GARUDA

Cyber Security

- Threat Hunting Framework
- Threat Intelligence & Attibution
- Digital Forensic Incident Response
- Digital Risk Protection
- Fraud Hunting Platform

make·IT·faster

telkomsigma

by Telkom Indonesia

AGENDA

I. Overview
II. Roadmap Professional Service
III. Challenge and Pain Point
IV. Market Strategy & Case Study

telkomsigma
make·IT·faster
by TelkomIndonesia

OVERVIEW

Product Professional Service, Business Model Canvas, Talent

telkomsigma
make•IT•faster
by Telkom Indonesia

GARUDA TECHNOLOGIES

Threat Intelligence & Attribution

High-fidelity threat intelligence data
& best-in-class custom research

Adversary-centric threat detection and proactive threat hunting

Threat Hunting Framework

Huntbox | Sensor
Polygon| Huntpoint

Advanced fraud detection and user authentication

Fraud Hunting Platform

Next-gen intellectual property protection

Digital Risk Protection

Anti-Piracy | Anti-Scam
Anti-Counterfeit

Services for the Battlefield

- Investigations
- Incident response
- Digital forensics
- Compromise assessment
- Security & risk assessment
- CERT

telkomsigma
make•IT•faster
by TelkomIndonesia

MAPPING SEGMENT

Cyber Security Solution Based on Industrial Market

MARKET INDUSTRY	GARUDA CYBERSECURITY SOLUTION								
	NG-SIEM	Vulnerability Assessment & Penetration Test	Fraud Hunting Platform	Threat Hunting Framework	Threat Intelligence & Attribution	Digital Forensic & Malware Analysis	Data Protection	Managed Security Service Provider 24/7	Managed Detection and Respond
Banking Financial Service & Insurance	✓	✓	✓	✓	✓	✓	✓	✓	✓
Goverement/Military/Police	✓	✓	✓	✓	✓	✓	✓	✓	✓
Energy/Manufacture	✓	✓	✗	✓	✓	✗	✓	✓	✓
Logistic/ Transportation/ Distribution	✓	✓	✗	✓	✗	✗	✓	✓	✗
Retail Profesional Services	✓	✓	✗	✓	✗	✗	✓	✓	✗
Healthcare/Medical	✓	✓	✗	✓	✓	✗	✓	✓	✓
Telecomunication/Media/Education	✓	✓	✗	✓	✓	✓	✓	✓	✓

This market assessment is based-on the level of cybersecurity needs, the allocation of funds for IT security and the level of cyberattacks against the industry's market.

telkomsigma make•IT•faster by TelkomIndonesia

Identify – Vulnerability Assessment

Deskripsi

Vulnerability Assessment merupakan proses identifikasi risiko dan kerentanan pada sistem, jaringan komputer, aplikasi, atau bagian lain yang ada di ekosistem IT. Fitur ini berfungsi untuk membantu bisnis menunjukan kelemahan di sistem IT seperti coding bugs, security holes, dan lainnya.

