

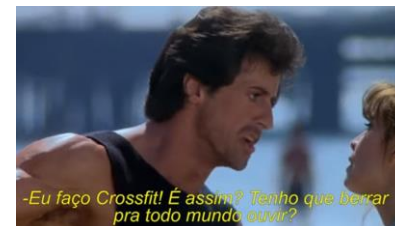


Como fazer uma jornada para nuvem quase sem turbulência

#TheDevConf 2021

#whoami

- Tales Casagrande
 - Catarinense
 - Recebo minhas correspondências em Curitiba
 - Cerveja – Café – Warzone – Gremista – Crossfiteiro
- Sales Engineer – Trend Micro
 - 14 anos na área de TI – 7 na área de Segurança
 - Formado em Análise e Desenvolvimento de Sistemas
 - Pós Graduado em Gestão de Projetos



SecurityForCloudBuilders



caf3ina



talescasagrande



Um mundo seguro para a troca de informações digitais

- Focada há mais de 30 anos em Cibersegurança
- Rentável desde a abertura do capital em 1998, com mais de US \$ 1,5 bilhão em vendas (FY2019)
- 500,000+ clientes comerciais
- 6800+ pessoas apaixonadas por segurança em mais de 65 países



Eva Chen, CEO e Co-founder da Trend Micro

Divulgação responsável para
fornecedores de software /
hardware



Inteligência de ameaças e pesquisa para
consumidores, empresas e governos



Parcerias públicas / privadas (por
exemplo, aplicação da lei)



