STMIK ELRAHMA YOGYAKARTA

SEMINAR KERJA PRAKTEK

ANALISIS PENGUJIAN HOST INTRUSION DETECTION SYSTEM PADA INFRASTRUKTUR AMAZON WEB SERVICE

MENGGUNAKAN WAZUH

@maszett

ngesec
lab & ngerumpi security

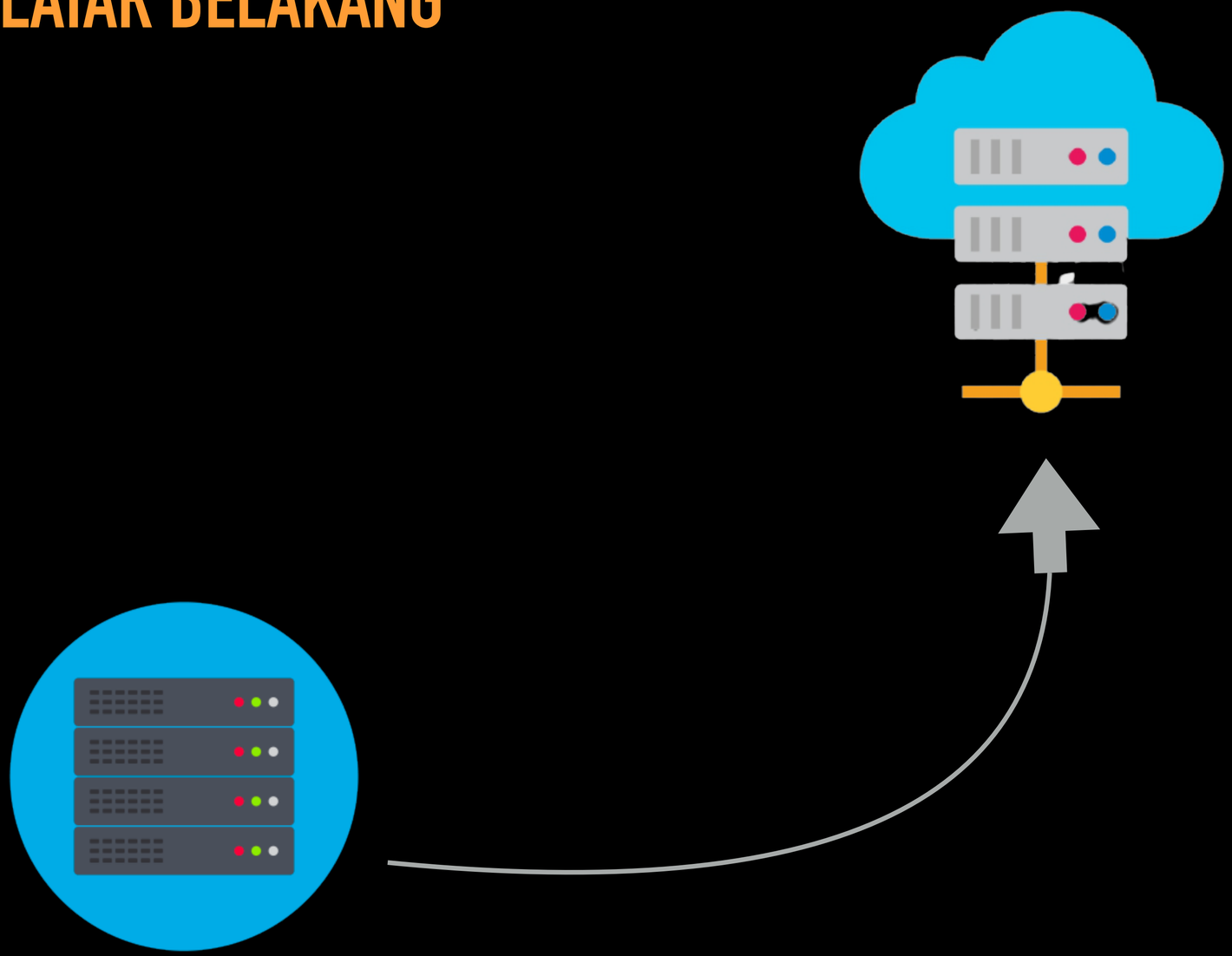
WHO AM I

- Mukhammad Khabiburrohman
- Cyber Security Enthusiast | OSCP | CEH | CND
- Nomor Mahasiswa : 12181649
- Prodi : Teknik Informatika
- Jenjang : Strata 1 (S1)

BAB 1 PENDAHULUAN

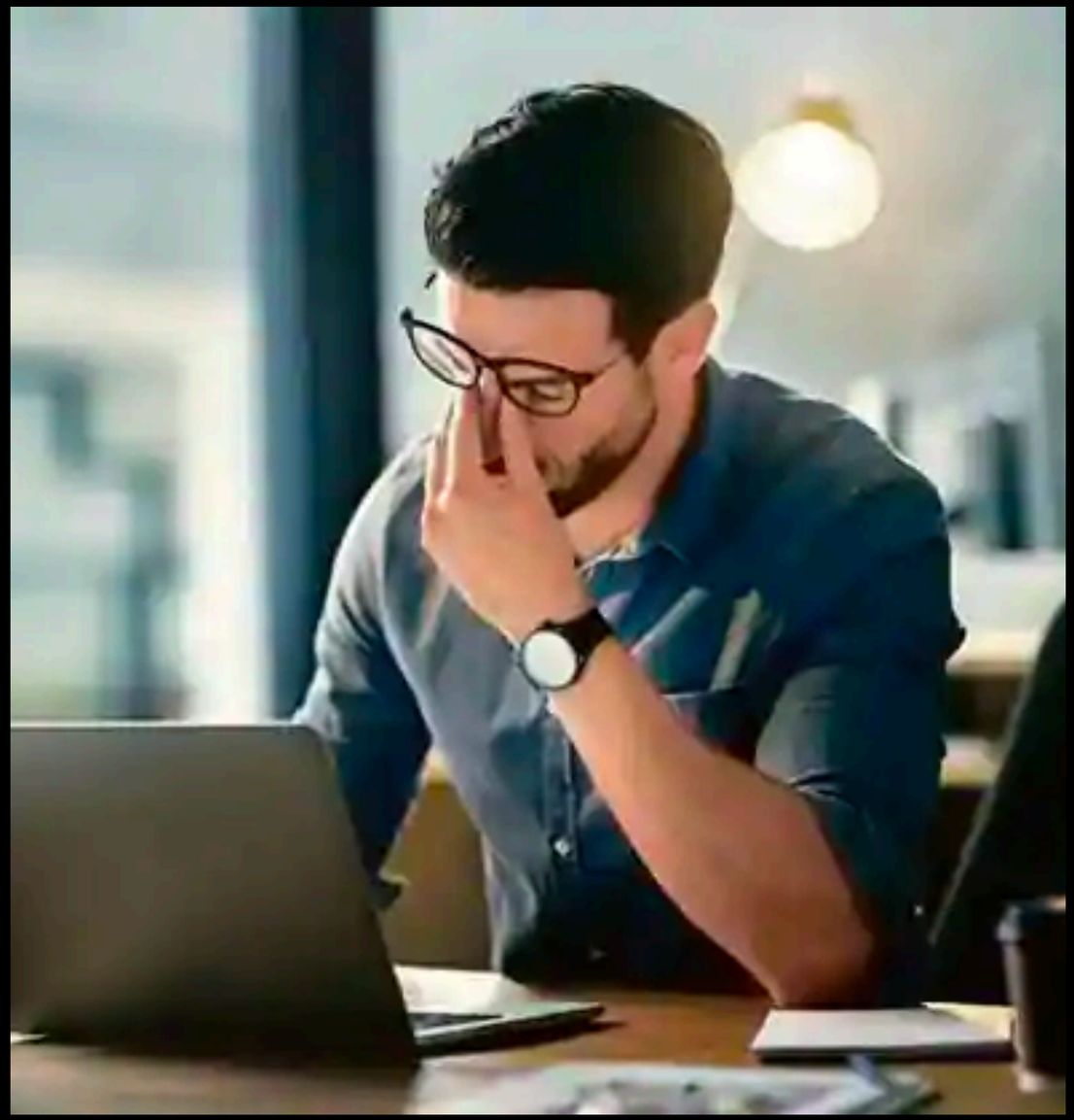
- Latar belakang
- Rumusan masalah
- Batasan masalah
- Tujuan & manfaat penelitian
- Metode penelitian

LATAR BELAKANG



RUMUSAN MASALAH

- Proses deteksi serangan masih manual
- Statistik threat incident yang tidak reliable
- Tidak ada security monitoring terpusat



HOW TO SOLVE THIS?

