TLP:GREEN

RNEP-GW

MÓDULO SIEM

fct csirt

RNEP-GW

GESTÃO DE LOGS

GESTÃO DE LOGS - LOG MANAGEMENT (LM)

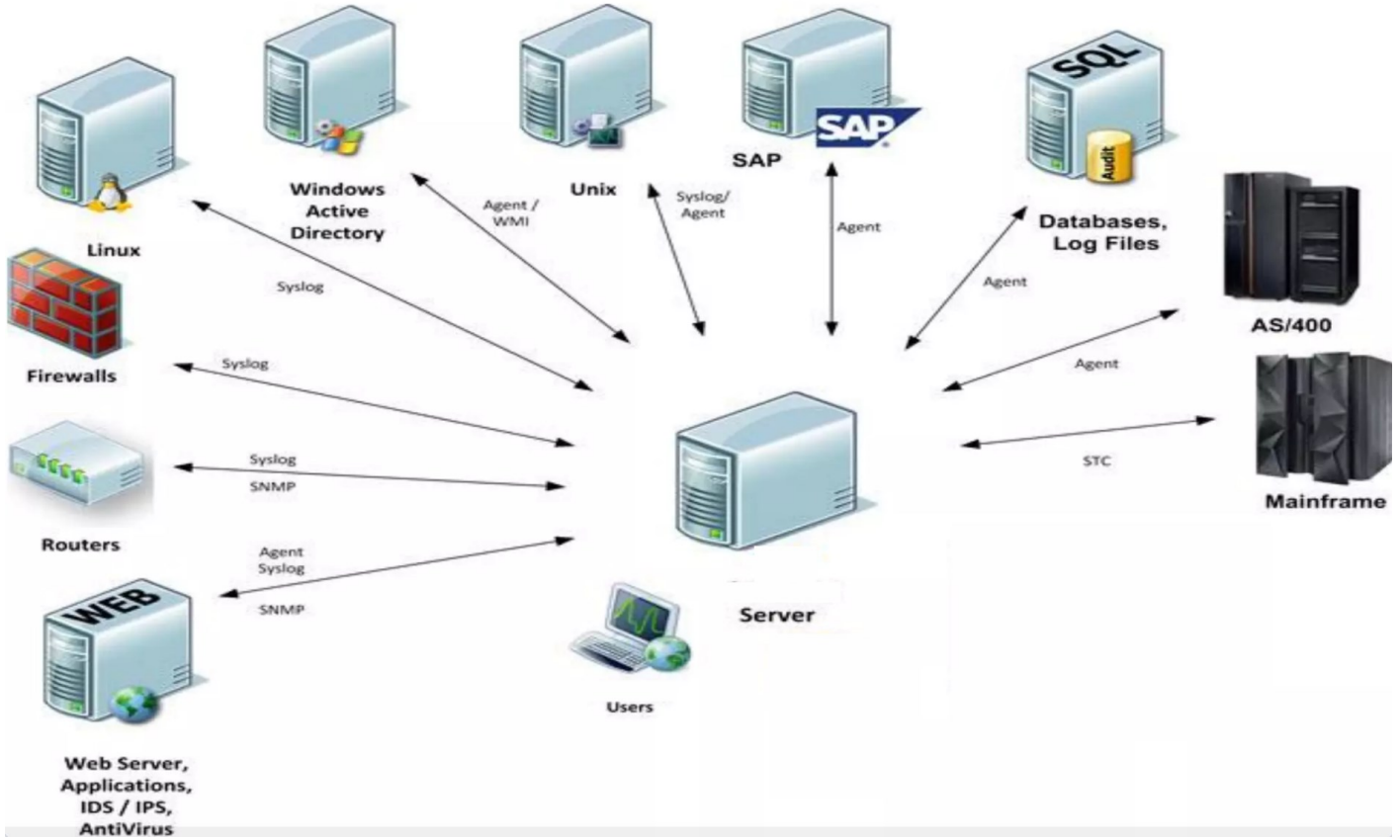
Guardar

Centralizar

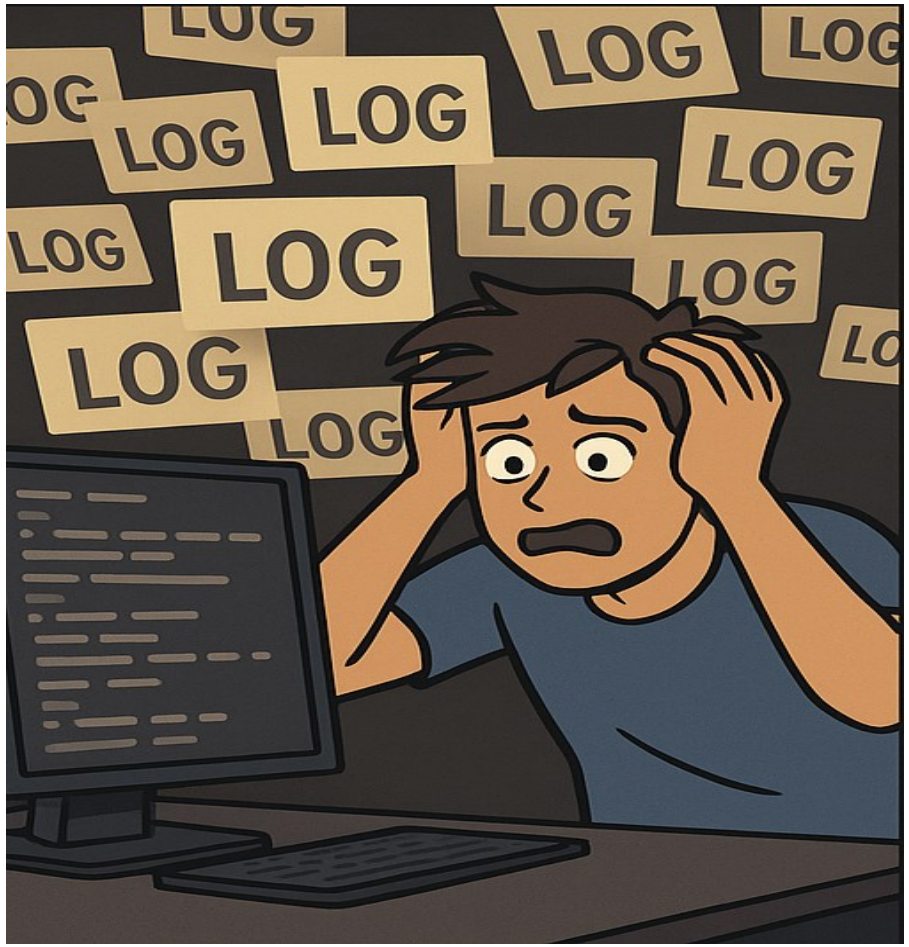
Retenção

Relatórios

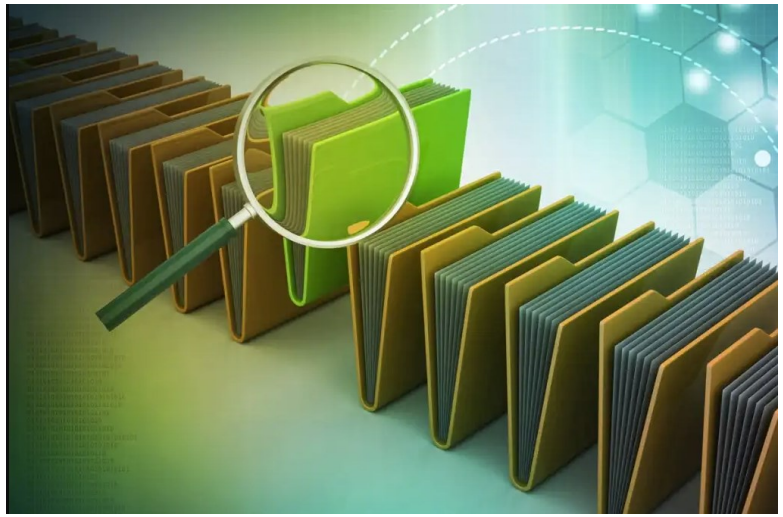
Procura



GESTÃO DE LOGS - DESAFIOS



5d2ffe44d5-1695975517	4.41M
693760ce98-1695975517	4.41M
2798493004-1695975517	4.40M
ba99d2f950-1695975517	4.40M
bbbe0fcdae-1695975517	4.13M
6caa87543e-1695975516	3.94M
cd38b98fe0-1695975516	3.94M
aeeed0f904-1695975516	3.93M
e7a35aa138-1695975516	3.93M
4177748c14-1695975516	3.71M
dbdc3a7393-1695975518	2.17M
1203480ee4-1695975518	2.17M
5a244954d2-1695975518	2.17M
d9cb718530-1695975518	2.17M



