# TJAKRABIRAWA

## COMPANY PROFILE

# Table of Contents

# Table of Contents

# Tjakrabirawa Introduction

# About Tjakrabirawa

Established in 2016 in Jakarta, Indonesia, Tjakrabirawa is a trusted leader in cybersecurity solutions. We empower clients with customized, professional security services **designed to strengthen resilience and drive secure business growth.**

Our expertise spans a broad range of cybersecurity services, including **penetration testing, digital forensics, and fraud analysis.** What sets us apart is our unique approach—combining technical excellence with a business-oriented mindset. This ensures that our solutions not only safeguard your assets but also support your business's growth and success.

# Securing Your Business in a Digital Age

Results of the **cyber security breach may still affect** your commerce weeks, in case not months, afterward. Underneath are five ranges where your trade may endure:

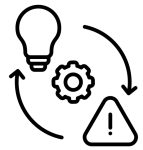
Financial losses

Loss of Productivity

Reputation Damage

Legal Liability

Business Continuity



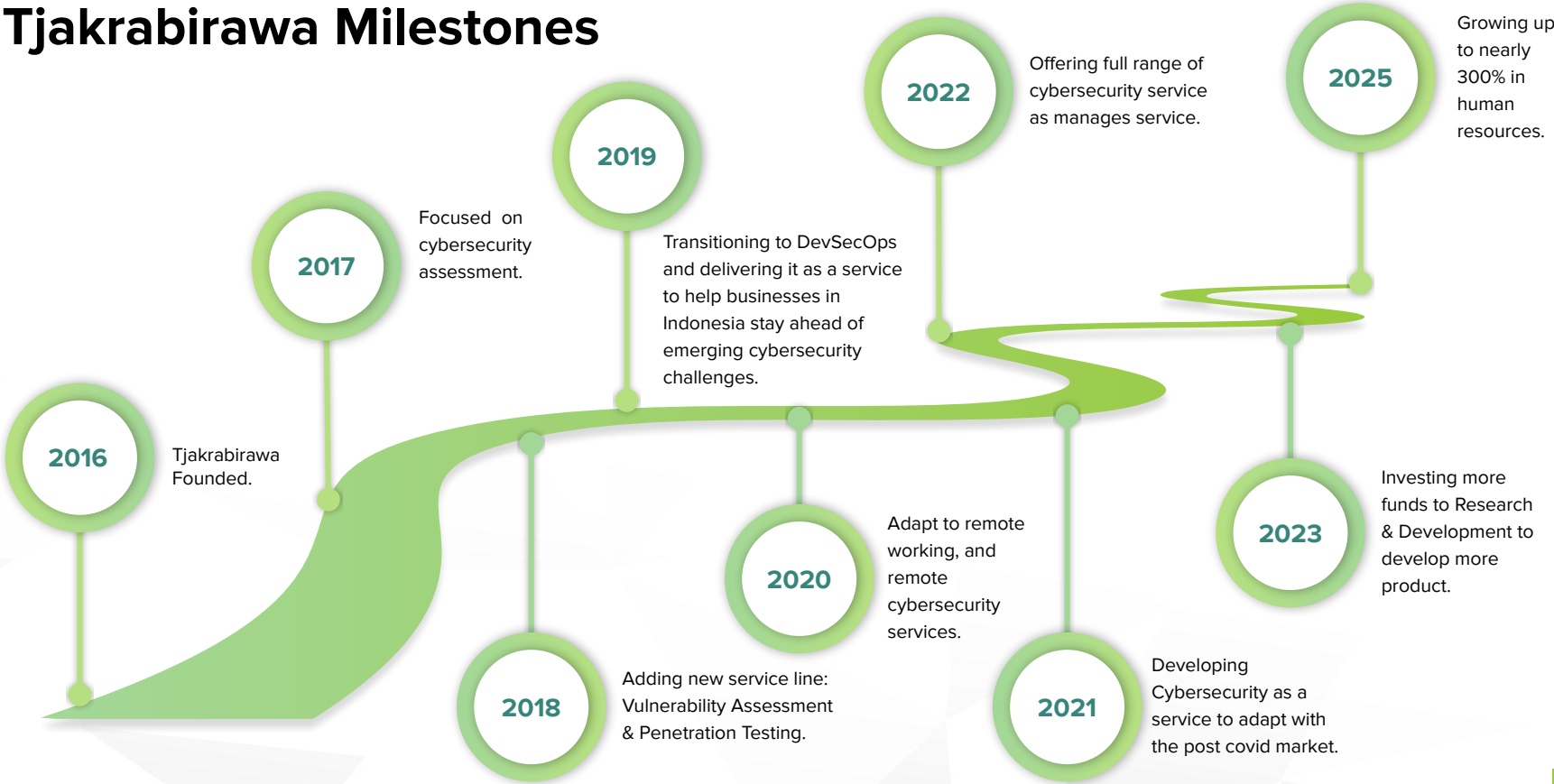
Business Continuity Problem

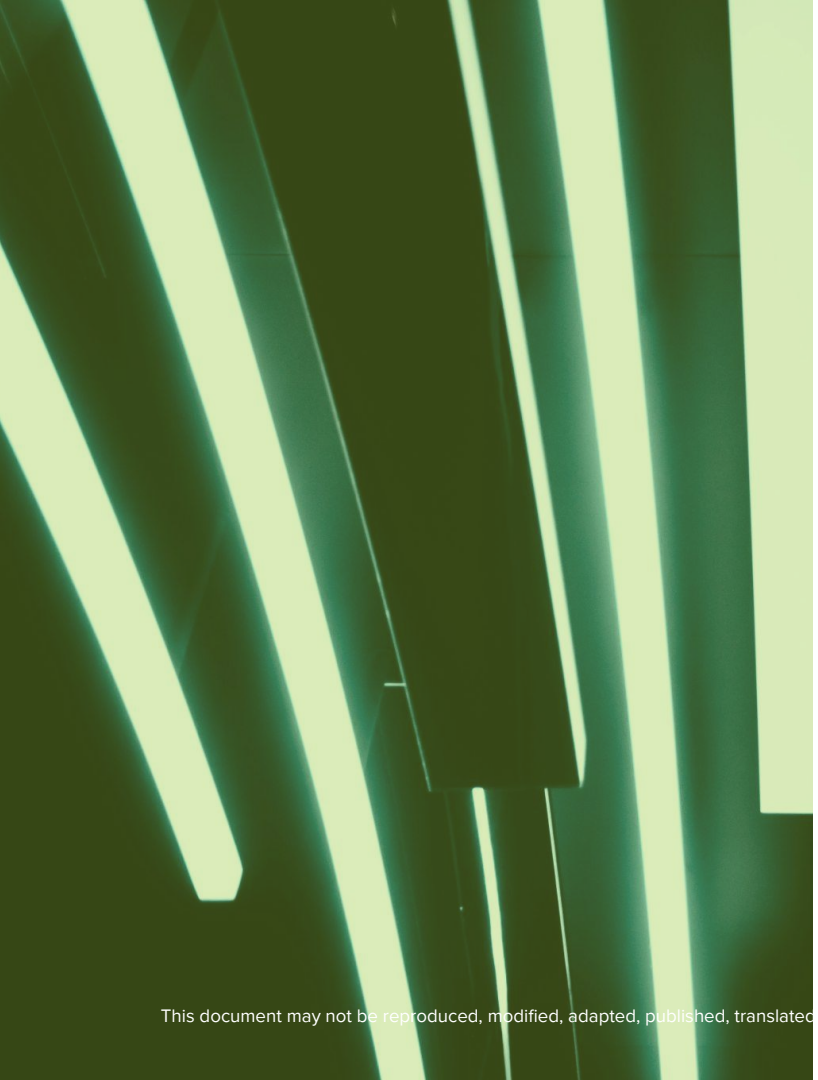
# Tjakrabirawa Commitment to Excellence

To be the leading cybersecurity partner, trusted for excellence, integrity, and **a relentless commitment to safeguarding our clients' digital futures.**

