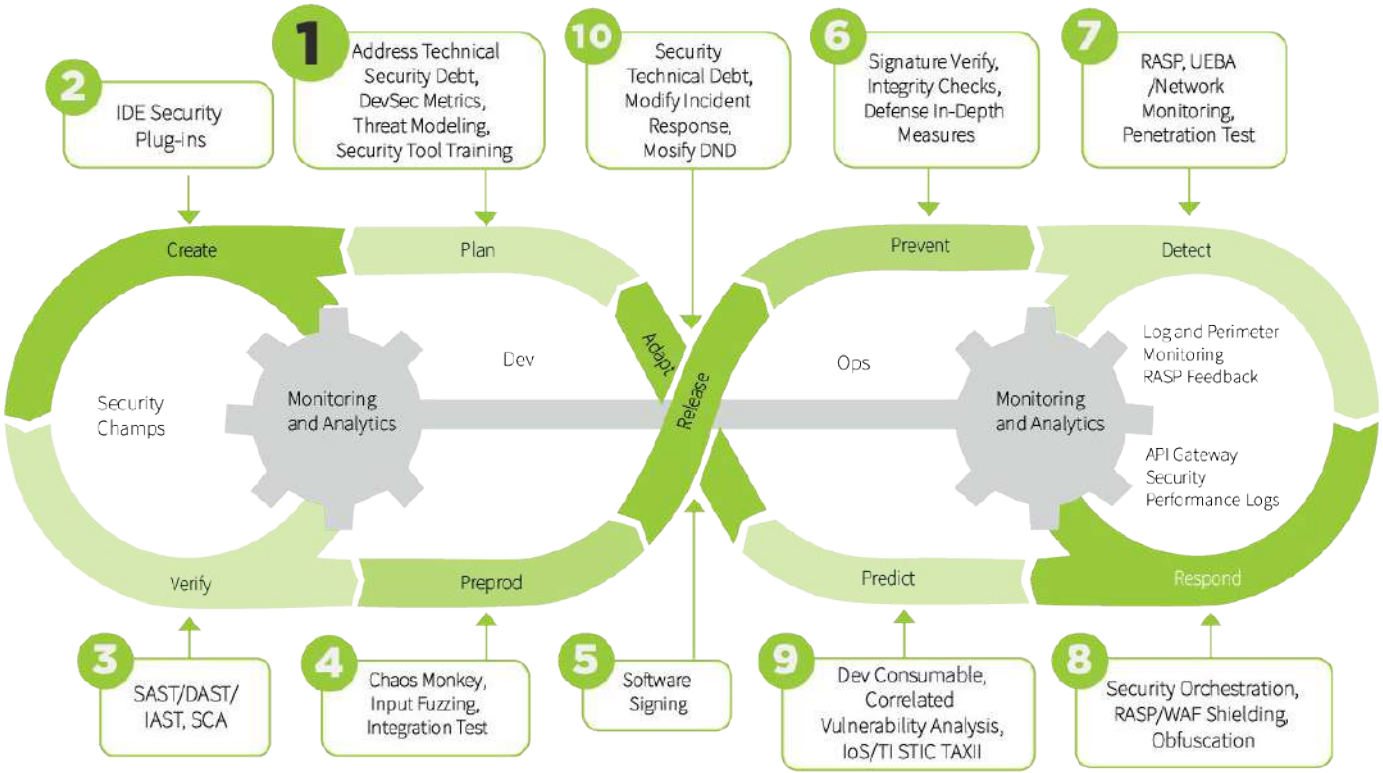
DEVSECOPS AS A SERVICE

PRODUCT

STATIC ANALYSIS SECURITY TESTING (SAST)	CONTAINER SECURITY	TRIAGING
SOURCE COMPOSITION ANALYSIS (SCA)	MANUAL PENTEST	REPORTING & RECOMMENDATIONS
SOFTWARE BILL OF MATERIAL (SBOM)	DYNAMIC ANALYSIS SECURITY TESTING (DAST)	BUG BOUNTY SERVICES

DEVSECOPS AS A SERVICE

TOOLCHAIN



B DIGITAL RISK PROTECTION

The SaaS-based platform combined with our global intelligence analyst increase the real-time visibility of sensitive data exposed online by over 80%. As a result, organizations receive predictive early actionable intelligence to identify and mitigate risks associated with ransomware, extortion, and data leakage.

