CyberArmy

Reinvent Cybersecurity

About Us

We started in 2018, CyberArmyID is a company in the field of Information and Cyber Security. Currently, We are focusing on **Digital & Services of Cyber Security.**
We also provides **Technical and Managerial Education** related to Information and Cyber Security.

CyberArmyID under the Legal Entity of
PT Global Inovasi Siber Indonesia

TOP 40 Innovative Startup at ASEAN-KOREA STARTUP WEEK 2019, Seoul South Korea


REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SERTIFIKAT MEREK

Menteri Hukum dan Hak Asasi Manusia atas nama Negara Republik Indonesia berdasarkan Undang-undang Nomor 20 Tahun 2016 Tentang Merek, memberikan hak Merek kepada:

Nama dan alamat Pemegang Merek	:	PT Global Inovasi Siber Indonesia Jl. Naripan No. 53, Kel. Kebon Pisang, Kec. Sumur Bandung, Kota Bandung, Jawa Barat 40112, Indonesia
Tanggal Penerimaan	:	18 Januari 2019
Nomor Pendaftaran	:	IDM000860830
Etiket Merek	:	CyberArmy

Brand Registered at Directorate General of Intellectual Property

Cyber Security Solution

CyberArmy
Reinvent Cybersecurity

CyberArmy
Bug Bounty and Vulnerability Coordination Center
www.cyberarmy.id

Bug Bounty Platform

Ensuring the vulnerabilities are discovered by Bughunters and appreciate the results.

Penetration Testing

Ensuring the vulnerabilities are discovered by CyberArmyID Team.

Vulnerability Bug Fixing

Helping developers to make improvement in application vulnerabilities.

Cyber Security Consultant

Helping organizations with Cyber Security Needs.

HELIUM
SIMPLIFY VULNERABILITY ASSESSMENT
www.helium.sh

Vulnerability Assessment Platform

Security cycle mechanism whose activities automatically identify vulnerabilities, classify, prioritize and mitigate risks.

CYBER ACADEMY
www.cyberacademy.id

Cyber Security Education Platform

Education to develop individual knowledge in the field of Cyber Security and Information Security.

We’re trusted by these companies and more

From Government, State-owned Enterprises, Bank, E-Commerce, Fintech, Health Care, Edu Tech, Portal Media, Artificial Intelligence, Hosting, University, Tech Startup and more.

CyberArmy
Reinvent Cybersecurity

Bug Bounty Program / Penetration Testing

Badan Siber dan Sandi Negara Republik Indonesia
Caraka Bhuwana
BPJS Kesehatan
Badan Penyelenggara Jaminan Sosial
JABAR DIGITAL SERVICE
myIndiHome
Pegadaian
Kredivo
Buy now, Pay later
Kitabisa.com
BHINNEKA
tiketux
fasapay
Galeri24
Pegadaian
bobobox
dewaweb
CLOUD HOSTING PARTNER
Assist.id
sharing happiness.org
Qwords.com
INDONESIALEAKS
GLOBAL DATA INSPIRASI
Pay OK
Scola
KUTPSIKOTES
Melayani Dengan Inovasi
And more ...

Cyber Security Consultant

Badan Siber dan Sandi Negara Republik Indonesia

Security Advisory
(Secure SDLC)

BANK BPD BALI
Bersama Anda Membangun Bali

Secure SDLC
Standard

Cyber Academy / In-house Training

Badan Siber dan Sandi Negara Republik Indonesia
Telkom Indonesia
the world in your hand
pindad
Pegadaian
IMIGRASI
GS BATTERY
KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA
PT PII
PENJAMINAN & INFRASTRUKTUR
swa media
innovative IT solution