GESTÃO DE LOGS - DESAFIOS

Analisar logs

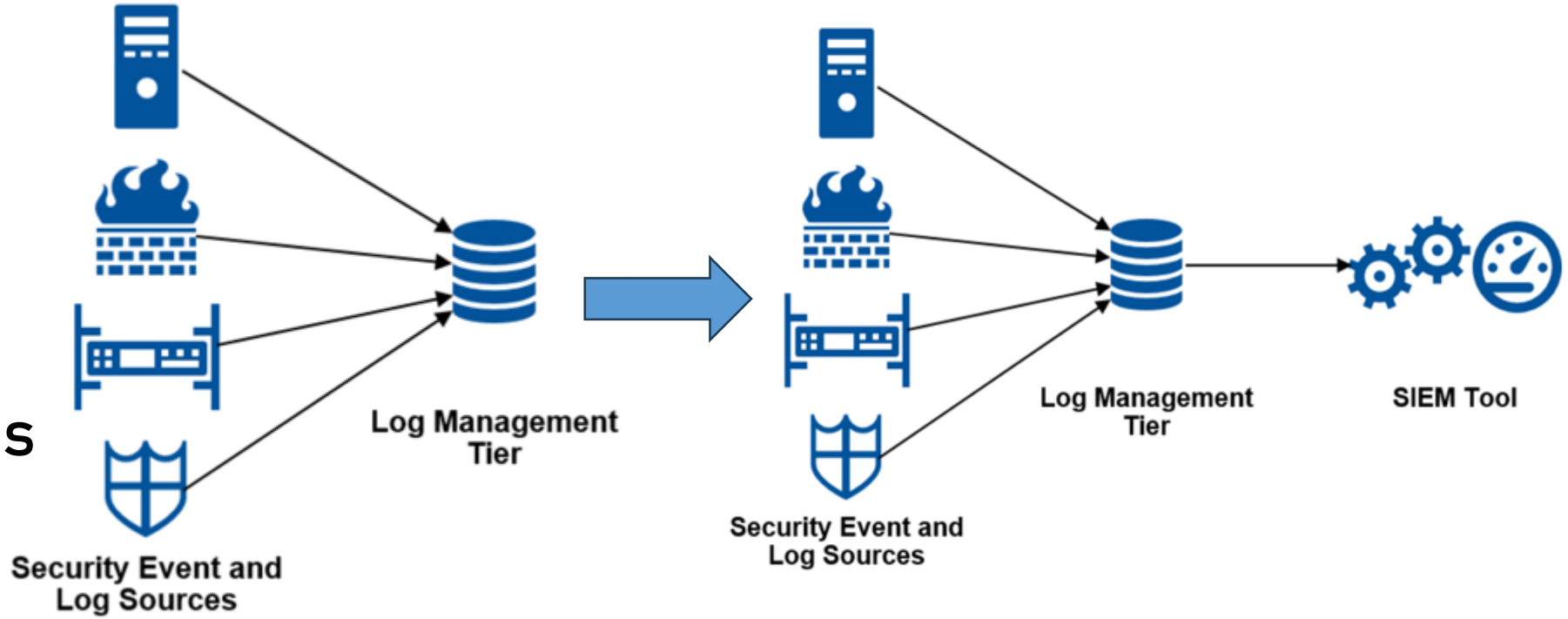
- Segurança

Centralizar

Compliance

Root Cause Analysis

Correlacionar



SIEM

SIEM

SIEM - OBJECTIVOS

Recolher logs

- Auditorias
- Segurança
- Compliance

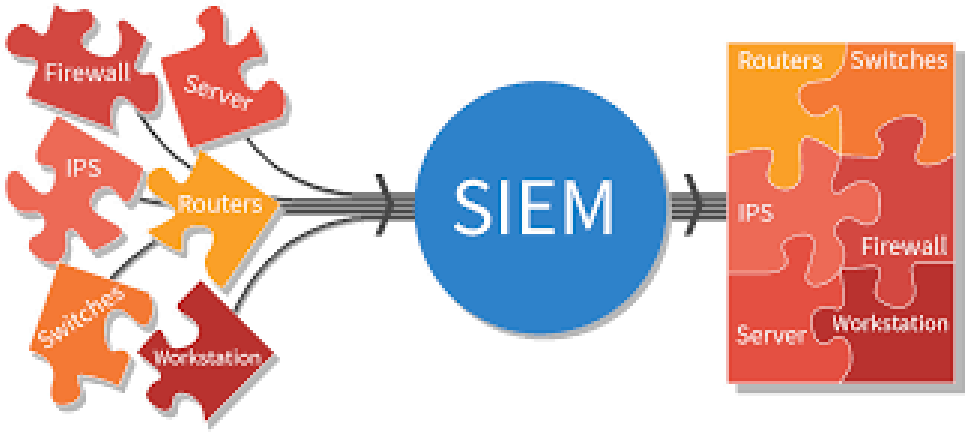
Identificar

- Ameaças
- Fugas de informação

Investigações

Relatórios

Dashboards



SIEM VS LM

Functionality	Security Information and Event Management (SIEM)	Log Management (LM)
Log collection	Collect security relevant logs + context data	Collect all logs
Log pre-processing	Parsing, normalization, categorization, enrichment	Indexing, parsing or none
Log retention	Retail parsed and normalized data	Retain raw log data
Reporting	Security focused reporting	Broad use reporting
Analysis	Correlation, threat scoring, event prioritization	Full text analysis, tagging
Alerting and notification	Advanced security focused reporting	Simple alerting on all logs
Other features	Incident management, analyst workflow, context analysis, etc.	High scalability of collection and storage

SIEM - SOLUÇÕES

Alternativas Comerciais:

- AlienVault Unified Security Management
- ArcSight ESM
- IBM Q Radar
- McAfee ESM
- Solarwinds Log & Event Manager
- Splunk

Alternativas Open-Source:

- AlienVault OSSIM
- Elasticsearch + Logstash + Kibana (ELK)
- OSSEC
- Wazuh

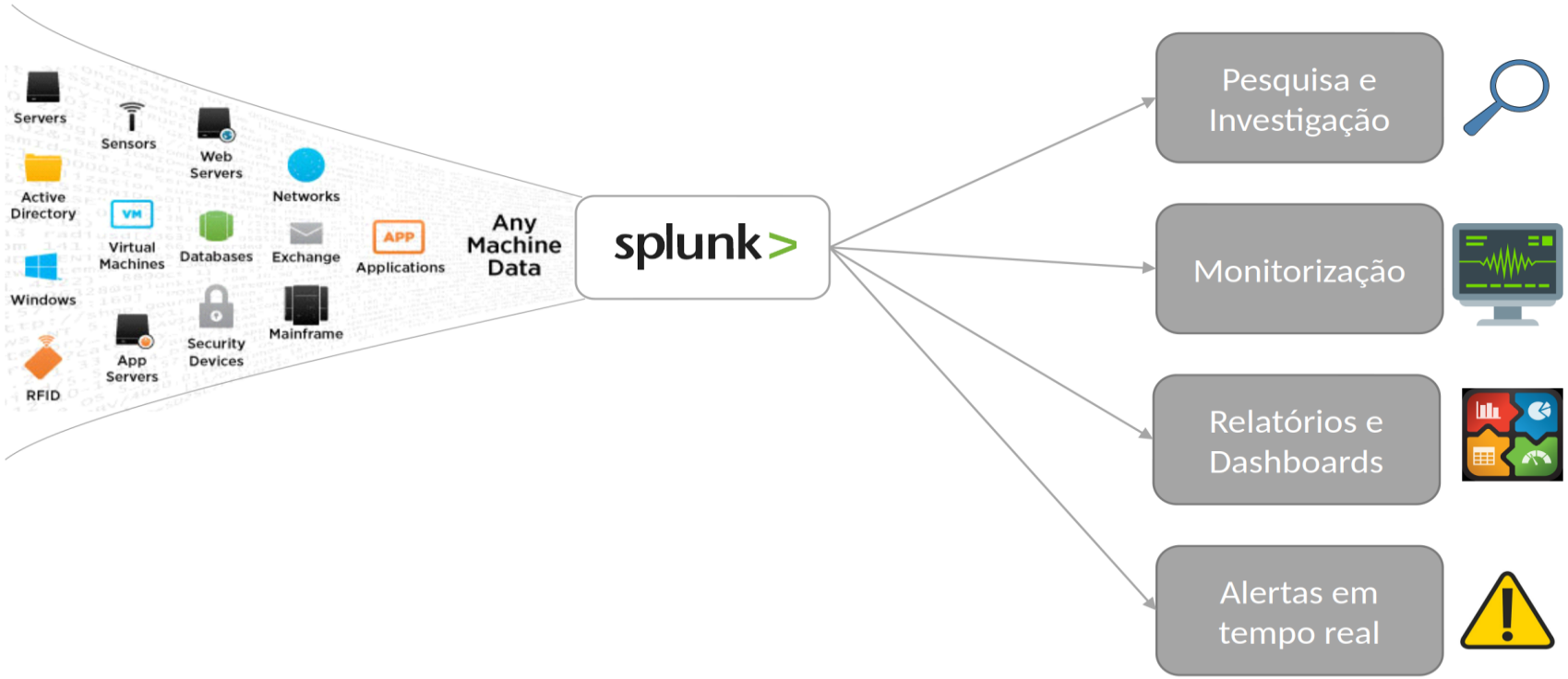
SIEM - SPLUNK

- Enterprise
- Cloud

- Gratuita
- Comercial

- Splunk Forwarder
- Splunk Indexer
- Splunk Search Head

- Apps & Add-ons



SIEM – PORQUE PRECISAMOS DE UM SIEM?