HOW DIGITAL RISK PROTECTION SERVICES HELP STRENGTH CLIENT DEFENSE PROGRAMS:

1 MANAGE BRAND REPUTATION RISK

- Phishing and Typo-squatted domains
- Social media and mobile app store monitoring
- Executive profile monitoring
- Website Watermarking/ Defacement detection
- Take downs

2 DETECT AND PREVENT FRAUD

- Compromised credit and debit cards
- Voucher, coupons, gift cards
- ATM/cars PINs
- Account take-over
- Business email compromise

3 REDUCE CYBER ATTACK SURFACE

- Critical vulnerabilities and open ports.
- Misconfigured cloud storage buckets (AWS, Azure).
- Source code leaks.
- Exposed secrets/API keys/Access tokens in GitHub.
- Bot Infected Systems.
- Vulnerability intelligence for priorities remediation.

4 MANAGE SUPPLY CHAIN CYBER RISK

- Vendor cyber risk scoring.
- Critical vulnerabilities in third party assets.
- Compromised vendor credentials on the dark web.
- Sensitive company data exposed in third party data breaches and ransomware attacks.
- Corporate date exposed in third party cloud storage.

5 PERSONALLY IDENTIFIABLE INFORMATION

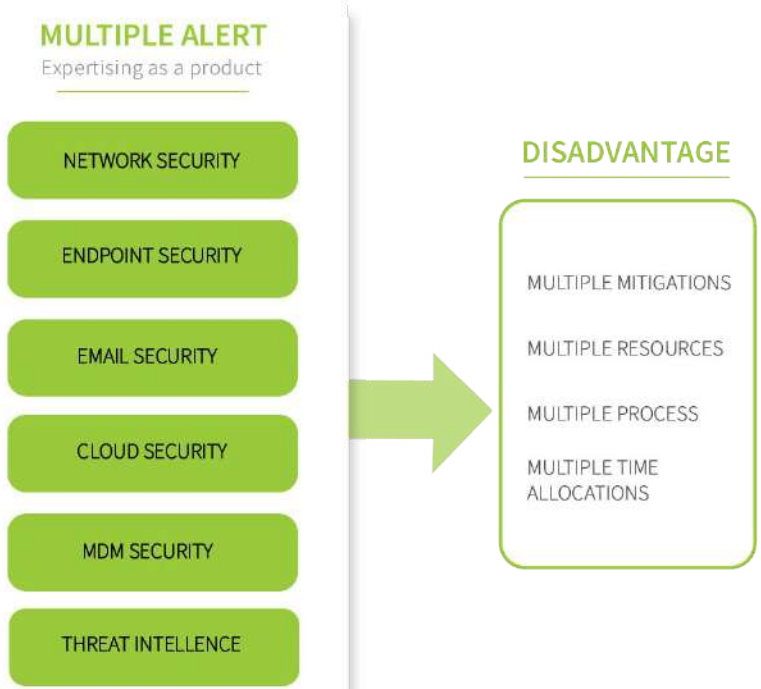
- Personally identifiable information (PII) leaks.
- Protection Health information (PHI) leaks.
- Exposed card holder data (PAN, CVV, PIN) in data breaches.

6 HUNTS FOR THREATS

- Global sensor network for IOC feeds
- Malware/Phishing campaigns.
- IOC integration with SIEM and SOAR solutions.
- Threat intelligence advisories.
- Weekly sensor intelligence reports.