Me

BATASAN MASALAH

PEMBAHASAN INI HANYA MENCAKUP ANALISIS PENGUJIAN SERANGAN YANG DITEKEKSI OLEH HOST INTRUSION DETECTION SYSTEM WAZUH PADA INSTANCE EC2 YANG TERINSTALL APLIKASI YANG RENTAN KEMANAN, PADA SERVICE EC2 DAN IAM.

BAB 2 TINJAUAN PUSTAKA

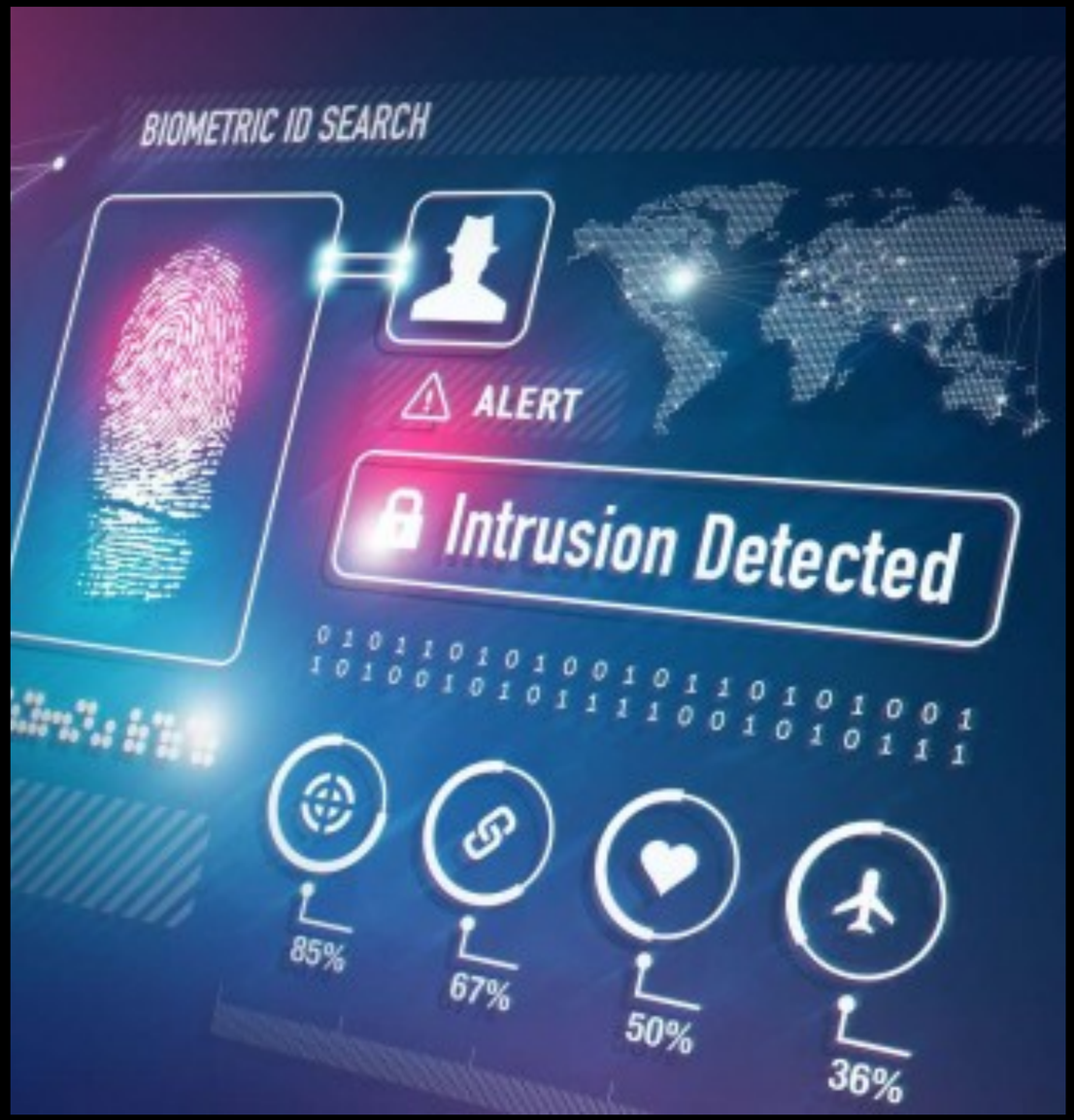
No	Nama, Tahun	Judul	Persamaan dan Perbedaan
1	Abdul Aziz, Arry Budi Kurnia (2015)	Monitoring Serangan Pada Jaringan Komputer Menggunakan SNORT berbasis SMS Gateway	Menggunakan NIDS Snort, menggunakan Gammu sebagai SMS Gateway
2	Thera Frista Dewi Karina Bulan (2017)	Sistem Monitoring Keamanan Jaringan Menggunakan Snort Dan SMS Alert Pada Jaringan LAB SMK Telekomunikasi Tunas Harapan	Menggunakan NIDS Snort, menggunakan Gammu sebagai SMS Gateway
3	Nizar Akbar Meilani(2018)	Analisis Pengujian Host Intrusion Detection System Wazuh	Menggunakan HIDS Wazuh, menggunakan ModSecurity dan PSAD
4	Eka Stephani Sinambela (2020)	Evaluasi Performansi Deteksi Serangan Pada HIDS OSSEC	Menggunakan HIDS OSSEC
5	Roni Reza Abdullah, Ade Nurhayati (2019)	Monitoring Sistem Keamanan Jaringan Berbasis Telegram Bot Pada Local Area Network	Menggunakan NIDS Snort, menggunakan Bot Telegram
6	Mukhammad Khabiburrohman (2021)	Analisis Pengujian Host Intrusion Detection System Pada Infrastruktur Amazon Web Service Menggunakan Wazuh	Menggunakan HIDS Wazuh, menggunakan Amazon GuardDuty dan CloudTrail

BAB 3 LANDASAN TEORI

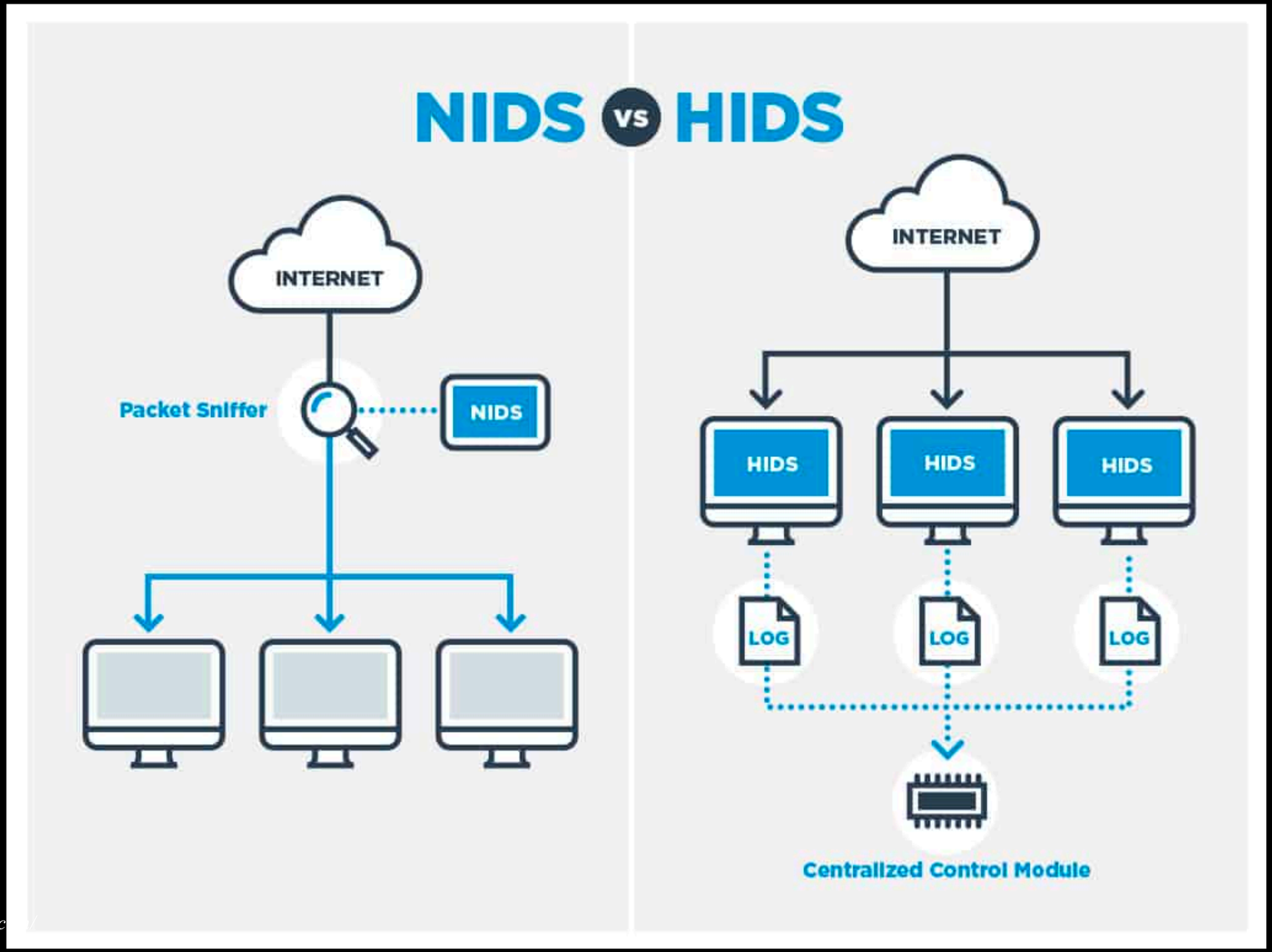
- Intrusion Detection System (IDS)
  - NIDS
  - HIDS
- Wazuh
  - Komponen Wazuh
  - Pengumpulan Data Log pada Wazuh
  - Analisis
- Amazon Web Service (AWS)

