MATERI L1 SOC ANALYST

UNIT KOMPETENSI 2

Melakukan Pemantauan Aset Teknologi Informasi
Terhadap Aktivitas Ancaman Siber

MEDIA PEMBELAJARAN L1 SOC ANALYST

Unit Kompetensi

Melakukan Pemantauan Aset Teknologi Informasi (Ti) Terhadap Aktivitas Ancaman Siber

Hasil Pembelajaran

Setelah mengikuti pembelajaran peserta didik diharapkan mampu melakukan analisis terhadap keamanan siber untuk menentukan kendali

Indikator Hasil Belajar

- Mengumpulkan informasi terkait efek dari insiden kemanan siber
- Mengidentifikasi dampak insiden siber
- Menentukan kendali terhadap insiden keamanan siber

Elemen Kompetensi

1. Mengidentifikasi daftar aset TI yang rentan terhadap ancaman siber
    a. Daftar aset TI diidentifikasi berdasarkan tingkat kegentingan.
    b. Daftar aktivitas siber yang mencurigakan diidentifikasi berdasarkan informasi ancaman.
    c. Daftar kerentanan aset TI secara umum dikumpulkan berdasarkan informasi internal dan eksternal
2. Mengidentifikasi dampak insiden kemanan siber
    a. Aktivitas siber yang teridentifikasi dianalisis sesuai prosedur
    b. Dokumentasi aktivitas dibuat berdasarkan temuan
3. Menentukan kendali terhadap insiden keamanan siber
    a. Rencana penanganan insiden keamanan siber dibuat berdasarkan prosedur.
    b. Ketersediaan akan sumber daya internal dalam penanganan insiden keamanan siber dipastikan sesuai kebutuhan.
    c. Eskalasi pengambilan keputusan berdasarkan kewenangan dilakukan sesuai prosedur.
    d. Laporan kegiatan investigasi awal untuk menentukan kendali terhadap insiden keamanan siber didokumentasikan sesuai prosedur.

A. Identifikasi Aset Teknologi Informasi

Apa itu Aset Teknologi Informasi ?

Semua elemen (sumber daya, perangkat keras, perangkat lunak, data, infrastruktur, dll) yang digunakan dalam konteks teknologi informasi (TI) pada sebuah organisasi, memiliki nilai ekonomi dan memberikan manfaat bagi organisasi dalam hal pengelolaan, penyimpanan, pemrosesan, dan penyebaran informasi.

Kriteria Unjuk Kerja

1. Daftar aset TI diidentifikasi berdasarkan tingkat kegentingan.
2. Daftar aktivitas siber yang mencurigakan diidentifikasi berdasarkan informasi ancaman.
3. Daftar kerentanan aset TI secara umum dikumpulkan berdasarkan informasi internal dan eksternal

Teknologi Informasi

1. Aset Fisik
    - Perangkat Keras : komputer, server, printer, perangkat jaringan
    - Perangkat Lunak: sistem operasi, aplikasi, database
2. Aset Non-fisik
    - Data: data pelanggan, data transaksi, data produk
    - Informasi: laporan, grafik, tabel
    - Pengetahuan: pengetahuan tentang bisnis
3. Aset Manusia
    - Teknisi TI
    - Analis TI

Aset Ti Berdasarkan tingkat kegentingan

1. Critical Assets Tingkat kepentingan tertinggi dalam mendukung operasi bisnis inti suatu organisasi**.** Sangat penting bagi kelangsungan operasional dan kesuksesan organisasi. Contoh : server pusat data, Sistem Layanan Pelanggan, Data Costumer
2. Important AssetsTingkat kepentingan signifikan, tidak sepenting aset kritis, namun masih mendukung proses operasional Contoh : Perangkat Lunak analisis data (Tableau), Perangkat Lunak keamanan informasi (firewall, IDS, IPS)
3. Supporting Assets
   Memiliki dampak yang lebih rendah jika terjadi gangguan atau kerusakan. Organisasi mungkin dapat bertahan dan melanjutkan operasi dengan relatif lancar jika aset pendukung mengalami masalah. Contoh : Perangkat administratif (printer, pengolah dokumen) dll.

Dokumentasi Aset TI

Dokumentasi aset TI harus mencakup informasi berikut:

1. Identitas aset, seperti nama, nomor seri, dan lokasi aset.
2. Deskripsi aset, seperti jenis, versi, dan fungsi aset.
3. Nilai aset, seperti nilai ekonomis, operasional, hukum, dan reputasi aset.
4. Tingkat kegentingan aset, seperti kritis, penting, atau biasa.
5. Kontrol keamanan yang diterapkan, seperti kontrol akses, kontrol otorisasi, dan kontrol enkripsi

Host	Product	Function	Internet Protocol Address	Operating System
Demilitarized Zone				
Bro	Bro	Network security monitor	172.16.0.20	Ubuntu 14.04
FathomSensor	RedJack Fathom	Network analysis	172.16.0.50	CentOS 7
OpenSwan	OpenSwan	Virtual Private Network (VPN)	172.16.0.67	Ubuntu 14.04
Router0	pfSense	Router/firewall	172.16.0.11 10.33.5.9	BSD pfSense appliance
Snort	Cisco/Sourcefire Snort	Intrusion Detection System	172.16.0.40	Ubuntu 14.04
Apt-cacher0	Ubuntu apt-cacher	Patch management	172.16.0.77	Ubuntu 14.04
WSUS	Microsoft WSUS	Patch management	172.16.0.45	Server 2012R2
IT Systems				
AD1	Microsoft Active Directory	Directory manager, AAA, DNS	172.16.1.20	Server 2012R2
AD2	Microsoft Active Directory	Directory manager, AAA, DNS	172.16.1.21	Server 2012R2
CA server	Microsoft Certifi-cate Authority	PKI certificate authority	172.16.1.41	Server 2012R2
Email Server	Postfix	Email server for the lab	172.16.1.50	Ubuntu 14.04
PE Master	Puppet Labs Puppet Enterprise	Configuration manage-ment	172.16.1.40	Ubuntu 14.04
Router1	pfSense	Router/firewall	172.16.0.12 172.16.1.1	BSD pfSense appliance
Ubuntu Client1	Ubuntu Desktop	Representative Linux client	DHCP	Ubuntu 14.04
Win7-Client1	Microsoft Windows7	Representative Windows client	DHCP	Windows 7 Enterprise
Win7-Client2	Microsoft Windows7	Representative Windows client	DHCP	Windows 7 Enterprise
Network Security				
Router2	pfSense	Router/firewall	172.16.0.13 172.16.2.11	BSD pfSense appliance
BelManage	Belarc BelManage	Software, hardware, configuration information	172.16.2.71	Windows Server 2012R2

Host	Product	Function	Internet Protocol Address	Operating System
BDA	Belarc BelManage Data Analytics	Analytic information for BelManage	172.16.2.72	Windows 7
OpenVAS	OpenVAS	Vulnerability analysis system	172.16.2.33	Ubuntu 14.04
Physical Asset Management				
Router3	pfSense	Router/firewall	172.16.0.14 172.16.3.11	BSD pfSense appliance
AssetCentral	AlphaPoint AssetCentral	IT and datacenter asset management system	172.16.3.103	CentOS7
CA ITAM	CA Technologies IT Asset Manager	Lifecycle asset manage-ment	172.16.3.92	Windows Server 2012R2
Physical Security				
Router4	pfSense	Router/firewall	172.16.0.15 192.168.1.11	BSD pfSense appliance
iStar Edge	Tyco iStar Edge	Security system with badge reader for door access	192.168.1.169	Embedded
NVR	Tyco/American Dynamics VideoEdge	Digital video recorder for IP security cameras	192.168.1.178	Suse Linux (JeOS)
Camera1	Illustra 600 IP camera	IP security camera	192.168.1.176	Embedded
Camera2	Illustra 600 IP camera	IP security camera	192.168.1.177	Embedded
CCure9000	CCure9000	Controller for iStar Edge and NVR	192.168.1.167	Windows 7
ITAM				
Router5	pfSense	Router/firewall	172.16.0.16 172.16.5.11	BSD pfSense appliance
Splunk	Splunk Enterprise	Data aggregation, storage, analysis and visualization	172.16.5.55	RHEL 7

Aktivitas Siber

1. *Information Security Event*
   Kejadian yang dapat mengancam keamanan informasi suatu organisasi. Kejadian ini dapat disebabkan oleh faktor internal atau eksternal, seperti serangan siber, kesalahan manusia, atau bencana alam
   Contoh: *Malware*, Phising, DoS, Pencurian Data.
2. *Information Security Vulnerability*
   Kelemahan dalam sistem informasi atau jaringan komputer yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan siber. Kerentanan ini dapat ditemukan di berbagai komponen sistem informasi, seperti perangkat lunak, perangkat keras, dan konfigurasi sistem.
   Contoh: Bug, Weak Password, Missconfiguration, Zero-day
3. *Network Activity*
   Aktivitas yang terjadi di jaringan komputer. Aktivitas ini dapat berupa komunikasi data antara perangkat di jaringan, akses ke sumber daya jaringan, dan penggunaan aplikasi jaringan.

Contoh: Login ke server, transfer file, anomaly trafik

Malware

Perangkat lunak yang dirancang untuk merusak, mengganggu, mencuri, atau menimbulkan tindakan 'buruk' atau tidak sah lainnya pada data, host, atau jaringan.

1. Virus
   Jenis *Malware* yang menyebar dengan memasukkan salinan dirinya ke program lain. Kebanyakan virus menyebar melalui drive memori external.
2. Trojan
   Perangkat lunak yang tampaknya legal, tetapi berisi kode berbahaya yang memanfaatkan hak istimewa pengguna yang menjalankannya.
3. Worm
   Worm komputer mirip dengan virus karena mereka mereplikasi dirinya s endiri dengan mengeksploitasi kerentanan di jaringan secara independen. Namun, setelah host terinfeksi, worm menyebar dengan cepat melalui jaringan.
4. Ransomeware
   Malware yang menyangkal akses (*denies access*) ke sistem atau data komputer yang terinfeksi dengan menggunakan algoritma enkripsi untuk mengenkripsi file dan data sistem.