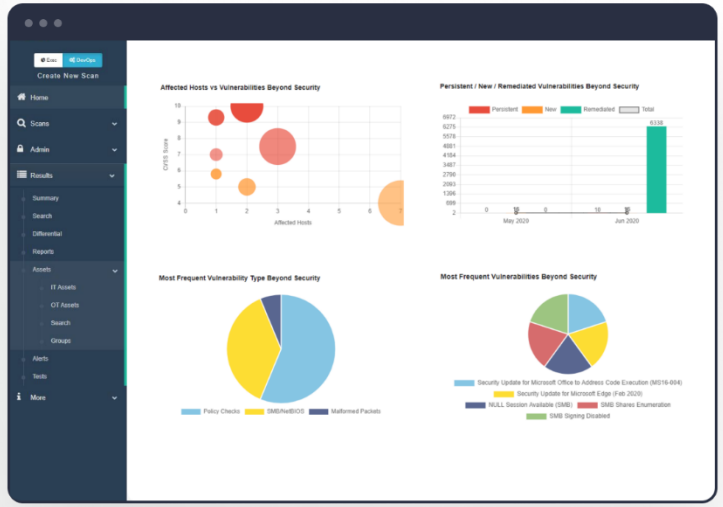
Keunggulan

- ✓ Metode penerapan yang fleksibel, bisa berbasis cloud, on premise atau hybrid.
- ✓ Cukup bayar berdasarkan IP's yang aktif
- ✓ Database virus selalu update, sehingga kegiatan dilakukan dengan databases virus paling baru
- ✓ Memberikan review dari forum-forum underground

Fitur Garuda VA

1. Extended Detection & Response
2. Static Application Security Testing
3. Dynamic Application Security Testing
4. ISO 27001, NIST, HIPAA, OWAPS, PCI ASV Scanning Compliance

UI UX Aplikasi



Basic Requirement

- **Vulnerability Manager Plus Server**
  - Intel Xeon E5 (8 core/16 thread) 2.6 GHz 40 MB cache, RAM 32 GB & HDD 120 GB (for internal network access)
- **Akses Internet**
  - Minimal 1 Mbps
  - Akses ke dalam internal infrastruktur pelanggan.
- **Kesiapan Data**
  - Data banyaknya IP's/Domain's yang akan di tes
  - Seberapa luas kegiatan yang akan di lakukan

Go to Market Strategy:

- Web
- Presentation
- Flyer/Booklet
- Video (on progress)
- Demo Product

Skema Bisnis (Untuk Implementasi)

1. Project Charge
2. Termin Payment
3. IP's/Domain's Based

Skema Sizing (Untuk Implementasi)

1. Jumlah IP's/Domain's
2. Jumlah infrastruktur IT
3. Ketersediaan anggaran
4. Ketersediaan akses internet
5. Waktu plan implementasi (timeline)
6. Scope pengadaan

telkomsigma make·IT·faster by TelkomIndonesia

Identify – Penetration Test

Deskripsi

Penetration Test (Pentest) adalah sebuah metode yang dilakukan untuk mengevaluasi keamanan dari sebuah sistem dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan. Hasil dari pentest ini berguna sebagai feedback bagi pengelola sistem untuk memperbaiki tingkat keamanan dari sistem komputer mereka.

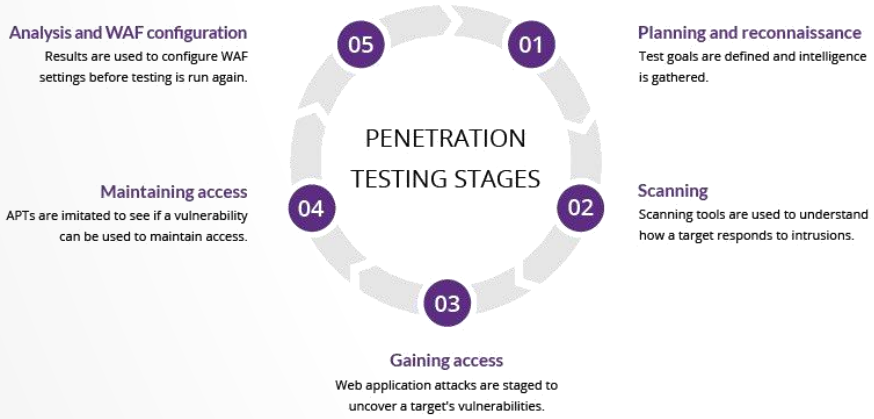
Keunggulan

- ✓ Metode pembayaran solusi yang fleksibel berdasarkan keinginan user
- ✓ Penyediaan prosedur yang lengkap dan dapat menunjukan bagaimana serangan dapat di lakukan
- ✓ Didukung oleh berbagai tenaga ahli berpengalaman
- ✓ Telah berpengalaman dalam pengembangan IT Infrastructure di Telkom Group selama lebih dari 15 tahun

Fitur Garuda Pentest

1. External Penetration Testing
2. Internal Penetration Testing
3. Web Application Security Assessment
4. Mobile Application Security Assessment
5. Online Banking Security Asssessment
6. Whitelist, Blacklist, Greylist Pentest.