We aim to build resilient infrastructures by delivering innovative, **next-generation security solutions** that proactively address emerging threats, ensuring continuous protection and sustainable growth for businesses worldwide.

# Tjakrabirawa Milestones





# Cybersecurity Landscape

**Cyber attacks are one of the top risks** facing companies today, affecting nearly all industries globally. By 2025, cyber attacks through IoT alone are **expected to double.**

# Why Choose Cybersecurity


Investing in cybersecurity is not just a cost but **a strategic advantage** that protects reputation, operational continuity, and customer trust.

# Cyber Attack in Number

**98%**

Cyber attacks rely on **social engineering.**

**92%**

**Malware** is delivered by email.

**79%**

**Cybercriminals ave** leveraging highly targeted social engineering attacks.

**67%**

Financial institutions reports an increase in **home equity loan fraud.**

# Cyber Attack Case in Indonesia

Data of 1.5 Tb **BSI customers were sold online for**

**$20.000.000**

Personal and financial information loss due to the ransomware attack.

**2021 an internet user claimed had 2.3 million Indonesians data** from KPU since 2013, and undermine to spill

**Rp200.000.0000**

**2 mio of BRI Life Insurance** customers were sold online **$7.000**

**91 mio of Tokopedia personal** data were sold online **$5.000**

**300**

**Central and local state impacted**

The data loss at the Pusat Data Nasional Sementara (PDNS) has caused significant disruption to immigration services and major airports in Indonesia.

# Cyber Attack Case in Indonesia

**Indodax cyber attack** potential lost

**$14.400.000**

Of unauthorized access and security lapses by North Korea Hacker.

**Bjorka exposed KPU user personal data of**

**105.000.0000**

Details of National ID numbers, home addresses, and others.

**1.3B Data**

**Ministry of Home Affairs, Kominfo** personal data was scattered online.

**26B Data**

**POLRI user data spread out;** names, employee numbers, phone numbers.

**26M Data**

**Indiehome user data spread out ;** browsing history, locations, and others.

**17M Data**

**PLN user personal data spread out ;** customer IDs, full names, addresses.

Source: restofworld.org

# Tjakrabirawa Accreditation & Certification

# Cybersecurity Accreditation & Affiliation



**PT. Tjakrabirawa Teknologi Indonesia** has been registered of Badan Siber Sandi Negara (BSSN) & Asosiasi Sistem Pembayaran Indonesia (ASPI).

# Tjakrabirawa Engineer Certification





**PT. Tjakrabirawa Teknologi Indonesia** professional technicians is dedicated to delivering exceptional service, putting expertise and attention to detail above simply relying on tools.

# Tjakrabirawa Clients

# Tjakrabirawa Clients

## Banking & Financial

bank bjb

Bank SBI Indonesia
A subsidiary of State Bank of India (SBI)

bank btpn

BNI

AIA

ARTAJASA

SHINHAN

cermati

ZIPMEX

indodana

byorange

btn

youtap

ALTO

Surya Anugrah Mulya

CGSCIMB
PT CGS-CIMB Sekuritas Indonesia

# Tjakrabirawa Clients

Telecommunications, Media, Transport, Manufacturing

# Tjakrabirawa Clients

## Information Technology

# Tjakrabirawa Clients

## Retail & Ecommerce

# Tjakrabirawa Clients

## Education


# Tjakrabirawa Clients

## Government

SINGAPORE ACCOUNTANCY COMMISSION

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

# Tjakrabirawa Rapid Assessment

# CYBER SECURITY RAPID ASSESSMENT

The quick evaluation of an organization's cybersecurity posture, identifying vulnerabilities, risks, and potential threats.

This process often involves automated tools, expert analysis, and the assessment of current security protocols.

The primary goal is to provide a clear understanding of the security environment and offer actionable insights in a short time frame.

## Benefits

1. **Quick Detection of Vulnerabilities**: Identifies security gaps faster, reducing the risk of exploitation.
2. **Resource Efficiency**: Saves time and resources by focusing on critical areas that need immediate attention.
3. **Proactive Risk Mitigation**: Allows for early intervention, preventing potential cyberattacks.
4. **Improved Decision-Making**: Provides organizations with data-driven insights to prioritize security investments and actions.
5. **Compliance Assurance**: Helps meet regulatory requirements by regularly assessing and improving security measures.

# CYBER SECURITY RAPID ASSESSMENT


## Cybersecurity Scorecard

**Benefits**

1. Real-Time Visibility
2. Improved Decision-Making
3. Clear Communication
4. Risk Reduction
5. Compliance Assurance
6. Performance Measurement
7. Team Accountability
8. Enhanced Trust

## Compromise Assessment

**Benefits**

1. Early Threat Detection
2. Improved Incident Response
3. Enhanced Visibility
4. Risk Mitigation
5. Regulatory Compliance
6. Actionable Recommendations
7. Cost Savings

## Attack Surface Management

**Benefits**

1. Comprehensive Visibility
2. Proactive Risk Reduction
3. Improved Security Posture
4. Cost Efficiency
5. Third-Party Security Assurance
6. Compliance Readiness
7. Faster Incident Response
8. Enhanced Resilience

# CYBER SECURITY INSURANCE

Cybersecurity insurance, also known as cyber liability insurance, is **a specialized type of insurance** that helps businesses mitigate the financial risks associated with cyberattacks, data breaches, and other cybersecurity incidents.

It provides **coverage for a range of losses stemming from cyber events**, such as data breaches, business interruption, cyber extortion (ransomware), and the legal liabilities that may arise from such incidents.

This insurance typically covers both first-party losses (costs incurred by the insured business) and third-party liabilities (costs incurred by external parties due to the business's security breach).

# Cybersecurity Platform

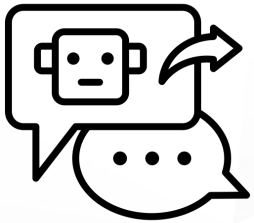
# Pentest & Vulnerability Management Dashboard (PEMDA)

# Pentest & Vulnerability Management Dashboard (PEMDA)

PEMDA is an AI-powered platform designed to automate and streamline vulnerability assessments and penetration testing (VAPT). It allows real-time monitoring and proactive risk management, ensuring a comprehensive security posture for organizations.