Denial of Service (DoS)

Denial of Service (DoS) menciptakan semacam gangguan dalam ketersediaan layanan jaringan untuk pengguna, perangkat, atau aplikasi

Komponen	Deskripsi
zombies	Sekelompok *host* yang disusupi. *Host* ini menjalankan kode berbahaya.
bots	*Malware* yang dirancang untuk menginfeksi *host* dan berkomunikasi dengan sistem penyerang.
botnet	Sekelompok *zombie* yang telah terinfeksi menggunakan *Malware* yang menyebar sendiri dan dikendalikan oleh penyerang.
handlers	*Command-and-control* (CnC or C2) *master server* yang mengendalikan kelompok zombie.
botmaster	Mengaktifkan layanan transfer file yang tidak sah pada perangkat akhir.

Kerentanan Pada Web App

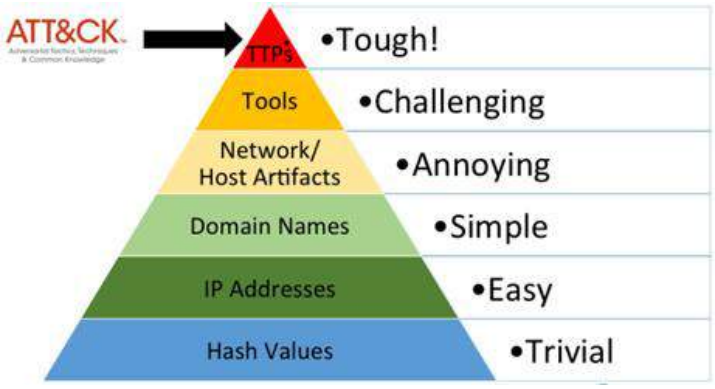
1. *SQL Injection*
   kerentanan yang disebabkan karena *attacker* mampu memanipulasi/ menyuntikan *query SQL* yang digunakan oleh aplikasi sehingga diterima oleh *BackEnd* Aplikasi dan kemudian *query* tersebut dijalankan oleh aplikasi *database.*

2. *Remote Code Execution (RCE)*
   kerentanan yang dapat membuat penyerang mengakses perangkat komputasi target dan membuat perubahan dari jarak jauh, di mana pun perangkat berada.
3. *Cross Xite Scripting* (XSS)
   Kerentanan yang dapat membuat attacker meng-injeksi kode javascript ke halaman aplikasi.
4. *Local File Inclusion*
   Kerentanan yang memungkinkan attacker membaca sembarang File yang ada pada server yang sama.
5. *File Upload*
   Kerentanan yang memungkinkan penyerang menempatkan sebuah file yang dia pilih ke dalam server target yang mengakibatkan eksekusi kode secara remote melalui file tersebut.
6. *Brute Force Attack*
   Serangan siber yang dilakukan dengan mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi hingga yang benar ditemukan. Serangan ini dapat dilakukan secara manual atau menggunakan perangkat lunak khusus.
7. *Web Defacement*
   Web defacement merupakan suatu serangan pada *website* yang mengubah tampilan asli atau konten dari sebuah *website*.
8. *Initial Access:*
   - *•Exploit Vulnerability Apps : SQL Injection, Cross-Site Scripting (XSS), File Upload Vulnerability*
   - *•Brute Force Attack*

Informasi Ancaman

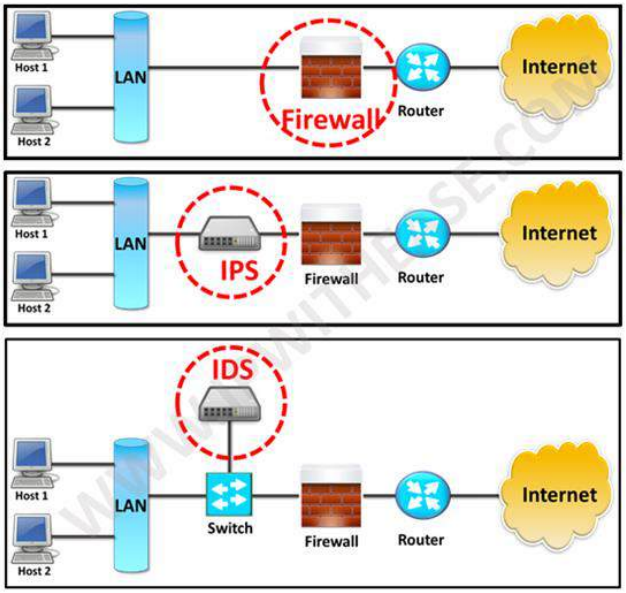
Informasi yang dapat digunakan untuk mengidentifikasi, menganalisis, memonitor dan merespon adanya suatu ancaman siber.

1. *Indicator of Compromises* (IoC)
   IOC adalah bukti bahwa serangan telah terjadi dan setiap serangan memiliki atribut unik yang dapat diidentifikasi.



2. *Tactics, Techniques, and Procedures* (TTP)
   Seperangkat metode yang digunakan oleh penyerang untuk melakukan serangan siber.

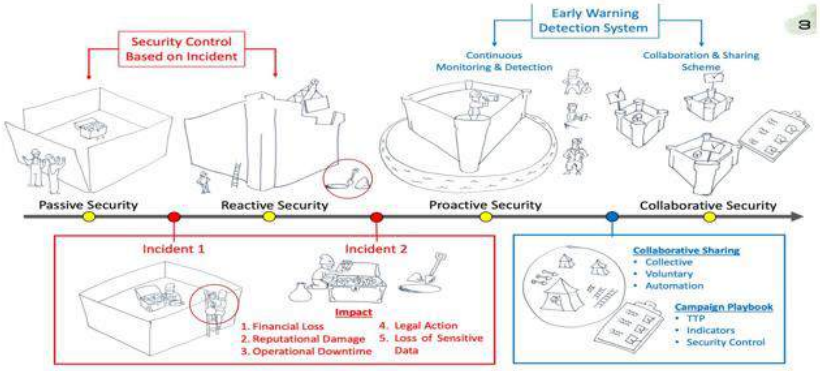
IDS/IPS



1. IDS adalah sistem yang dirancang untuk mendeteksi potensi serangan atau aktivitas mencurigakan di jaringan.
2. IPS adalah evolusi dari IDS yang lebih lanjut. Selain mendeteksi potensi serangan, IPS juga memiliki kemampuan untuk mencegah atau menghentikan serangan tersebut secara otomatis.

B. Pemantauan Aset Teknologi Informasi (TI)

Cyber Security Phase



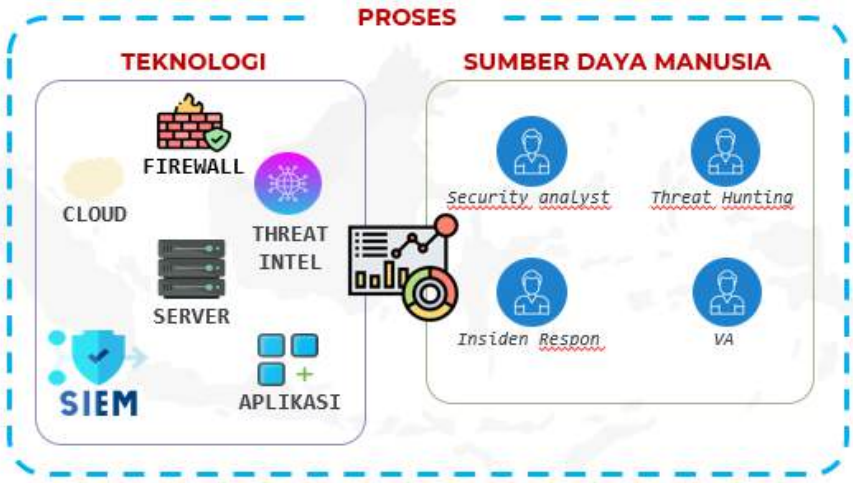
Gambar diatas menggambar empat fase dalam cybersecurity yang meliputi:

1. *Passive Security*
   Merupakan fase awal tanpa deteksi proaktif dan dengan keamanan yang dasar
2. *Reactive Security*
   Fase setelah terjadinya insiden 1. dampaknya meliputi Perusakan reputasi, *downtime* operasional, tindakan hukum, dan hilangnya data sensitif.
3. *Proactive Security*
   Fase yang menerapkan *early warning system*, seperti monitoring dan deteksi untuk mencegah terjadinya insiden lebih lanjut (incident 2)
4. *Collaborative Security*
   Semua pihak bekerja sama dengan saling berbagi informasi (*collaborative sharing*), otomatisasi, dan menggunakan panduan langkah-langkah (playbook) untuk merespons ancaman dengan cepat. Fase ini juga di dukung oleh alat seperti Threat Intelligence Platform (TIP) dan langkah-langkah pengendalian keamanan.

Security Operation Center (SOC)

Security Operation Center (SOC) merupakan tim yang terorganisir dan memiliki kemampuan yang mumpuni untuk melakukan monitoring secara berkelanjutan. Meningkatkan postur keamanan organisasi dengan melakukan pendeteksian, analisa dan tanggap insiden menggunakan bantuan teknologi serta proses dan prosedur yang terdefinisi dengan baik.

berikut adalah elemen dari SOC:



Elemen SOC terbagi menjadi dua bagian utama yakni teknologi dan Proses SDM

Teknologi:

1. *Firewall* untuk memblokir akses tidak sah
2. Cloud dan server yakni infrastruktur penyimpanan dan pengolahan data
3. SIEM (*Security Information and Event Management*) yakni sistem untuk monitoring dan analisis keamanan.
4. Threat Intel yakni data intelijen ancaman untuk deteksi dini.
5. Aplikasi yakni perangkat lunak pendukung operasional SOC.