The Difference

CyberArmy
Reinvent Cybersecurity

	Vulnerability Assessment	Penetration Testing	Crowdsourced Security Testing
Perfomed by	**Automated tools** (with human oversight)	**Manual Testing** (1 – 5 Pentester with Professional)	**Manual Testing (10 – 400 Pentester with Professional & Community)**
Objective	Identifying Vulnerabilities	To test your security measures and probe specific weak points a hacker could exploit	To test your security measures and probe specific weak points a hacker could exploit
Method & Tools	Limited Method & Tools	Limited Method & Tools	**Rich Method & Tools**
Report Result	**Rich Pontential Vulnerability Results**	Limited Exploit Results	**Rich Exploit Results**
Time Report	A few minutes (Daily Pontential Vulnerability Report)	2 – 4 Weeks (No Daily Exploit Report)	**A few Hours (Daily Raw Exploit Report on Dashboard CyberArmy)**
Contents of the report	List of Potential Vulnerabilities	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation, recommendation	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation, recommendation
Dashboard Analytics	Yes (Analytics Report & Severity Risk)	No	**Yes (Analytics Report & Severity Risk)**
Notification	Yes (Mail Notification)	No	Yes (Mail Notification)
Program Type	Private	Private	**Private or Public**

CyberArmy
Bug Bounty and Vulnerability Coordination Center

Bug Bounty Program

Bug Bounty Program is a company's initiative that appreciates the findings of security holes from ethical hackers, also called Bughunters in an application / system / service.

Companies can find vulnerabilities earlier before irresponsible parties find and exploit them. Through this program, companies also can implement security controls on an ongoing basis.

Benefit of Bug Bounty Program:

Continuous Security Testing
Period 1 – 12 Months

Rich of Findings

Reducing the Risk of Vulnerability

The Vulnerability is closed quickly

Program Types

There are two types of program in Bug Bounty Program

Public Program

Your Bug Bounty program will be published to all Bughunters. This will provide opportunities for hundreds of Bughunters to find vulnerabilities in your application.

Private Program

Your Bug Bounty program will be published to Bughunter who gets an invitation. We select competent Bughunters to follow the bug bounty program in applications that store sensitive information.

Bug Bounty Program

CyberArmy
Bug Bounty and Vulnerability Coordination Center

Service Flow

1. **CREATE COMPANY ACCOUNT**

2. **ACCOUNT VALIDATION**
   - Company Agreement
   - Non Disclosure Agreement

3. **PUBLISH**
   - Create Bugbounty Program
   - Perform Bughunting
   - Receive Valid Reports

Bughunter's Profile

From Professional and Community

CyberArmy
Bug Bounty and Vulnerability Coordination Center

2000+ Registered Bughunters

600+ Verified Bughunters

< 4 Hours

The fastest Critical Vulnerability Finding received

< 1 Hours

The fastest High Vulnerability Finding received

Acknowledged by

Google, ASUS, SAMSUNG, Symantec, Apple, Adobe, npm, PayPal, Dropbox, Rockstar, RAZER, Ford, Lenovo, flickr, RSA, McAfee by Intel, MOTOROLA MOBILITY

And Many More...

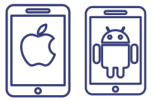
Security Testing Details

CyberArmy
Bug Bounty and Vulnerability Coordination Center

API (Application Programming Interface)

In Scope Vulnerabilities Checklist :

- ✓ Bruteforce JWT Token
- ✓ Input validation
- ✓ Not limit requests for DDoS/Bruteforce attacks
- ✓ Not using whitelist method in redirect url
- ✓ Sensitive data are not encrypted
- ✓ Sensitive data stored in JWT payload
- ✓ Use Basic Auth, not use standard authentication



iOs/Android Application

In Scope Vulnerabilities Checklist :

- ✓ Client Code Quality
- ✓ Code Tampering
- ✓ Extraneous Functionality
- ✓ Improper Platform Usage
- ✓ Insecure Authentication
- ✓ Insecure Authorization
- ✓ Insecure Communication
- ✓ Insecure Data Storage
- ✓ Insufficient Cryptography
- ✓ Reverse Engineering