Threats



Vulnerabilities
& Exploits



Targeted
Attacks



AI & ML



IoT



OT / IIoT



Cybercriminal
Undergrounds



Future Threat
Landscape



research

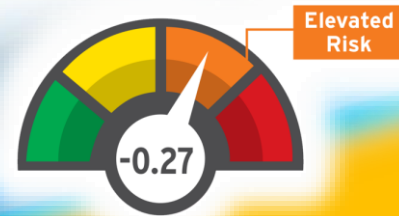


Trend Micro Core
Tecnologia & Produtos

Transformação Digital

*Nuvem,
Big data, AI, IoT,
Automação...*

Transformação Digital

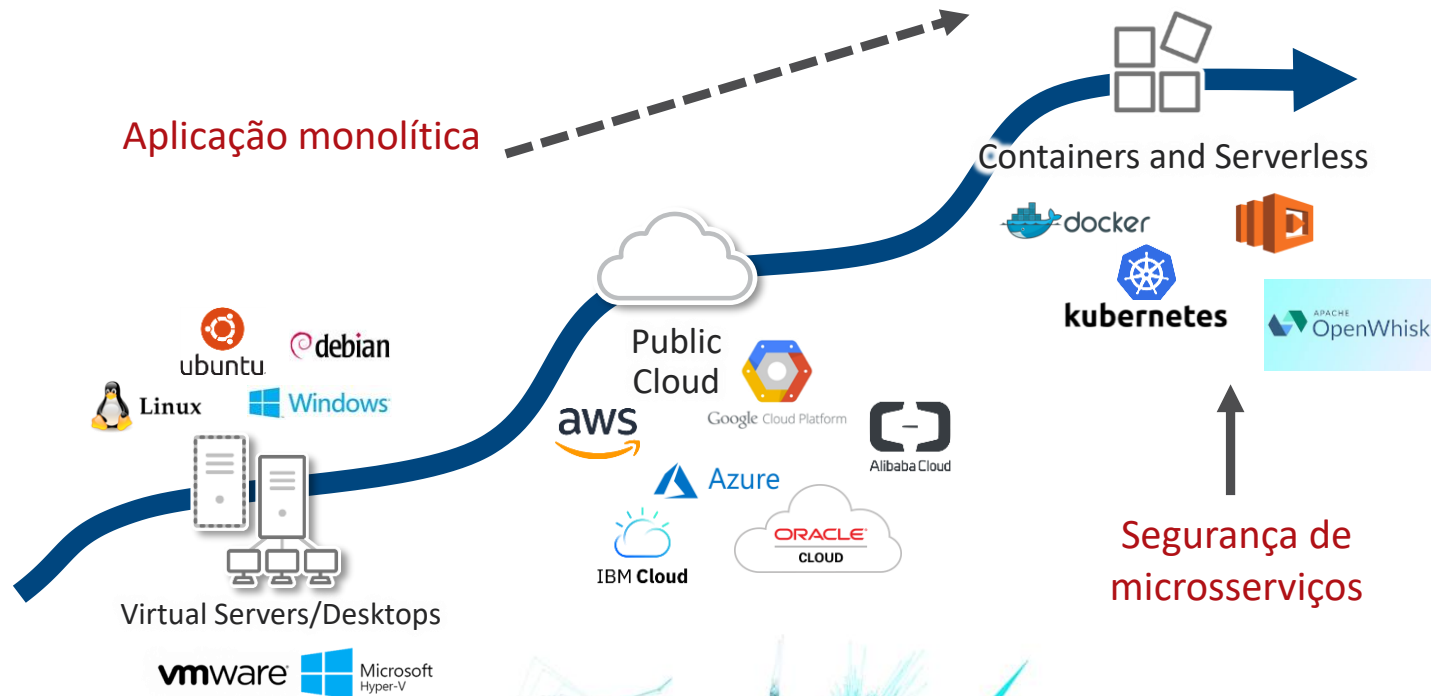


73% das organizações tiveram pelo menos uma violação de dados em 2019, 21% tiveram 7 ou mais

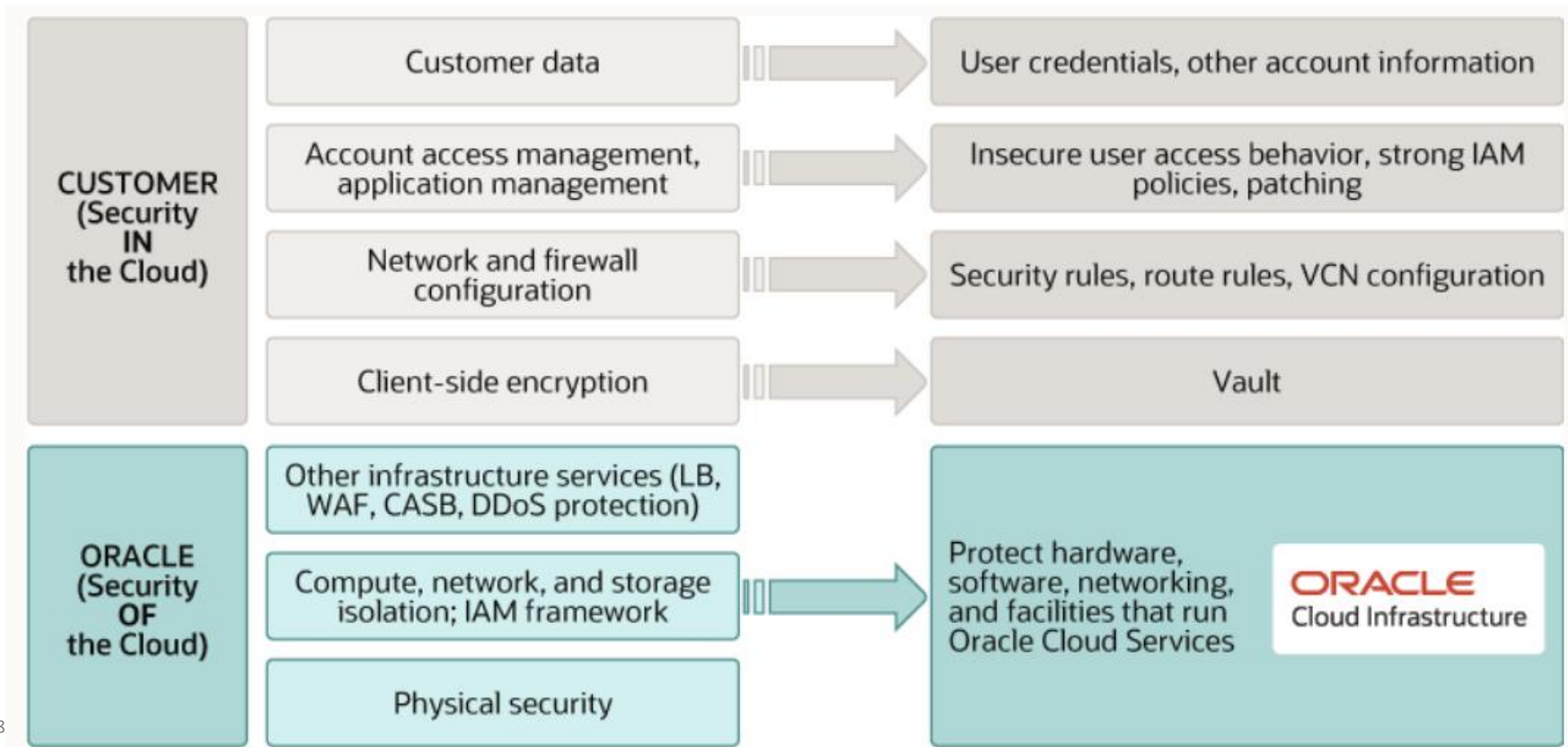
Os 2 principais problemas de risco são o **desalinhamento organizacional** e a complexidade geral