Proses sumber daya manusia:

1. *Security Analyst* untuk menganalisis ancaman dan kejadian keamanan.
2. *Threat Hunting* untuk mencari ancaman secara proaktif.
3. *Incident Response* untuk menangani dan merespons insiden keamanan.
4. VA (*Vulnerability Assessment*) untuk menilai kerentanan sistem.

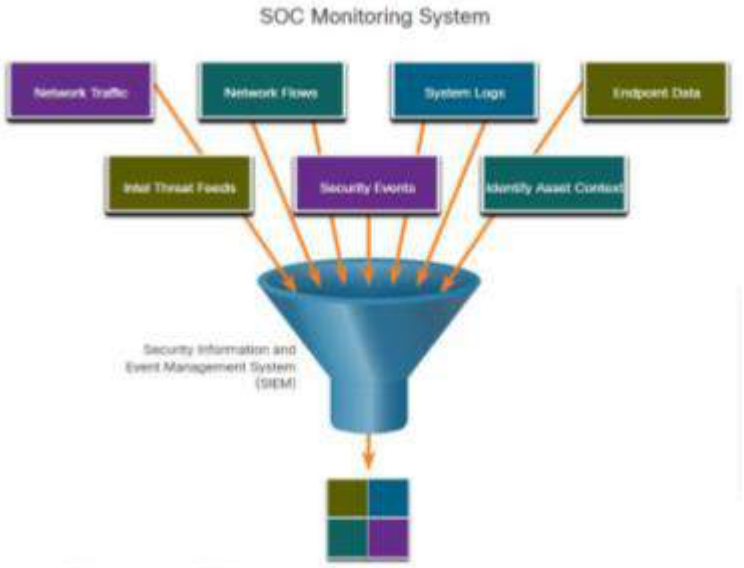
Elemen Sumber Daya Manusia SOC : Tier SOC

Tiers	Responsibilities
Tier 1 Alert Analyst	Pantau peringatan yang masuk, verifiaksi bahwa insiden sebenarnya telah terjadi, dan teruskan tiket ke Tingkat 2, jika perlu.
Tier 2 Incident Responder	Bertanggung jawab atas penyelidikan mendalam atas insiden dan menyarankan perbaikan atau tindakan yang harus di ambil.
Tier 3 Threat Hunter	Ahli dalam jaringan, titik akhir, intelijen ancamanm rekayasa balik *Malware*, dan melacak proses *Malware* untuk menentukan dampaknya dan bagaimana cara menghapusnya. Mereka juga sangat terlibat dalam berburu potensi ancaman dan menerapkan alat deteksi ancaman. Pemburu ancaman mencari ancaman dunia maya yang ada di jaringan tetapi belum terdeteksi.

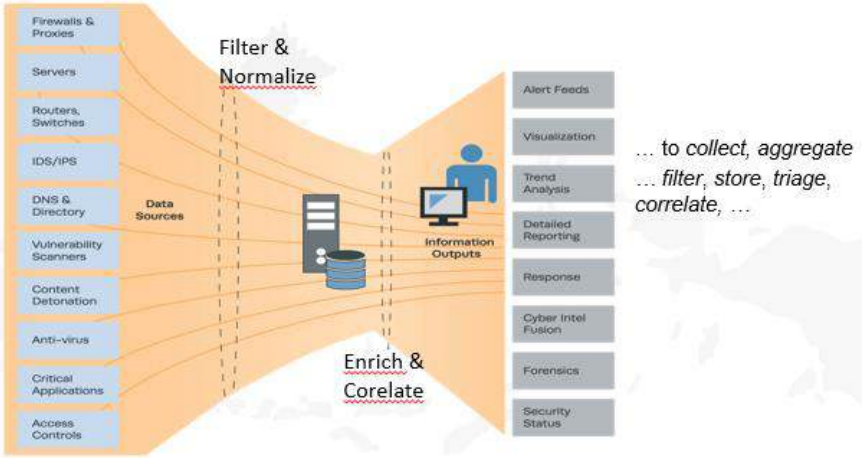
SOC Manager	Mengelola semua sumber daya SOC dan berfungsi sebagai titik kontak untuk organisasi atau pelanggan yang lebih besar.

Security Information and Event Management (SIEM)

SIEM merupakan tool yang digunakan untuk mengumpulkan (collect), agregasi (aggregate), filter, penyimpanan (store), triase (triage), korelasi (correlate), dan visualisasi. Digunakan untuk melakukan analisis dan reviu secara realtime ataupun event yang sudah lalu.



SIEM Architecture



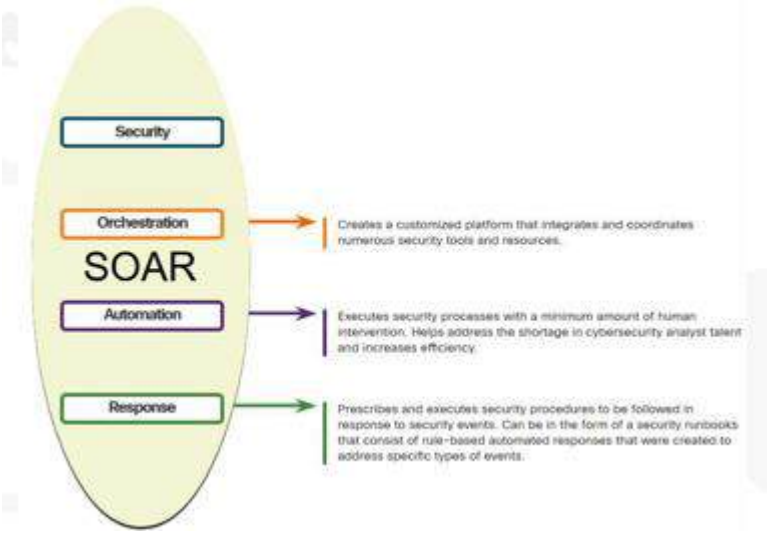
Arsitektur ini terdiri atas dua tahapan utama yakni:

1. Filter & normalize: pada tahapan ini Berbagai sumber data (seperti firewall, server, router, IDS/IPS, DNS, vulnerability scanner, anti-virus, aplikasi, dan kontrol akses) dikumpulkan, disaring, dan dinormalisasi untuk menghasilkan data yang lebih terstruktur.
2. Enrich & Correlate: Data yang sudah dinormalisasi kemudian diperkaya dan dikorelasikan untuk menghasilkan informasi yang lebih bermakna, seperti alert feeds, visualisasi tren, analisis, laporan terperinci, respons, cyber intel

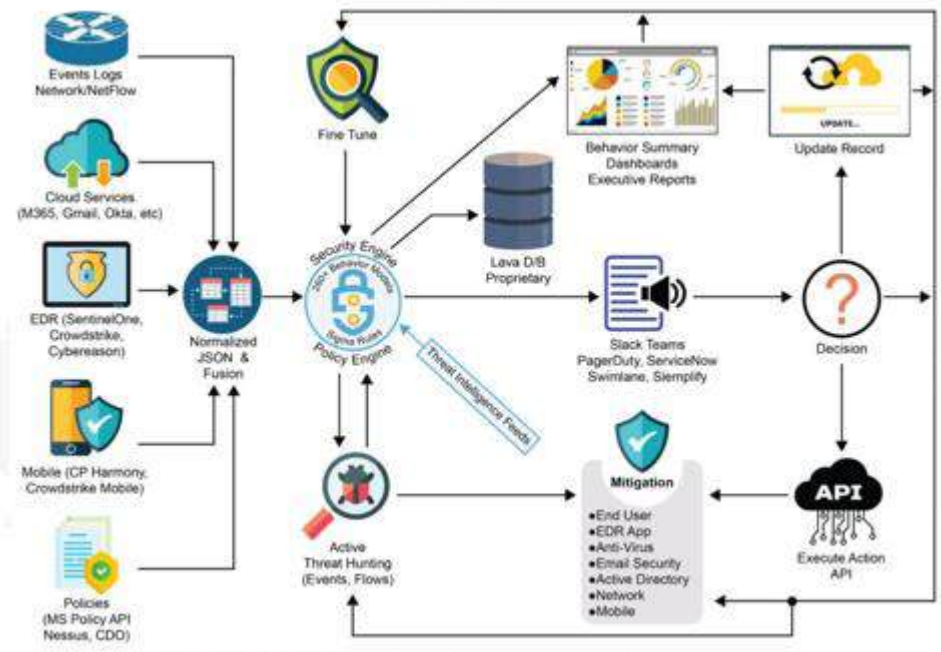
fusion, forensik, dan status keamanan. Proses ini mencakup pengumpulan, agregasi, penyaringan, penyimpanan, triase, dan korelasi data.

***Security Orchestration, Automation and Response* (SOAR)**

Platform SOAR mirip dengan SIEM karena mereka menggabungkan, menghubungkan, dan menganalisis alert. Selain itu, teknologi SOAR mengintegrasikan threat intelligent dan mengotomatiskan investigasi insiden dan alur kerja respons berdasarkan buku pedoman (playbooks) yang dikembangkan oleh tim keamanan.