Flow Proses



Basic Requirement

- **Akses**
  - Minimal 1 Mbps
  - Akses ke dalam internal infrastruktur pelanggan.
- **Kesiapan Data**
  - Data banyaknya infrastruktur yang akan di test
  - Seberapa luas kegiatan yang akan di lakukan

Go to Market Strategy:

- Web
- Presentation
- Flyer/Booklet
- Video (on progress)
- Demo Product

Skema Bisnis (Untuk Implementasi)

1. One Time Charge
2. Termin Payment
3. Monthly Payment

Skema Sizing (Untuk Implementasi)

1. Jumlah sistem
2. Ketersediaan akses untuk di jangkau oleh team pentester.
3. Waktu plan implementasi (timeline)
4. Scope pengadaan.

telkomsigma make·IT·faster by TelkomIndonesia

Protect – Managed Security Service

Deskripsi

Manage Security Service ialah sebuah layanan pengelolaan sistem keamanan IT sebuah perusahaan yang dilakukan oleh Managed Security Service Provider (MSSP). MSP24x7 memiliki Security Operation Center (SOC) yang dibangun untuk memenuhi kebutuhan pengelolaan sekuriti perusahaan klien. Sehingga klien tidak perlu mengeluarkan biaya besar untuk membangun dan mengoperasikan SOC sendiri.

Keunggulan

- ✓ Pengawasan 24/7/365
- ✓ Memiliki akses ke lebih dari 100 komunitas di darkweb dan deepweb.
- ✓ Memiliki kerja sama dengan principal yang memiliki akses ke interpol.
- ✓ Memiliki sistem threat hunting yang mutakhir.
- ✓ Agnostic brand operated.

Fitur Garuda Manage Security Service

1. Memiliki tenaga ahli L1 24/7 onsite/remote
2. Memiliki tenaga ahli L2 onsite/remote
3. Memiliki tenaga ahli L3 yang dapat melakukan offensive dan defensive cyber security
4. Layanan yang fleksibel sesuai dengan kebutuhan customer

Ilustrasi

Basic Requirement

- **Akses Internet untuk onsite**
  - Minimal 1 Mbps
- **Kesiapan Data**
  - Memberikan data infrastruktur IT
  - Memberikan akses ke SIEM ataupun monitoring lainnya milik customer
  - Menyediakan ruang lingkup kegiatan sehingga kegiatan dapat terlaksana dengan baik
  - Memberikan batasan akses sehingga tidak mengganggu infrastruktur lainnya

Go to Market Strategy:

- Web
- Presentation
- Flyer/Booklet
- Video (on progress)

Skema Bisnis (Untuk Implementasi)

1. One Time Charge
2. Termin Payment
3. Monthly Payment

Skema Sizing (Untuk Implementasi)

1. Jumlah infrastruktur IT
2. Kecepatan akses public (Internet)
3. Ketersediaan anggaran
4. Ketersediaan akses internet
5. Waktu operasi (timeline)
6. Scope pengadaan

telkomsigma make·IT·faster by TelkomIndonesia

Detect – Managed Detection & Response

Deskripsi

Manage Detection and Response merupakan solusi yang di miliki oleh Garuda Cyber Security, untuk melakukan analisa terhadap lintasan data yang masuk ke dalam infrastruktur IT dan melakukan response terhadap data baik data yang positif ataupun negatif