C MANAGED THREAT HUNTING

Offering 24/7 Active Threat Hunting to stay ahead of the curve and minimizing the risk and exposure of Data Breach.

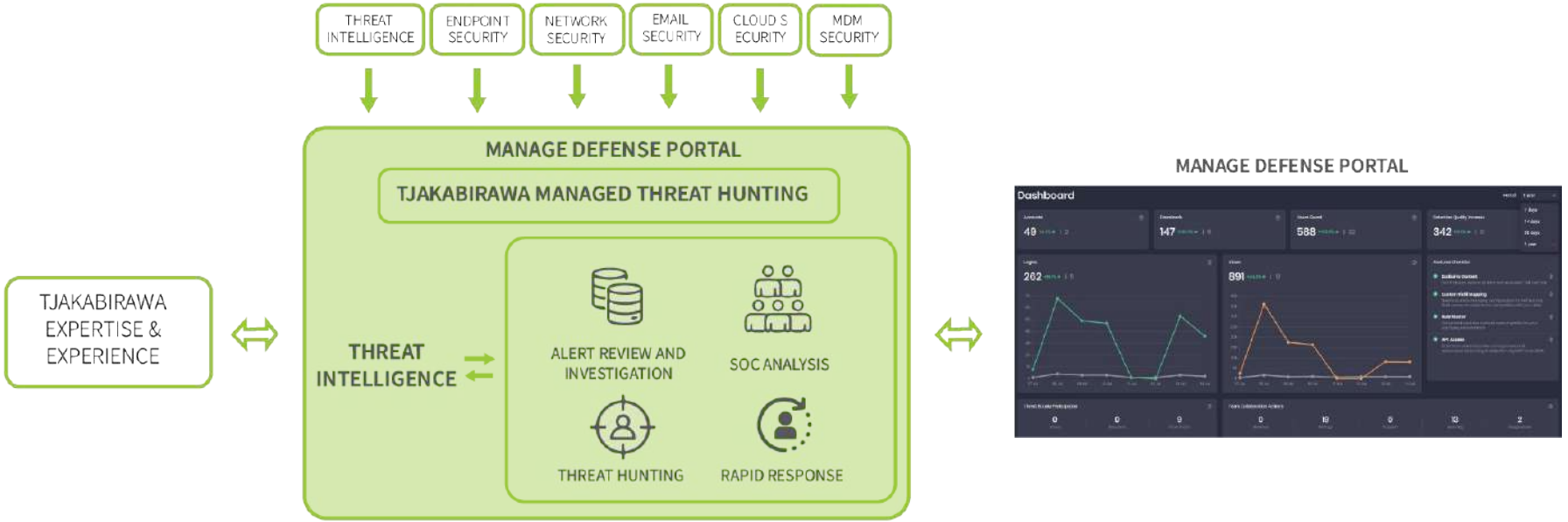


MANAGED THREAT HUNTING

FLOW

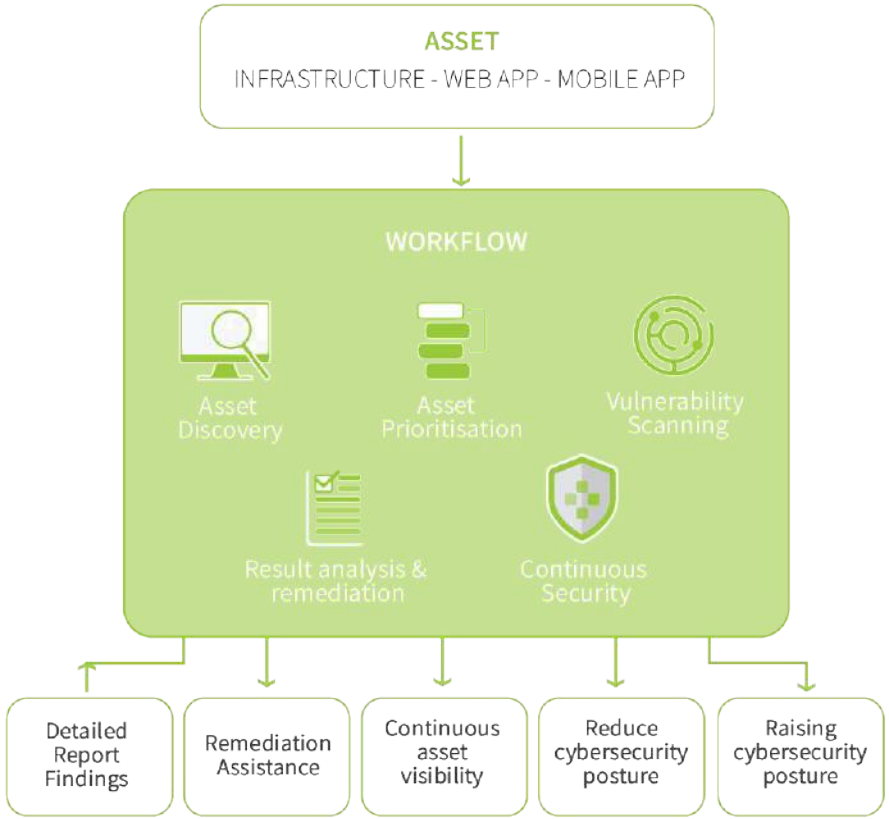
MANAGED THREAT HUNTING