## The advantage of PEMDA

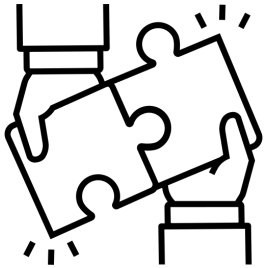
Continuous, real-time monitoring for seamless vulnerability management.



Uses AI to provide timely alerts and automate responses.

# Features

Real-time monitoring and vulnerability assessments.

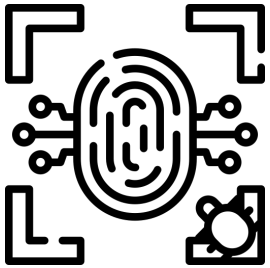


Integration with popular messaging platforms *(e.g., WhatsApp, Slack).*

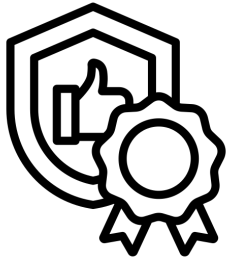
Granular role-based access control (RBAC) and data encryption.

Automated reporting and security posture analytics.

# Key Responsibilities



Automates vulnerability scanning and remediation.



Delivers proactive security recommendations.

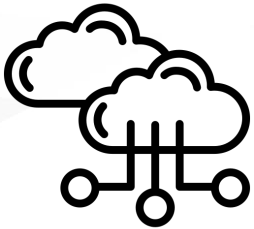
Seamlessly integrates with existing project management tools like Jira for efficient issue tracking.

# DevSecOps as a Service

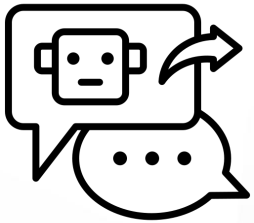
# DevSecOps as a Service Platform

This service integrates security into the entire software development lifecycle (SDLC). It enables real-time threat detection and automated remediation, embedding security into development and operational processes, without slowing down the release cycle.

## The advantage of DevSecOps



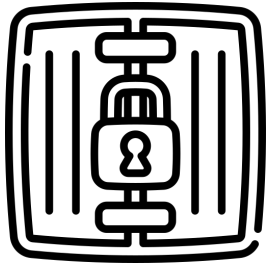
Seamless integration into CI/CD pipelines for quick feedback.



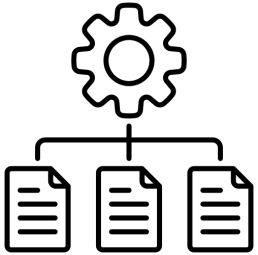
Reduces operational overhead by automating security.

# Features


Static and dynamic security testing.

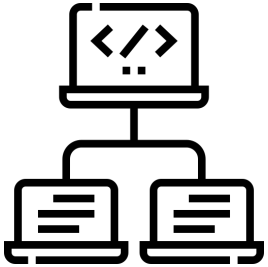


Container security scanning for misconfigurations.

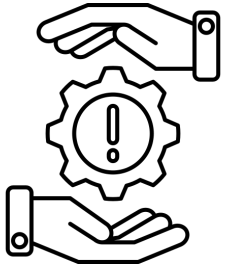


Automated security fixes integrated into developers' workflows.

# Key Responsibilities



Proactive identification of vulnerabilities from code to production.



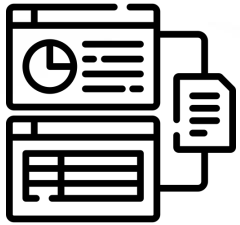
Continuous scanning and automated remediation for real-time threat mitigation.

# Zero Trust Network Access (ZTNA)

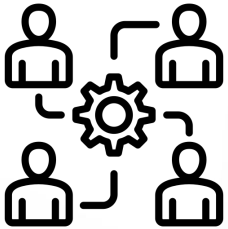
# Zero Trust Network Access

ZTNA offers a modern solution for secure access to cloud-based and hybrid work environments. Using Zero Trust principles, the platform eliminates the need for traditional, complex VPNs, offering scalable, identity-based access with enhanced security.

**The advantage of ZTNA**



Simplifies access with no need for complex VPN setups.



Enhances collaboration with temporary access management.

# Features

Instant public access links for secure, temporary service exposure.

Continuous Zero Trust security verification with token-based access.

Supports legacy applications with traditional authentication methods.

# Key Responsibilities

Implement Zero Trust security models for access control.

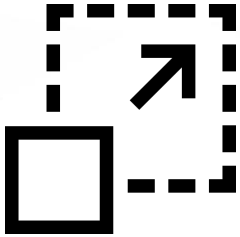
Ensure compliance and audit readiness through continuous monitoring

# Virtual Security Operations Center (vSOC)

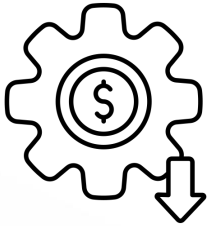
# Virtual Security Operations Center

vSOC is a cloud-based cybersecurity solution offering 24/7 monitoring, real-time threat detection, and swift incident response. It integrates cutting-edge threat intelligence with automation to protect organizations without requiring a full in-house security team.

## The advantage of vSOC

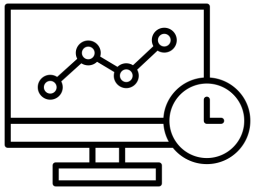


Scalable, cost-effective security solution for any size business.

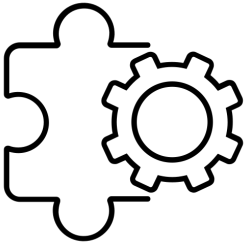


Reduces operational risk by responding to incidents faster.

# Features



Real-time monitoring and automated incident detection.



Seamless integration with existing security tools (SIEM, IDS/IPS).

Automated reporting and dashboards for on-demand client insights.

# Key Responsibilities

Detect and respond to threats rapidly using real-time intelligence.

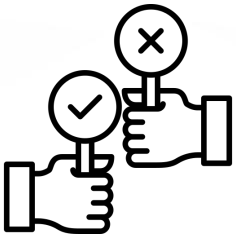
Provide actionable security reports for executives and security teams

# Threat Intelligence

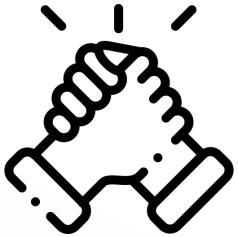
# Threat Intelligence

Tjakrabirawa's Threat Intelligence Platform (TIP) centralizes real-time threat data from multiple sources to empower proactive security efforts. It enables collaboration and quick decision-making for organizations to stay ahead of evolving threats.

## The advantage of Threat Intelligence



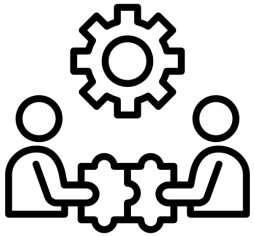
Aggregates external threat data for real-time decision-making.



