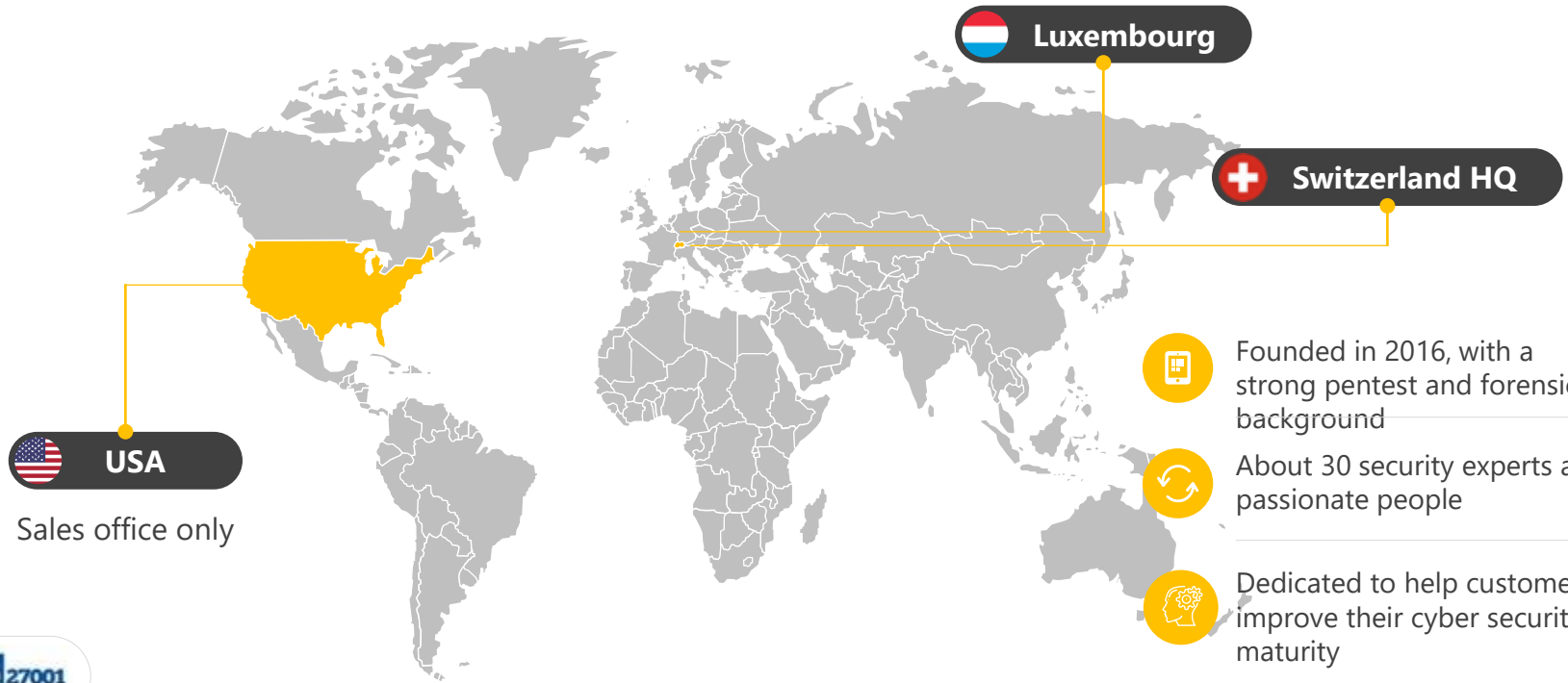





SOC IMPLEMENTATION

*How to address this challenge,
shorten reaction time and
increase visibility.*

HACKNOWLEDGE



-  Founded in 2016, with a strong pentest and forensic background
-  About 30 security experts and passionate people
-  Dedicated to help customer to improve their cyber security maturity



THE CONTEXT



CYBERSECURITY

TOO COMPLEX,
TOO EXPENSIVE,
TOO LATE...



Complex



Expensive



Challenging

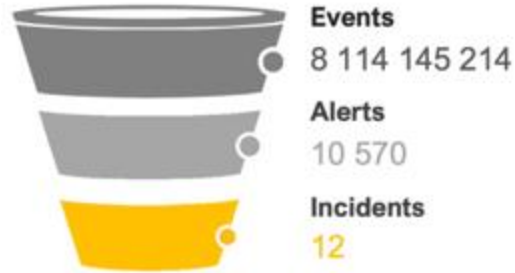


Time
Consuming



THE GOAL

Humanly impossible to handle



Adressable



OUR VALUES



VENDOR INDEPENDENT, OPEN SOURCE SOLUTION :

We chose to be independent from commercial solutions directly related to log volume and we combined multiples Open Sources solutions to detect, collect, correlate and store log events



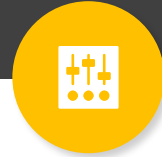
THE RIGHT PRICE – THE RIGHT LOGS :

Our vision is to be UseCase oriented and select the logs who can give real value to the scenario we want to detect. The price will slightly follow the security maturity level you want to achieve



NO MAGIC BUT SIMPLE AND EFFECTIVE

***SOLUTION:** We focus on efficient, secure and reliable components. We do not believe in magic solutions. We help companies identify IT security threat and shorten the time between breach & detection.*



GROW AND IMPROVE BY FIELD EXPERIENCE:

We strongly believe in mutual exchange and we make our solution improve by real security cases from attacks or pen test append on customer's environment and share to the community



HOW WE DID IT



CREATE DEDICATED SENSORS

+

EXPLOIT EXISTING LOGS

- > Active Directory
- > Network security solutions
- > Endpoint behavior products
- > UNIX/LINUX
- > Cloud solutions...