INTRUSION DETECTION SYSTEM (IDS)

- Intrusion Detection System atau IDS adalah perangkat (atau aplikasi) yang memonitor jaringan dan / atau sistem untuk kegiatan berbahaya atau pelanggaran kebijakan dan memberikan laporan ke administrator atau station manajemen jaringan.
- Tipe IDS
  - HIDS (Host Intrusion Detection System)
  - NIDS (Network Intrusion Detection System)



Source : https://lms.onnocenter.or.id



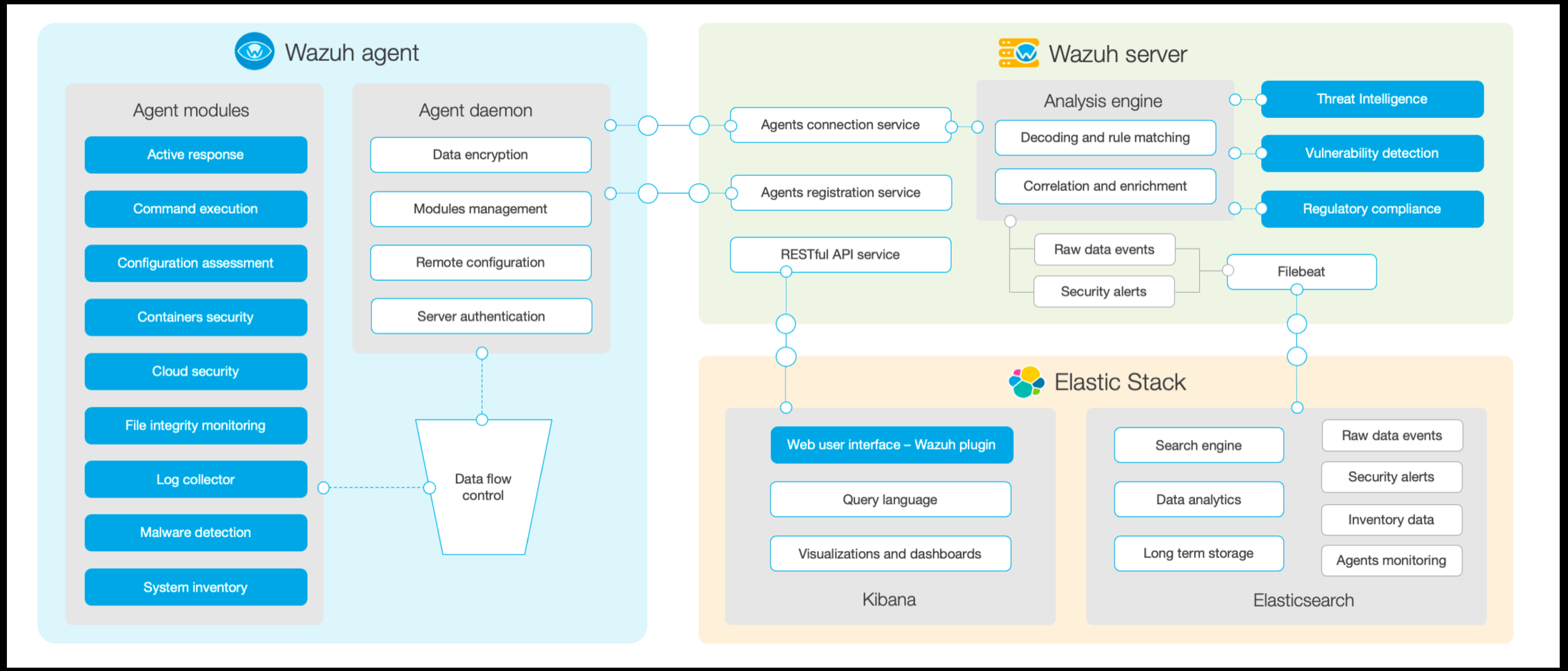
Source : https://www.google.c

WAZUH

- Wazuh merupakan perangkat berbasis Open Source yang berfungsi sebaga sistem deteksi intrusi berbasis host (endpoint). Wazuh melakukan analisis log, pemeriksaan integritas, pemantauan registri windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif.
- Wazuh merupakan perangkat yang menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau host pada sistem operasi dan juga pada tingkat aplikasi.

Source : https://govcsirt.bssn.go.id

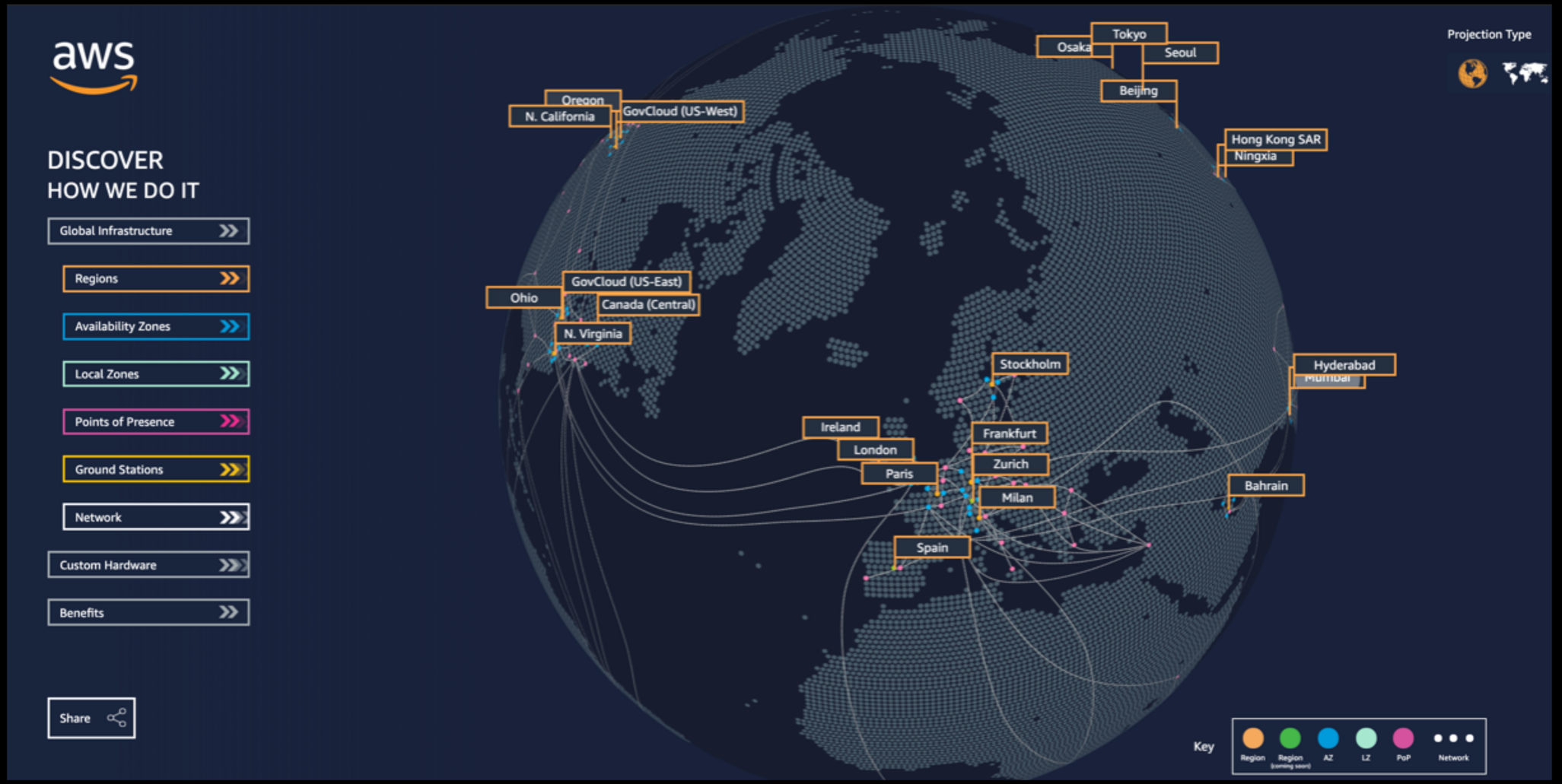
KOMPONEN WAZUH



AMAZON WEB SERVICE (AWS)

- Amazon Web Services (AWS) adalah platform cloud yang komprehensif dan digunakan secara luas di dunia, menawarkan lebih dari 500 layanan dan fitur unggulan yang lengkap dari pusat data secara global.
- Jutaan pengguna termasuk beberapa startup dengan pertumbuhan yang cepat, perusahaan besar, dan lembaga pemerintah menggunakan AWS untuk memangkas biaya, menjadi lebih sigap, dan inovasi lebih cepat.