Supports collaboration for enhanced cybersecurity defense.

# Features

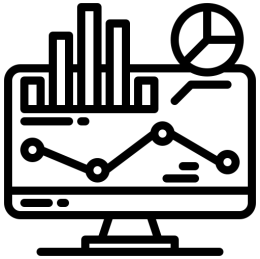
Proactive threat detection and incident prevention.



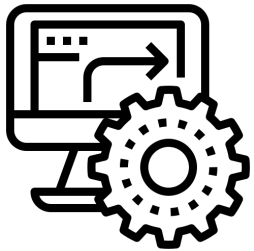
Collaboration tools for sharing intelligence and optimizing responses.

Supports compliance with security standards such as GDPR and NIST.

# Key Responsibilities



Continuously monitor for emerging threats and malicious activity.



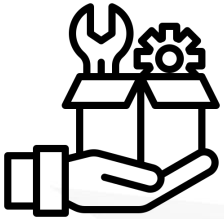
Automate threat intelligence workflows to improve operational efficiency

# Cloud-Native Application Protection Platform (CNAPP)

# Cloud-Native Application Protection Platform (CNAPP)

CNAPP is an all-in-one security platform designed to protect cloud-native applications throughout their entire lifecycle. It combines Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Infrastructure as Code (IaC) scanning, and runtime protection for a comprehensive security solution.

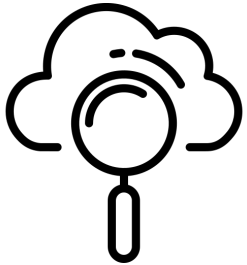
## The advantage of CNAPP



Provides end-to-end security from development to production.

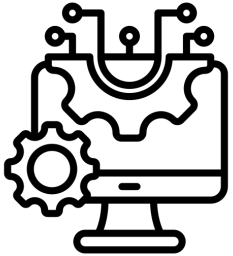
Offers real-time threat detection with proactive risk mitigation.

# Features



Cloud Security Posture Management (CSPM) for continuous cloud misconfiguration detection.

Cloud Workload Protection Platform (CWPP) for runtime protection of VMs, containers, and serverless applications.



Infrastructure as Code scanning for security misconfigurations.

# Key Responsibilities

Automate security assessments and remediation in cloud-native environments.

Provide real-time alerts and remediation of cloud security risks.

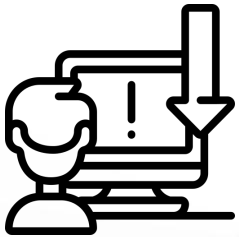
# Security Awareness Platform

# Security Awareness Platform

The Security Awareness Platform is designed to train and empower employees to recognize and respond to cyber threats. It offers engaging content and interactive modules that raise awareness and help create a culture of security within organizations.

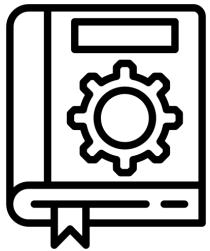
## The advantage of Security Awareness Platform

Cost-effective and scalable training solution for organizations of all sizes.



Increases employee vigilance and reduces human errors in security protocols.

# Features



Interactive training modules with simulated phishing campaigns.

Regularly updated content based on emerging cyber threats.

Tracking and reporting of employee progress and engagement.

# Key Responsibilities

Educate employees on the latest cyber threats and best practices.

Provide timely training and updates to keep up with evolving security risks.


Generate reports to measure the effectiveness of security awareness training.

# Tjakrabirawa Managed Services

# Tjakrabirawa Managed Services

## More value, less time

01

### DevSecOps as a Service

Enhance the security of your CI/CD pipeline with a simple, low-effort service delivery model that seamlessly integrates into your workflow.

02

### Cloud Security Protection

All-in-one cloud security designed to safeguard your environment from every angle.

03

### Zero Trust as a Service

Strengthen Your Security:
A managed model that enforces strict access controls and operates on the principle of ***'never trust, always verify'.***

04

### vSOC

vSOC provides expert monitoring to protect your network, detecting threats, fraud, and vulnerabilities with services like threat intelligence, dark web, and attack surface monitoring.

# Tjakrabirawa Managed Services

## More value, less time

05

### CISO as a Service

Elevate your security strategy with our Managed CISO Services—providing top-tier, third-party information security leadership to protect your organization from evolving threats.

06

### Managed Breach Attack Simulations

Empower your defense strategy with a seamless, automated approach to continuous offensive security.

07

### Digital Risk Protections

Intercept the first signs of cyber attacks: protect your credentials, block phishing efforts, and prevent sensitive data and IP from being exposed.

08

### Bug Bounty & VDP Platform

We are offering a crowdsourcing initiative that invites ethical hackers and security researchers to assist in identifying software vulnerabilities and bugs.

# Tjakrabirawa Managed Services

## More value, less time

09

### Managed VAPT & Redteam

Protect your business with our Continuous Vulnerability Assessment & Penetration Testing—keeping your defenses strong by spotting and fixing security flaws before they can be exploited.

10

### DFIR as a Service

Combat cyber threats and secure your digital assets with the guidance of our experienced professionals.

11

### Compliance as a Service

- ISO 27001
- PDP Preparation
- IT Audit
- IT Roadmap
- IT Blueprint

12

### Takedown Service

Tjakrabirawa is your trusted cybersecurity partner, offering fast and effective take-down services to remove malicious websites, fake apps, and fraudulent Google listings, ensuring your digital presence is secure and **your business protected.**

# MSSP Platform

Accessible Cybersecurity Managed Service

01

**DevSecOps & ZTNA Platform**

Rolling on Q1, 2025

02

**Forensic as a Service Platform**

Rolling on Q1, 2025

03

**Red & Blue Team CTF Platform**

Rolling on Q2, 2025

04

**Security Awareness, Compliance & GRC Platform**

Rolling on Q2, 2025

05

**Threat Intel Platform**

Rolling on Q2, 2025

06

**Security Awareness & Phishing Platform**

Soon

07

**GRC Platform**

Soon

05

**Forensic Platform**

Soon

06

**Red & Blue Team**

Soon

# Tjakrabirawa Adhoc Services

# Tjakrabirawa Core Business

## Adhoc Services

**Ala Carte**

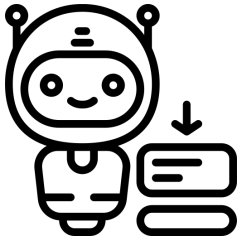
**Cybersecurity**

**Service.**

# Tjakrabirawa Community Services

# Tjakrabirawa Complimentary Services for Community

**BOT Service**
**for everyone.**



## Business Inquiry

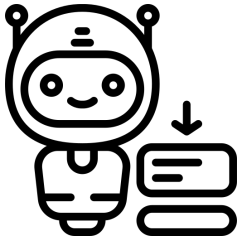
Talk to our representative on
**WhatsApp 0821 1247 6992**
To get a real-time answer for your cyber security curiosity, and professional career or internship opportunity.