A falta de visibilidade e conectividade entre ambientes apresenta risco significativo

Mudanças de infraestrutura e aplicativos

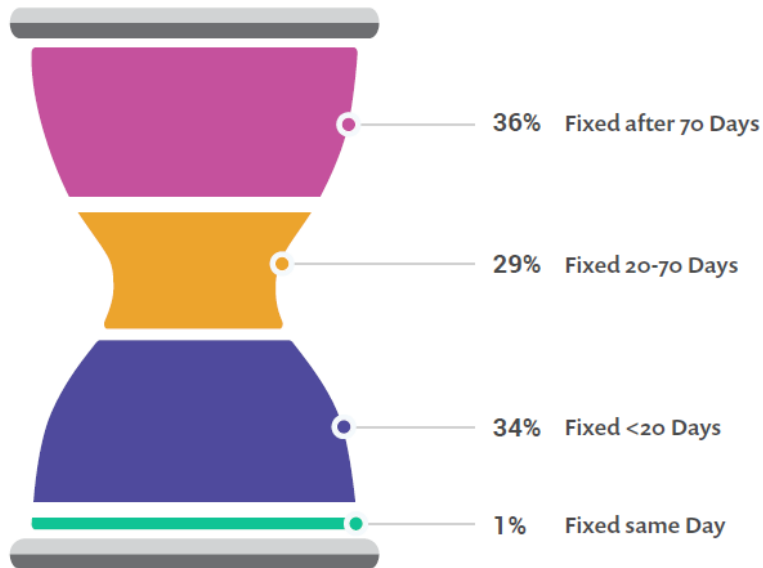


A tal da responsabilidade compartilhada...