INFRASTRUKTUR AWS



AMAZON GUARDDUTY

- Amazon GuardDuty merupakan layanan deteksi ancaman yang secara berkelanjutan memantau aktivitas mencurigakan dan perilaku tidak sah untuk melindungi akun AWS, beban kerja, dan data pengguna yang tersimpan di Amazon S3.
- Dengan GuardDuty, kini pengguna memiliki opsi cerdas dan hemat biaya untuk deteksi ancaman yang berkelanjutan di AWS. Layanan ini menggunakan machine learning, anomaly detection, dan inteligensi ancaman yang terintegrasi untuk mengidentifikasi dan memprioritaskan potensi ancaman.

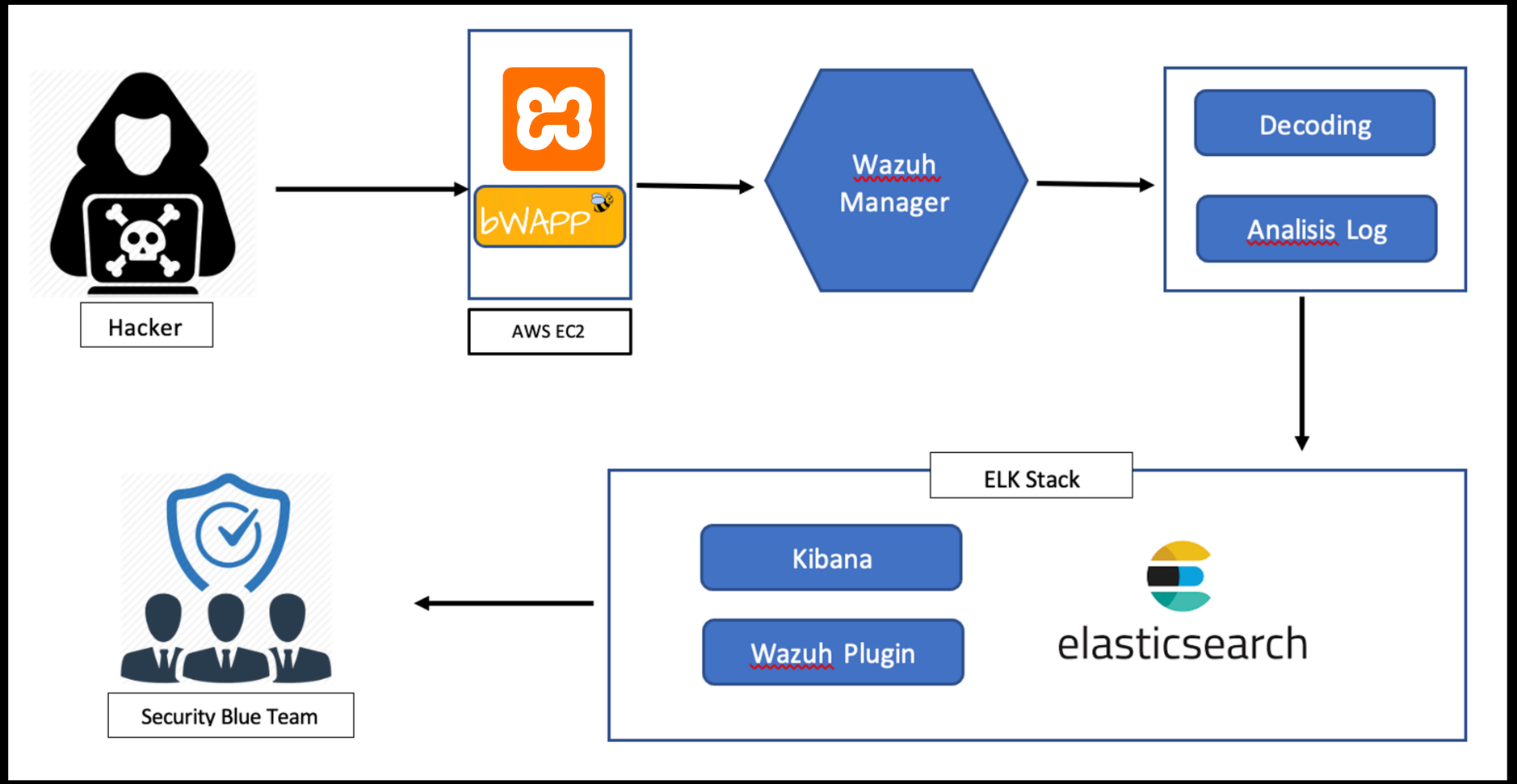
AWS CLOUDTRAIL

- AWS CloudTrail adalah layanan yang memungkinkan tata kelola, kepatuhan, audit operasional, dan audit risiko akun AWS. Dengan CloudTrail, pengguna dapat masuk, terus memantau, dan menyimpan aktivitas akun yang terkait dengan tindakan di seluruh infrastruktur AWS.

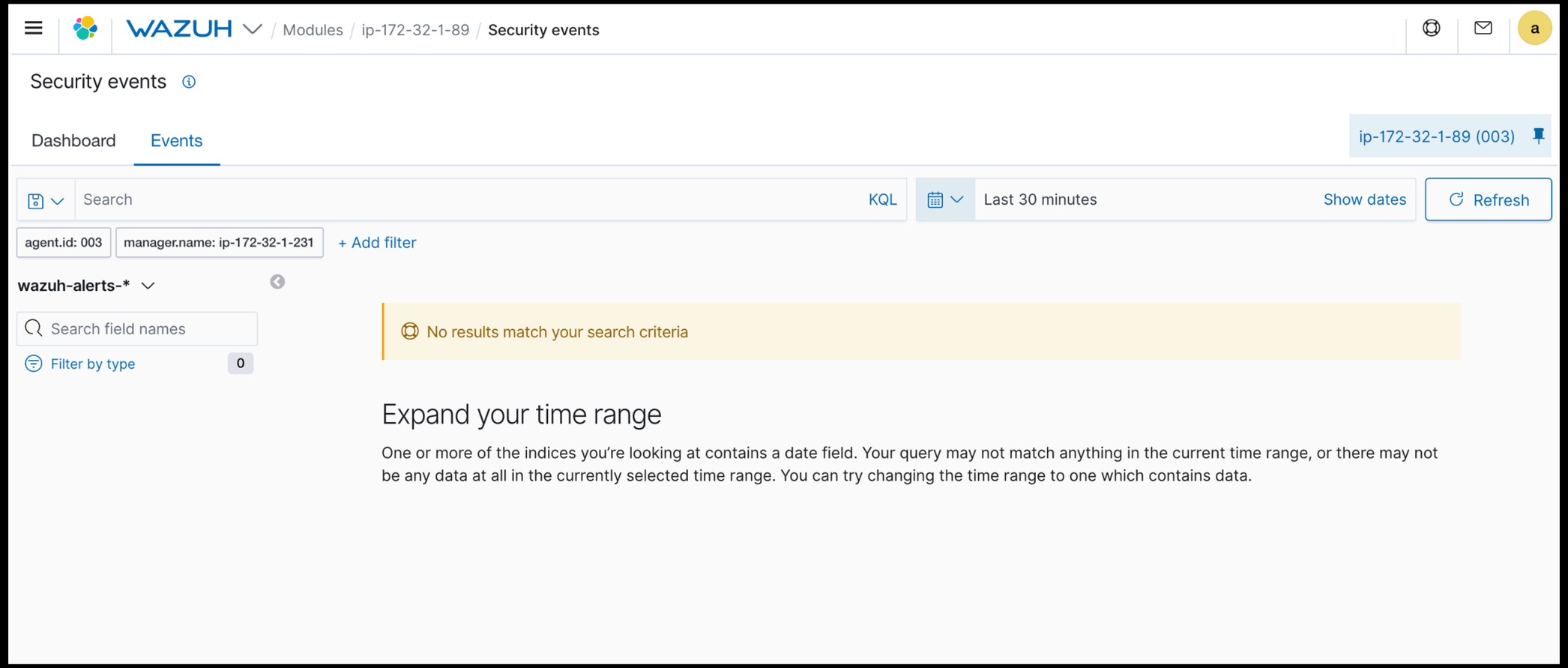
BAB 4 PEMBAHASAN PENGUJIAN HIDS WAZUH

- Pengujian HIDS Wazuh Pada Instance EC2 AWS
  - Pengumpulan informasi dengan nmap
  - Web scanning menggunakan Nikto
  - Pengujian serangan Pada bWAPP
- Pengujian HIDS Wazuh Pada Service AWS
  - Pengumpulan informasi dengan nmap
  - Pengujian terhadap service EC2 AWS
  - Pengujian terhadap service IAM