Berikut adalah contoh Arsitektur *Security Orchestration, Automation and Response* (SOAR)



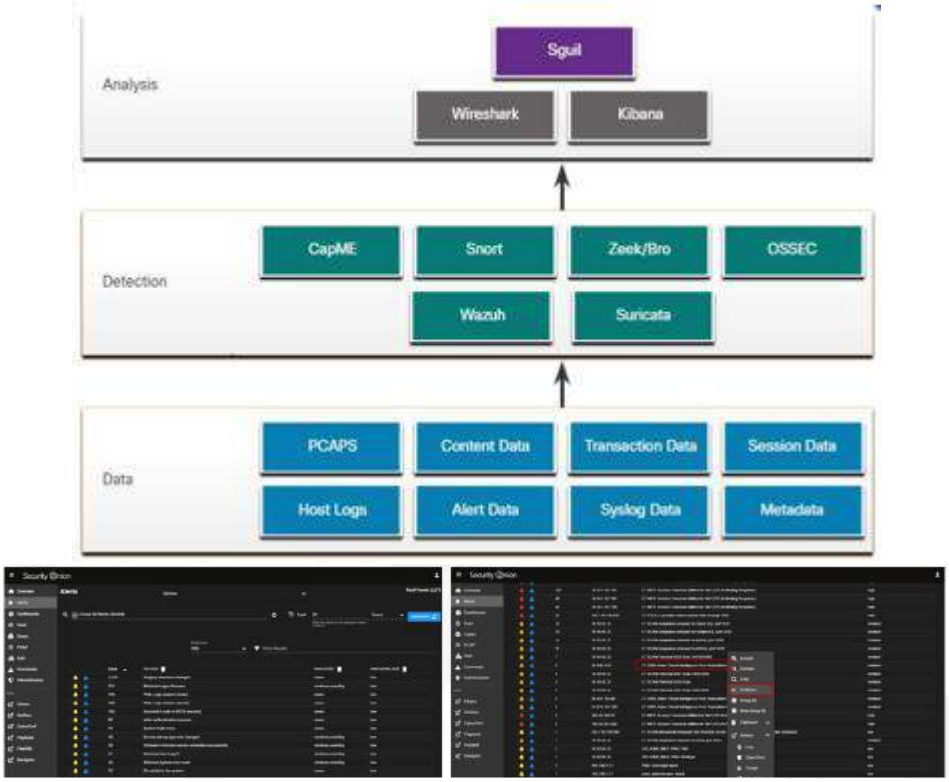
Source : https://ptp.cloud/soar-based-security-monitoring/

Gambar diatas dirancang untuk memantau, menganalisis, dan menangani ancaman dengan lebih cerdas dan otomatis. Sistem ini mengumpulkan data dari berbagai sumber, seperti aktivitas di cloud, perangkat mobile, atau ancaman yang sedang

aktif, lalu memprosesnya melalui inti sistem yang disebut Security Engine. Di sini, data disatukan dan disesuaikan agar lebih mudah dipahami, sekaligus diperbarui dengan informasi ancaman terbaru. Sistem ini juga punya fitur untuk menyempurnakan aturan keamanan, menyimpan data secara langsung, dan menampilkan hasil analisis dalam bentuk dashboard atau laporan yang mudah dibaca oleh tim. Untuk komunikasi dan kerja sama tim, ada alat seperti paging atau swimlane yang membantu menyederhanakan proses. Jika ada ancaman, sistem bisa langsung mengambil tindakan, misalnya melalui API, untuk memblokir atau menangani masalah, baik itu di level pengguna, web, direktori aktif, atau perangkat mobile. Intinya, sistem ini bekerja secara terpadu untuk mendeteksi dan menangani ancaman dengan cepat dan efisien.

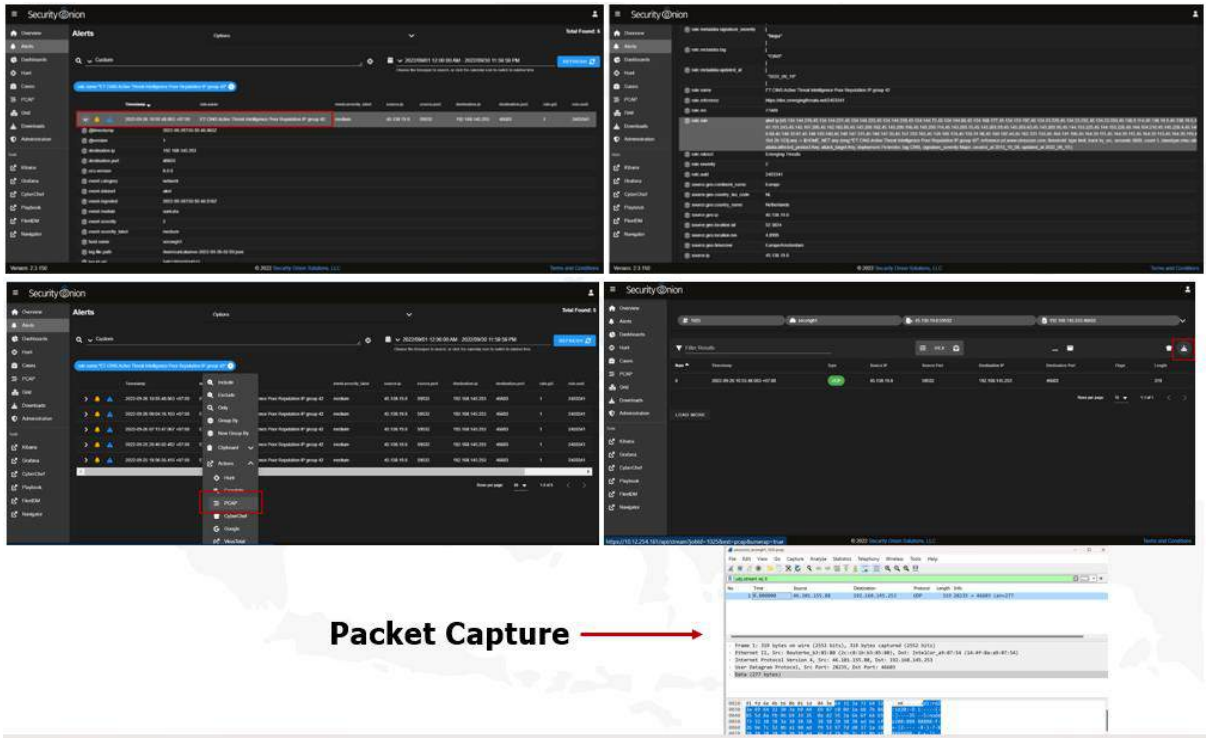
Contoh SIEM: Security Onion

Security Onion adalah rangkaian *tool* Pemantauan Keamanan Jaringan atau *Network Security Monitoring* (NSM) *open source* yang berjalan pada distribusi Linux Ubuntu



Dapat dilihat pada gambar sebelah kiri terdapat daftar peringatan yang muncul, misalnya ada aktivitas mencurigakan seperti ancaman yang terdeteksi dari alamat IP tertentu pada tanggal 23 Oktober 2023. Setiap peringatan ini menunjukkan informasi dasar seperti waktu kejadian, alamat IP yang terlibat, dan jenis ancaman yang ditemukan. sementara, pada gambar sebelah kanan terdapat tampilan yang lebih detail dari salah satu peringatan yang dipilih, menampilkan informasi lengkap seperti lokasi geografis (dalam hal ini Rusia), alamat IP sumber dan tujuan, serta data teknis seperti port yang digunakan dan protokolnya. Ada juga opsi untuk

mengambil tindakan, seperti menandai peringatan atau menyelami lebih dalam untuk analisis lebih lanjut.