Web Application

In Scope Vulnerabilities Checklist :

- ✓ Account takeover
- ✓ Authentication bypass
- ✓ Cross-site request forgery
- ✓ Cross-site scripting (XSS)
- ✓ IDOR/Broken Access Control, sensitive actions by user
- ✓ Information disclosure / Sensitive data exposure
- ✓ Privilege escalation
- ✓ Exposed Administrative Panels that don't require login credentials
- ✓ SQL injection
- ✓ Server Side Template Injection (SSTI)
- ✓ Server-Side Request Forgery (SSRF)
- ✓ XML External Entity Attacks (XXE)
- ✓ Remote/Arbitrary code execution
- ✓ Directory Traversal Issues
- ✓ Local File Disclosure (LFD)
- ✓ Timing or enumeration attacks that have a tangible risk to security or privacy

What They Said

Anton Setiyawan, S.Si., M.M.
Director of Digital Economic Protection,
State Cyber and Crypto Agency

"The existence of CyberArmy as a **crowdsourced cybersecurity service entity is an important step for the Cyber Indonesia ecosystem** . First, it shows the ability and progress of the local Cyber Security industry.

Secondly, this is an innovation in **getting quality Cyber Security services at a cost that is not burdensome.**

Third, this can be an example of developing the potential of millennial generation in contributing to **maintaining national cyber security** . **We have collaborated several times** with them and **always get the expected results** . Hopefully CyberArmy services will continue to grow and become even better in the future. Thank you."

Christofer Simbar
Information Security Analyst BPJS

"As a new player in the crowdsourced cybersecurity industry, **the services provided by Cyberarmy exceed our expectations. Through Cyberarmy we can prevent the exploitation of critical security holes that have never been found by 3 penetration testing service providers beforehand ."**

Head of KIPD ICT Center
Ministry of Foreign Affairs

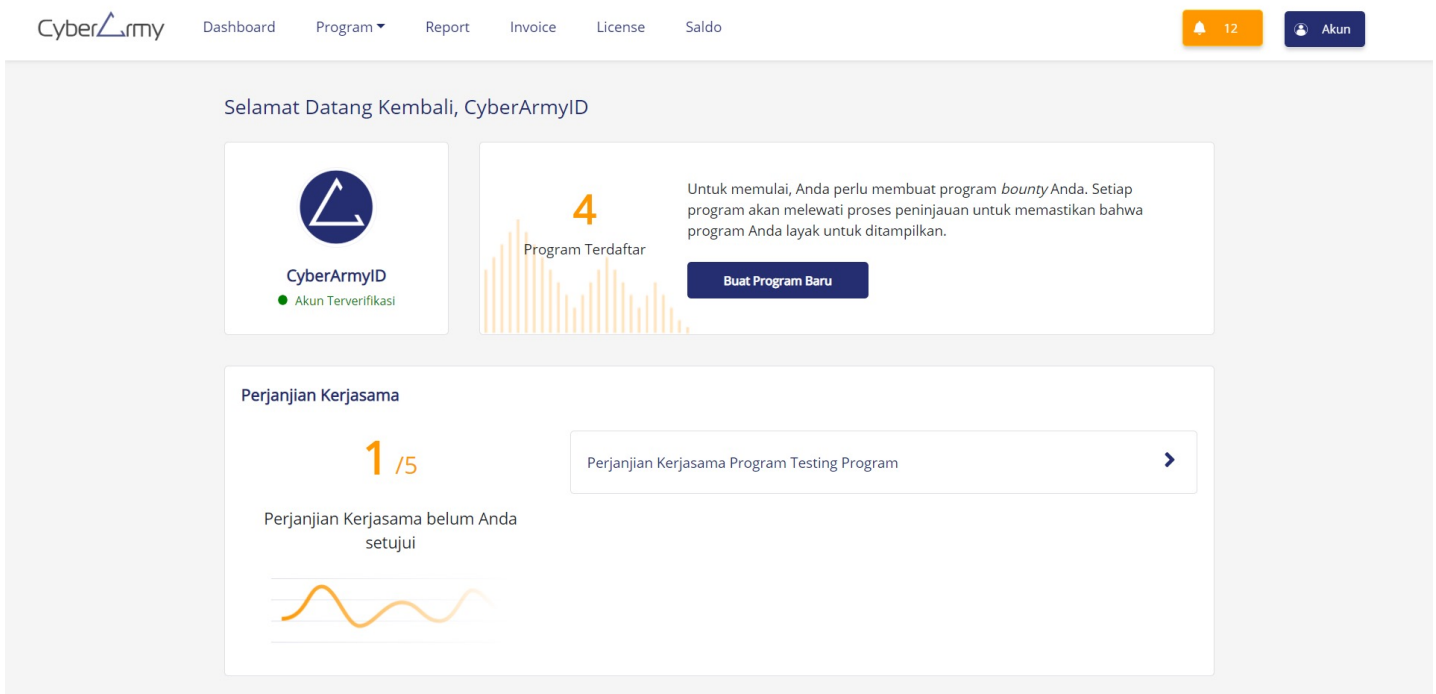
"Most cyber security cases in Indonesia are hacking cases that target government sites. **We are greatly helped by CyberArmy services** with its bug bounty in order **to strengthen cyber resilience at the Ministry of Foreign Affairs** ."