- > Passive devices
- > Centrally managed



- > Filtered based on Use Cases



- > Detect hostile activity
- > Anomalies detection
- > Enriched alerts



SENSORS FEATURES

OUR SENSORS

- › Custom development
- › Optimized
- › Hardware or virtual
- › Multiples Network interfaces



Log collector

- › Push / Fetch
- › Cache and filter



IDS

- › Span , tap , rspan, erspan
- › Updated regularly
- › Different feeds
 - › CIRCL, FIRST, Commercial, Gov...



Honeypots

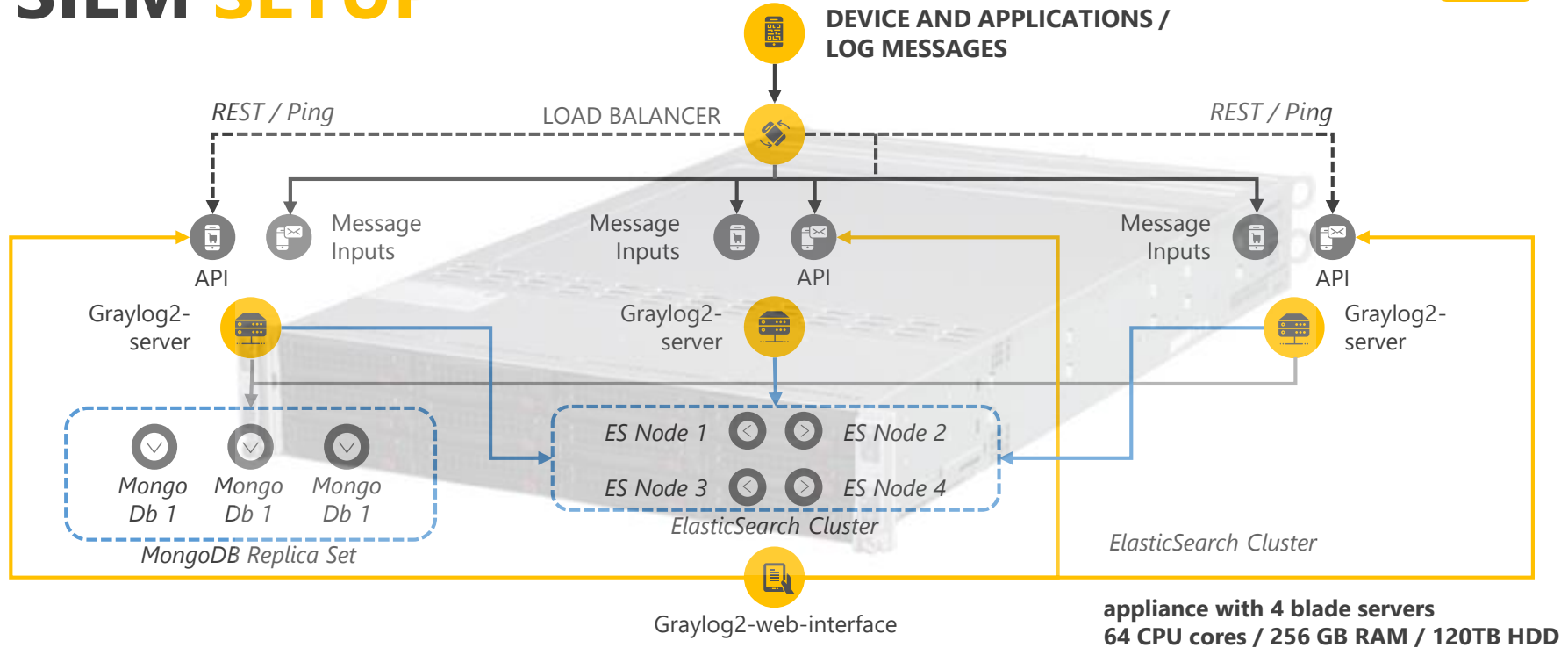
- › As many as needed
- › Low or high interaction
- › Different services : file, web, VOIP, DB,..



Vulnerability scanning

- › Launched from sensor
- › Customized zones and scheduling
- › Helps to prioritize and understand alerts

SIEM SETUP



Hardware VS Virtual platform



AND MORE...

OTHER FEATURES AND SERVICES



- 01** Keyword monitoring (threat intel)
- 02** Canaries
- 03** Sandbox
- 04** Regular security reports
- 05** Phishing tests
- 06** Cyber security awareness





THANK YOU !

QUESTIONS ?

SEE YOU SOON


Hacknowledge