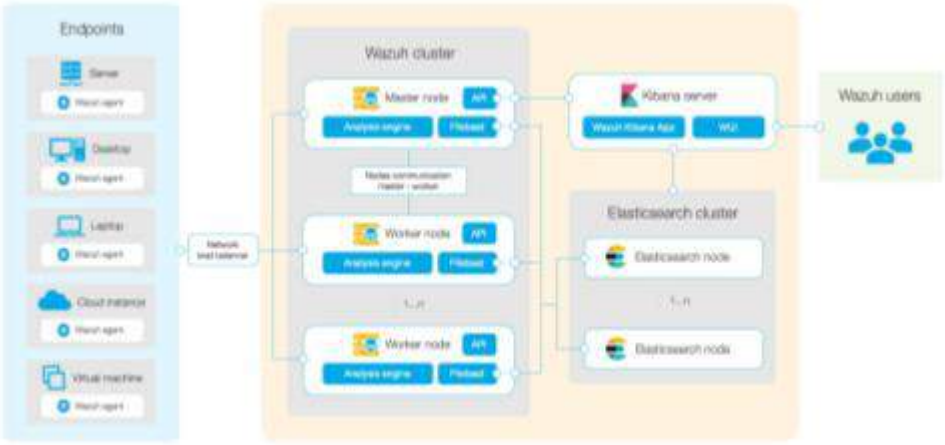


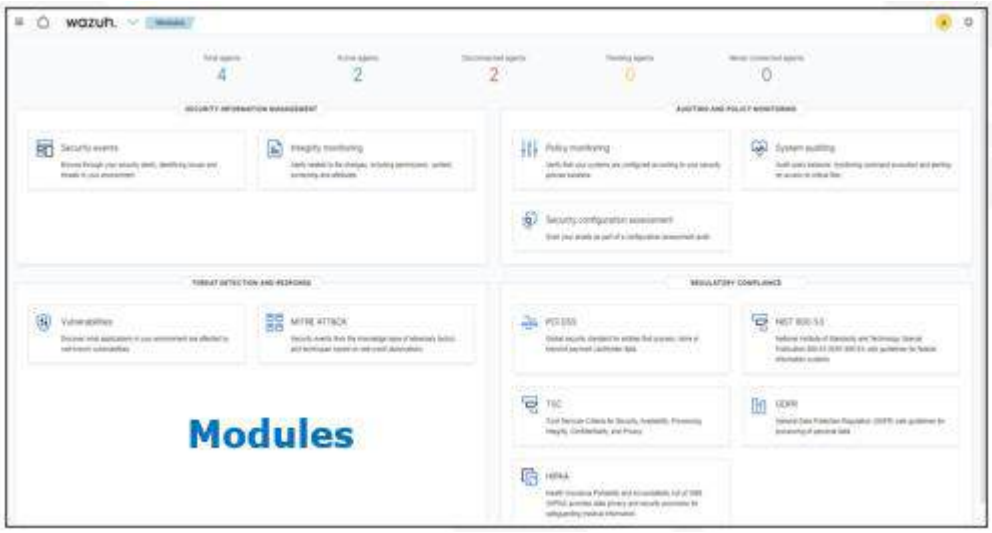
Contoh SIEM: Wazuh

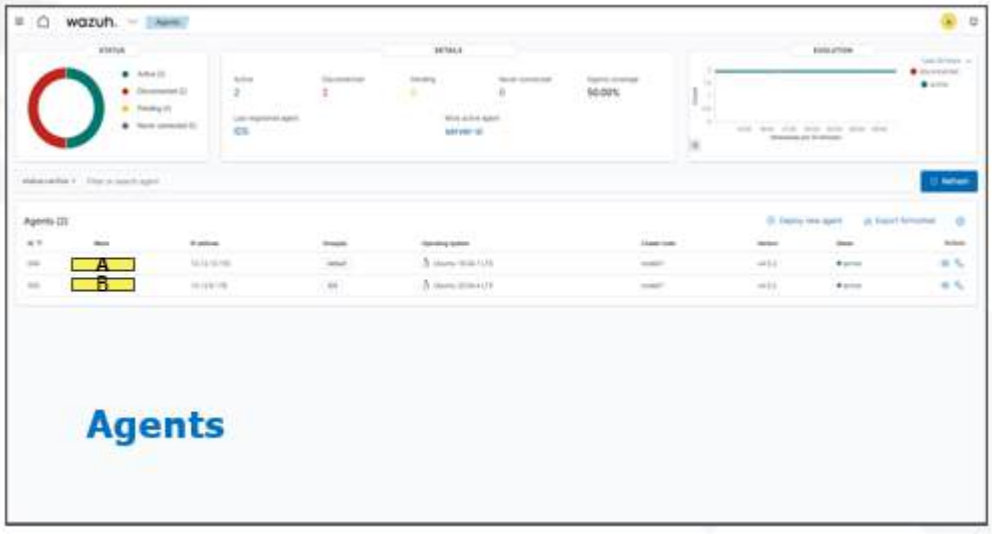
Wazuh adalah *platform open-source* yang dirancang untuk meningkatkan keamanan siber dan deteksi ancaman di berbagai Infrastruktur aset elektronik. Dapat memberikan audit *log* dan pelaporan yang terperinci untuk memenuhi persyaratan kepatuhan keamanan

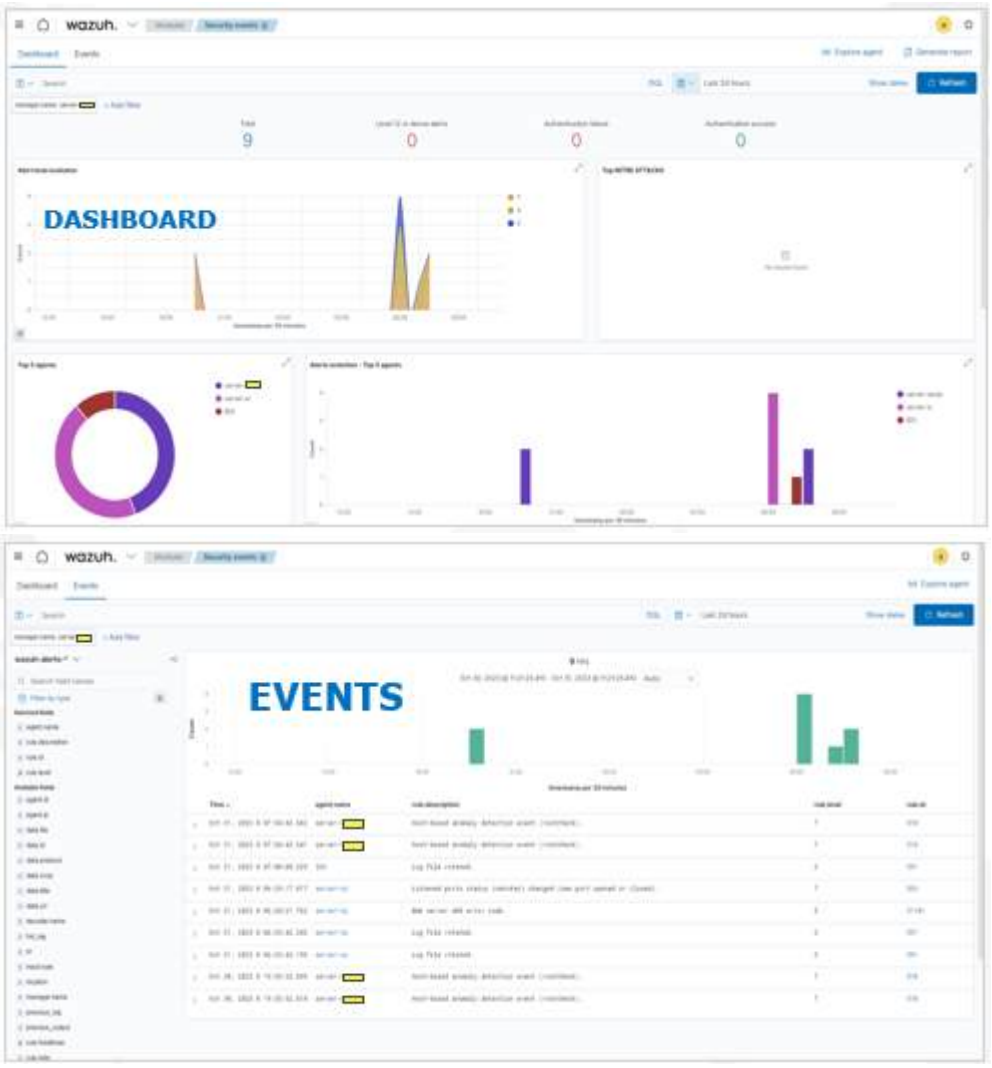
Wazuh memiliki komponen utama

1. *Log collection*
2. *Log analysis (customizable set of over 3000 HIDS rules)*
3. *File integrity monitoring*
4. *Host-based anomaly detection*
5. *Security compliance scanning for known vulnerabilities*
6. *Real time alerting (e-mail, SMS, Slack, etc)*
7. *Active response (a HIDS-driven IPS implementation)*

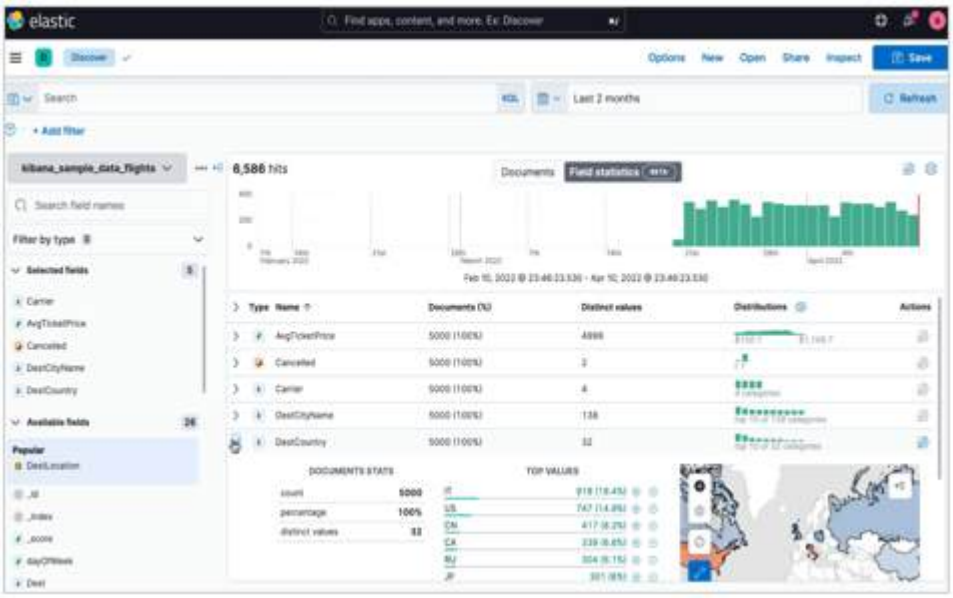

Endpoints
Wazuh cluster
Master node
API
Analysis engine
Filebeat
Kibana server
Wazuh users
Worker node
Elasticsearch cluster
Elasticsearch node


wazuh.
Security events
Integrity monitoring
Policy monitoring
System auditing
Security configuration assessment
Vulnerabilities
MITRE ATT&CK
PCI DSS
NIST 800-53
TSC
GDPR
HIPAA
Modules