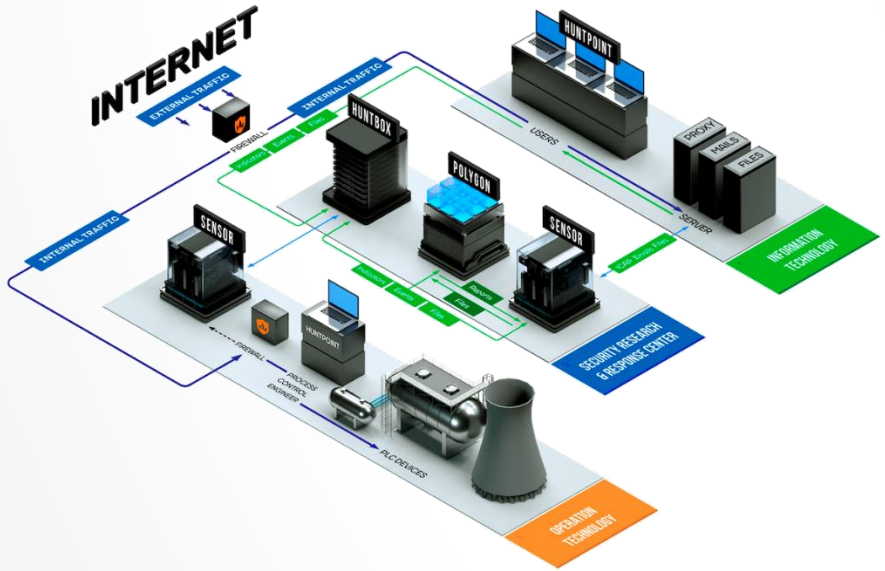
Keunggulan

- ✓ Deteksi ancaman yang sebelumnya tidak diketahui berdasarkan data Threat Intelligence & Attribution.
- ✓ Korelasi otomatis peristiwa dan peringatan, dan atribusi berikutnya ke jenis malware dan/atau aktor ancaman
- ✓ Global proactive threat hunting
- ✓ Alat yang digunakan merupakan alat terbaik yang dapat melakukan malware detonation, data enrichment, correlation dan analisis
- ✓ Dapat memberikan laporan lengkap terkait kemungkinan serangan

Fitur Garuda Manage Detection and Response

1. Threat Hunting
2. Threat Research
3. Behavior Analysis
4. Forensic Investigation
5. Dapat di deploy secara cloud/onpremise/hybrid

Architecture



Basic Requirement

- **Akses Internet**
  - Minimal 1Mbps
- **Kesiapan Data**
  - Memberikan data infrastruktur yang akan di proteksi.
  - Melakukan Compremise Assessment dan Pre-IR(Incident Response).
  - Memberikan data topology sebagai bahan analisa agar tidak mengganggu sistem yang sudah berjalan
  - Memberikan akses API agar dapat terintergrasi dengan sistem MDR

Go to Market Strategy:

- Web
- Presentation
- Flyer/Booklet
- Video (on progress)
- Demo Product

Skema Bisnis (Untuk Implementasi)

1. One Time Charge
2. Termin Payment
3. Monthly Payment
4. On Cloud
5. Hybrid
6. On Premise

Skema Sizing (Untuk Implementasi)

1. Seberapa besar infrastruktur IT
2. Ketersediaan anggaran
3. Ketersediaan akses yang aman
4. Waktu operasi (timeline)
5. Scope pengadaan

telkomsigma make·IT·faster by TelkomIndonesia

Detection – Digital Risk Protection

AI-Driven Digital Risk Identification & Mitigation Platform

trusted · IT · company
telkomsigma
by Telkom Indonesia

Modules

ANTI-SCAM

Protection against online brand abuse

- Scam and phishing
- Fake partnerships and trademark abuse
- Fake accounts and groups on social media
- Fake mobile apps

ANTI-COUNTERFEITING

Protection against illegal online sales of goods and services

- Illegal sale of goods on the internet
- Grey import
- Breaches of partnership agreements

ANTI-PIRACY

Protection against illegal distribution of digital content

- Video content
- Online streams
- Software, computer, games
- Books, newspapers, articles
- Music

