

# LOG: cosa sono e perché è importante conservarli

LINUX DAY 2018 - RIETI



PRESENTED BY DAVIDE PALA



# Su di me ...

- Appassionato di tecnologia.
- Security specialist.
- Sostenitore della filosofia open source.
- Cofounder dell'associazione Cyber Saiyan.



<https://twitter.com/DavidePala83>



<https://www.linkedin.com/in/davide-pala>



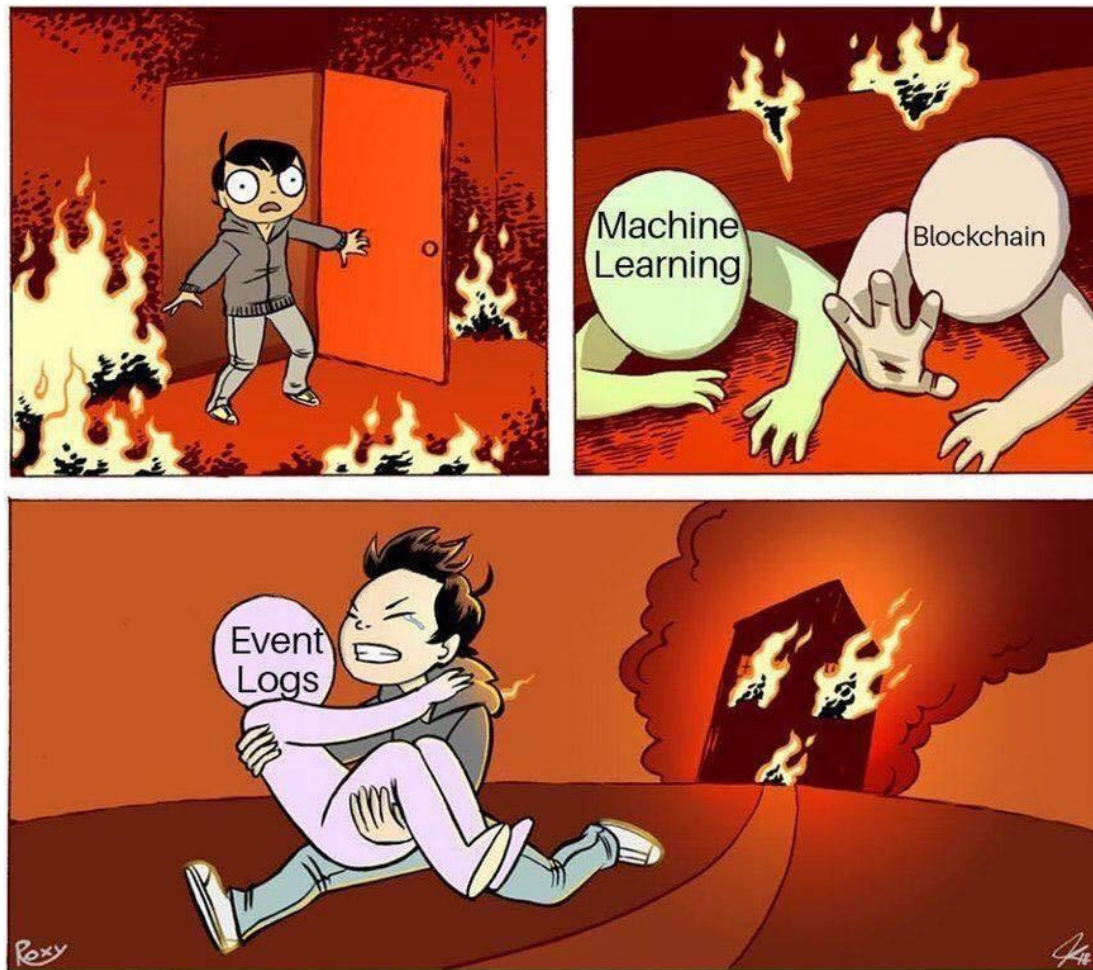
<https://www.facebook.com/davide.pala>



PRESENTED BY DAVIDE PALA



# SAGGEZZA...



# LOG ... Partiamo dalle origini



Il solcometro veniva usato per misurare la velocità di navigazione, esso consisteva un un cordino legato ad un ceppo, in inglese "log".

Le misurazioni venivano registrate regolarmente in un libro chiamato "logbook".



# Cosa contengono i log?

- Attività del sistema:

Tutte le operazioni svolte dal sistema operativo nel corso del suo normale funzionamento.

- Attività dell'utente:

Le operazioni frutto dell'interazione dell'utente con il sistema, esempio il login.

- Registro eventi:

Gli eventi esterni al sistema che tuttavia lo interessano, ad esempio un arresto o il rilevamento di un errore hardware



PRESENTED BY DAVIDE PALA



# Dove sono i log?

All'interno di apposite directory del sistema operativo. Per i sistemi linux /var/log mentre per i sistemi windows %windir%\System32\winevt\Logs.

Non tutti i sistemi sono dotati di log locali. Spesso apparati privi di storage richiedono la configurazione di un repository remoto o l'installazione di hardware aggiuntivo.



PRESENTED BY DAVIDE PALA



# A cosa servono i log?

- Security compliance.  
Rispetto delle best practice relativamente alla sicurezza.
- Regulation compliance.  
Compliance rispetto alla normativa.
- Troubleshooting.  
Analisi degli eventi da un punto di vista privilegiato.
- Forensic.  
Rilevazione di evidenze occorse nel passato.
- Incident Response.  
Detection in tempo reale degli incidenti di sicurezza.



PRESENTED BY DAVIDE PALA



# Come si gestiscono i log?

- Abilitati.
- Centralizzati.
- Garantita l'integrità.
- Archiviati a norma di legge.

Sebbene vi sia il legittimo interesse la racconta e conservazione dei log deve essere effettuata nel rispetto delle norme vigenti.



PRESENTED BY DAVIDE PALA







# Le sfide del log management

- Storage:

Dimensionamento, affidabilità, scalabilità.

- Processabilità:

Correlazione, normalizzazione, consultazione ed esportazione.

- Integrabilità:

Compatibilità con i sistemi, throughput di memorizzazione.

- Affidabilità:

Dimensionamento, affidabilità, scalabilità.



PRESENTED BY DAVIDE PALA



# Cosa offre il mondo open:

## GRAYLOG

- Storage:

Basato su elastic search e mongoDB.

- Processabilità:

Possibilità di effettuare query, strumenti come stream e pipeline.

- Integrabilità:

Compatibilità con gli standard e supporto a plugin.


- Affidabilità:

Scalabilità orizzontale e architettura clusterizzabile.



PRESENTED BY DAVIDE PALA





# DEMO TIME!

Normalizzazione con

graylog



PRESENTED BY DAVIDE PALA



*Thanks to all !!*  
*AND .....*

FOLLOW US



<https://www.cybersaiyan.it>  
<https://www.romhack.io>