wazuh.
A
B
Agents

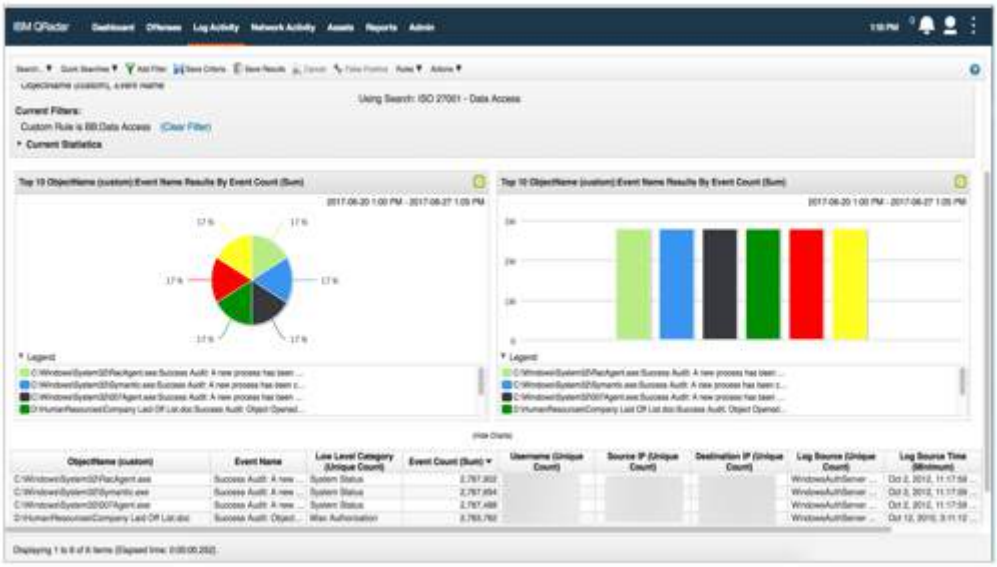


Contoh SIEM: ELS stack



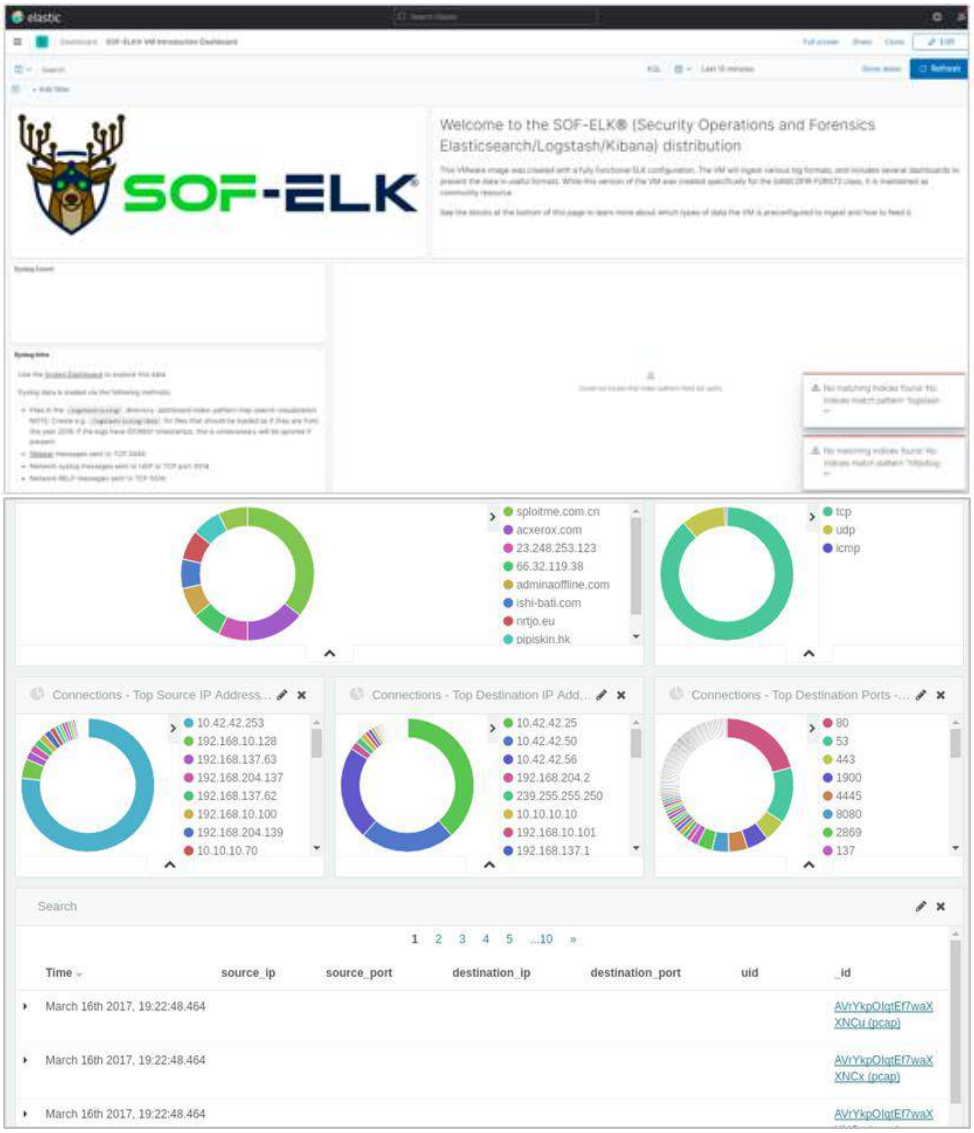
Contoh SIEM: Splunk

Contoh SIEM: IBM Security Qradar



Contoh SIEM: Logrythm

SOF-ELK



Anomali Trafik

Pola atau perubahan yang tidak biasa (*abnormal activity*) dan signifikan dalam traffic jaringan. *Anomaly traffic* ini termasuk kondisi dimana *traffic* 'secara statistik' lebih besar daripada yang diharapkan, hingga adanya aktivitas/perubahan sah (*legitimate*) ataupun aktivitas/perubahan yang tidak sah (*illegitimate*) pada jaringan.

Contoh aktivitas sah yang dimaksud adalah adanya aktivitas pengubahan data dan lonjakan pengaksesan yang masih dalam batas wajar, sedangkan aktivitas tidak sah yang dimaksud adalah adanya aktivitas lonjakan pengaksesan yang sangat masif (DDoS), pemindaian port, *virus, worm*, dll.

Evaluasi Alert

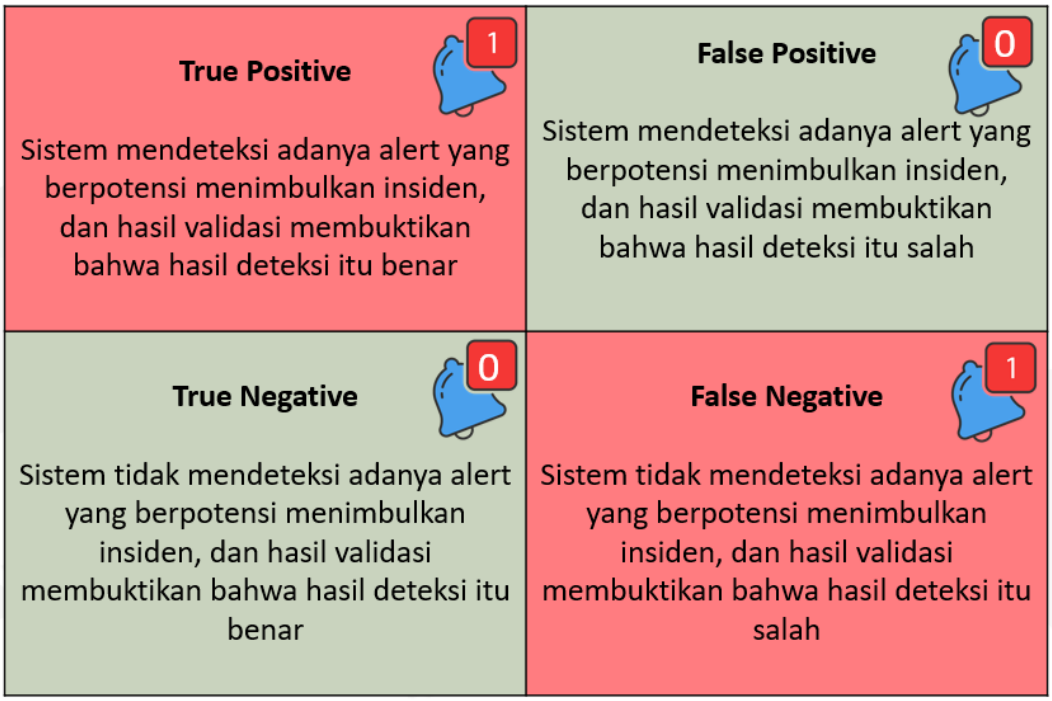
True dan False

Justifikasi berdasarkan hasil validasi alert yang terdeteksi.

True : Hasil deteksi sistem benar

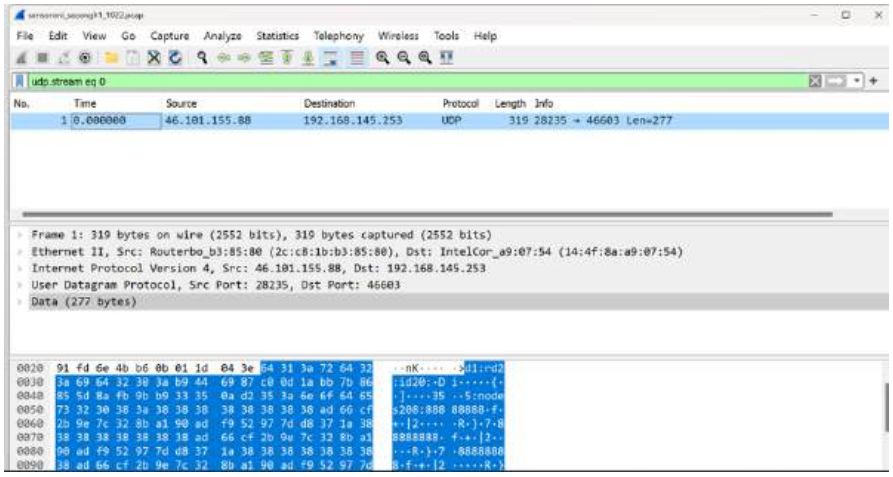
False : Hasil deteksi sistem salah

Positive dan Negative
Hasil deteksi sistem
Positive : Sistem mendeteksi adanya alert yang berpotensi menimbulkan insiden
Negative : Sistem tidak mendeteksi adanya alert yang berpotensi menimbulkan insiden