LEAK DETECTION

Detection of sensitive data published on paste-sites and dark web

- Credentials
- Code leaks
- Sensitive data

VIP PROTECTION

Monitoring and mitigation fake accounts for C-level impersonation

- Fake accounts on social media
- Digital appearance analysis

Analyzing detected infringements & Prioritizing what to enforce

RESOURCES FOR ANALYSIS

- Domain names
- Databases of phishing resources
- Search engines
- Social media
- Mobile apps store
- Online classifieds and marketplaces
- Advertising
- Instant messenger
- Deep/dark web

AUTOMATED

- BRAND NAME MENTIONS
- VIOLATION DETERMINTATION
- ENFORCEMENT PRIORITAZION

AUTOMATED & MANUAL

- **Comprehensive takedown procedure reach an 85% pre-trial takedown rate on average**
- RESPONSE

Response – Incident Response

Deskripsi

Incident Response merupakan sebuah layanan milik Garuda yang bertujuan untuk membantu customer yang mengalamai data breaches, sehingga diperlukan tim untuk membantu memperbaiki data breaches yang terjadi.

High Level Step

- **Forensic Analysis** – Analysis of logs from workstations and servers used by cybercriminals to identify the initial attack vector, applied tools and techniques, exploited vulnerabilities.
- **Malware Analysis** – Basic or advanced static and dynamic analysis of malicious code discovered during an investigation to determine other affected assets and prevent further intrusions
- **Network traffic analysis** – Perform network traffic monitoring and suspicious behaviour detection missed by signature-based cybersecurity systems using our Threat Hunting Framework sensor

Skema Bisnis Minimum 100 Hours

1. One Time Charge
2. Termin Payment
3. Monthly Payment
4. Per Incident Payment
5. Per Item Request

Go to Market Strategy:

- Web
- Presentation
- Flyer/Booklet
- Video (on progress)

Where we search	Three level approach		
	Network	Endpoints	Threat Intelligence
What we search	**Malicious payloads** • Bank Trojans • Backdoors • Crypto Miners • RATs • WMI backdoors • Exploits • Keyloggers • Web shells • Rootkits	**Threat actor activity** • Remote execution • Spear phishing • Network scanning • Reconnaissance • Privilege escalation • Lateral movement • Data exfiltration	**Tools** • LSASS dumpers • Mimikatz • Network scanners • Remote tools • Psexec • Powershell

Using the methodology Our Analysts will cover minimum below list of use cases:

- Credentials theft
- Data leakage
- Targeted Malware attack
- Malware proliferation
- DDoS attack
- Ransomware attack
- Phishing attack
- Hacked network resource
- Competive espionage
- Intellectual property breach
- Online banking fraud
- Email fraud
- ATM and card processing fraud
- Account takeover
- Blackmailing by cyber channels

Recover – Investigation Service

Interpol & Europol Official Partner

Three Magecart operatives arrested in Indonesia

By **Doug Olenick** January 27, 2020

Several members of a group allegedly behind hundreds of Magecart-style attacks were arrested last month in Indonesia as the result of an international law enforcement operation. Interpol's ASEAN Cyber Capability Desk and the Indonesian National Police just announced late last week the December 20, 2019 arrest of three members of a group allegedly behind a...

Official partner of Interpol and Europol

Recommended by the Organization for Security and Cooperation in Europe (OSCE)