EXPERTISE AS A SOFTWARE



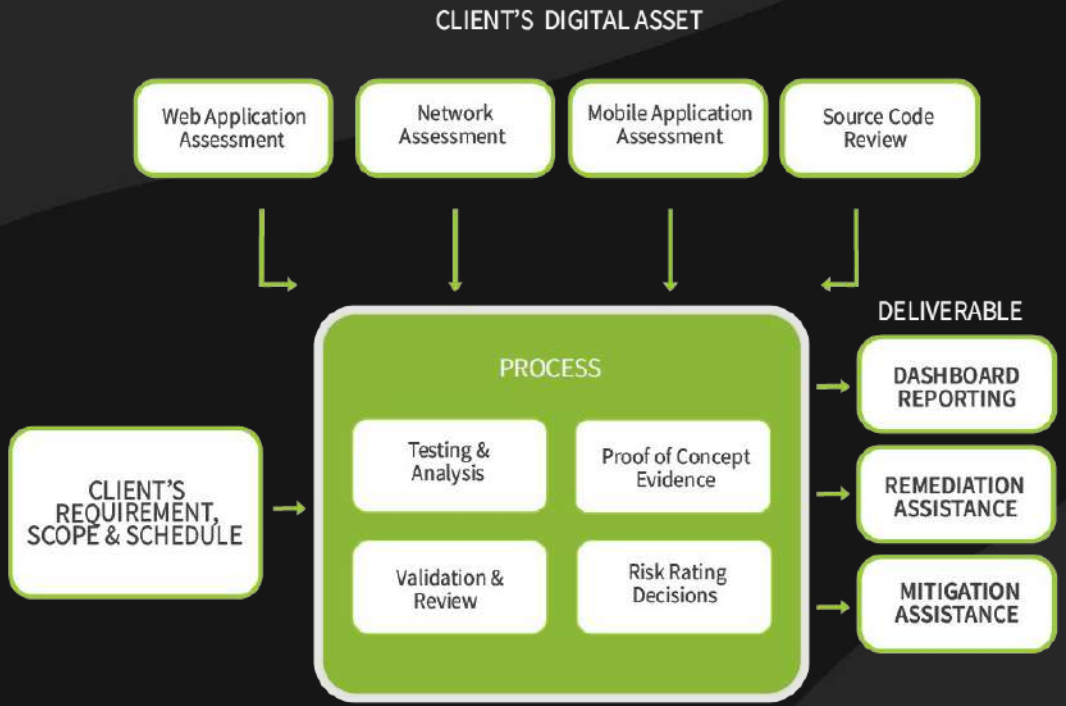
D CONTINUOUS SECURITY VALIDATION

Offering vulnerability Management end to end services to conduct assessment, triaging, remediation assistance and management, to protect the organization crown jewel.