Fuga de informação

- Ameaças externas
- Ameaças internas

Ataques

- Inteligentes
- Sofisticados
- Complexos

Logs

- Mais
- Maiores

SIEM - CARACTERÍSTICAS

SIEM - WORKFLOW

SIEM - VANTAGENS

LOG COLLECTION

Universal Log Collection

Log collection method

- Agente
- Sem agente

Centralized log collection

USER ACTIVITY

Monitorização de actividades

- Sistemas
- Utilizadores

CORRELAÇÃO LIVE

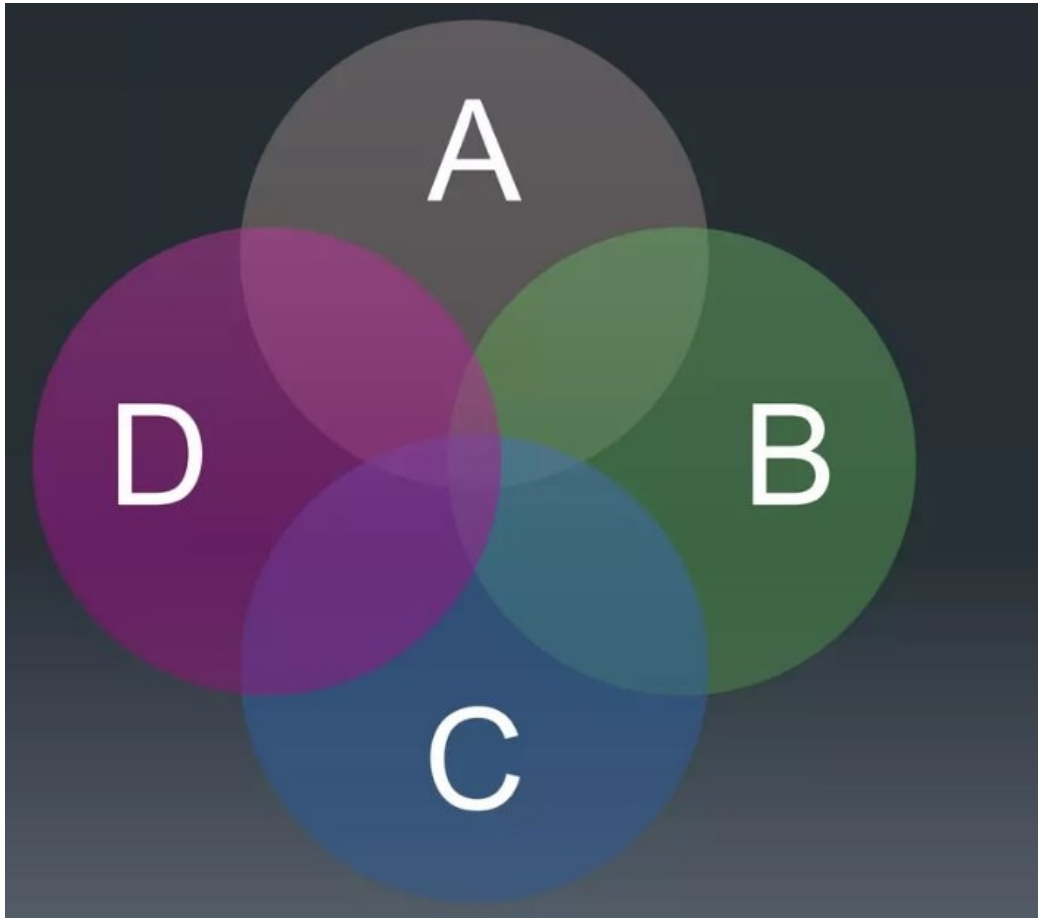
Tempo Real

Correlacionar eventos
- Network
- Sistemas
- Aplicacionais

Regras

Pesquisas

Alertas



RETENÇÃO DE LOGS

Guardar centralmente
- Sistemas
- Dispositivos
- Aplicações

Protecção contra adulteração

Facilidade de consultar e correlacionar

RELATÓRIOS

Regulamentos

Facilidade

Customizar

Visualização

INTEGRIDADE

Integridade
- Ficheiros
- Pastas

Alterações
- Criadas
- Acedidas
- Vistas
- Apagadas
- Modificadas
- Renomeadas
- ...