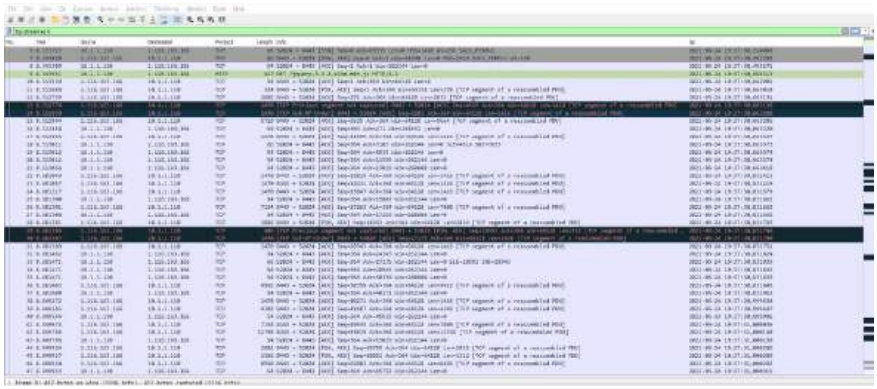


C. Analisis Aktivitas Siber Yang Teridentifikasi

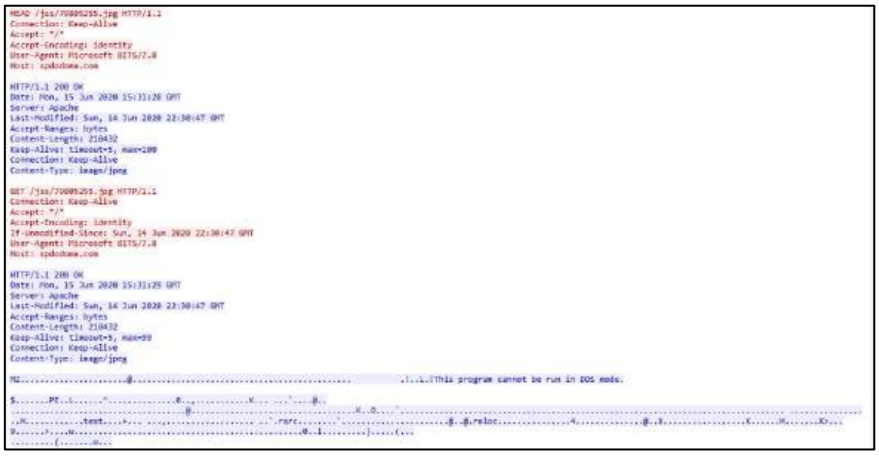
Network Traffic Analysis (Wireshark)



Contoh PCAP Analysis #1



Contoh PCAP Analysis #2



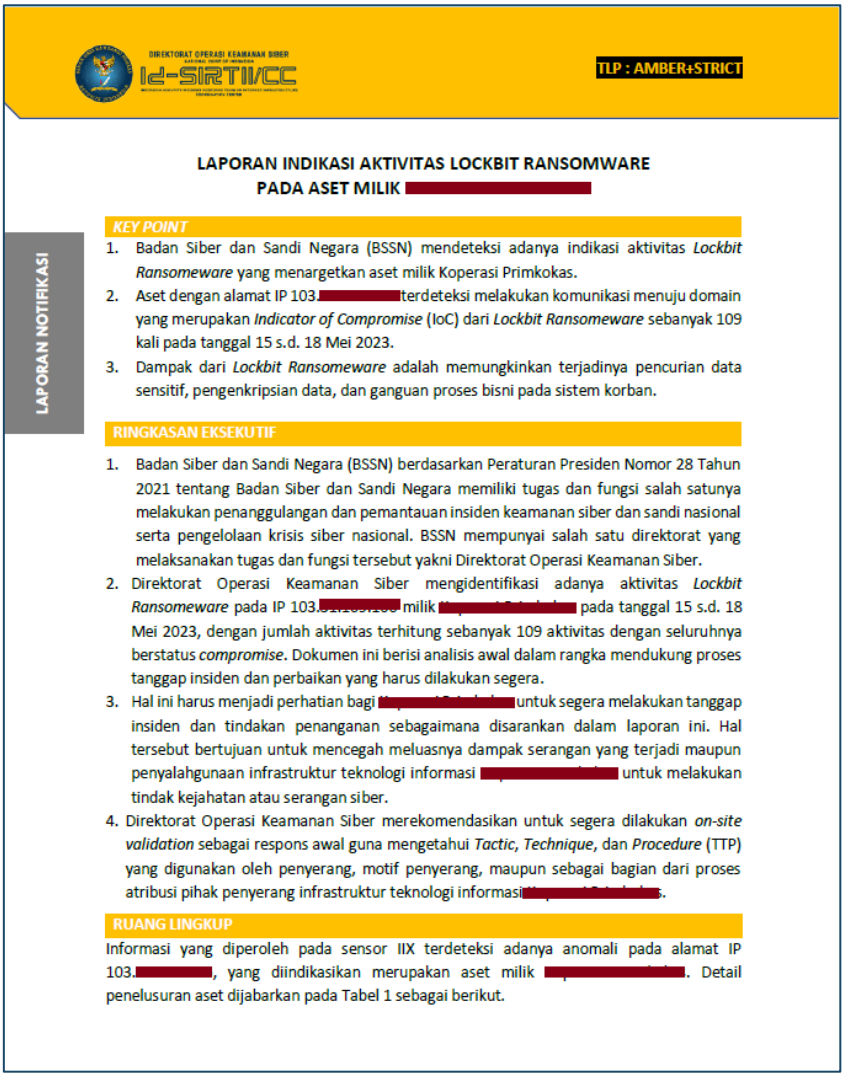
Platform Analisis Sumber Terbuka

Beberapa Platform Sumber terbuka yang dapat dimanfaatkan untuk melakukan analisis anomali keamanan siber yang terdapat pada Log.

1. Anyrun
   Platform berbasis cloud untuk analisis *Malware* secara interaktif, memungkinkan pengguna mengamati perilaku file atau URL dalam lingkungan sandbox.
2. Cuckoo
   Sandbox open-source yang dapat digunakan untuk menganalisis *Malware* dengan menjalankan file mencurigakan dalam lingkungan terisolasi dan mencatat aktivitasnya.
3. Virustotal
   Layanan online yang memungkinkan analisis file, URL, IP, dan domain menggunakan berbagai mesin antivirus serta sumber intelijen ancaman.
4. OTX Alientvault
   Platform berbagi intelijen ancaman (Threat Intelligence) yang menyediakan informasi tentang serangan siber, indikator kompromi (IOC), dan data ancaman global.
5. AbuseIPDB
   Database sumber terbuka yang menyimpan laporan tentang alamat IP berbahaya, berguna untuk mendeteksi dan memblokir ancaman berbasis IP.
6. Shodan
   Mesin pencari perangkat yang terhubung ke internet, berguna untuk mengidentifikasi layanan yang terbuka, kelemahan keamanan, serta ancaman potensial dalam jaringan.

Dokumentasi Temuan

Temuan anomali harus didokumentasikan berupa serangan, Timestamp, dan Bukti Evidence



DIREKTORAT OPERASI KEAMANAN SIBER
id-SIRTI/CC

TLP : AMBER+STRICT

LAPORAN NOTIFIKASI

LAPORAN INDIKASI AKTIVITAS LOCKBIT RANSOMWARE
PADA ASET MILIK [redacted]

KEY POINT

1. Badan Siber dan Sandi Negara (BSSN) mendeteksi adanya indikasi aktivitas *Lockbit Ransomeware* yang menargetkan aset milik Koperasi Primkokas.
2. Aset dengan alamat IP 103.[redacted] terdeteksi melakukan komunikasi menuju domain yang merupakan *Indicator of Compromise* (IoC) dari *Lockbit Ransomeware* sebanyak 109 kali pada tanggal 15 s.d. 18 Mei 2023.
3. Dampak dari *Lockbit Ransomeware* adalah memungkinkan terjadinya pencurian data sensitif, pengenkripsian data, dan ganguan proses bisni pada sistem korban.

RINGKASAN EKSEKUTIF

1. Badan Siber dan Sandi Negara (BSSN) berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara memiliki tugas dan fungsi salah satunya melakukan penanggulangan dan pemantauan insiden keamanan siber dan sandi nasional serta pengelolaan krisis siber nasional. BSSN mempunyai salah satu direktorat yang melaksanakan tugas dan fungsi tersebut yakni Direktorat Operasi Keamanan Siber.
2. Direktorat Operasi Keamanan Siber mengidentifikasi adanya aktivitas *Lockbit Ransomeware* pada IP 103.[redacted] milik [redacted] pada tanggal 15 s.d. 18 Mei 2023, dengan jumlah aktivitas terhitung sebanyak 109 aktivitas dengan seluruhnya berstatus *compromise*. Dokumen ini berisi analisis awal dalam rangka mendukung proses tanggap insiden dan perbaikan yang harus dilakukan segera.
3. Hal ini harus menjadi perhatian bagi [redacted] untuk segera melakukan tanggap insiden dan tindakan penanganan sebagaimana disarankan dalam laporan ini. Hal tersebut bertujuan untuk mencegah meluasnya dampak serangan yang terjadi maupun penyalahgunaan infrastruktur teknologi informasi [redacted] untuk melakukan tindak kejahatan atau serangan siber.
4. Direktorat Operasi Keamanan Siber merekomendasikan untuk segera dilakukan *on-site validation* sebagai respons awal guna mengetahui *Tactic, Technique*, dan *Procedure* (TTP) yang digunakan oleh penyerang, motif penyerang, maupun sebagai bagian dari proses atribusi pihak penyerang infrastruktur teknologi informasi [redacted].

RUANG LINGKUP

Informasi yang diperoleh pada sensor IIX terdeteksi adanya anomali pada alamat IP 103.[redacted], yang diindikasikan merupakan aset milik [redacted]. Detail penelusuran aset dijabarkan pada Tabel 1 sebagai berikut.