CONTINUOUS SECURITY VALIDATION

ARCHITECTURE DIAGRAM



E BREACH ATTACK SIMULATIONS

Offering safe and reliable Adversary Emulation to validate the defensive perimeter, by people process and technology aspect

Which area can we improve / reduce?

Are we susceptible with the breach that happened to company ABC?

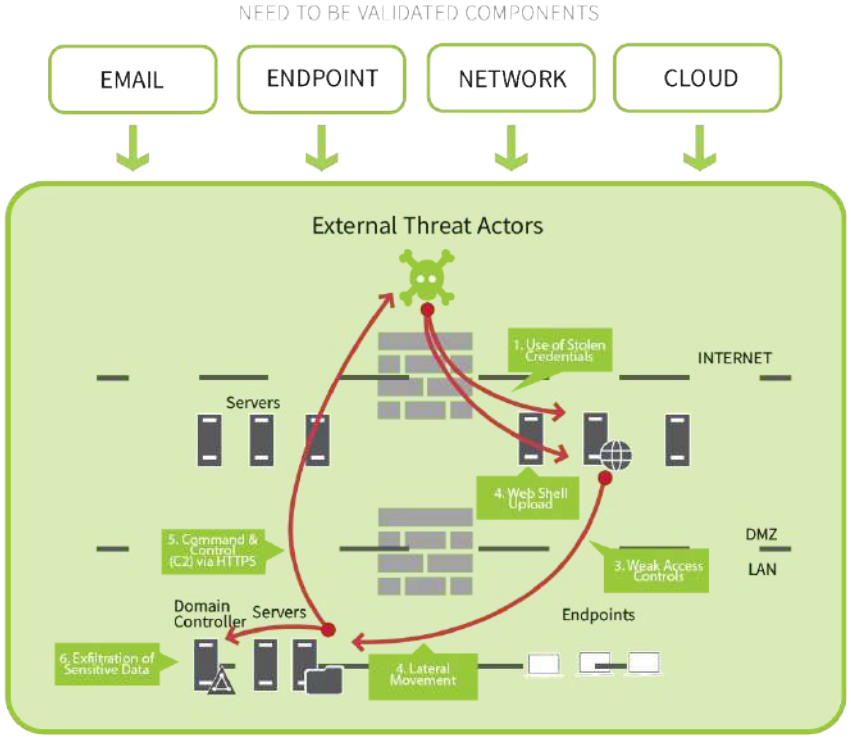
Could actor XYZ compromise our business?

How to validate our defense mechanism?

Can we breached by the latest attack?