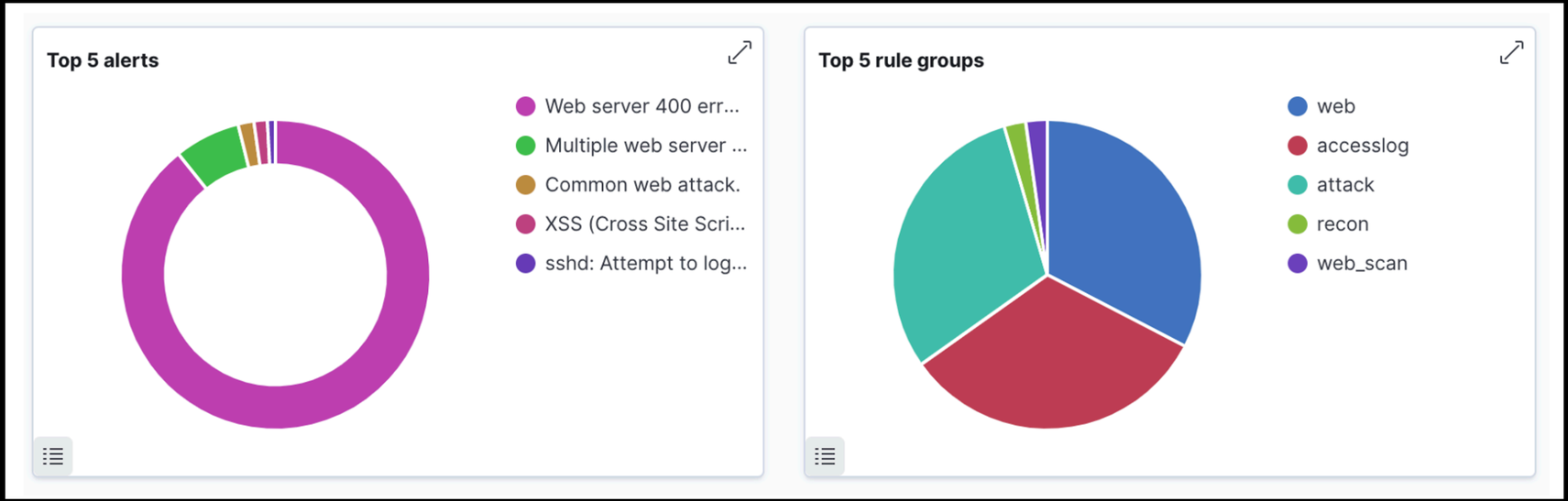
SKEMA PENGUJIAN HIDS WAZUH PADA INSTANCE EC2 AWS



PENGUMPULAN INFORMASI DENGAN NMAP



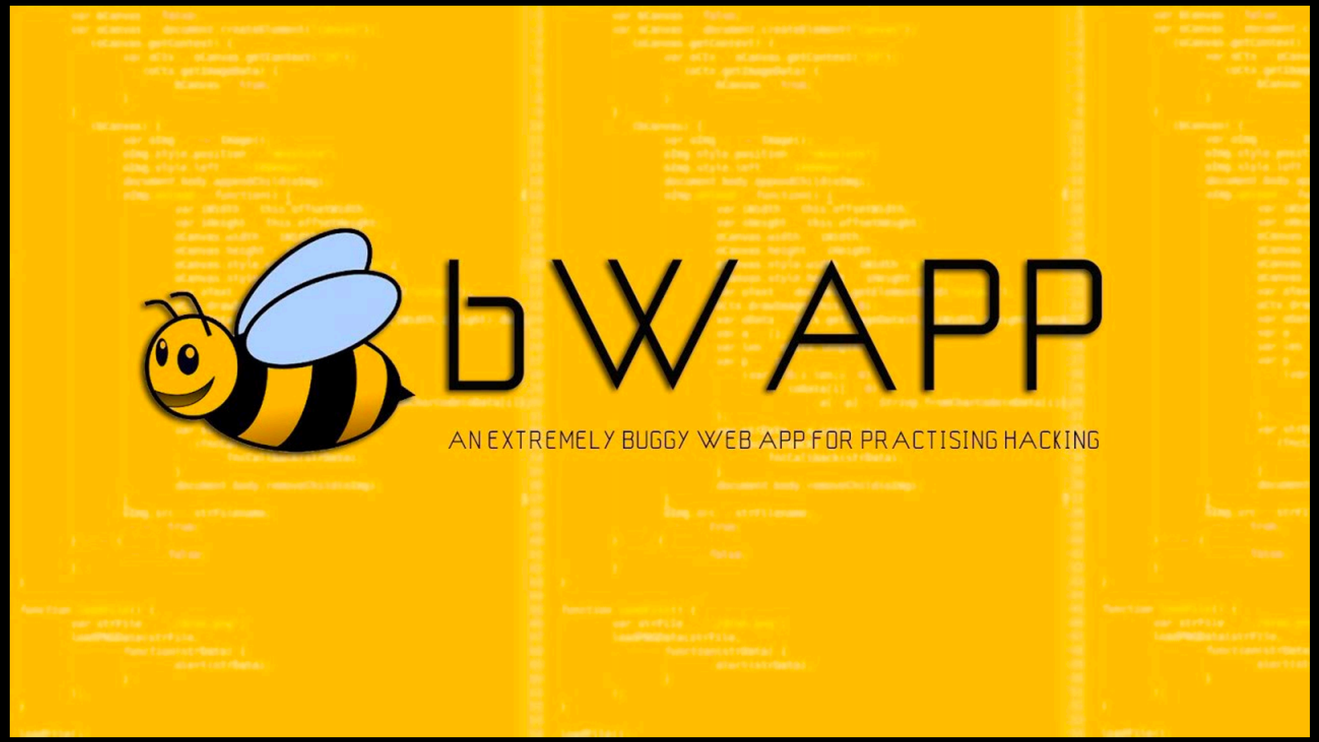
STATISTIK WEB SCANNING MENGGUNAKAN NIKTO



No	rule.description	Count
1	Web server 400 error code.	11328
2	XSS (Cross Site Scripting) attempt.	317
3	Common web attack.	346
4	Multiple web server 400 error codes from same source ip.	762
5	sshd: Attempt to login using a non-existent user	188

PENGUJIAN SERANGAN PADA BWAPP

- Sql Injection
- Cross Site Scripting (XSS)
- OS Command Injection
- Local File Inclusion (LFI)
- Directory Traversal



SQL INJECTION ATTACK

	Time	rule.description	rule.level	rule.id
>	Jan 17, 2021 @ 11:32:11.609	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:32:11.607	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:32:09.605	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:57.592	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:55.628	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:55.628	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:55.589	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:53.587	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:51.587	SQL injection attempt.	6	31103
>	Jan 17, 2021 @ 11:31:51.587	SQL injection attempt.	6	31103

CROSS SITE SCRIPTING (XSS) ATTACK

	Time	rule.description	rule.level	rule.id
>	Jan 17, 2021 @ 11:31:15.546	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:39.448	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:39.444	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:37.450	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:37.446	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:37.442	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:35.476	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:35.476	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:35.439	XSS (Cross Site Scripting) attempt.	6	31105
>	Jan 17, 2021 @ 11:29:31.435	XSS (Cross Site Scripting) attempt.	6	31105