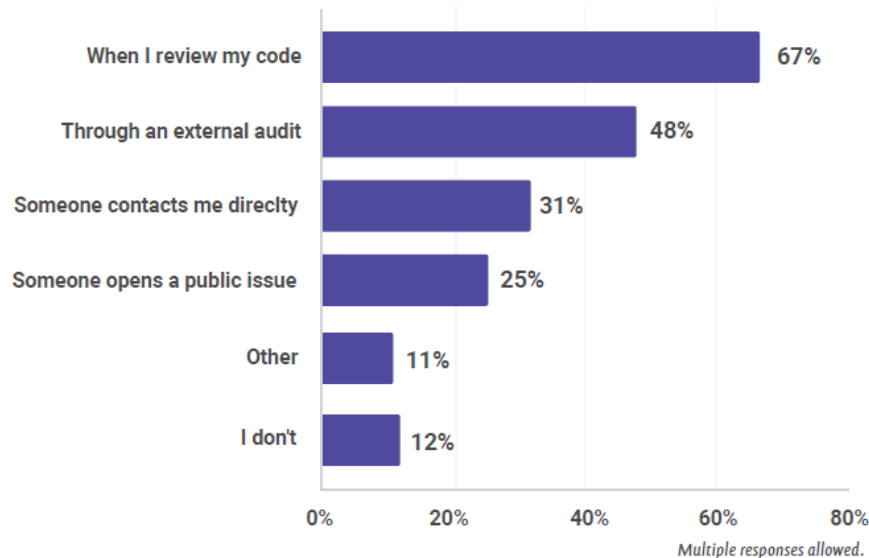


State of Open Source Security Report

Vulnerabilidades corrigidas em projetos verificados

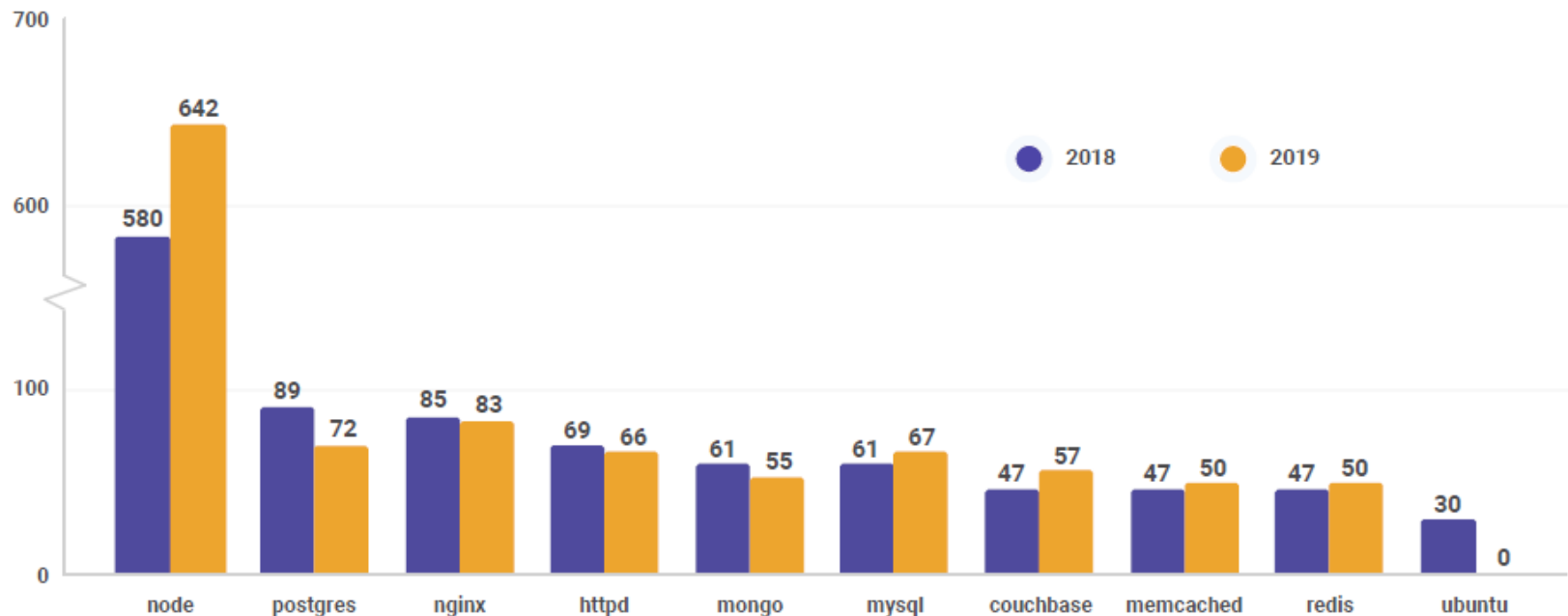


Como você descobre vulnerabilidades em seu código?



Docker IMAGES

Vulnerabilidades nas imagens oficiais do contêiner





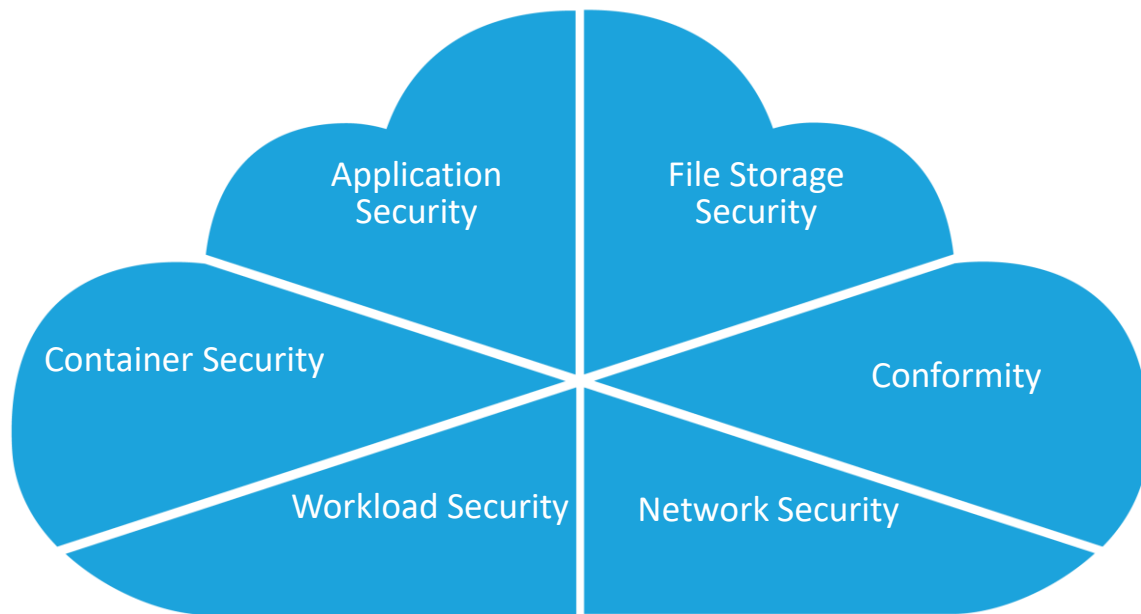
Você se identifica com esses questionamentos?