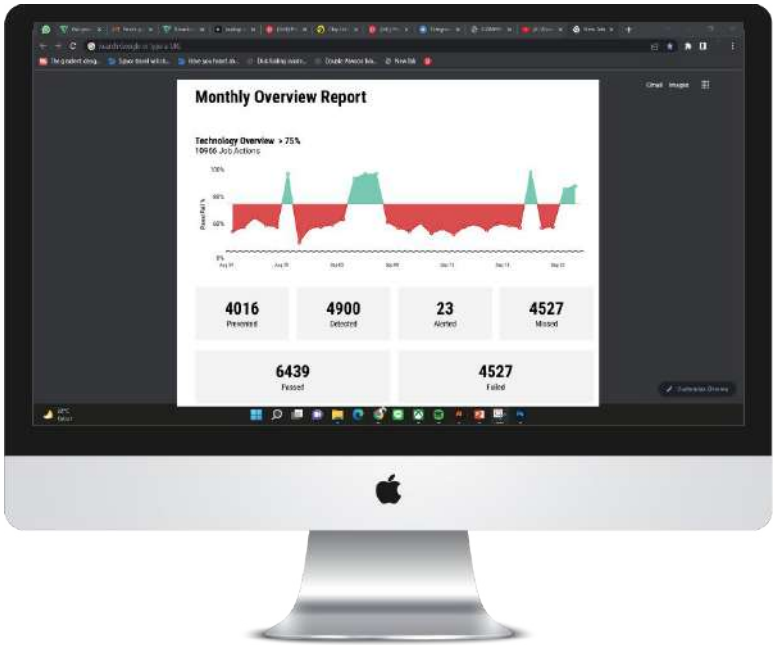
BREACH ATTACK SIMULATIONS

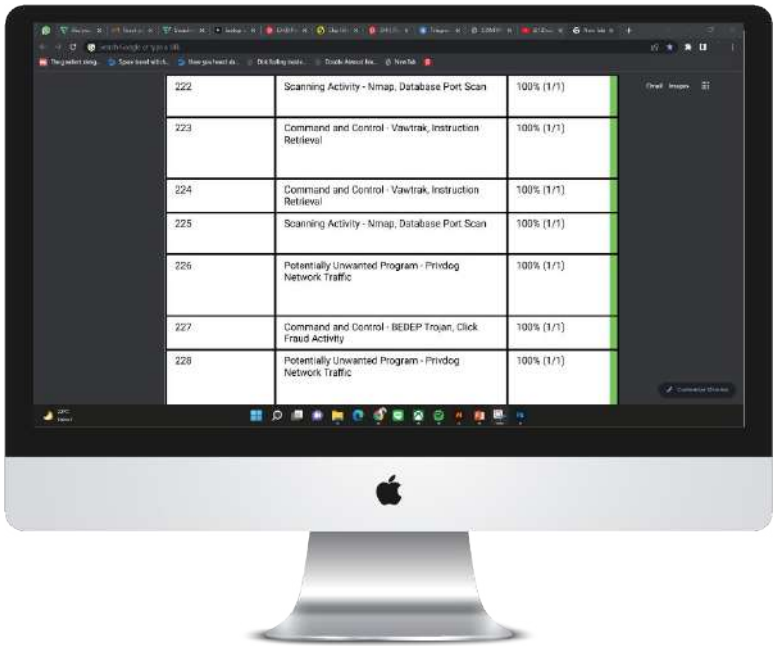
ARCHITECTURE DIAGRAM



BREACH ATTACK SIMULATIONS

REPORT SAMPLE

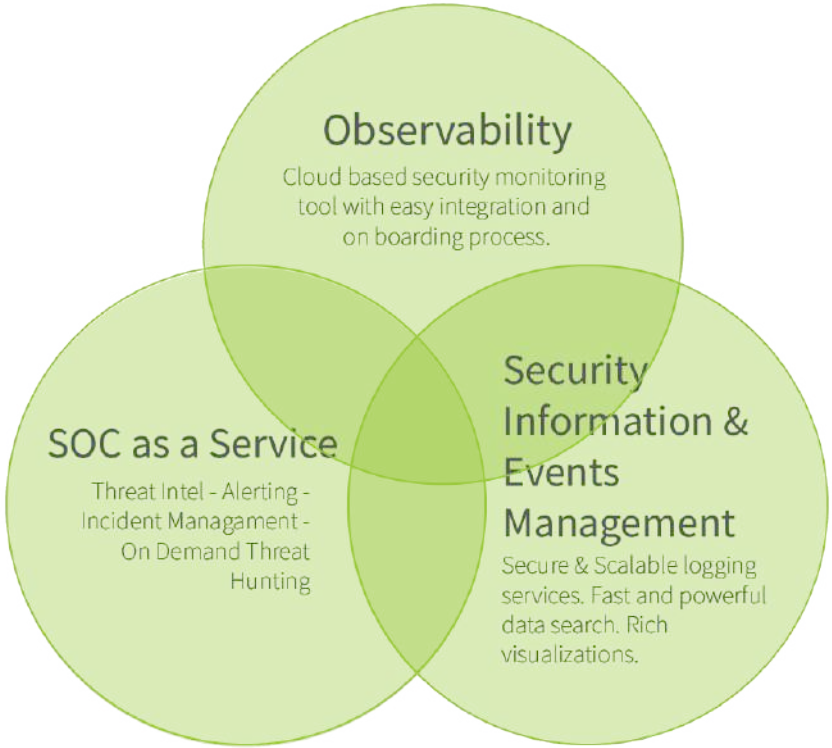




222	Scanning Activity - Nmap, Database Port Scan	100% (1/1)
223	Command and Control - Vawtrak, Instruction Retrieval	100% (1/1)
224	Command and Control - Vawtrak, Instruction Retrieval	100% (1/1)
225	Scanning Activity - Nmap, Database Port Scan	100% (1/1)