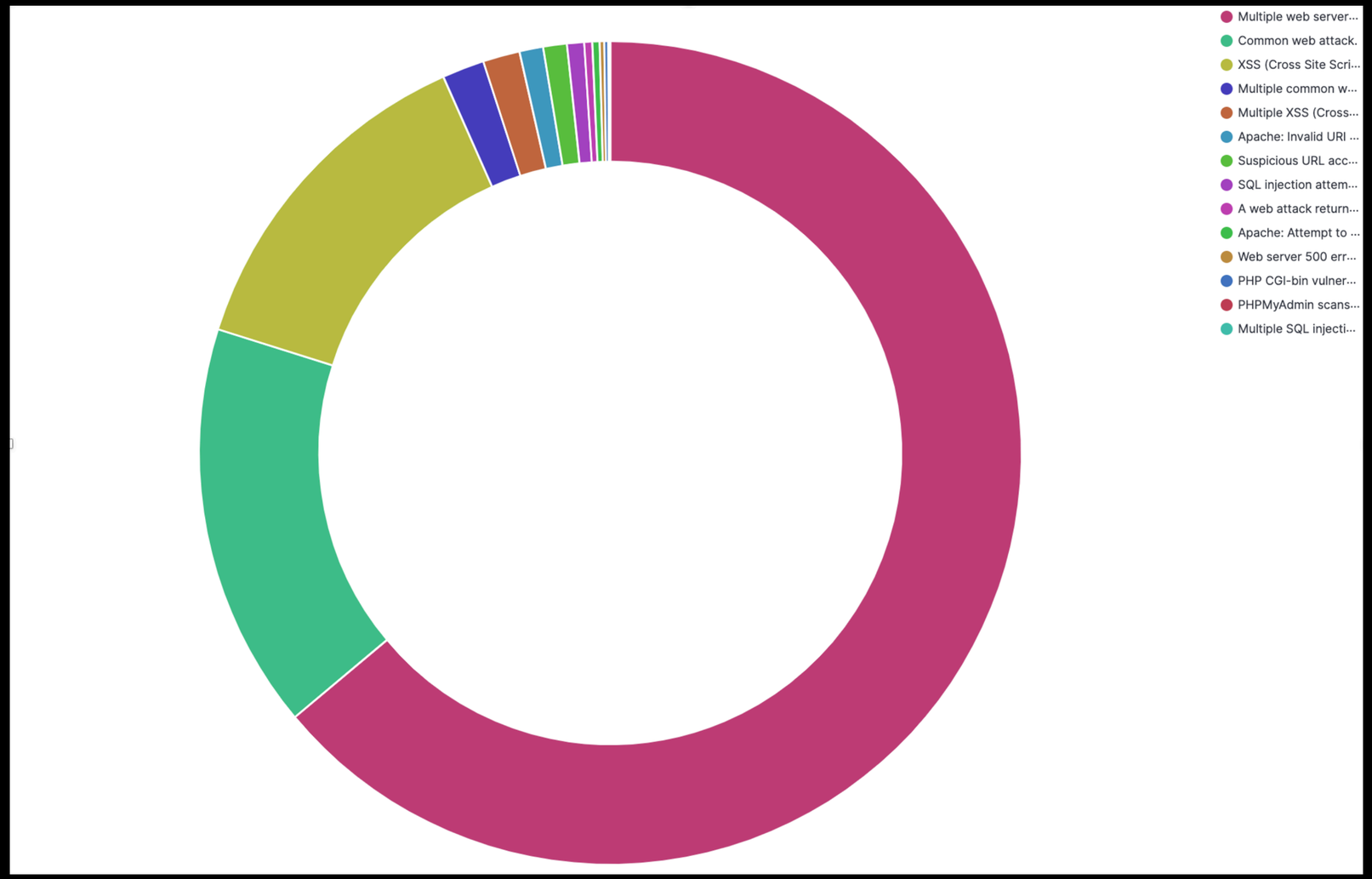
OS COMMAND INJECTION ATTACK

	Time	rule.description	rule.level	rule.id
›	Jan 17, 2021 @ 11:42:46.200	Audit: Command: /usr/bin/whoami	3	80792
›	Jan 17, 2021 @ 11:42:42.183	Audit: Command: /usr/bin/whoami	3	80792
›	Jan 17, 2021 @ 11:22:11.005	Audit: Command: /usr/bin/whoami	3	80792
›	Jan 17, 2021 @ 11:02:05.925	Audit: Command: /usr/bin/whoami	3	80792

LOCAL FILE INCLUSION / DIRECTORY TRAVERSAL

Time	rule.description	rule.level	rule.id
Jan 17, 2021 @ 11:21:30.966	Common web attack.	6	31104
Jan 17, 2021 @ 11:20:46.935	Common web attack.	6	31104
Jan 17, 2021 @ 11:20:42.931	Common web attack.	6	31104
Jan 17, 2021 @ 11:01:27.875	Common web attack.	6	31104
Jan 17, 2021 @ 11:01:23.870	Common web attack.	6	31104
Jan 17, 2021 @ 11:01:11	Common web attack.	6	31104
Jan 17, 2021 @ 11:01:05.851	Common web attack.	6	31104
Jan 17, 2021 @ 11:01:03.848	Common web attack.	6	31104
Jan 17, 2021 @ 11:00:59.844	Common web attack.	6	31104
Jan 17, 2021 @ 11:00:53.838	Common web attack.	6	31104

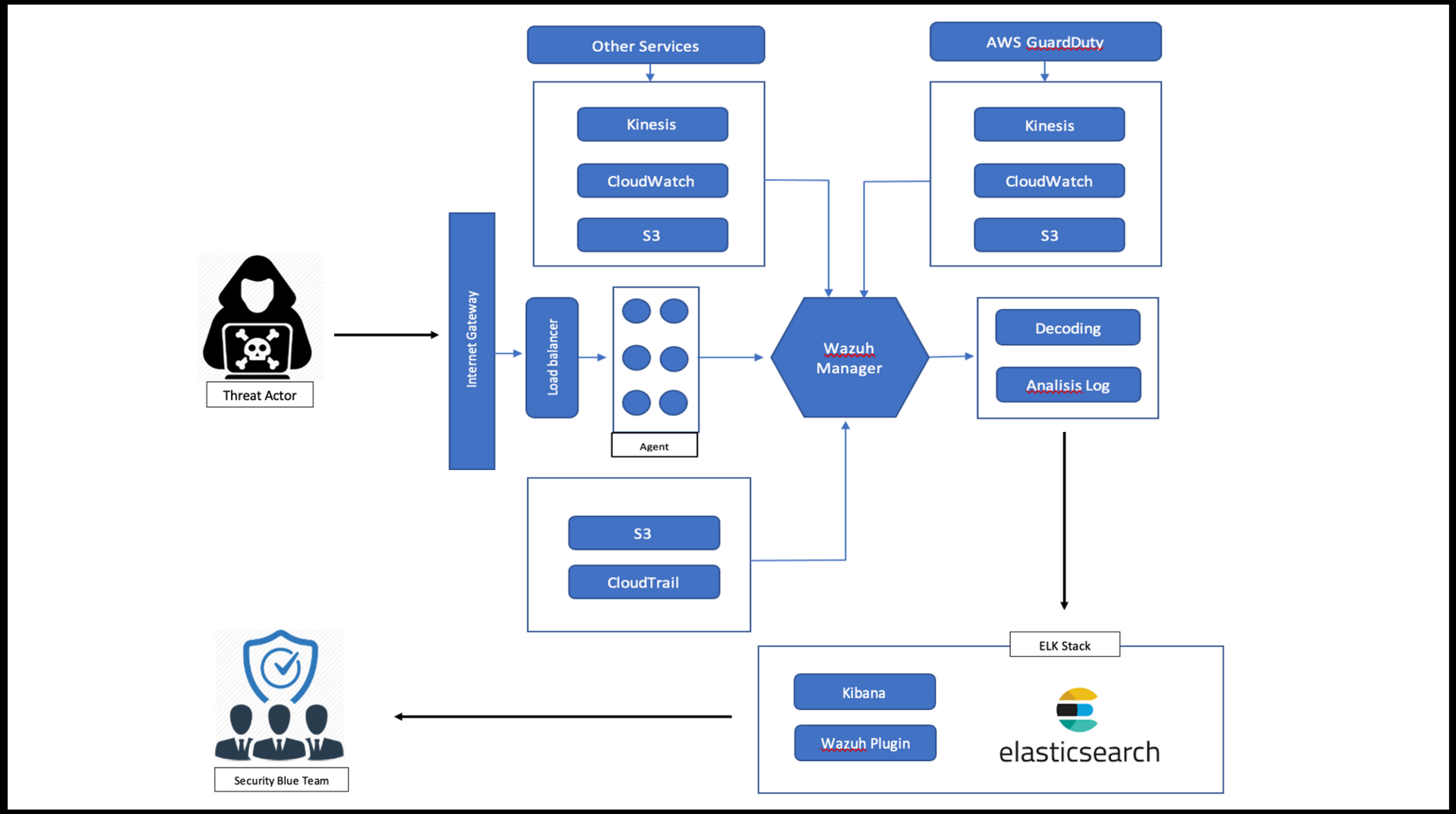
DIAGRAM PERINGATAN SETELAH PENGUJIAN SERANGAN PADA BWAPP