- Como posso ter visibilidade ante que as coisas vão longe demais?
- Como podemos saber que não existe nenhum conteúdo malicioso em nossos sistemas?
- Como a segurança se encaixa em nosso pipeline?
- Eu tenho um inventario de vulnerabilidades/bug da minha aplicação?
- Quanto tempo minha aplicação ficou “fora” devido um ataque?

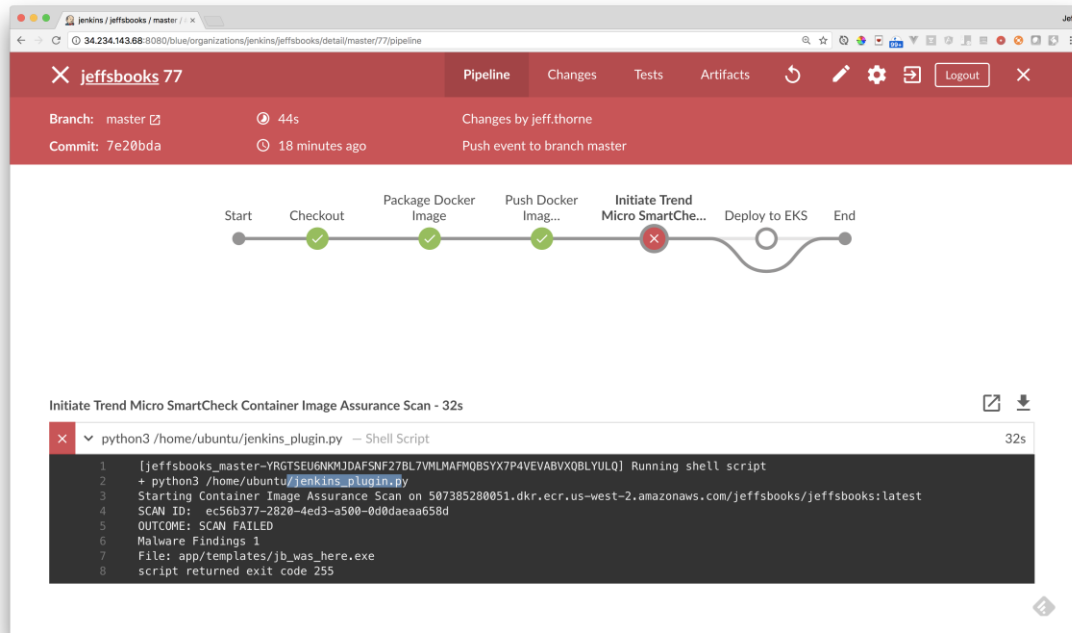


Trend Micro Cloud One™

Plataforma de Serviços de Segurança para Cloud Builders



Integração com Pipeline CI/CD



jenkins / jeffsbooks / master

jeffsbooks 77

Branch: master 44s Changes by jeff.thorne

Commit: 7e20bda 18 minutes ago Push event to branch master

Pipeline Changes Tests Artifacts

Start Checkout Package Docker Image Push Docker Image... Initiate Trend Micro SmartCheck Container Image Assurance Scan - 32s Deploy to EKS End