226	Potentially Unwanted Program - Privdog Network Traffic	100% (1/1)
227	Command and Control - BEDEP Trojan, Click Fraud Activity	100% (1/1)
228	Potentially Unwanted Program - Privdog Network Traffic	100% (1/1)

F VIRTUAL SECURITY OPS CENTRE

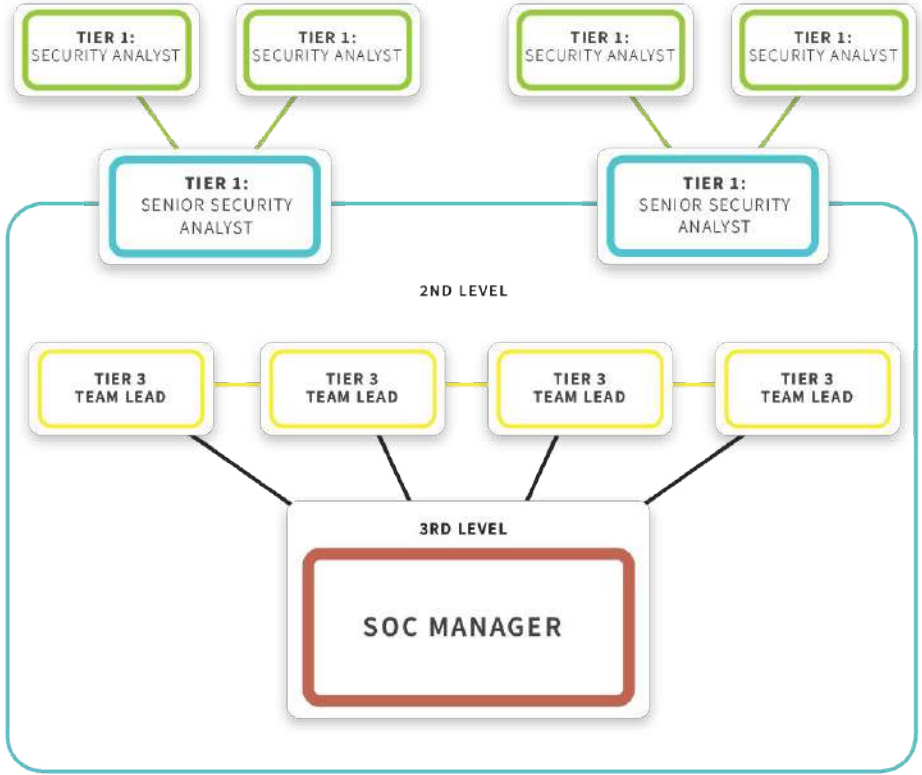
Offering an managed, comprehensive data monitoring solution where security analysts continuously survey an enterprise's digital network, detect nefarious activity, and respond to emerging threats.