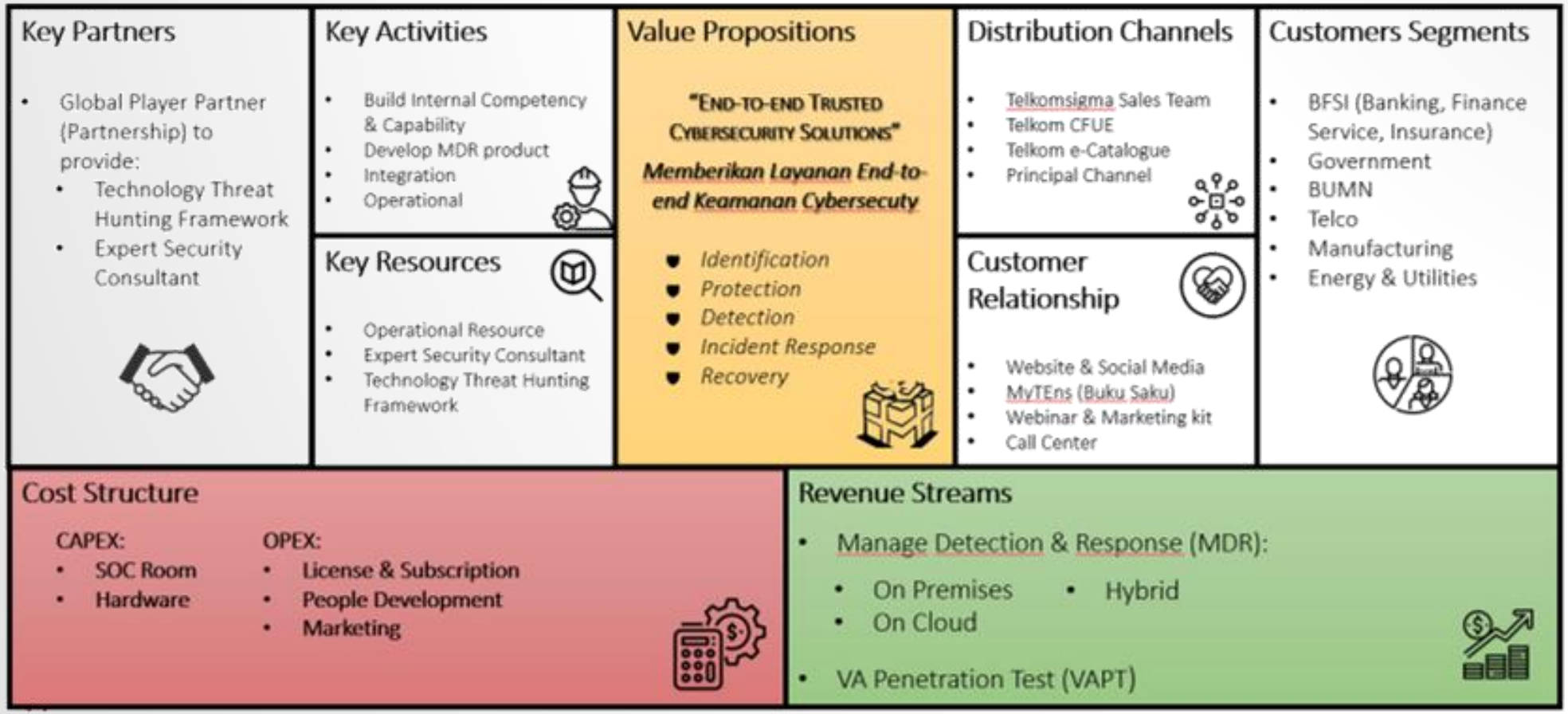
Recommended by the global provider of secure financial messaging services (SWIFT)

Group-IB's products are recognized by the world's leading research companies — Gartner, IDC, Forrester

Group-IB experts hold numerous industry-recognized certifications, including OSCP, OSWE, CEH, GCFA, PCI QSA, and others

Group-IB is a member and partner of leading organizations aimed at developing and connecting security information sharing communities

BUSINESS MODEL CANVAS



make·IT·faster
telkomsigma
by TelkomIndonesia

PEOPLE COMPETENCIES

SECURITY		Total		NETWORK		Total		INFRASTRUCTURE		Total
EC-Council	CEH (Certified Ethical Hacker)	2		Cisco	CCNA	2		VMWARE	VCP	1
	CHFI	2			CCNP	1				
	ECIH	1						Redhat	RHCE	1
				H3C	HCNA	1				
Group – IB	MDR Analyst	9								
	SOC Analyst	8								
	THF	13								

ROADMAP PROFESSIONAL SERVICE

telkomsigma
make•IT•faster
by Telkom Indonesia

GARUDA CYBERSECURITY ROADMAP

	2021	2022	2023	2024	2025	2026
Phase						
Product & Service	▪ Managed Detection & Response ▪ Vulnerability & Penetration Test	▪ Threat Intelligence & Attribution	▪ Digital Forensic Laboratory	▪ Product Owned Manufacturing with OEM Program	▪ Capacity Upgrade	
Staging	Foundation security - Baseline security monitoring and operations capability	Staging SOC 1.0: Core security monitoring and operations capability	Evolve – SOC 2.0 Enhanced detection and response capability	Mature – Advance ASOC 1.0 Intelligence led, Advanced capability	Continues Improvement	
Preparation	SOC Monitoring room	SOC Analysist room	SOC Laboratory room	SOC R&D room	SOC training room	
Competency & Capability	⊕ Threat Hunting ◎ Cyber Threat Analyst ◎ Digital Forensic ◎ Threat Intelligence	⊕ Threat Hunting ◎ Cyber Threat Analyst ◎ Digital Forensic ⊕ Threat Intelligence	⊕ Threat Hunting ⊕ Cyber Threat Analyst ◎ Digital Forensic ⊕ Threat Intelligence	⊕ Threat Hunting ⊕ Cyber Threat Analyst ⊕ Digital Forensic ⊕ Threat Intelligence		
Investment						

telkomsigma
make•IT•faster
by TelkomIndonesia

CHALLENGE AND PAIN POINT

telkomsigma
make•IT•faster
by Telkom Indonesia

CHALLENGE AND PAIN POINT

Challenge

- Wide Market In Telkom Group Territories
- Building Awareness To Customers
- Covid'19 Culture Changing & Increasing Of Cyber Threat

Pain Point

- Huge Resources Needs
- Emerging Competitors
- Distributor / Reseller Preferences
- Changing Regulatory Environment

MARKET STRATEGY & CASE STUDY

telkomsigma
make•IT•faster
by Telkom Indonesia

CASE STUDY

1. Technology Strategy

- Open discussion and study comparison
- Must know customer pain, principal expert might help
- Give a Demo
- Offer solution

Opportunities:
- Kejagung Bank Data Intelligent (QO)
- Pusiber Kementerian Pertahanan (QO)

2. Assessment Strategy

- Free Security Assessment
- Give Underground Source Review & Leaks (if Found)
- Give a free Passive Scanning to check security weakness
- Offer solution

Opportunities:
- BPJS Kesehatan MSSP (won)
- Kementerian BUMN (won)
- NPCX1 Port Authority
- Peruri (Won)
- Pertamina (Won)

3. Incident Strategy

- Help customer with their cyber case (ransomware, breach, etc.)
- Give a free Digital Forensic Incident Response
- Give a free Investigation Service
- Offer solution

Opportunities:
- BPJS Kesehatan Forensic & Investigation services (won)
- Angkasa Pura 2

4. Event & Seminars

- Cyber Security Product Update
- Marketing Collateral
- Correspondences
- Follow-up

Opportunities:
- PT. KAI
- Perben Kemenkeu
- Bank DKI
- Etc.

Terima Kasih

Спасибо

- **Telkom Landmark Tower II**, 23rd Floor Jakarta
- **Graha Telkomsigma, Bumi Serpong Damai**, Jalan Kapt. Subijanto Dj, Lengkong Gudang, Kec. Serpong, Kota Tangerang Selatan

+62 21 8086 4830

+62 21 5388538

Rizka.Ardiantary@sigma.co.id

telkomsigma
make·IT·faster
by Telkom Indonesia