



UNIVERSITÀ DI PARMA

Progetto SIEM

Introduzione

- Evoluzione Tecnologica
- Sicurezza Informatica dei Dati
- Prioritizzazione della **Cybersecurity**:
 - Furti di Dati Personali
 - Perdite Finanziarie
 - Danni Reputazionali

Contesto

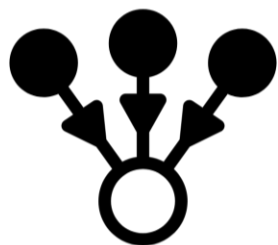
Ambiente Universitario

- Ampio bacino d'utenza = Ampia superficie d'attacco
- Rete «*Bring Your Own Device*»
- Uso di rete **Aperto**
- Grande quantità di **Dati sensibili** e della **Ricerca**
- Poca consapevolezza



Obiettivo

Grandi quantità di Dati



Piattaforma Centralizzata



Individuazione dell'Attacco

Benefici:

- Efficienza Operativa
- Diminuzione Tempo di Risposta
- **Anomaly Detection**
- Conformità Normativa

Fonti Dati

Dati Raccolti = **Log**

1. FortiGate: Firewall di Perimetro

- Prevenzione delle Intrusioni (IPS)
- VPN
- Filtraggio Indirizzi IP
- Controllo Applicazioni



2. Microsoft Defender (M365)

- Protezione Anti-Phishing
- Protezione EndPoint (Dispositivi)
- Threat Intelligence



Fonti Dati

3. Esfiltrazioni DarkWeb

- Controllo Password
@studenti.unipr.it
@unipr.it
@guest.unipr.it
- Botnet



4. Altro...



Piattaforma Centralizzata (SIEM) Security Information and Event Management

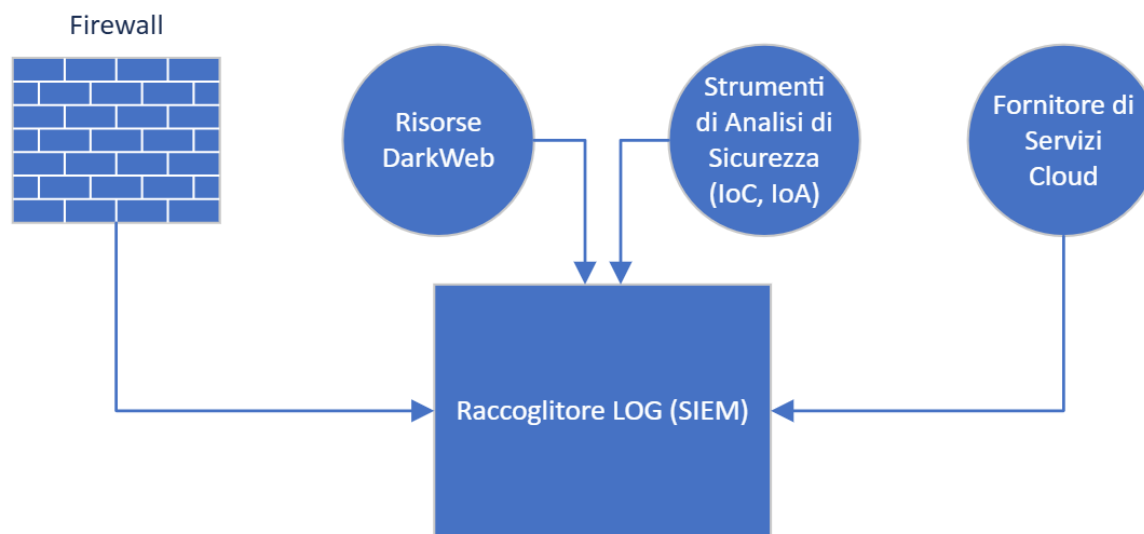
- Raccolta, Correlazione e Analisi Log

- **ElasticSearch** via **Docker**

- on-premise
- Docker-Compose file
- Binding mount

- Struttura Modulare:

- Kibana (Web-UI)
- LogStash (agentless Log ingestion)
- Elastic Agent (agent-based Log ingestion)
- ES node