TABEL PERINGATAN SETELAH PENGUJIAN SERANGAN PADA BWAPP

No	rule.description	Count	Percentage
1	Multiple web server 400 error codes from same source ip	2.469	63,91%
2	Common Web Attack	616	15,95%
3	XSS (Cross Site Scripting) Attempt	521	13,49%
4	Multiple web attack from same source ip	64	1,66%
5	Multiple XSS attempts (Cross Site Scripting) from same source ip	56	1,45%
6	Apache : Invalid bad URI (bad client request)	36	0,93%
7	Suspicious URL access	36	0,93%
8	Sql Injection attempt	26	0,67%
9	A web attack return code 200 (success)	12	0,31%
10	Apache: Attempt to access forbidden file or directory	11	0,28%
11	Web server 500 error code (internal error)	7	0,18%
12	PHP CGI-bin vulnerability attempt	6	0,16%
13	PHPMyAdmin scans (looking for setup.php)	2	0,05%
14	Multiple Sql Injection attempts from same source ip	1	0,03%

SKEMA PENGUJIAN HIDS WAZUH PADA INSTANCE EC2 AWS



PENGUMPULAN INFORMASI DENGAN NMAP

	Time	data.aws.source	rule.description	rule.level	rule.id
>	Jan 17, 2021 @ 19:12:45.023	guardduty	AWS GuardDuty: NETWORK_CONNECTION - Outbound portscan from EC2 instance i-066da16971b05.	6	80302
>	Jan 17, 2021 @ 13:12:44.564	guardduty	AWS GuardDuty: NETWORK_CONNECTION - Outbound portscan from EC2 instance i-066dd03aa16971b05.	6	80302
>	Jan 17, 2021 @ 13:12:44.534	guardduty	AWS GuardDuty: NETWORK_CONNECTION - Outbound portscan from EC2 instance i-066dd03aa16971b05.	6	80302
>	Jan 17, 2021 @ 13:12:44.488	guardduty	AWS GuardDuty: NETWORK_CONNECTION - Outbound portscan from EC2 instance i-066dd03aa16971b05.	6	80302

PENGUJIAN TERHADAP SERVICE EC2 AWS

- Membuat Security Group EC2
- Menjalankan instance EC2 baru
- Menghentikan instance EC2

MEMBUAT SECURITY GROUP EC2

t data.aws.awsRegion	ap-southeast-1
t data.aws.aws_account_id	619022404121
t data.aws.eventCategory	Management
t data.aws.eventID	10b980fa-6a24-4ccd-aa40-bde50af94769
t data.aws.eventName	CreateSecurityGroup
t data.aws.eventSource	ec2.amazonaws.com
t data.aws.eventTime	2021-01-17T06:39:44Z
t data.aws.eventType	AwsApiCall
t data.aws.eventVersion	1.08
t data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/ap-southeast-1/2021/01/17/619022404121_CloudTrail_ap-southeast-1_20210117T0645Z_gMxMlYh8646NLDma.json.gz
t data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t data.aws.managementEvent	true
t data.aws.readOnly	false
t data.aws.recipientAccountId	619022404121
t data.aws.requestID	41265d4b-36b0-4a99-b8e4-89e0e26c4aa5
t data.aws.requestParameters.groupDescription	launch-wizard-18 created 2021-01-17T13:39:30.211+07:00
t data.aws.requestParameters.groupName	launch-wizard-18
t data.aws.requestParameters.vpcId	vpc-74644513
t data.aws.responseElements._return	true

MENJALANKAN INSTANCE EC2 BARU

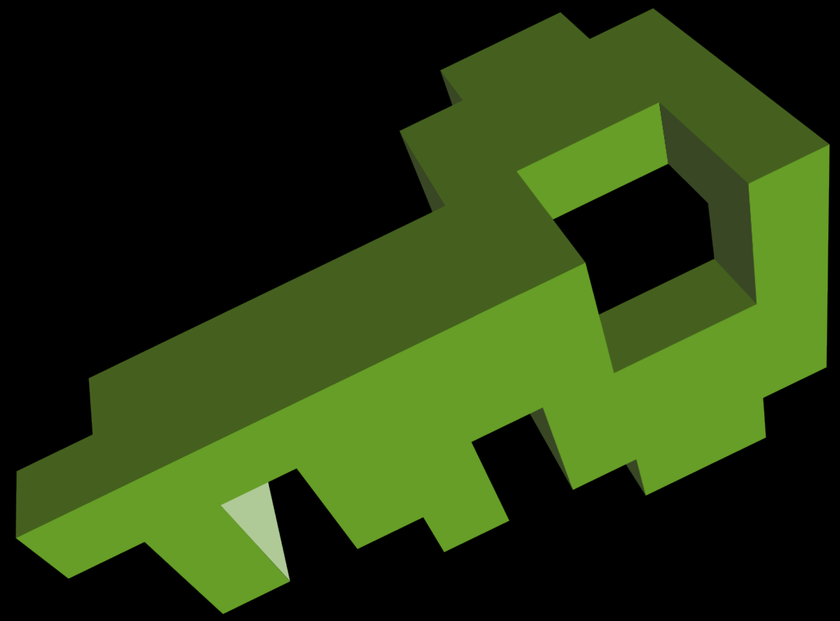
t data.aws.awsRegion	ap-southeast-1
t data.aws.aws_account_id	619022404121
t data.aws.eventCategory	Management
t data.aws.eventID	3e44f4e4-19cc-4fb1-9f89-66d4b6b49baf
t data.aws.eventName	RunInstances
t data.aws.eventSource	ec2.amazonaws.com
t data.aws.eventTime	2021-01-17T06:41:23Z
t data.aws.eventType	AwsApiCall
t data.aws.eventVersion	1.08
t data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/ap-southeast-1/2021/01/17/619022404121_CloudTrail_ap-southeast-1_20210117T0645Z_gMxMlYh8646NLDma.json.gz
t data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t data.aws.managementEvent	true
t data.aws.readOnly	false
t data.aws.recipientAccountId	619022404121
t data.aws.requestID	71cc14f3-96bc-4b2f-96c0-efe2e795d7a7
ⓘ data.aws.requestParameters.blockDeviceMapping.items	> { "ebs": { "volumeType": "gp2", "deleteOnTermination": true, "volumeSize": 8 }, "deviceName": "/dev/sda1"

MENGHENTIKAN INSTANCE EC2

t	agent.name	ip-172-32-1-231
t	data.aws.awsRegion	ap-southeast-1
t	data.aws.aws_account_id	619022404121
t	data.aws.eventCategory	Management
t	data.aws.eventID	24a111e0-0e14-4825-ac45-25e44153cb68
t	data.aws.eventName	StopInstances
t	data.aws.eventSource	ec2.amazonaws.com
t	data.aws.eventTime	2021-01-21T09:10:11Z
t	data.aws.eventType	AwsApiCall
t	data.aws.eventVersion	1.08
t	data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/ap-southeast-1/2021/01/21/619022404121_CloudTrail_ap-southeast-1_20210121T0915Z_HFxToGrfsdW31SuZ.json.gz
t	data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t	data.aws.managementEvent	true
t	data.aws.readOnly	false
t	data.aws.recipientAccountId	619022404121
t	data.aws.requestID	e0ce07d8-2a47-4226-a251-c8a072cca3b7
t	data.aws.requestParameters.force	false

PENGUJIAN TERHADAP SERVICE IAM

- Membuat user baru
- Membuat user tanpa hak akses
- Melakukan proses login dengan kredensial yang salah
- Melakukan proses login dengan kredensial yang benar



MEMBUAT USER BARU

t agent.name	ip-172-32-1-231
t data.aws.awsRegion	us-east-1
t data.aws.aws_account_id	619022404121
t data.aws.eventCategory	Management
t data.aws.eventID	f680c29d-b67f-44ac-b4ae-bcfdaf69bc43
t data.aws.eventName	CreateUser
t data.aws.eventSource	iam.amazonaws.com
t data.aws.eventTime	2021-01-21T09:31:21Z
t data.aws.eventType	AwsApiCall
t data.aws.eventVersion	1.08
t data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/us-east-1/2021/01/21/619022404121_CloudTrail_us-east-1_20210121T0935Z_TsVt480zDUhr7Q7t.json.gz
t data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t data.aws.managementEvent	true
t data.aws.readOnly	false
t data.aws.recipientAccountId	619022404121
t data.aws.requestID	a8274344-9696-40dc-a611-c2cb58ac19ba
? data.aws.requestParameters.tags	
t data.aws.requestParameters.userName	hacker

MEMBUAT USER TANPA HAK AKSES

t agent.name	ip-172-32-1-231
t data.aws.awsRegion	us-east-1
t data.aws.aws_account_id	619022404121
t data.aws.errorCode	AccessDenied
t data.aws.errorMessage	User: arn:aws:iam::619022404121:user/hacker is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::619022404121:user/anu
t data.aws.eventCategory	Management
t data.aws.eventID	7539fab6-f98b-4d2a-9bc8-60c40ea377da
t data.aws.eventName	CreateUser
t data.aws.eventSource	iam.amazonaws.com
t data.aws.eventTime	2021-01-21T09:35:36Z
t data.aws.eventType	AwsApiCall
t data.aws.eventVersion	1.08
t data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/us-east-1/2021/01/21/619022404121_CloudTrail_us-east-1_20210121T0940Z_lmOoMO5IREMBtPN4.json.gz
t data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t data.aws.managementEvent	true
t data.aws.readOnly	false
t data.aws.recipientAccountId	619022404121
t data.aws.requestID	42b5f15c-78f1-4513-9137-a54e4cd90f18
t data.aws.source	cloudtrail
t data.aws.sourceIPAddress	182.1.86.190

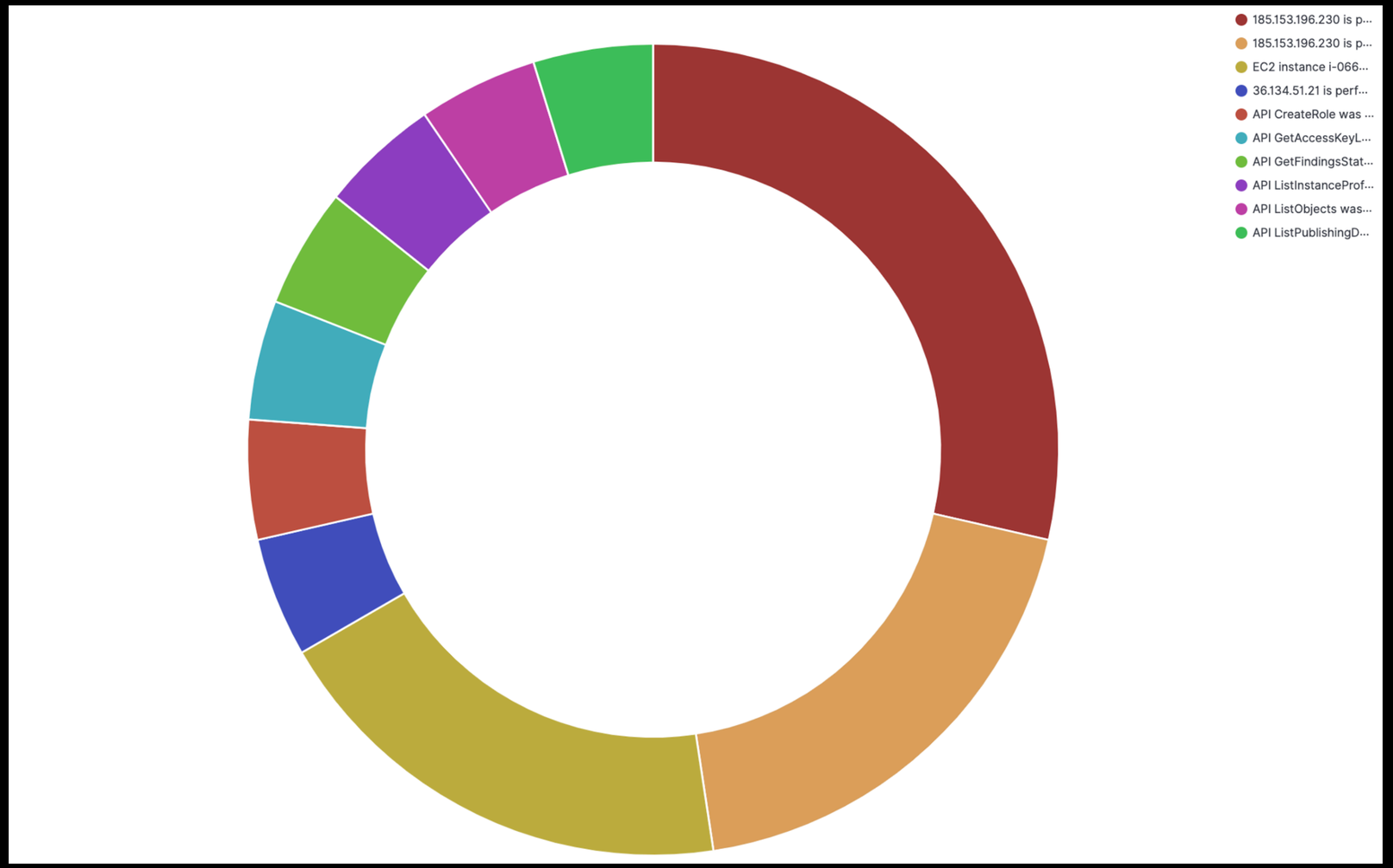
MELAKUKAN PROSES LOGIN DENGAN KREDENSIAL YANG SALAH

t	data.aws.awsRegion	us-east-1
t	data.aws.aws_account_id	619022404121
t	data.aws.eventCategory	Management
t	data.aws.eventID	5299bf40-4eb5-4d7e-b1e3-a942c8812e4d
t	data.aws.eventName	ConsoleLogin
t	data.aws.eventSource	signin.amazonaws.com
t	data.aws.eventTime	2021-01-21T09:32:38Z
t	data.aws.eventType	AwsConsoleSignIn
t	data.aws.eventVersion	1.08
t	data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/us-east-1/2021/01/21/619022404121_CloudTrail_us-east-1_20210121T0935Z_u4yCaYaRluxCBylz.json.gz
t	data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t	data.aws.managementEvent	true
t	data.aws.readOnly	false
t	data.aws.recipientAccountId	619022404121
t	data.aws.responseElements.ConsoleLogin	Failure
t	data.aws.source	cloudtrail

MELAKUKAN PROSES LOGIN DENGAN KREDENSIAL YANG BENAR

t	data.aws.awsRegion	us-east-1
t	data.aws.aws_account_id	619022404121
t	data.aws.eventCategory	Management
t	data.aws.eventID	5299bf40-4eb5-4d7e-b1e3-a942c8812e4d
t	data.aws.eventName	ConsoleLogin
t	data.aws.eventSource	signin.amazonaws.com
t	data.aws.eventTime	2021-01-21T09:32:38Z
t	data.aws.eventType	AwsConsoleSignIn
t	data.aws.eventVersion	1.08
t	data.aws.log_info.log_file	AWSLogs/619022404121/CloudTrail/us-east-1/2021/01/21/619022404121_CloudTrail_us-east-1_20210121T0935Z_u4yCaYaRluxCBylz.json.gz
t	data.aws.log_info.s3bucket	aws-cloudtrail-logs-619022404121-d758afad
t	data.aws.managementEvent	true
t	data.aws.readOnly	false
t	data.aws.recipientAccountId	619022404121
t	data.aws.responseElements.ConsoleLogin	Success
t	data.aws.source	cloudtrail

DIAGRAM 10 PERINGATAN PALING BANYAK PADA SERANGAN SERVICE AWS



TABEL 10 PERINGATAN PALING BANYAK PADA SERANGAN SERVICE AWS

data.aws.description: Descending	Count
185.153.196.230 is performing SSH brute force attacks against i-066dd03aa16971b05. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.	7
EC2 instance i-066dd03aa16971b05 is performing outbound port scans against remote host 172.32.1.89.	6
185.153.196.230 is performing SSH brute force attacks against i-07e6bd68c5132ef2f. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.	4
36.134.51.21 is performing SSH brute force attacks against i-0c9df11dd70584401. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.	1
API CreateRole was invoked using root credentials from IP address 182.2.37.219.	1
API DescribeVolumes was invoked using root credentials from IP address 182.2.75.136.	1
API GetAccessKeyLastUsed was invoked using root credentials from IP address 182.1.74.183.	1
API GetAccessKeyLastUsed was invoked using root credentials from IP address 182.1.86.190.	1
API GetEnrollmentStatus was invoked using root credentials from IP address 182.1.67.38.	1
API GetFindingsStatistics was invoked using root credentials from IP address 182.2.36.23.	1

KESIMPULAN

SARAN

BAB 5 PENUTUP

THANKS