Alertas

ANALISES FORENSES

Investigar
Localizar
Encontrar
Raw Data

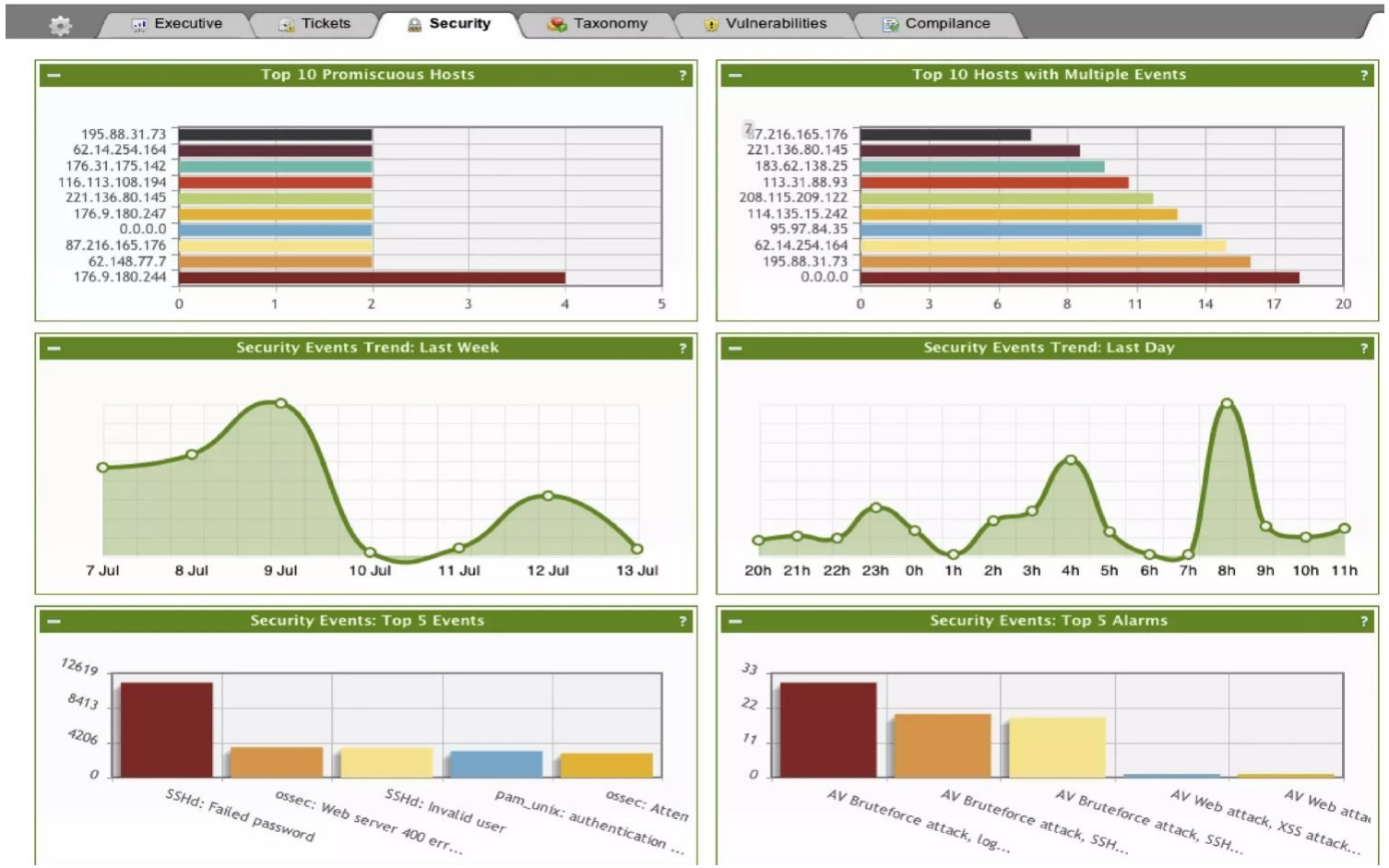
- Intuitivo
- User friendly

DASHBOARDS

Perspectiva

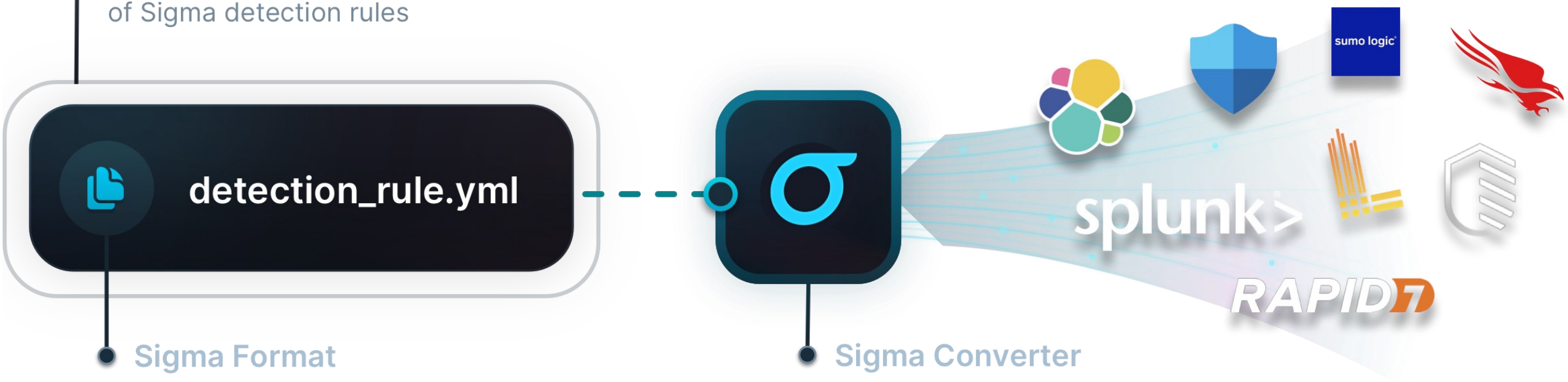
Apresentar

Costumizar



INTEROPERABILIDADE - SIGMA

Rule Packs
Community-compiled packs
of Sigma detection rules



Sigma Format
Generic, sharable detection rules

Sigma Converter
Converts Rules to any
supported SIEM Query

SIEM - FALHAS

SIEM - FALHAS

Planeamento

Implementação

Operacional

> Security is not a product, but a process.
>
> Bruce Schneier

IDEIAS CHAVE

- Um SIEM é uma peça central do funcionamento de qualquer equipa de segurança

- Permite construir dashboards e gerar alertas a partir de pesquisas efetuadas

- A optimização de um SIEM é uma tarefa recorrente e contínua

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc