

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

SIEM - SPLUNK

Fábio Mestre



splunk>



Agenda

- O que é um SIEM?
- Qual o propósito de um SIEM?
- Como funciona um SIEM?
- SIEM conhecidos
- SPLUNK
- Regras Sigma
- Duvidas e questões



O QUE É UM SIEM?

COMO FUNCIONA?

O que é um SIEM?

- Um SIEM, ou **Security Information and Event Management**, é uma solução de segurança que oferece análise, monitorização e correlação de eventos de segurança em tempo real, bem como a agregação e gravação de informação para processos de *compliance* e auditoria.

Qual o propósito de um SIEM?

- O objetivo de um SIEM é agregar logs e eventos de uma forma centralizada, de modo a permitir correlação e normalização da informação para gerar alertas e/ou incidentes, com base em regras específicas.
- O SIEM permite ter uma visão global de possíveis ameaças à rede ou infraestrutura, que seria muito difícil ou impossível de manter com ferramentas separadas ou verificações manuais.

Qual o propósito de um SIEM?

- Um SIEM disponibiliza três funcionalidades importantes:
 - Detecção de Ameaças em tempo real
 - Investigação de incidentes de segurança
 - Diminuição de tempo de resposta aos eventos de segurança detetados

Como funciona um SIEM

- Um SIEM recebe dados de eventos produzidos por aplicações, serviços, netflows, infraestrutura, sistemas e logs, analisa os dados em tempo real e gera alertas com base em regras.
- Esses dados são obtidos por uma de duas maneiras: via um agente configurado em cada uma das máquinas/servidores/dispositivos ou via serviços como SSH, WMI entre outros.

Lista de alguns SIEM conhecidos

- Alternativas Comerciais:

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



- Alternativa Open-Source:

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



SPLUNK

Splunk

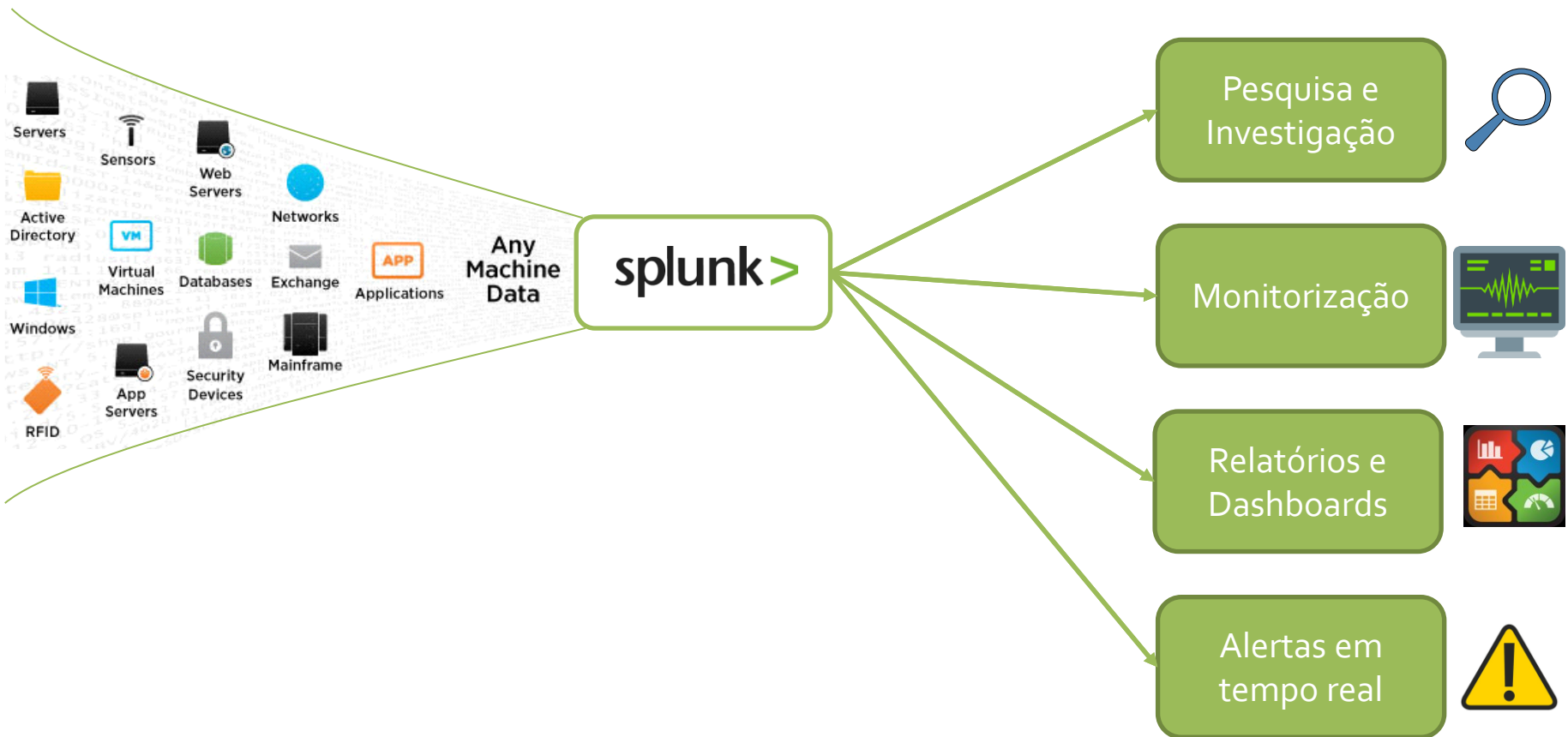
- O SPLUNK é um software que pode ser utilizado como um SIEM, que permite agregar, analisar, transformar, visualizar, partilhar e realizar diversas operações sobre dados obtidos das mais diversas fontes, tais como computadores, dispositivos de rede, máquinas virtuais, emails, bases de dados entre outros.



Splunk

- Disponível em duas variantes:
 - Splunk Enterprise
 - Splunk Cloud
- Versão gratuita (trial) e versão paga:
 - https://www.splunk.com/pt_br/view/SP-CAAAE8W

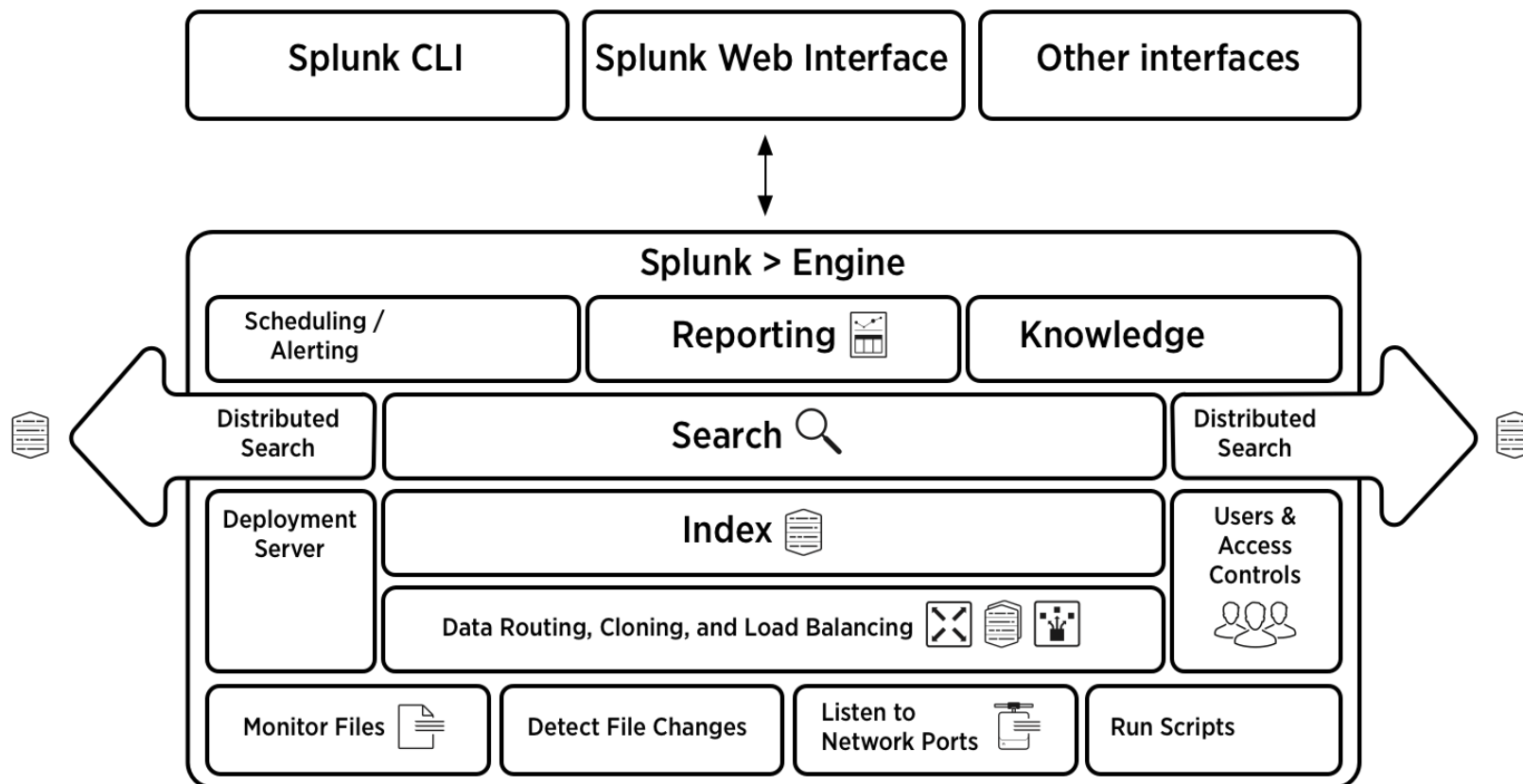
Splunk – Fluxo de Dados



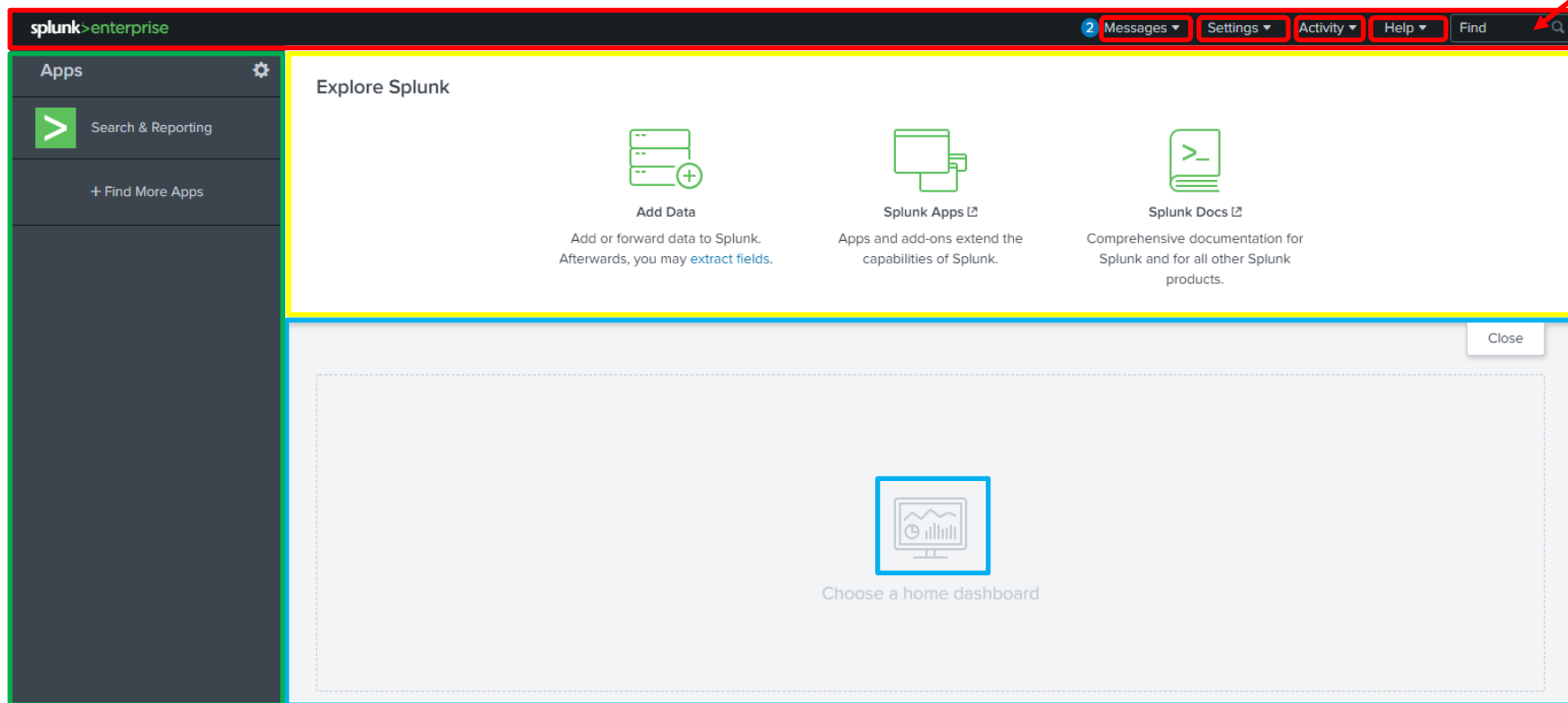
Splunk – Componentes

- O Splunk está dividido em três componentes principais:
 - Splunk Forwarder
 - Splunk Indexer
 - Splunk Search Head

Splunk - Arquitetura



Splunk - Navegação




Splunk – Adicionar dados

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources


Q



Cloud computing

Get your cloud computing data in to the Splunk platform.


10 data sources



Networking

Get your networking data in to the Splunk platform.


2 data sources



Operating System

Get your operating system data in to the Splunk platform.

1 data source




Security

Get your security data in to the Splunk platform.

3 data sources

4 data sources in total


Or get data in with the following methods



Upload

files from my computer


Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



Monitor

files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



Forward

data from a Splunk forwarder

Files - TCP/UDP - Scripts

Categorias:

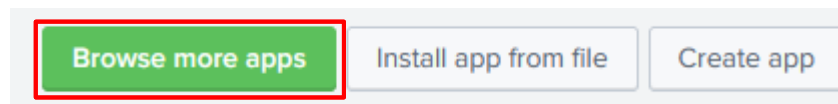
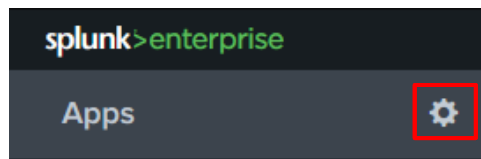
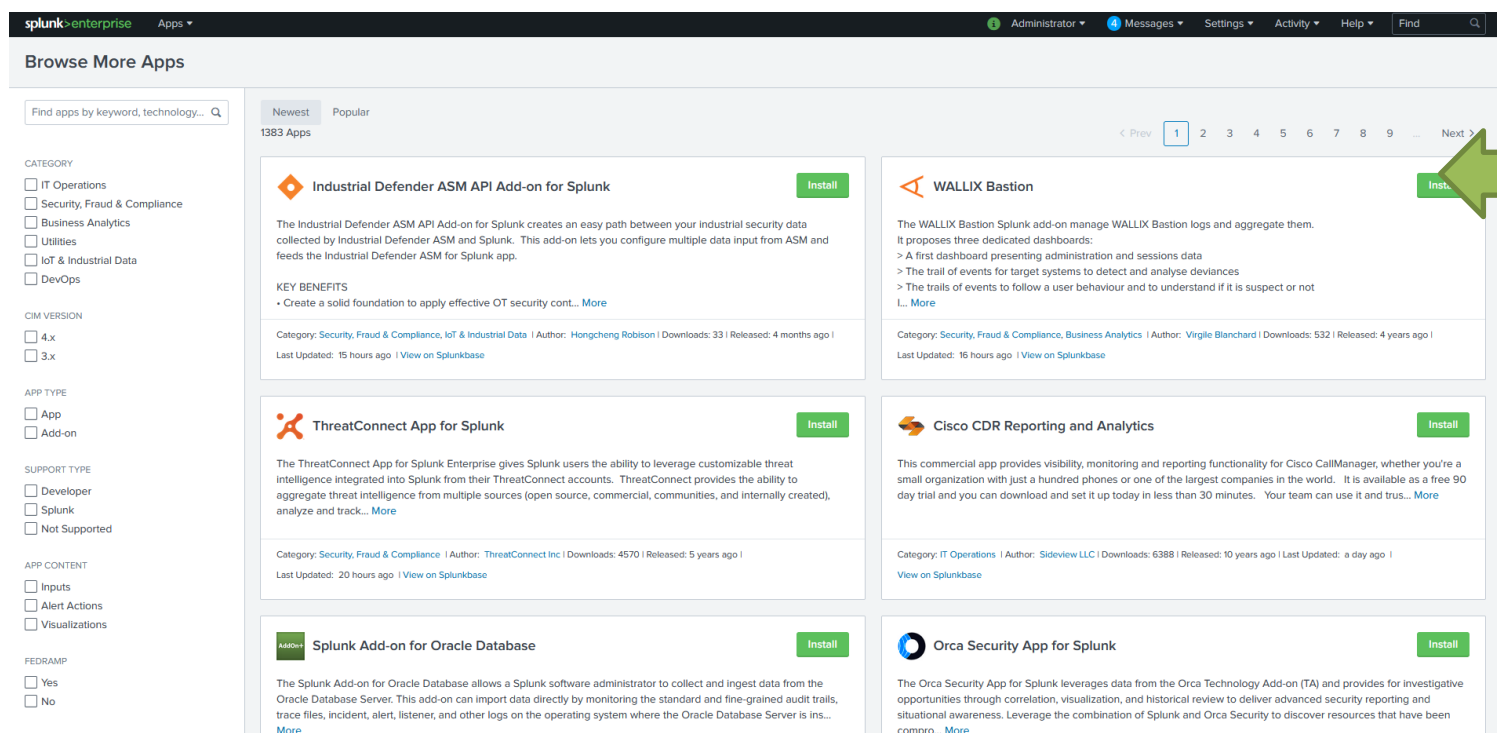
- Ficheiros e diretorias
- Eventos de rede
- Infraestrutura
- Cloud
- Bases de dados
- Endpoint Security
- Virtualização
- Windows
- APIs, HTTP
- Scripts

Splunk Apps & Addons

- O Splunk disponibiliza a capacidade de instalar aplicações e addons, com o propósito de aumentar as funcionalidades e capacidades da aplicação:
 - Um addon é por norma um único componente que pode ser reutilizado diversas vezes.
 - Uma aplicação pode ser construída em cima de diferentes addons para criar algo com um determinado propósito.

splunkbase™

Splunk Apps & Addons

Browse More Apps

Find apps by keyword, technology...

CATEGORY

- ☐ IT Operations
- ☐ Security, Fraud & Compliance
- ☐ Business Analytics
- ☐ Utilities
- ☐ IoT & Industrial Data
- ☐ DevOps

CIM VERSION

- ☐ 4.x
- ☐ 3.x

APP TYPE

- ☐ App
- ☐ Add-on

SUPPORT TYPE

- ☐ Developer
- ☐ Splunk
- ☐ Not Supported

APP CONTENT

- ☐ Inputs
- ☐ Alert Actions
- ☐ Visualizations

FEDRAMP

- ☐ Yes
- ☐ No

1383 Apps

Industrial Defender ASM API Add-on for Splunk [Install](#)

The Industrial Defender ASM API Add-on for Splunk creates an easy path between your industrial security data collected by Industrial Defender ASM and Splunk. This add-on lets you configure multiple data input from ASM and feeds the Industrial Defender ASM for Splunk app.

KEY BENEFITS

- Create a solid foundation to apply effective OT security cont... [More](#)

Category: Security, Fraud & Compliance, IoT & Industrial Data | Author: Hongcheng Robison | Downloads: 33 | Released: 4 months ago | Last Updated: 15 hours ago | [View on Splunkbase](#)

WALLIX Bastion [Install](#)

The WALLIX Bastion Splunk add-on manage WALLIX Bastion logs and aggregate them. It proposes three dedicated dashboards:

- > A first dashboard presenting administration and sessions data
- > The trail of events for target systems to detect and analyse deviances
- > The trails of events to follow a user behaviour and to understand if it is suspect or not

[L... More](#)

Category: Security, Fraud & Compliance, Business Analytics | Author: Virgile Blanchard | Downloads: 532 | Released: 4 years ago | Last Updated: 16 hours ago | [View on Splunkbase](#)

ThreatConnect App for Splunk [Install](#)

The ThreatConnect App for Splunk Enterprise gives Splunk users the ability to leverage customizable threat intelligence integrated into Splunk from their ThreatConnect accounts. ThreatConnect provides the ability to aggregate threat intelligence from multiple sources (open source, commercial, communities, and internally created), analyze and track... [More](#)

Category: Security, Fraud & Compliance | Author: ThreatConnect Inc | Downloads: 4570 | Released: 5 years ago | Last Updated: 20 hours ago | [View on Splunkbase](#)

Cisco CDR Reporting and Analytics [Install](#)

This commercial app provides visibility, monitoring and reporting functionality for Cisco CallManager, whether you're a small organization with just a hundred phones or one of the largest companies in the world. It is available as a free 90 day trial and you can download and set it up today in less than 30 minutes. Your team can use it and trust... [More](#)

Category: IT Operations | Author: Sideview LLC | Downloads: 6388 | Released: 10 years ago | Last Updated: a day ago | [View on Splunkbase](#)

Splunk Add-on for Oracle Database [Install](#)

The Splunk Add-on for Oracle Database allows a Splunk software administrator to collect and ingest data from the Oracle Database Server. This add-on can import data directly by monitoring the standard and fine-grained audit trails, trace files, incident, alert, listener, and other logs on the operating system where the Oracle Database Server is ins... [More](#)

Orca Security App for Splunk [Install](#)

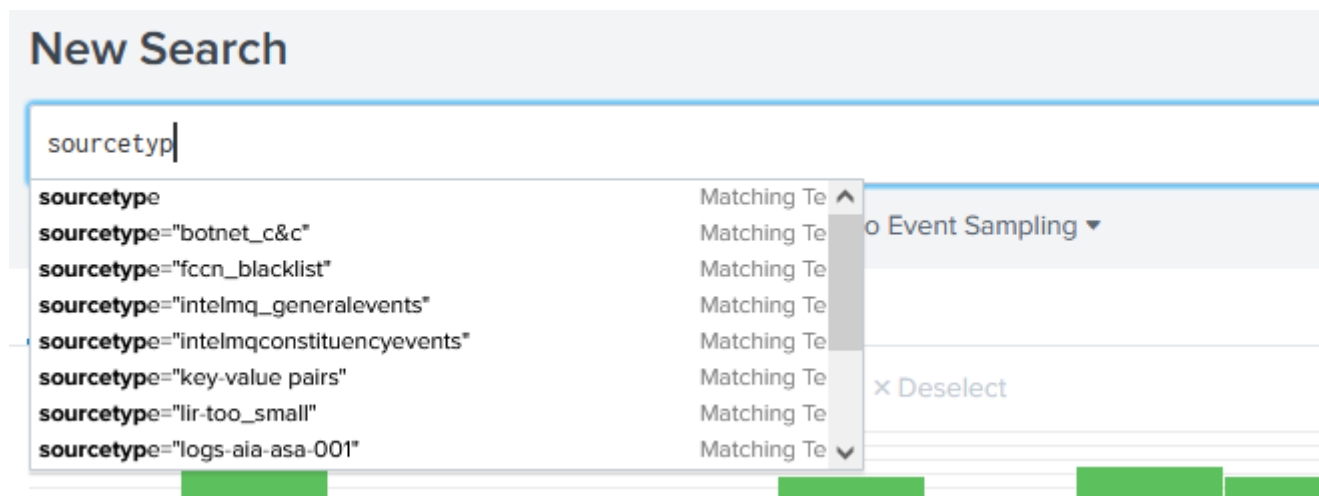
The Orca Security App for Splunk leverages data from the Orca Technology Add-on (TA) and provides for investigative opportunities through correlation, visualization, and historical review to deliver advanced security reporting and situational awareness. Leverage the combination of Splunk and Orca Security to discover resources that have been compro... [More](#)

Splunk – Search & Reporting

- Aplicação instalada por defeito, também chamada de aplicação de pesquisa.
- Utilizada para efetuar pesquisas nos dados recebidos pelo Splunk, utilizando uma linguagem chamada SPL (Search Processing Language).

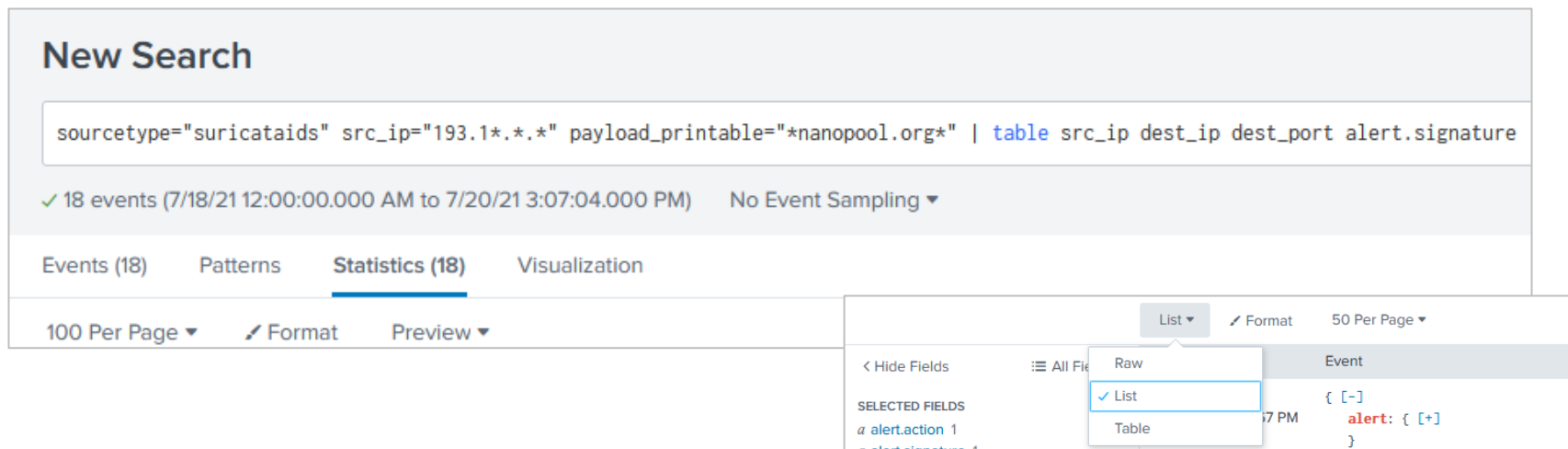
Splunk – Search & Reporting

- Dispõe de uma forma de IntelliSense para auxiliar na construção das queries.



Splunk – Search & Reporting

- Uma pesquisa no Splunk consiste uma serie de comandos e argumentos encadeados, de forma a obter eventos, extrair, transformar e analisar informação a partir dos dados indexados.



New Search

sourcetype="suricataids" src_ip="193.1*.*.*" payload_printable="*nanopool.org*" | table src_ip dest_ip dest_port alert.signature

✓ 18 events (7/18/21 12:00:00.000 AM to 7/20/21 3:07:04.000 PM) No Event Sampling ▼

Events (18) Patterns **Statistics (18)** Visualization

100 Per Page ▼ Format Preview ▼

< Hide Fields ≡ All Fields List ▼ Format 50 Per Page ▼
 SELECTED FIELDS
 a alert.action 1
 a alert.signature 1

Raw
☒ List
 Table

Event
 { [-]
 7 PM alert: { [+]
 }

Splunk – Search & Reporting

- É possível definir também o intervalo de tempo sobre a qual a pesquisa assenta, com a opção de escolher uma predefinição ou personalização:

Presets

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

Relative

Real-time

Date Range

Date & Time Range

Advanced

Relative

Earliest:

5

Days Ago

Latest:

Now

Beginning of today

6/26/21 12:00:00.000 AM

No snap-to

Beginning of day

6/21/21 3:47:28.000 PM

Apply

Real-time

Earliest:

15

Months Ago

Latest:

now

3/26/20 3:54:57.000 PM

Apply

Splunk – Search & Reporting

- É também possível efetuar pesquisa por datas e pesquisas avançadas:

▼ Date Range

Between ▼ 06/25/2021 and 06/26/2021
00:00:00 24:00:00

Apply

▼ Date & Time Range

Between ▼ 07/18/2021 00:00:00.000 and 07/20/2021 16:22:57.000
HH:MM:SS.SSS HH:MM:SS.SSS

Apply

▼ Advanced

Earliest: Latest:

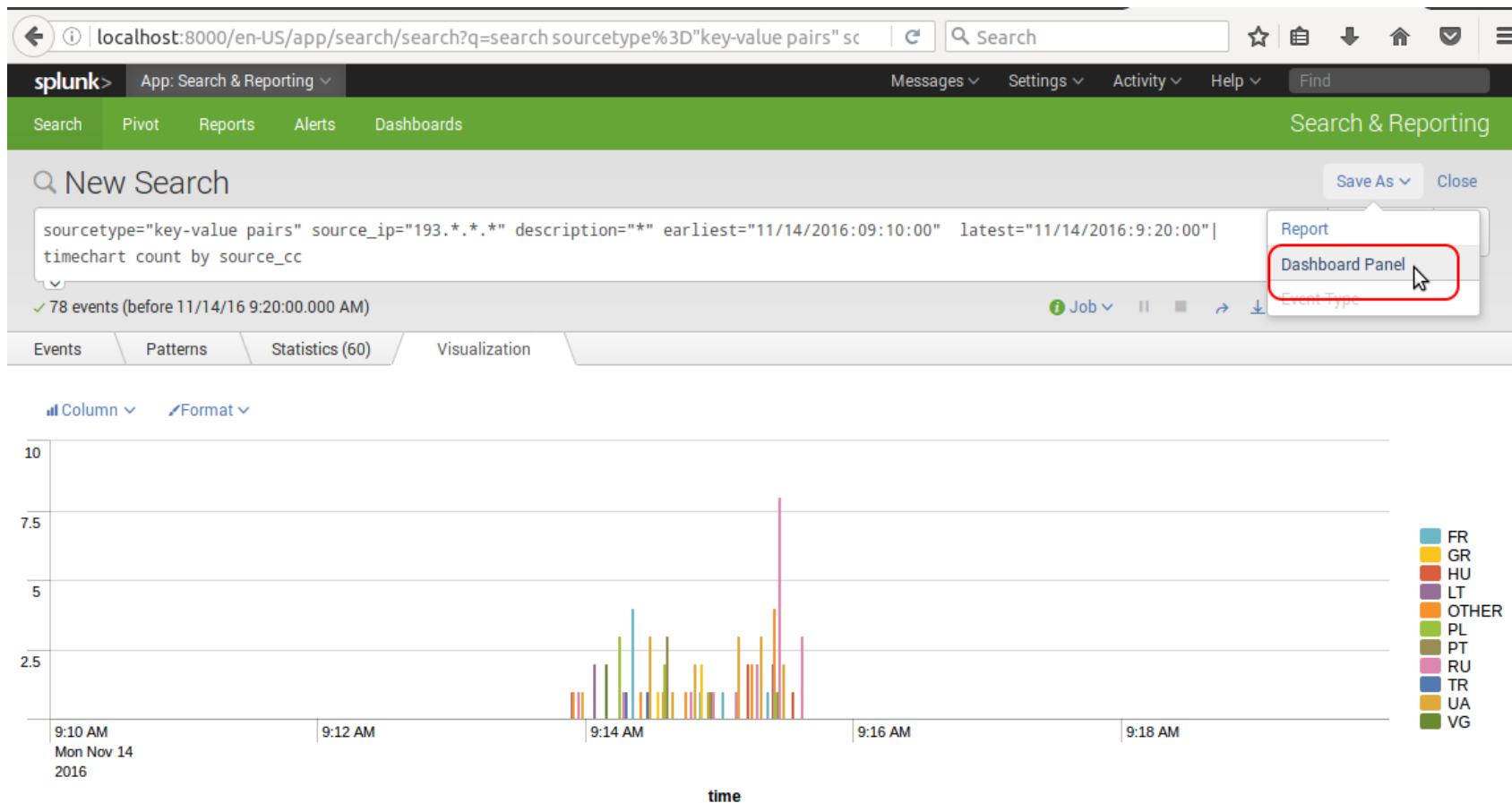
-3d@d -h@h
6/23/21 12:00:00.000 AM 6/26/21 3:00:00.000 PM

[Documentation](#) Apply

Splunk – Search & Reporting

- A sintaxe de comandos e filtros é extensa e permite efetuar pesquisas simples ou complexas. Um guia de referência pode ser encontrado em <https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf>.
- Mais detalhes sobre a sintaxe SPL em: <https://docs.splunk.com/Documentation/Splunk/8.2.3/SearchReference/UnderstandingSPLsyntax>

Splunk – Search & Reporting



REGRAS SIGMA

Splunk – Regras Sigma



<https://github.com/SigmaHQ/sigma> – Repositório do projeto

Splunk – Regras Sigma

splunk> App: Sigma Searches

Reports

Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report.
Open the report in Pivot or Search to refine the parameters or further explore the data.

63 Reports

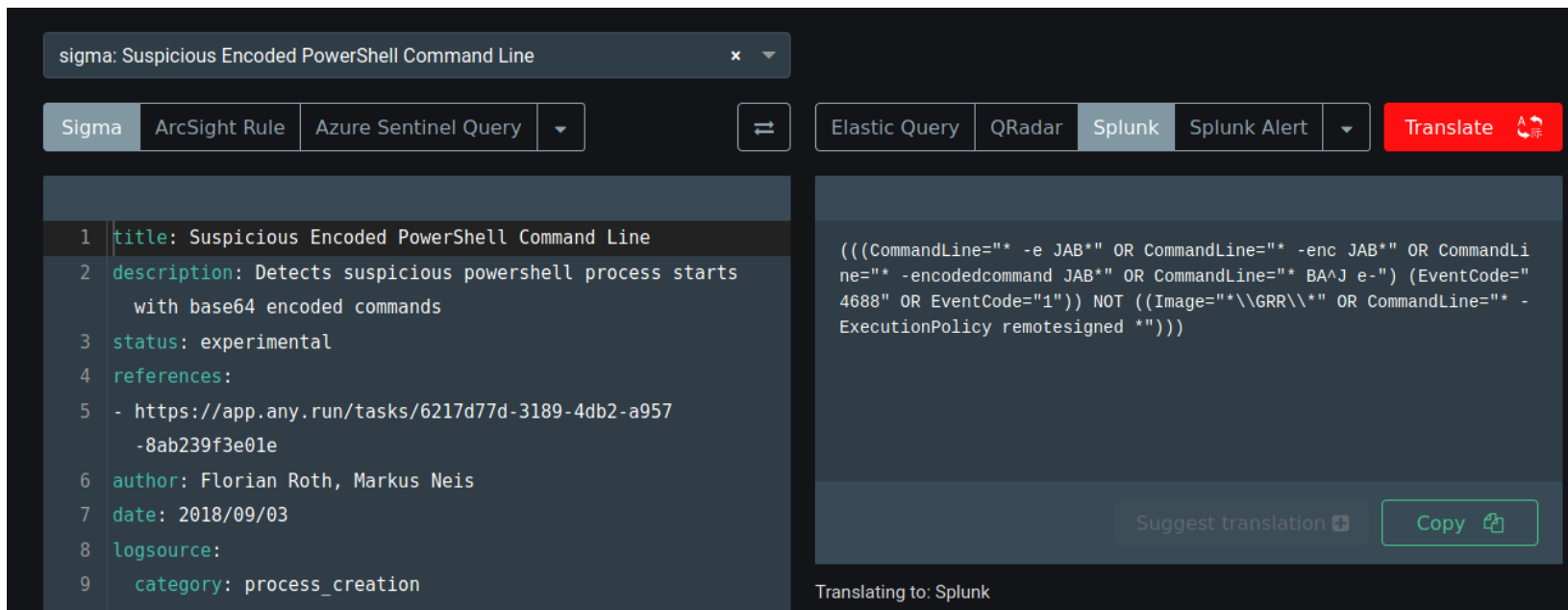
All Yours This App's filter

i	Title ^	Actions	Next Scheduled Time	Owner	App	Sharing
>	All Critical Severity Signatures	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	All High Severity Signatures	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	All Low Severity Signatures	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	All Medium Severity Signatures	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	critical:windows:sysmon - UAC Bypass via Event Viewer	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	critical:windows:unknown - Mimikatz Usage	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:apache:unknown - Apache Segmentation Fault	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:linux:clamav - Relevant ClamAV Message	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:linux:unknown - Buffer Overflow Attempts	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:linux:unknown - Suspicious Activity in Shell Commands	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:unknown:unknown - Webshell Detection by Keyword	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:windows:application - Relevant Anti-Virus Event	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:windows:powershell - Malicious PowerShell Commandlets	Open in Search Edit	None	nobody	TA-Sigma-Searches	App
>	high:windows:powershell - PowerShell PSAttack	Open in Search Edit	None	nobody	TA-Sigma-Searches	App

<https://github.com/dstaulcu/TA-Sigma-Searches> – Uma aplicação para o Splunk que contém uma série de relatórios derivados de regras sigma



Splunk – Regras Sigma



The screenshot shows the Sigma rule editor interface. At the top, a search bar contains the text "sigma: Suspicious Encoded PowerShell Command Line". Below the search bar, there are tabs for "Sigma", "ArcSight Rule", "Azure Sentinel Query", "Elastic Query", "QRadar", "Splunk", and "Splunk Alert". The "Sigma" tab is currently selected. The main area is divided into two panels. The left panel displays the Sigma rule in a structured format:

```
1 title: Suspicious Encoded PowerShell Command Line
2 description: Detects suspicious powershell process starts
  with base64 encoded commands
3 status: experimental
4 references:
5 - https://app.any.run/tasks/6217d77d-3189-4db2-a957
  -8ab239f3e01e
6 author: Florian Roth, Markus Neis
7 date: 2018/09/03
8 logsource:
9   category: process_creation
10  product: windows
```




The right panel displays the translated Splunk query:

```
((CommandLine="* -e JAB*" OR CommandLine="* -enc JAB*" OR CommandLi
ne="* -encodedcommand JAB*" OR CommandLine="* BA^J e-") (EventCode="
4688" OR EventCode="1")) NOT ((Image="*\\GRR\\*" OR CommandLine="* -
ExecutionPolicy remotesigned *")))
```

At the bottom of the right panel, there is a "Suggest translation" button and a "Copy" button. Below the translated query, it says "Translating to: Splunk".

<https://uncoder.io/> - Ferramenta online para converter regras Sigma

Em Resumo

-  Existem diversas alternativas ao SPLUNK mas é o que utilizamos no RCTS CERT.
-  Possui uma linguagem poderosa e flexível, capaz de criar pesquisas simples e complexas.
-  Permite construir *dashboards* e gerar alertas a partir de pesquisas efetuadas.



Obrigado