Bherly Novrandy
VP Engineering at Kitabisa.com

" **CyberArmy helps anticipate security gaps that pose a great risk to business continuity**, so that **we can produce safer and more trusted products** for users of Kitabisa."

Vulnerability Management Dashboard

For Bugbounty Program and Penetration Testing



Continuous Monitoring

Valid Reports, Risk Category and Risk Severity Level Statistic

All Vulnerability Report on Dashboard

CyberArmy
Bug Bounty and Vulnerability Coordination Center

CyberArmy Dashboard Program Report 368 Akun

Laporan Program Platform CyberArmyID

Tampilkan 10 Search

Accept | Status Hadiah Uang | Status Kerentanan | Tingkat Resiko

No	Nama Temuan	Dilaporkan Oleh	Status Laporan	Tanggal	Hadiah Uang	Status Kerentanan	Tingkat Risiko	Detail
1	Email Spoofing	exzettabyte	Accept	26/03/2020 15:53:42	-	Unresolved	Duplicate P5-Informational	→
2	Website Tidak Bisa Meng-handle Multiple Request Sehingga Down	mrdoel	Accept	24/03/2020 14:11:46	-	Unresolved	P4-Low	→
3	Sistem Verifikasi ID Yang Tidak Aman CWE-345	mrdoel	Accept	24/03/2020 08:57:50	-	Unresolved	P5-Informational	→
4	Bypass Pembatasan Karakter Pada Form Tentang Anda dan Keahlian CWE-131	mrdoel	Accept	24/03/2020 07:50:37	-	Unresolved	P4-Low	→
5	Username Enumeration Melalui Lupa Password CWE 204	mrdoel	Accept	16/03/2020 15:29:40	-	Unresolved	P5-Informational	→
6	Exposed Source Code	alpinshit1337	Accept	15/03/2020 11:54:44	-	Unresolved	P4-Low	→
7	Missing check variable type	bhrdn	Accept	18/02/2020 19:20:51	-	Unresolved	P5-Informational	→
8	Misconfigurasi Email Server	Galuh290199	Accept	18/02/2020 09:33:27	-	Unresolved	Duplicate P5-Informational	→
9	Account Takeover Via Registrasi Menggunakan Gmail	mrdoel	Accept	06/02/2020 10:32:41	-	Unresolved	Not Applicable	→
10	Cross-site scripting	iin	Accept	31/01/2020 17:49:53	-	Unresolved	P5-Informational	→

« 1 2 3 4 5 6 7 8 9 »

Detail Report and Private Discussion with Bughunter

CyberArmy
Bug Bounty and Vulnerability Coordination Center

CyberArmy | Dashboard | Program | Report | 368 | Akun

Bug Hunter	mrdoel
Nama Aplikasi	Platform CyberArmyID
Nama Temuan	Bypass Reset Password Key To Send Unlimited Email
Deskripsi	Halo tim Cyber Army, saya menemukan bug dimana email reset password yang dikirim ke email user bisa kita bypass sehingga bisa mengirim email yang sangat banyak (tidak terbatas).
Kategori Aplikasi	Website
Kategori Laporan	Input validation
Laporan Lengkap (PDF File)	Lihat
Status Laporan	Accept
Status Kerentanan	Belum Diperbaiki
Tanggal	02 January 2020 14:28:35
Tingkat Risiko	P3 Medium
Hadiah Lainnya	Merchandise
Status Hadiah Lainnya	Dikirim

Back | Update

Diskusi Laporan

mrdoel
Untuk Remediasi. Bisa juga menggunakan Captcha

02 January 2020,15:05

CyberArmyID
Hi mrdoel

Terimakasih atas laporan Anda. Setelah kami analisa, laporan ini masuk ke dalam risiko medium.

Untuk hadiahnya mohon menunggu ya!

Terimakasih.

03 January 2020,16:35

Isi komentar disini

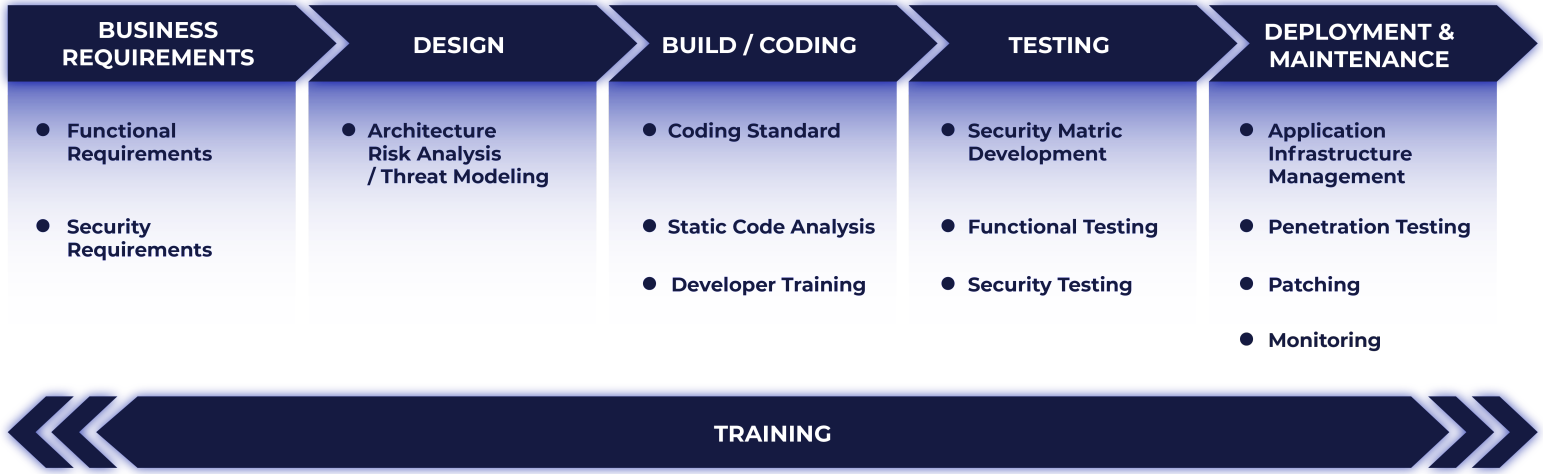
Choose File | Komentar

Secure SDLC Consulting

Software Development Life Cycle (SDLC) is a framework that defines the processes used by organizations to build applications from scratch to operational use.

It is in this case that the concept of Secure SDLC emerges. A secure SDLC process (Secure SDLC) ensures that security assurance activities such as architecture analysis, threat modeling, penetration testing, source code review, and monitoring are an integral part of development efforts.

Secure Software Development Life Cycle Process



Our Clients

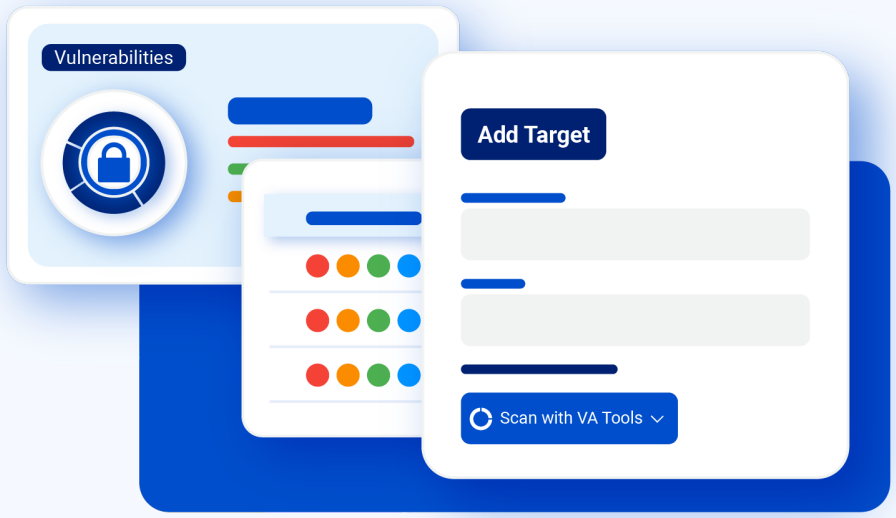
Security Advisory
(Secure SDLC)

Secure SDLC
Standard

Powerful Cloud-based

Vulnerability Assessment Platform

Vulnerability Assessment is the process of identifying risks and vulnerabilities in systems, computer networks, applications, or other parts of the IT ecosystem.



www.helium.sh

Benefits

HELIUM
SIMPLIFY VULNERABILITY ASSESSMENT

Automate Continuous Security Assessment

Schedule your scans and periodically evaluate your systems for the vulnerabilities.

Easy to use

No need to install a bunch of tools on your machine. You only need login and run the assessment, no hassle anymore. Helium also provide API Access.

Team Collaboration

Working with the team to collaborate and deliver better security assessment.

Save Time

Don’t worry about configuration and maintenance. All you need here and always up to date, including the latest tools.

Speed up your scans

Helium running while you have logout. You can scan and go to sleep. We'll do for the rest.

Cost Efficient for All

Cost efficient for personal or companies of all size. Helium provides vulnerability scanning with unlimited assessments for affordable price.

HELIUM
SIMPLIFY VULNERABILITY ASSESSMENT

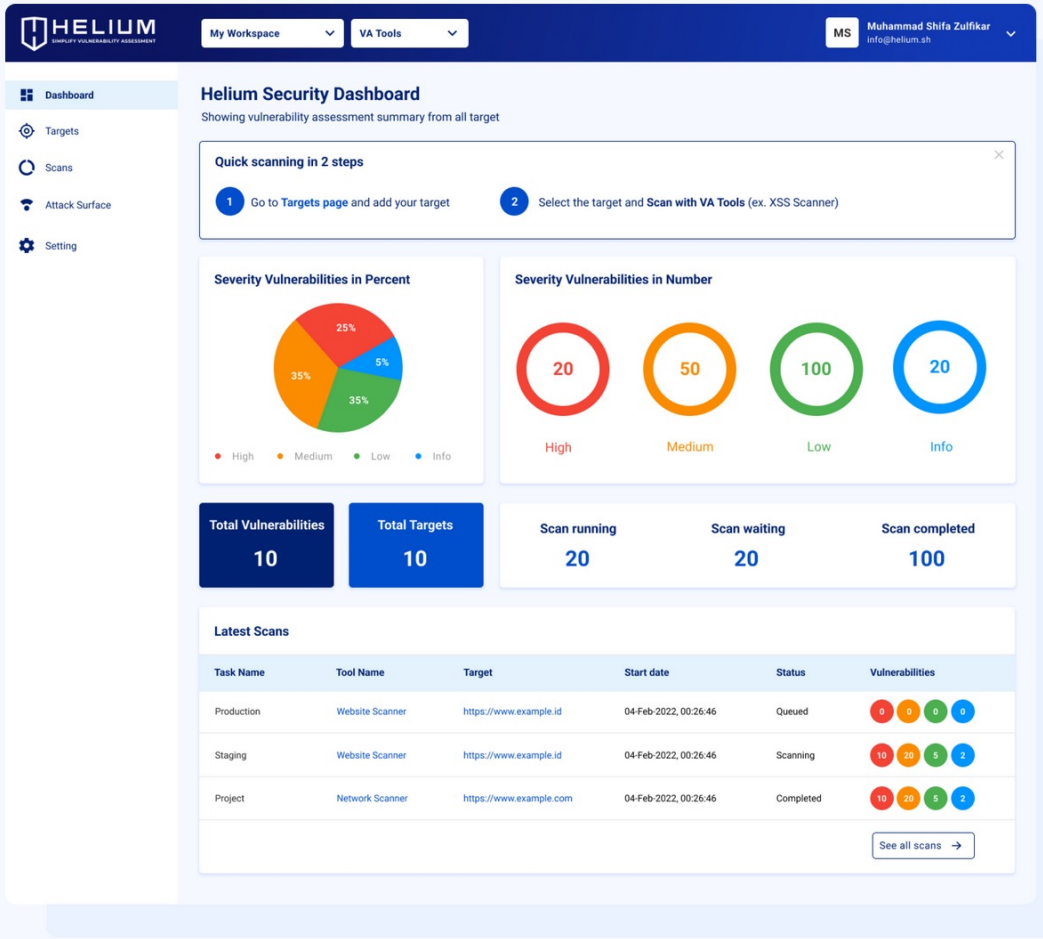
Automate Vulnerability Assessment with powerful cloud-based tools

Try to scan your website

www.example.com

I am authorized to scan this target and I agree to the Terms of Service

Scan Target



Trusted by expert at

HELIUM
SIMPLIFY VULNERABILITY ASSESSMENT

BADAN PUSAT STATISTIK

KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

KEMENKO POLHUKAM REPUBLIK INDONESIA

CIMAHI
SALUYU NGAWANGUN JATI MANDIRI

SATYA KARYA KERTA RAHARJA

GEMAH RIPAH REPEH RAPIH

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA

KABUPATEN KERAWANG
PANGKAL PERJUANGAN

KOTA Bogor

LOMBOK BARAT
PATUT PATUH PATJU

IMIGRASI

SATYA ADHI WICAKSANA

Dinas Kesehatan
Propinsi Daerah Istimewa Yogyakarta

KOTA BONTANG
BESSAI BERINTA

GEMAH RIPAH LOH JINAWI

JakGo.
JAKARTA.GO.ID

Pemerintah Kota Pekalongan

Pemalangkab.go.id
Pemerintah Kabupaten Pemalang

PEMERINTAH KABUPATEN SUBANG
DISKOMINFO
DINAS KOMUNIKASI DAN INFORMATIKA

Cyber Security Education Platform

CYBER ACADEMY

Focuses on developing Individual and Corporate in Cyber Security

In-house Training

- **Security Awareness**
- **Secure Software Development Life Cycle**
- **Secure Coding**
- **Penetration Testing**

Our Clients

Online Course

There are 2 types of learning

- **Self-paced Learning “Belajar Online”**
  Materials, Quiz, Exam and Q&A are available on the platform
- **Live Class**
  Instructor led, virtual streaming of your course with instructor Q&A

Cybersecurity Labs

Access All Labs seamlessly

CYBER ACADEMY

Belajar Online | Live Class | In-House Training | Promo | Masuk | Daftar

Bangun Karirmu sebagai Cyber Security Profesional

Pelajari Konsep dan Teknik Cyber Security dari para Pengajar Terbaik yang berpengalaman di Industri sampai Bisa!

Belajar Sekarang

CYBER SECURITY LIVE CLASS

Kamu dapat belajar dan berinteraksi secara langsung dengan Pengajar Terbaik dalam setiap sesi sampai Bisa!

Benefit Live Class

Belajar dari Pengajar Terbaik
Pengajar kami berasal dari Dosen dan Praktisi yang berpengalaman di dunia Industri

Akses E-Learning Kapanpun
Kamu akan mendapatkan Materi dan Hasil rekaman sesi Live Class

Kelas Interaktif
Kamu dapat berinteraksi langsung secara online dengan pengajar

Sertifikat Kompetensi
Sertifikat ini tersedia di Live Class dengan menyelesaikan semua Modul, Tugas, Kuis dan Ujian

LIVE CLASS

Cyber Security ANALYST

Pengajar
Onno W. Purbo
Pakar IT

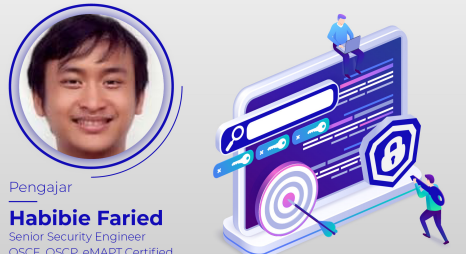
LIVE CLASS

CYBER INCIDENT RESPONSE FUNDAMENTAL

Pengajar
Mohamad Endhy Aziz
CISSP, ECIH, CHFI, CEH
Cybersecurity Specialist

LIVE CLASS

WEB PENETRATION TESTING FUNDAMENTAL



Pengajar
Habibie Faried
Senior Security Engineer

Secure SDLC Training

Secure Software Development Life Cycle (Secure Coding) is an educational activity for developers regarding methods for developing secure applications.

Developers will learn various attack techniques on applications, explain how attacks can occur and will open insight for developers about what things must be considered in making applications safely.

CYBER ACADEMY

www.cyberacademy.id

Public Workshop

In-house Training at Telkom Indonesia

Secure Coding Workshop for Startup, collaboration with BSSN

In-house Training at Telkom Indonesia

Penetration Testing Training

Penetration Testing is an educational activity aimed for technical people.

This activity is to increase understanding of attack techniques on a system. Participants will learn various attack techniques that can be carried out on the system so that they can explain how the attack can occur.

CYBER ACADEMY

www.cyberacademy.id

In-house Training at Telkom Indonesia

In-house Training at Telkom Indonesia

In-house Training at Telkom Indonesia

In-house Training at Telkom Indonesia

Cyber Security Awareness

Security Awareness is an educational activity with the target participants being all individuals in an organization.

The purpose of this education is to provide an understanding of the risks and impacts of the information used, understand the potential of threats and increase awareness of information and cyber security.

CYBER ACADEMY

www.cyberacademy.id

PT Pindad (Persero)

IT Division at Telkom Group

IT Division at Telkom Indonesia

State Cyber and Crypto Agency (BSSN)

CyberArmy

Reinvent Cybersecurity

PT Global Inovasi Siber Indonesia

Address: Jl. Naripan No.53, Kb. Pisang, Sumur Bandung

Kota Bandung, Jawa Barat, Indonesia

Phone Number : +62812 9393 1337

Email : business@cyberarmy.id

Website : www.cyberarmy.id