Timestamp	Klasifikasi	Threat Name	Victim IP	Jumlah
2023-05-15 08:43:57	Malware	Lockbit Ransomeware Ransomware activity	103.3[redacted]	1
2023-05-15 12:55:05	Malware	Lockbit Ransomeware Ransomware activity	103.3[redacted]	1
2023-05-15 17:02:25	Malware	Lockbit Ransomeware Ransomware activity	103.3[redacted]	1
...	..	..	..	..
2023-05-18 22:03:13	Malware	Lockbit Ransomeware Ransomware activity	103.3[redacted]	1
Jumlah				48

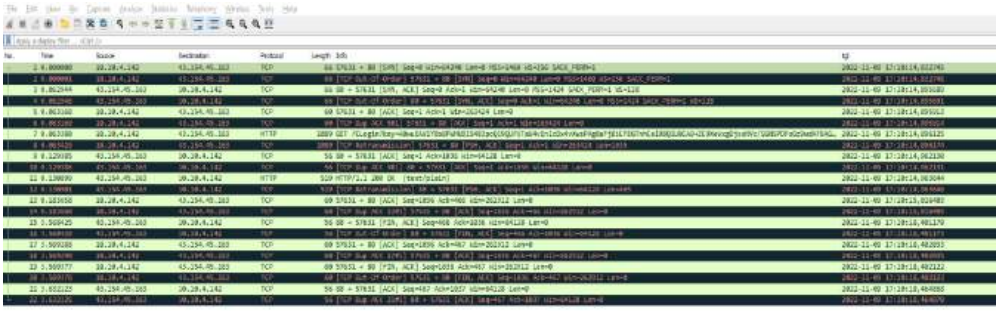
1. Monitoring Aset (Contoh)
   a. Deteksi Alert terkait Trojan.LingyunNet.A

Count	rule.name
3,383	ET MALWARE Win32/LingyunNet.A Heartbeat
1,505	ET MALWARE Win32/LingyunNet.A Heartbeat Response
94	ET MALWARE Win32/LingyunNet.A CnC Checkin

   b. Didapatkan informasi nama *Malware*, *source* IP, *destination* IP, dan arah komunikasi

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2022-11-10 12:27:56.715 +08:00	ET MALWARE Win32/LingyunNet.A Heartbeat	high	10.10.4.142	55171	43.128.75.78	801
2022-11-09 15:55:11.685 +08:00	ET MALWARE Win32/LingyunNet.A Heartbeat	high	10.10.8.71	59740	43.128.75.78	801
2022-11-10 12:27:49.816 +08:00	ET MALWARE Win32/LingyunNet.A Heartbeat	high	10.10.4.142	53877	43.154.154.166	916
2022-11-10 11:05:25.392 +08:00	ET MALWARE Win32/LingyunNet.A Heartbeat Response	high	43.128.75.78	801	10.10.4.142	55171
2022-11-10 12:19:48.399 +08:00	ET MALWARE Win32/LingyunNet.A CnC Checkin	high	10.10.4.142	49195	43.154.45.163	80

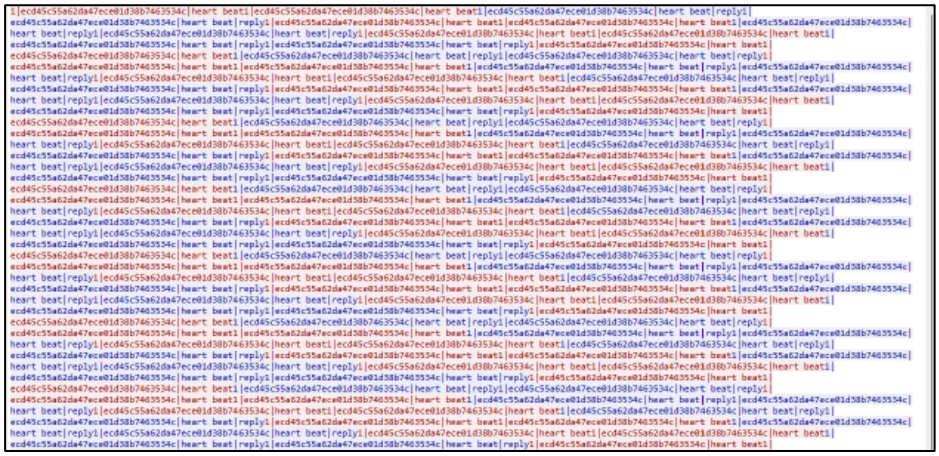
   c. Menganalisis komunikasi pada PCAP



Didapatkan informasi:

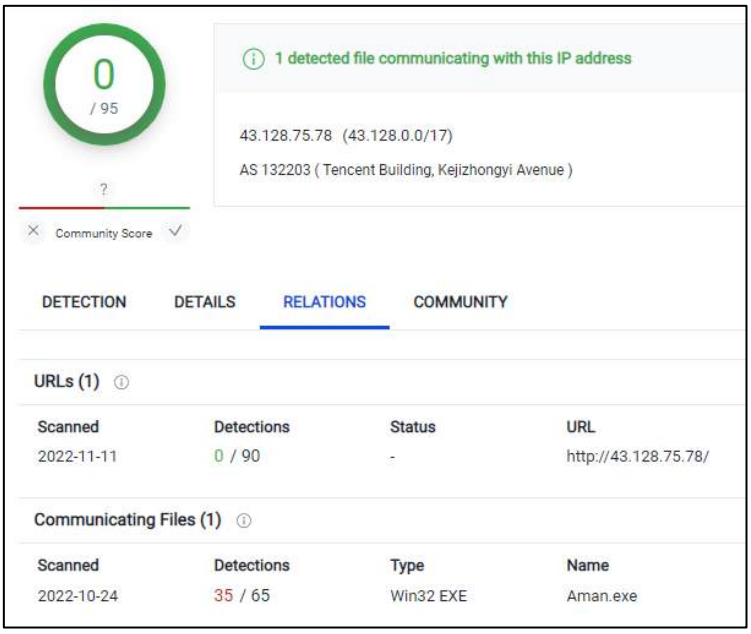
Rincian Komunikasi IP 10.10.4.142 dengan IP 43.154.154.163 (domain zcky.na.lb[.]holadns[.]com)

Response Komunikasi dari IP 43.128.75.78



d. Melakukan pengayaan informasi melalui pemeriksaan IoC

No	IOC	VirusTotal	OTX AlientVault
1	43.154.45.163	Clean (0/95) Komunikasi dengan 27 *File Malware*	Tidak terdapat pulse
2	43.154.154.166	Malware (1/95) Komunikasi dengan 78 *File Malware*	Memiliki asosiasi dengan 3 file. berdasarkan deteksi Msdefender 1 file diantaranya adalah Trojan:Win32/Zombie.A
3	43.128.75.78	Clean (0/95) Komunikasi dengan malware PUA Win32/LingyunNet.A	Tidak terdapat pulses
4	zcky.na.lb.holadns.com	Clean (0/95) Komunikasi dengan 16 *File Malware*	Tidak terdapat pulses
5	zcky.na.lb.martianinc.co	Clean (0/95) Komunikasi dengan 19 *File Malware*	Tidak terdapat pulses
6	bf5e4ebee61392c6e5d28b543e5373f8	Malware (37/70) antivirus ESET-NOD32 merupakan malware PUA Win32/LingyunNet.A	Tidak Terdapat pulses



Terlihat hasil 0 dari 95 vendor *security* mendeteksi aktivitas *malicious*.

Terdeteksi 1 file (Aman.exe) yang berkomunikasi dengan IP 43.128.75.78 dengan reputasi 35 dari 65 vendor *security* mendeteksi aktivitas *malicious*.

Reputasi file Aman.exe pada VirusTotal, menunjukkan 6 URL yang dideteksi pernah berkomunikasi dengan file tersebut, salah satunya adalah sebagai berikut:

http://zcky.na.lb.holadns.com/CLogin?
key=ARx/EwZzM006YGFC0I97BH0lQw9VBwpFOh9/FX5aDBstD1oMAQYJQTl/CgdST3tBfwt9E1BjV1ktNX9Qfl1kUishZFA/cCwEOkJmAGhcdF94
HHEJemMwXjoxfxx6Y38LKQh4HStwLE4qUURdaAVwA38MXA17Xj9HLjJGPlZgAAoGVlEfLHAGUzFvBgRrbnhFVQtfHm5nL0EqC3gRU2BZCi0PW
gwrczQFLmx%20Q3xMc0h7ln4TeV4nSC4yfxF6XXQYKSF8EiheJE0ufHpDfFxzS3siehN5XidLLiV/FX5aBA0GNnxTLF4NfCp8cXp4cl1beiV5DW1jU
1kHVFoNU3BSCCsPdBYsWVRcOkF6AnhcdwB5DFcOe14KWiwMc1Z4XXslKw94USxdEl0HVWVNUgReRFQPelJ9WhZYAlVaEW5NWlEoD2QQKE
0sRypWfUNobnheezV6Un1fLHYsl2wiemJ4USgxeBwrcTxALmx1cmBPA3BnDGJVeGABSC0cbCN6c2MlKg5gVypnJFM7cHlXUI97QX8lfRNtbCxe
Lg9/UH5efBltC3sSPGwvWC5BegJ4WmR3YyV6F31aKEU6PnwKeXR8Vy0MfBYsWitDOmB5WH9lewR/C3UQbWNTCgUifxN6TgFQKA90UChwAQ
wFfGlHfnJjB2wielRtTjMGOgxwC3lNdwwqMmMJPGMsTi5seV58W39KeCJ6Hn1aVg9YX1pdXlBRWFBYX1tdWFhQCAolWlslXFpfWQ==