Borse di studio GARR
Orio Carlini

SISTEMA INTEGRATO DI SICUREZZA INFORMATICA PER LA GESTIONE PROATTIVA DELLE MINACCE

Nicolò Thei

Università degli Studi di Parma

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Premessa

- Evoluzione Tecnologica
  - Tecnologia e Connettività
  - Sicurezza
- Sicurezza Informatica
  - Minacce (Malware, Phishing …)
  - Poca consapevolezza

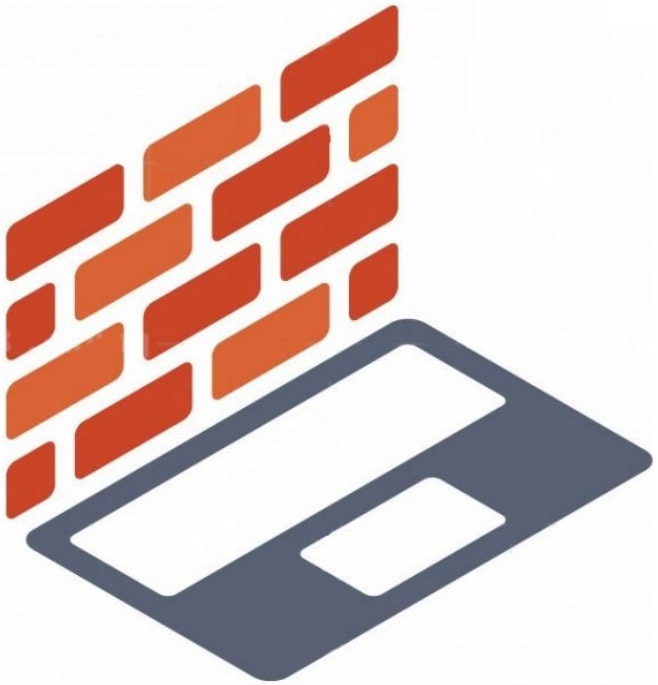
Contesto

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

- **Rete GARR**
  - Avvisi GARR-CERT

Lo stato Attuale

- Strumenti di **Sicurezza**
  - Firewall
  - *Intrusion Prevention System*
- Piattaforme di **Monitoraggio** e **Analisi**
  - Consultazione periodica
- Ricerca **credenziali compromesse**
  - Consultazione periodica



Obiettivo del Progetto

Sviluppare una soluzione **DINAMICA** e **Proattiva**

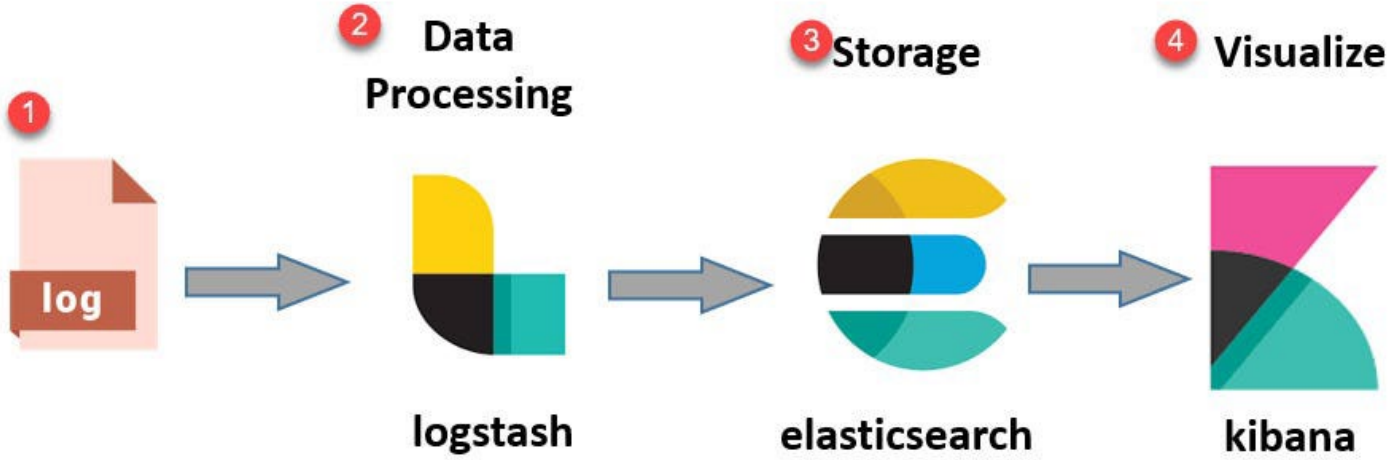
1. Monitoraggio continuo -> **Raccolta Dati**
2. Analisi sui **Dati raccolti**
3. Azioni correttive **Automatiche**
4. Reportistica

Fase di Raccolta Dati

- Automazione della Raccolta Dati
- Integrazione multi-sorgente
- Filtraggio e Correlazione
- SIEM: *Security Information & Event Management*

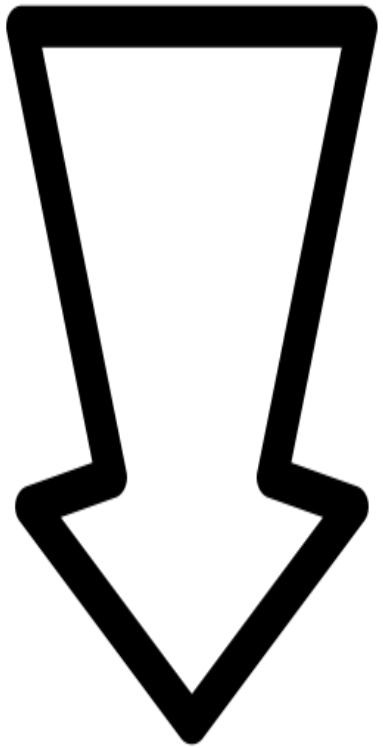
SIEM

- Uso di Elasticsearch (**ELK**)
  - Alte Capacità di Analisi
  - Scalabile e Flessibile



Analisi sui Dati

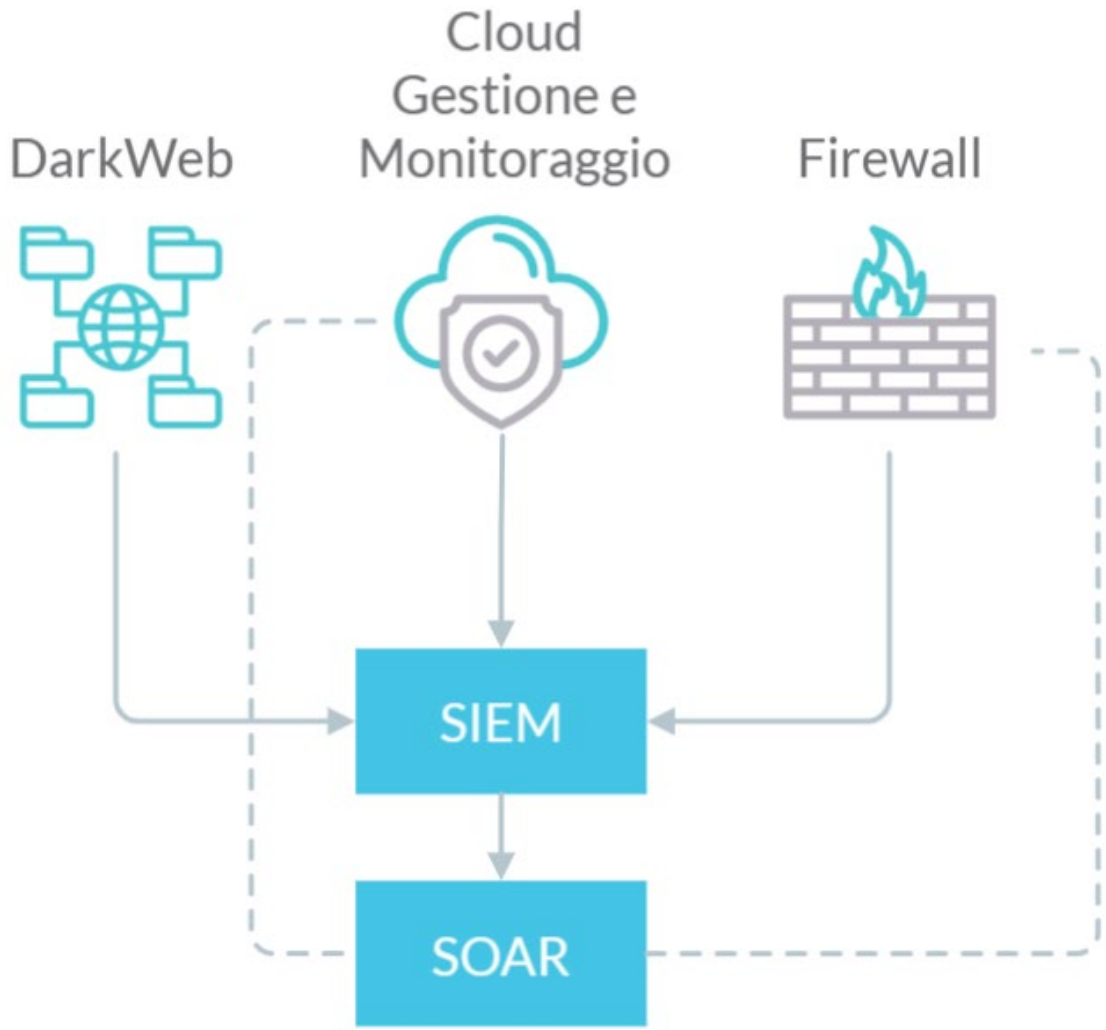
1. Traffico Grezzo (RAW)
2. Log di Sistema
3. Alert di Sicurezza
4. Indicatori di Compromissione (**IoC**)



Automatismi con SOAR

- *Security Orchestration, Automation and Response*
- **Automazione** dei Processi di Sicurezza
- **Benefici**:
  - Efficienza
  - Riduzione dei Tempi di Risposta
  - Minimizzazione dell'Errore Umano

Schema



Grazie

Borsista: Nicolò Thei

Tutor: Raffaele Cicchese