Raccolta Log - Log Ingestion

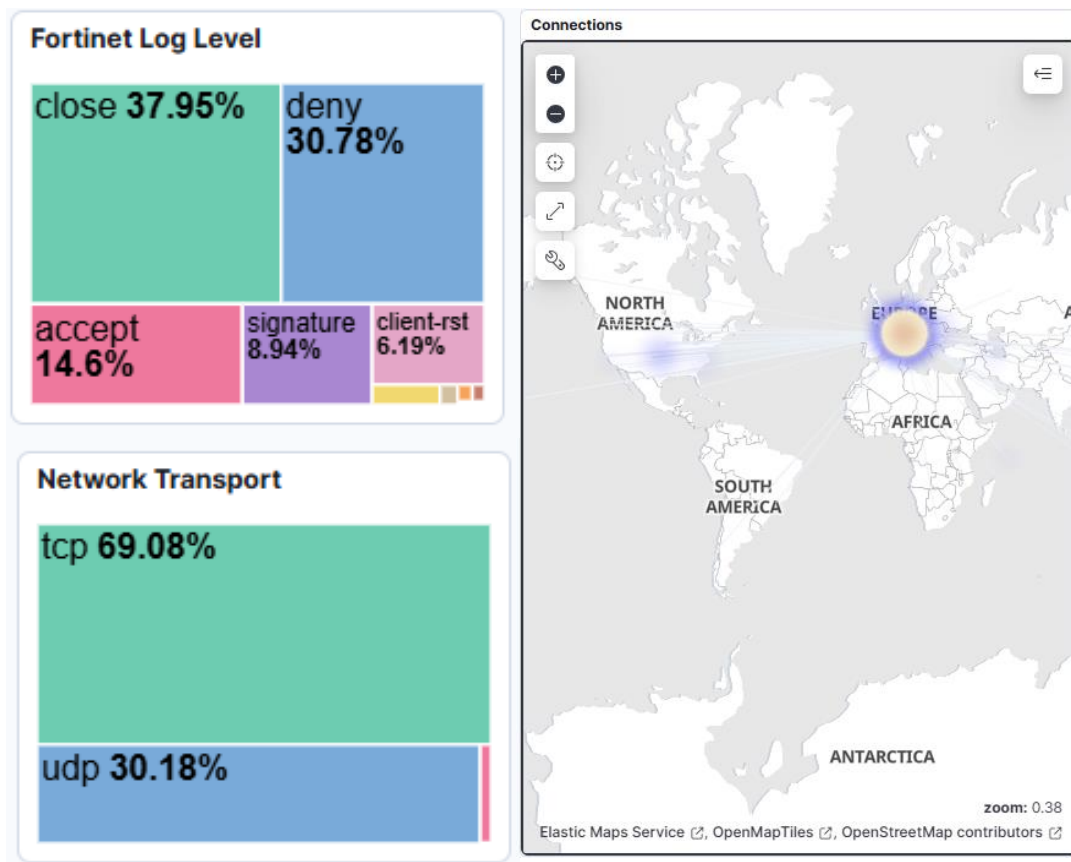
Composti da **chiave:valore**

- Filtraggio
- Analisi Rapida
- Storage Efficiente

```
{  
  "timestamp": "2024-09-12T08:16:29Z",  
  "event_type": "LOGIN_FAILED",  
  "source_ip": "192.168.1.100"  
}
```

1. Plug-In nativi (*Integrations*):
 - + Facilità d'implementazione
 - + Aggiornamenti automatici
 - Personalizzazione limitata
2. Logstash
 - + Flessibilità
 - Complessità
3. Script (Python, Java, Go ...)
 - + Controllo totale
 - Sviluppo e Manutenzione

Visualizzazione Dati – Kibana UI



k m365_defender.alert.evidence.user_account.user_principal_name <REDACTED>@studenti.unipr.it

k m365_defender.alert.title Impossible travel activity

k m365_defender.alert.severity high

IP related.ip 128.90.xxx.xx

f message

A user account signed in from a suspicious browser and an unusual location based on the user's typical browsing behavior. An attacker might have compromised the user account and is signing in on behalf of the user, indicating unauthorized access. Prompt investigation is recommended to mitigate possible security risks.

Rilevamento delle Anomalie – Anomaly Detection

- **Population:** identifica comportamenti anomali all'interno di un insieme di dati (popolazione) per rilevare deviazioni significative.
- **Rare:** identifica eventi rari o insoliti all'interno di un dataset.
- **Categorization:** classifica i dati in categorie specifiche e identifica eventi che non si adattano ai modelli normali di ciascuna categoria.
- **Single Metric, Multi Metric, Geo ...**


☐ > rare_destination_country
Managed







network security

Time	Severity ⓘ ↓	Detector	Found for	Influenced by
September 20th 2024	87	Detects rare country names.	Brunei	destination.as.organization.name: Unified National Networks ⓘ destination.geo.country_name: Brunei ⓘ destination.ip: 202.160.xx.xxx ⓘ

Caso di Studio

Urgente






  Reply  Reply all  Forward  

Thu 8/15/2024 6:03 PM

Gentile utente
Oggi, dal 15.8.2024 al 21.8.2024, verrà effettuato un aggiornamento che prevede la chiusura di tutti gli account inutilizzabili.
La preghiamo di controllare l'attività del suo account effettuando nuovamente il login tramite questo link: [CLICCA QUI](#).

Firma il tuo 5xmille all'Università di Parma. Aiutaci a potenziare la capacità di accoglienza, soprattutto abitativa, per le studentesse e gli studenti. - Indica 00308780345 nella tua dichiarazione dei redditi.

 Reply  Reply all  Forward

Caso di Studio



Documents (10,520)

15 Aug, 2024 @ 00:00:00.000 - 17 Aug, 2024 @ 16:18:17.180 (interval: Auto - hour)

<div>k</div> email.from.address	<REDACTED>@unipr.it
<div>k</div> email.subject	Urgente
<div>k</div> email.to.address	<REDACTED>@unipr.it
<div>📅</div> event.created	16 Aug, 2024 @ 20:59:26.983
<div>📍</div> host.ip	160.154.xxx.xxx

<div>k</div> m365_defender.alert.evidence.delivery_action	delivered
<div>k</div> m365_defender.alert.evidence.delivery_location	inbox
<div>k</div> m365_defender.alert.t.title	Email reported by user as malware or phish
<div>k</div> m365_defender.alert.evidence.urls	https://warmcool.com.tr/ou/outlk.html