TJAKRABIRAWA COMMITTED TO DELIVER THE NEXT GEN VSOC

VIRTUAL SECURITY OPS CENTRE

STRUCTURE




1
MANAGED SERVICE
PRODUCT
ADHOC SERVICE
2

A VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

A vulnerability assessment is the **process of identifying and quantifying known security vulnerabilities in an environment.** It is a surface-level evaluation of your information security posture, indicating weaknesses as well as providing the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk.

A penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization. Using many tools and techniques, the penetration tester attempts to exploit critical systems and gain access to sensitive data.

B AUDIT & COMPLIANCE SERVICE

A comprehensive review of an organization's adherence to regulatory guidelines. Audit reports evaluate the strength and thoroughness of compliance preparations, security policies, user access controls and risk management procedures over the course of a compliance audi

C RED TEAMING

A red team assessment is a goal-based adversarial activity that requires a big-picture, holistic view of the organization from the perspective of an adversary. This assessment process is designed to meet the needs of complex organizations handling a variety of sensitive assets through technical, physical, or process-based means.

The purpose of conducting a red teaming assessment is to demonstrate how real world attackers can combine seemingly unrelated exploits to achieve their goal.

D INCIDENT HANDLING & RESPONSE

Incident response. I**t is a set of technical activities done in order to analyze, detect, defend against, and respond to an incident.** It is a part of the incident handling and incident management process. It is often used in synchrony with the term incident handling.

E SOURCE CODE REVIEW

Secure code review is a manual or automated process that examines an application's source code. **The goal of this examination is to identify any existing security flaws or vulnerabilities.**

F ROBOTIC PROCESS AUTOMATIONS

Robotic process automation (RPA) is **a software technology that makes it easy to build, deploy, and manage software robots that emulate humans actions** interacting with digital systems and software.

G BUG BOUNTY SERVICES

A bug bounty program, also called a vulnerability rewards program (VRP), **is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs.** Bug bounty programs are often initiated to supplement internal code audits and penetration tests as part of an organization's vulnerability management strategy.

H SECURITY MONITORING TEAM

Tjakrabirawa will provides Layer 1 2 or 3 Analyst to manned the existing client Security Operation Centre.

I SECURITY CHAMPION DEVELOPMENT

Tjakrabirawa will train pool of security champion to help with the development and implementations of DevSecOps Culture in the client premises

J TRAINING & SECURITY AWARENESS PROGRAM

Online/Offline Cybersecurity training delivery to ensure the needs of client cyber knowledge. Cloud classroom based for Security Awareness Program with Phishing campaign included with the package.

K DATABASE SECURITY

Consult, Design, and Implementing Database Security to adhere with GDPR and future PDP regulations to provides a centralized location for documenting and managing the relevant aspects of the meta information pertaining to the personal information your organization collects both internally (e.g., from employees) and externally (e.g., from customers).

L PASSWORDLESS AUTHENTICATIONS

Tjakrabirawa will provides you with **Consultation, Design and Implementation** of a multi-factor authentication that's passwordless, meaning you will be able to verify a user's identity without usernames, OTPs, SMS or typing of any kind.

M ZERO TRUST

Tjakrabirawa will provides you with **Consultation, Design and Implementation of a security framework requiring all users,** whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

TECHNOLOGY PARTNER

CYBLE

KEYSIGHT TECHNOLOGIES

MANDIANT

eranyacloud

Checkmarx

tenable

SECURE CODE WARRIOR

radware

PALADION

TRUSONA

CHECK POINT

DARKTRACE

FireEye

proofpoint.

FEELING INSECURE?

CONTACT US

Address
PT. Tjakrabirawa Teknologi Indonesia
Manhattan Square
Jalan TB Simatupang Kav 15
125489 Jakarta Selatan

Telephone
021 - 80641090

1StopCyberSolution
0821 - 1247 - 6992

Email
info @tjakrabirawa.id

Web
www.tjakrabirawa.id