## What You Will Get from Business Inquiry Services

1. **Always Available**
   Chatbots never sleep! They're ready 24/7, ensuring customers can get the help they need, whenever they need it, without waiting.
2. **Save Money**
   With chatbots handling basic tasks, businesses can cut down on staff costs. Chatbots can manage many conversations at once, making things more efficient without extra expenses.
3. **Handle High Traffic**
   Whether it's a busy day or a big promotion, chatbots can easily manage hundreds of customers at once, without slowing down or missing a beat.
4. **Consistent Support**
   No more human errors! Chatbots give the same reliable answer every time, ensuring customers always get accurate and trustworthy information.
5. **Smart Insights**
   Chatbots can gather useful data from every chat, helping businesses understand their customers better. This helps improve products and services for even more satisfied users.

# Tjakrabirawa Complimentary Services for Community

**BOT Service**
**for everyone.**



## Business Inquiry

Talk to our representative on
**WhatsApp 0821 1247 6992**
To get a real-time answer for your cyber security curiosity, and professional career or internship opportunity.

## What You Will Get from Business Inquiry Services

1. **Always Available**
   Chatbots never sleep! They're ready 24/7, ensuring customers can get the help they need, whenever they need it, without waiting.
2. **Save Money**
   With chatbots handling basic tasks, businesses can cut down on staff costs. Chatbots can manage many conversations at once, making things more efficient without extra expenses.
3. **Handle High Traffic**
   Whether it's a busy day or a big promotion, chatbots can easily manage hundreds of customers at once, without slowing down or missing a beat.
4. **Consistent Support**
   No more human errors! Chatbots give the same reliable answer every time, ensuring customers always get accurate and trustworthy information.
5. **Smart Insights**
   Chatbots can gather useful data from every chat, helping businesses understand their customers better. This helps improve products and services for even more satisfied users.

# Tjakrabirawa Complimentary Services for Community

**Free Service**

**for everyone.**

## Vulnerability Disclosure Program

A trusted platform for ethical vulnerability reporting, fostering responsible disclosure and enhancing global cybersecurity.

## What You Will Get from Vulnerability Disclosure Program

1. **Early Detection**: Ethical hackers can spot vulnerabilities before malicious actors exploit them.
2. **Enhanced Security**: Fixing issues proactively strengthens your overall security posture.
3. **Cost Efficiency**: Identifying and fixing problems early can save you from costly breaches later.
4. **Building Trust**: Shows customers and partners that you're serious about cybersecurity.
5. **Compliance**: Helps meet security requirements or standards in certain industries.
6. **Community Engagement**: Creates positive relationships with the ethical hacking community.
7. **Reputation Protection**: Avoids negative publicity from exploited vulnerabilities.
8. **Continuous Improvement**: Keeps your security systems evolving with the latest threats.
9. **Bug Prioritization**: Helps you focus on the most critical issues first.
10. **Reduced Risk of Legal Trouble**: Having a clear process for reporting reduces misunderstandings with security researchers.

# Tjakrabirawa Complimentary Services for Community

**Free Service**
**for everyone.**

## Bank Account Check

Stay ahead of fraud with fast and accurate bank account verification, ensuring your financial peace of mind.

## What You Will Get from Bank Account Check

**1. Fraud Prevention:** Verifies if the bank account exists and is valid, reducing the risk of fraud in financial transactions.

**2. Accurate Transactions:** Minimizes errors in payments by ensuring bank details are correct before processing transactions.

**3. Improved Compliance:** Helps businesses and institutions comply with anti-money laundering (AML) and know-your-customer (KYC) regulations by validating account ownership.

**4. Faster Payment Processing:** Streamlines processes by identifying issues with bank details upfront, avoiding delays or failed transactions.

**5. Better Customer Experience:** Enhances trust by ensuring secure and error-free payments, leading to higher customer satisfaction.

**6. Operational Efficiency:** Reduces administrative overhead caused by handling failed payments or investigating invalid account details.

**7. Risk Mitigation:** Confirms account ownership to avoid unauthorized transactions or misdirected payments.

# Tjakrabirawa Complimentary Services for Community

**Free Service**
**for everyone.**

**Bank Account Report**

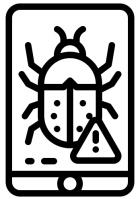
Take action against fraudulent or suspicious accounts by reporting them for a safer financial ecosystem.

**What You Will Get from Bank Account Report**

1. **Alerts and Notifications**: Many banks provide instant alerts when a transaction is made over a certain threshold, which helps account holders react quickly if something unusual occurs.
2. **Fraud Investigation Support**: In case fraud is suspected, a detailed bank account report provides vital information for investigators, helping them understand the scope and timeline of fraudulent activities.

# Tjakrabirawa Complimentary Services for Community

**Free Service**
**for everyone.**



**APK Scan**

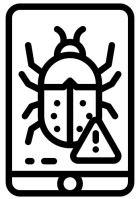
Analyze Android application files (APK) for malware, privacy risks, and security vulnerabilities.

## What You Will Get from APK Scan

1. **Detect Malicious Code**: Scanning helps you catch hidden malware or viruses that could harm your device or steal personal data.
2. **Safety First**: You can check if the APK is safe before installing it, so you won't accidentally install a shady app that might mess with your phone or data.
3. **Verify Source**: If the APK isn't from an official store (like Google Play), scanning it can tell you if it's been tampered with or is from a trustworthy source.
4. **Prevent Unauthorized Access**: Helps protect your private info by spotting any APK that might be designed to sneak into your personal data or accounts.
5. **Avoid Bloatware**: Some APKs come with unnecessary extra stuff or ads that slow your phone down. Scanning can help you avoid those too.
6. **Compliance Check**: If you're working with sensitive apps or data, scanning can ensure it follows certain security standards or regulations.

# Tjakrabirawa Complimentary Services for Community

**Free Service**
**for everyone.**



**URL Scan**

Scan and analyze URLs to detect malicious websites, phishing links, or other online threats.

## What You Will Get from URL Scan

1. **Find Malicious Links**: Helps detect if a URL is linked to malware or phishing sites, keeping you safe from potential attacks.
2. **Security Check**: Scans for vulnerabilities in a site, like outdated software or security holes, making it easier to spot risky sites.
3. **Detect Spam**: It can check if the URL is part of a spam campaign, so you can avoid unwanted or harmful content.
4. **Privacy Protection**: Helps you ensure that your data isn't being harvested or tracked in ways you don't want.
5. **URL Reputation**: It gives you an idea of whether the site has a bad reputation or is flagged for suspicious activity.
6. **Safe Browsing**: Allows you to browse more confidently by giving you a heads-up about potential dangers.
7. **Prevention for Businesses**: Helps companies monitor links they might be sharing to avoid potential harm or negative effects on their users.

# DevSecOps

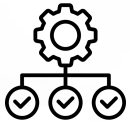
# DevSecOps as a Service

**DevSecOps** is a method that combines **security** with **DevOps**. Instead of adding security at the end, it makes security a part of every step in the development process. This helps teams find and fix security issues early, while still moving quickly to develop and release software. Everyone—developers, security experts, and operations teams—works together to keep the software secure.

## The 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

Flx cost

Include bug bounty services

# DevSecOps as a Service

## Features

### Static Testing

- Source of composition analysis
- Software bill of material
- Secret scanning
- Static analysis of security testing

### Dynamic Testing

- Dynamic analysis security testing
- Vulnerability assessment and penetration testing

### Infrastructure Testing

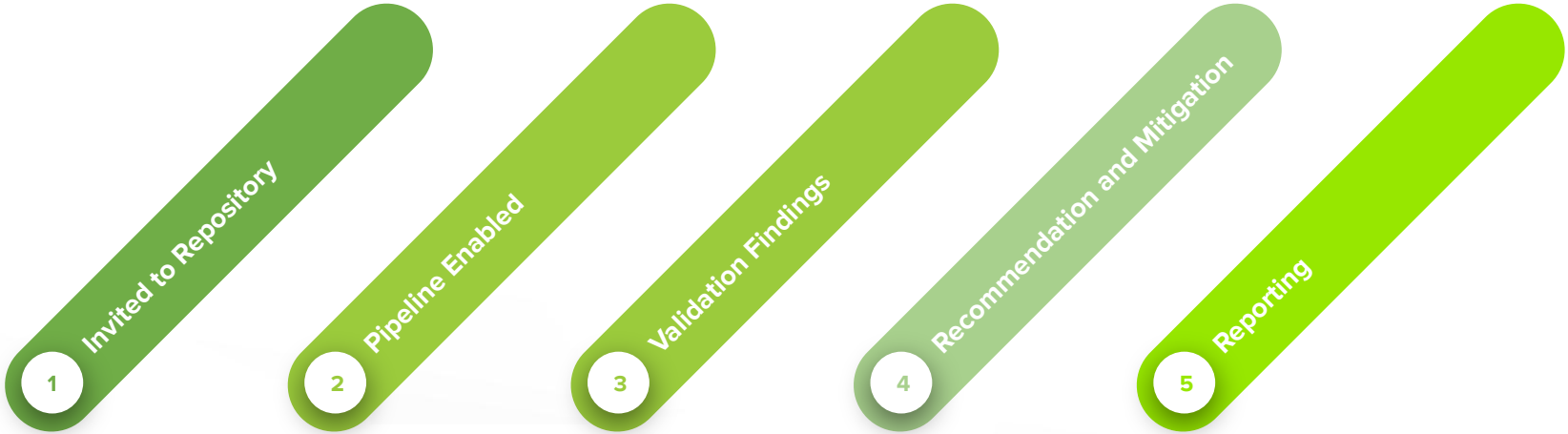
- Audit as code
- Container security

### Additional Features

- Threat modeling
- Secret management

# DevSecOps as a Service

## Integration Flow



# DevSecOps as a Service

## Programming Language Support

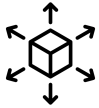
# Cloud Security Platform

# Cloud Security Platform

A Cloud Security Platform is a set of integrated tools that protect cloud-based environments. As businesses move their data and applications to the cloud, safeguarding these resources is crucial to prevent cyber threats, data breaches, and ensure compliance with regulations.

## Benefits

**Comprehensive Protection**
Multi-layered defense against cyberattacks.

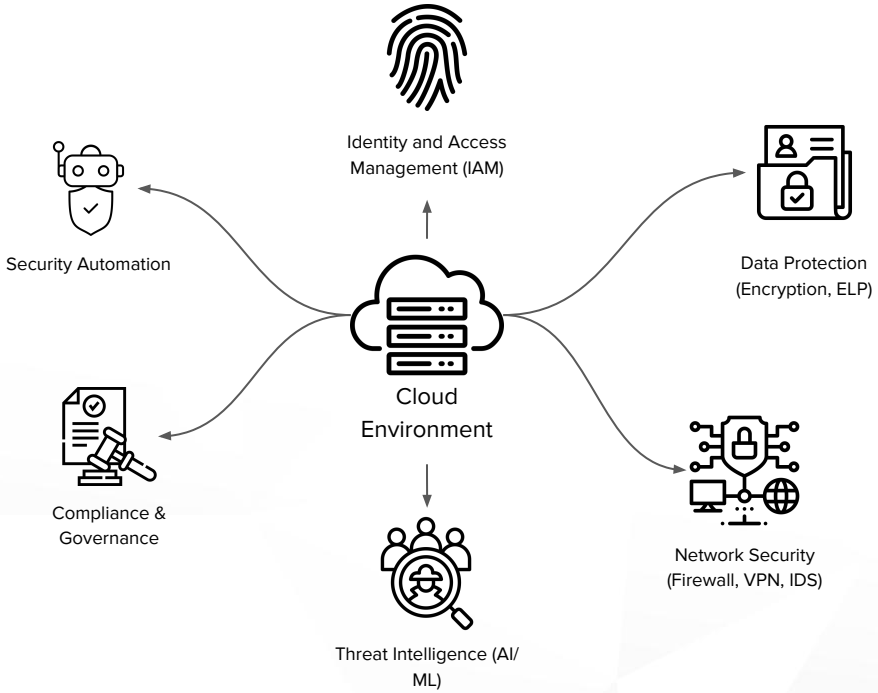


**Scalability**
Easily adapts as businesses grow.

**Cost Efficiency**
Reduces need for on-premises infrastructure.

**Real-TIme Threat Detection**
AI-driven threat monitoring for quick responses.

# Cloud Security Platform



# Zero Trust as a Service

# Zero Trust as a Service

**Zero Trust** is a cybersecurity approach that assumes **nothing** is trusted by default, **inside** or **outside** the network. **"Never trust, always verify"** is the core principle.

## Why Zero Trust?

- **Increased Threats**: Traditional perimeter-based security models are outdated, especially with the rise of cloud computing, remote work, and advanced persistent threats (APTs).
- **Data Protection**: Helps protect sensitive data by ensuring that only authorized entities can access it, reducing the risk of insider threats and data breaches.
- **Scalability and Flexibility**: As businesses scale and evolve, Zero Trust can easily adapt to different architectures, including on-premises, cloud, and hybrid environments.

# Zero Trust as a Service

## Key Principles

**Verify Continuously**
Always authenticate users and devices before allowing access.

**Least Privilege Access**
Grant only the minimum access needed for tasks.

**Micro-Segmentation**
Break networks into smaller zones to limit unauthorized access.

**Monitor and Log Activities**
Continuously track and analyze network activity to detect threats early.

## Core Component

**Identity & Access Management (IAM)**
Strong authentication like MFA to verify users.

**Device Security**
Ensure devices meet security standards before granting access.

**Network Security**
Use micro-segmentation and encryption to secure the network.

**Application & Data Protection**
Control access to applications and data to prevent unauthorized use.

# Virtual Security Operations Center (vSOC)

# Virtual Security Operations Center (vSOC)

A **Virtual Security Operations Center (vSOC)** is a cloud-based, decentralized security infrastructure that enables businesses to monitor, detect, and respond to security threats in real-time. Unlike traditional Security Operations Centers (SOCs) that rely on a centralized physical location, vSOC is operated remotely, providing flexibility and scalability for organizations.

# Virtual Security Operations Center (vSOC)

## Key Features

**Cloud-Enabled**: vSOC utilizes cloud technology to provide 24/7 security monitoring without the need for physical hardware.

**Scalability**: Easily adaptable to the size and needs of the organization, with the ability to scale security services as threats evolve.

**Cost-Effective**: With no need for large on-premise infrastructure, vSOC is a more affordable option, especially for smaller businesses.

**Real-Time Monitoring**: Continuous surveillance of the IT environment to quickly identify and respond to potential threats.

**Threat Intelligence**: Uses advanced analytics, machine learning, and threat intelligence feeds to detect vulnerabilities and cyber-attacks.

## vSOC Benefits

**Improved Security**: 24/7 monitoring reduces the likelihood of security breaches going unnoticed.

**Faster Incident Response**: Instant alerts and incident responses to mitigate the impact of potential threats.

**Access to Expertise**: vSOC solutions often come with access to cybersecurity experts without the need for in-house personnel.

**Reduced Downtime**: Proactive identification and resolution of security issues prevent costly downtime and damage.

**Compliance Assurance**: Helps organizations maintain compliance with industry regulations such as GDPR, HIPAA, and PCI-DSS by monitoring and reporting security events.

# CISO as a Service

# CISO as a Service

A **Chief Information Security Officer (CISO)** is an executive responsible for overseeing an organization's information security program. The CISO's primary goal is to protect the organization's digital assets, data, and systems from cybersecurity threats.

## Key Responsibilities

**Cybersecurity Strategy**
Create and implement a plan to protect the organization's data and systems from cyber threats.

**Incident Response and Recovery**
Lead the response to security breaches or attacks, ensuring quick recovery and minimal damage.


**Compliance and Audits**
Oversee and support the team responsible for maintaining security, ensuring they have the right tools and training.


**Risk Management**
Identify potential security risks and take steps to reduce or eliminate them.

**Team Leadership**
Oversee and support the team responsible for maintaining security, ensuring they have the right tools and training.

**Communicate with Leadership**
Report on security issues and updates to the company's executives and board members.

# Managed Breach Attack Simulation

# Managed Breach Attack Simulation

A **Managed Attack Simulation** (MAS) is a controlled, ethical hacking exercise that mimics real-world cyber-attacks to identify security weaknesses. It provides proactive insights into the organization's defense mechanisms, vulnerability points, and response readiness.

## Key Responsibilities

**Simulate Real-World Attacks**: Mimic actual cyber threats to test response and defense strategies.

**Identify Security Gaps**: Spot vulnerabilities in systems, networks, and people.

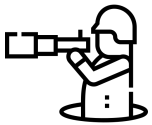
**Test Response Mechanisms**: Evaluate the effectiveness and speed of incident response.

**Enhance Security Awareness**: Raise awareness among employees regarding potential threats (e.g., phishing, social engineering).

# Managed Breach Attack Simulation Scope

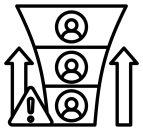
Custom-tailored to the client's environment, covering networks, endpoints, web apps, and human behavior.

**Planning**
Define attack vectors and targets.



**Reconnaissance**
Gather intel about the target.

**Exploitation**
Simulate cyber-attacks (e.g., phishing, malware).



**Escalation and Pivoting**
Move across the network to test deeper defenses.

**Reporting**
Provide detailed findings, risk levels, and remediation advice.

# Type of Managed Breach Attack Simulation

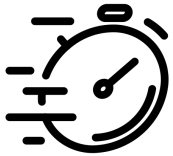
**Red Team Engagements**
Advanced, multi-vector attacks aimed at breaching the organization using sophisticated tactics and techniques.


**External Attack**
Attacks originating from outside the organization, targeting exposed systems (e.g., public-facing websites, email systems).

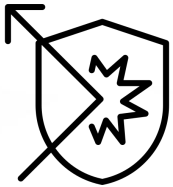
**Internal Attacks**
Simulate an insider threat or attack by a compromised user or employee.

# Benefit of Managed Attack Simulations

**Comprehensive Risk Assessment**
Identify weak spots across the entire security landscape.



**Better Incident Response**
Test and refine your organization’s response to cyber-attacks.



**Improved Defense Posture**
Enhance threat detection and prevention measures.

**Real-Time Insights**
Receive actionable insights for immediate remediation.

# Digital Risk Protection

# Digital Risk Protection

**Digital Risk Protection (DRP)** refers to the set of tools, practices, and strategies that organizations use to manage and mitigate the risks associated with their digital presence.

This includes everything from monitoring and defending against cyber threats, data breaches, and online fraud to ensuring compliance and protecting brand reputation in the digital world.

# Digital Risk Protection Key Responsibilities

1. **Threat Intelligence:**
   - Continuous monitoring of cyber threats targeting the organization or its industry.
   - Identifying emerging threats, such as phishing, ransomware, and other malicious activities.
2. **Brand and Identity Protection:**
   - Safeguarding an organization's online identity, including its social media accounts, websites, and domain names.
   - Preventing impersonation, fake accounts, and misuse of brand assets.
3. **Data Privacy and Compliance:**
   - Ensuring data protection standards are met, and sensitive customer or organizational data is not exposed or misused.
   - Adhering to legal regulations such as GDPR, HIPAA, or CCPA.
4. **Vulnerability Management:**
   - Detecting and addressing vulnerabilities in software, networks, and systems that could be exploited by attackers.
   - Proactive patching and security updates to reduce the attack surface.
5. **Incident Response:**
   - Developing a response plan for when a digital risk, such as a cyberattack, occurs.
   - Rapid containment, investigation, and recovery to minimize damage and downtime.

# Why is Digital Risk Protection Important

**Protects Against Data Breaches**
By identifying and addressing vulnerabilities before they are exploited, DRP helps avoid costly data breaches.

**Improves Compliance**
DRP helps meet the necessary legal and regulatory requirements for data security and privacy, reducing the risk of fines.

**Preserves Brand Reputation**
Managing risks in the digital world ensures your company maintains its reputation and avoids damage from impersonation or fraud.

**Supports Operational Continuity**
By preparing for potential incidents and monitoring digital risks, DRP minimizes downtime and maintains business operations.

# Bug Bounty & VDP Platform

# Bug Bounty & VDP Platform

*Ensuring Cybersecurity Through Collaborative Efforts*

## What is Bug Bounty

A **Bug Bounty** program is a security initiative where organizations offer rewards (financial or otherwise) to ethical hackers (also known as "security researchers") who identify and report security vulnerabilities in their systems or software. It encourages the discovery of issues before malicious actors can exploit them.

## What is VDP Platform

A **Vulnerability Disclosure Program (VDP)** is a formal process where an organization allows security researchers and the general public to report discovered vulnerabilities without the incentive of a financial reward, unlike Bug Bounty programs. The focus is on providing a clear, safe, and structured way for vulnerabilities to be disclosed.

# Bug Bounty & VDP Platform

*Ensuring Cybersecurity Through Collaborative Efforts*

## Functionality of Bug Bounties

- **Organizations** set up a platform or work with third-party providers (such as HackerOne, Bugcrowd, etc.).
- **Researchers** identify and report vulnerabilities found in an organization's application, website, or infrastructure.
- **Rewards** are given based on the severity of the vulnerabilities reported, with higher rewards for critical issues.

## Functionality of VDP Platform

- **Organizations** publish a clear disclosure policy, outlining how vulnerabilities should be reported, and often offer acknowledgment for responsibly reported findings.
- **Researchers** submit vulnerabilities via a secure channel (usually email or a form) and are expected to follow responsible disclosure guidelines.
- **Public Acknowledgment** may be offered after the vulnerability is patched, giving credit to the reporter.

# Bug Bounty & VDP Platform

*Ensuring Cybersecurity Through Collaborative Efforts*

| Feature | Bug Bounty | VDP Platform |
|---|---|---|
| Incentive | Financial rewards or other incentives | No financial rewards, but recognition is given |
| Target Audience | Ethical hackers/security researchers | Any researcher or individual, including non-technical users |
| Scope | Often focused on specific software/system | Broader, sometimes less focused |
| Program Structure | Formal platform with defined rules & rewards | May or may not have a formal platform |

# Benefits Bug Bounty & VDP Platform

*Ensuring Cybersecurity Through Collaborative Efforts*

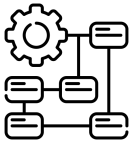
## Bug Bounty

**Proactive Security**
Identifies vulnerabilities before they are exploited.

**Diverse Perspective**
Access to global ethical hackers with diverse skill sets.

**Cost-Efficiency**
Only pays for valid vulnerabilities found.

## VDP Platform



**Structured Process**
Provides clear guidelines for safe reporting.

**Collaboration**
Encourages responsible disclosure from researchers.

**Reputation Building**
Enhances trust by being transparent about security efforts.

# Managed VAPT & Red Team

# What is Managed VAPT?

**Vulnerability Assessment & Penetration Testing (VAPT)** is a comprehensive security service that identifies, assesses, and helps mitigate security vulnerabilities in IT systems. Managed VAPT takes this a step further by providing ongoing monitoring and remediation, with expert-led assessments, to ensure that vulnerabilities are identified and addressed proactively.

## Key Responsibilities

**Vulnerability Assessment**: Automated & manual scans to detect vulnerabilities in apps, networks, and systems.

**Penetration Testing**: Simulating real-world cyberattacks to exploit vulnerabilities.

**Continuous Monitoring**: Ongoing tests to ensure security hygiene and adapt to evolving threats.

## Benefits

Detect vulnerabilities before attackers exploit them.

Ensure compliance with security standards.

Minimize risk of breaches and data compromise.

# What is Red Teaming?

A **Red Team** is a simulated attack strategy used to evaluate an organization's security posture. Unlike penetration testing, which is often more targeted, red teaming involves a full-scale simulated cyberattack, mimicking real-world adversaries. The goal is to test the organization's defenses, response protocols, and overall preparedness for an actual attack.

## Key Components

**Reconnaissance & OSINT**: Gathering intelligence to identify attack vectors.

**Social Engineering**: Testing employee awareness through phishing and manipulation tactics.

**Physical Security Testing**: Breaching physical security measures.

**Incident Response Evaluation**: Assessing detection, response, and recovery protocols.

## Benefits

Identify overlooked vulnerabilities.

Evaluate employee awareness and security culture.

Test response protocols to ensure effective handling of attacks.

# Why Choose Managed VAPT & Red Team?

- **Proactive Security**: Regular, thorough assessments help identify vulnerabilities before they are exploited by malicious actors.
- **Expertise and Experience**: Managed services are led by cybersecurity experts with advanced tools and methodologies to simulate sophisticated attacks.
- **Comprehensive Protection**: From network vulnerabilities to social engineering, both VAPT and Red Team tests provide a 360° view of your organization's defenses.
- **Risk Mitigation**: Prioritize vulnerabilities based on severity and impact to improve risk management.

# Digital Forensic & Incident Response as a Service

# What is Digital Forensic & Incident Response?

**Digital Forensic:** The process of recovering, analyzing, and preserving digital evidence in a manner that is legally admissible.

**Incident Response:** The process of managing a cybersecurity incident to minimize damage and recovery systems.

## Digital Forensic Process

1. **Identification:** Find relevant digital evidence (devices, logs, media).
2. **Preservation:** Safeguard evidence to prevent alteration (e.g., creating forensic images).
3. **Analysis:** Examine evidence using specialized tools (files, metadata, logs).
4. **Presentation:** Present findings in a clear report, often for legal use.

## Incident Response Process

1. **Preparation:** Set up tools, resources, and response plans.
2. **Detection & Identification:** Detect suspicious activity through monitoring tools and alerts.
3. **Containment:** Isolate affected systems to prevent further damage.
4. **Eradication:** Remove malicious elements and vulnerabilities.
5. **Recovery:** Restore systems to normal operations.
6. **Lessons Learned:** Analyze the incident to improve future responses.

# Why DFIR Matters?

**Prevent Future Incidents**
Learning from incidents to fortify defenses.

**Legal Evidence**
Ensuring digital evidence is reliable for legal proceedings.

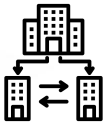
**Minimize Damage**
Responding quickly to contain and mitigate security breaches.

# Compliance as a Service

# Compliance as a Service

**Cybersecurity Compliance as a Service (CaaS)** provides businesses with external expertise to ensure their cybersecurity practices align with industry regulations, standards, and frameworks (e.g., GDPR, HIPAA, PCI DSS, ISO 27001).

## Who Needs CaaS?



**Small to Medium Enterprises (SMEs)**:
Often lack the resources for full-time cybersecurity teams.

**Healthcare, Finance, and E-commerce**:
Industries with sensitive data requiring stringent compliance.

**Large Enterprises**:
Must adhere to multiple regulatory frameworks across regions.

# How CaaS Works


**Assessment and Gap Analysis**
A thorough audit of current practices and systems against relevant regulations.

**Implementation of Best Practices**
Development and implementation of policies and controls to close compliance gaps.

**Continuous Monitoring**
24/7 monitoring of systems, identifying any potential non-compliance issues or vulnerabilities.

**Regular Reporting**
Reports and dashboards that show compliance status, progress, and risk levels.

**Incident Response & Remediation**
Immediate response to compliance failures, with steps for correction and reporting to authorities.

TJAKRABIRAWA
INTELLIGENT SECURITY SERVICES

# Feeling Insecure?


**Address**
Manhattan Tower 12th Floor
TB Simatupang 12560 Indonesia

**Email**
info@tjakrabirawa.id

**Website**
www.tjakrabirawa.id

**1Stop Cyber Hotline**
0821 1247 6992