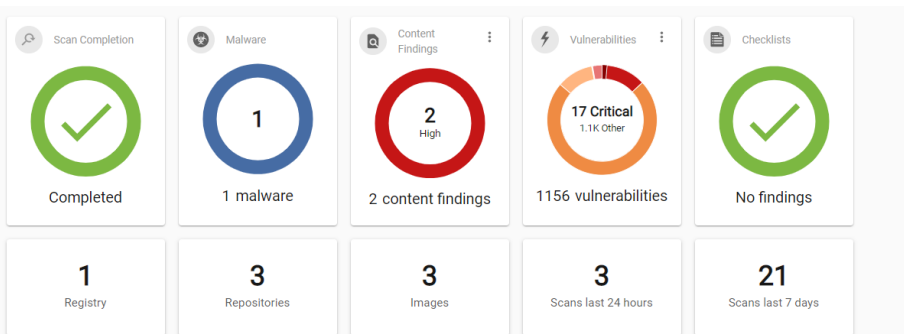
Initiate Trend Micro SmartCheck Container Image Assurance Scan - 32s

```
python3 /home/ubuntu/jenkins_plugin.py -- Shell Script 32s
1 [jeffsbooks_master-YRGTSEU6NMUJDAFNF27BL7VMLMAFMQBSYX7P4VEVABVXQ8LYULQ] Running shell script
2 + python3 /home/ubuntu/jenkins_plugin.py
3 Starting Container Image Assurance Scan on 507385280051.dkr.ecr.us-west-2.amazonaws.com/jeffsbooks/jeffsbooks:latest
4 SCAN ID: ec56b377-2820-4ed3-a500-0d0daaa658d
5 OUTCOME: SCAN FAILED
6 Malware Findings 1
7 File: app/templates/jb_was_here.exe
8 script returned exit code 255
```

Scan Integrado:

- Criar tarefa de scan no pipeline
- API para automação do scan
- Scan em qualquer estágio
- Bloqueio do Deploy baseado no resultado do scan
- Apenas imagens aprovadas podem prosseguir na esteira

Informações para Remediação



Registries

Registry Name

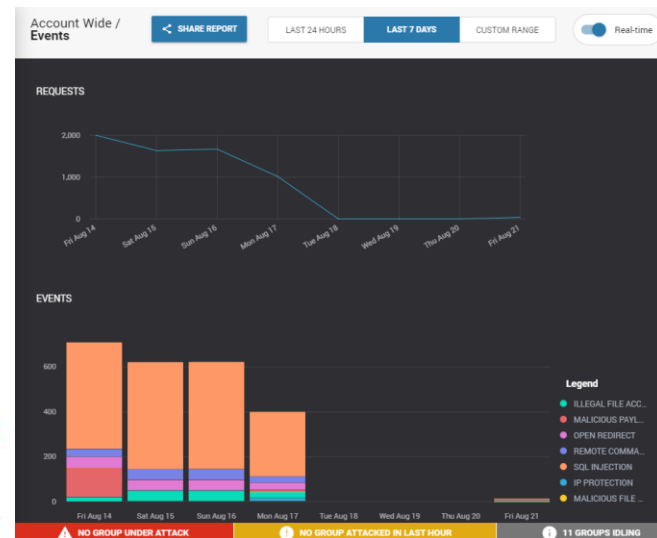
Nexus Rego

Other Findings			
<div>  Vulnerabilities: </div> <div> <div>Legend</div> <div>  Available in newer version </div> </div>			
Package	Severity	Vulnerabilities	
com.fasterxml.jackson.core.jackson-databind 2.10.0	Critical	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-174739  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-174739  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-450207  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-450207  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-450317  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-450317  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-455417  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-455417  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461319  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461319  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461313  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461313  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461703  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461703  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461974  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-461974  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-469674  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-469674  10.0 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-469876  10.0 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-469876  10.0 (not mitigated)
	High	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-471293  9.8 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-471293  9.8 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-484500  9.8 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-484500  9.8 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724486  9.1 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724486  9.1 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724489  9.1 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724489  9.1 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724502  9.1 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724502  9.1 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724501  9.1 (not mitigated)	 JDKY-JAVA-COMFASTERXML-JACKSONCORE-724501  9.1 (not mitigated)
		 JDKY-JAVA-COMFASTERXML-JACKSONCORE-723802  9.1 (not mitigated)	

CVE-2017-12132										
Name	CVE-2017-12132									
Description	The DNSD used in the GNU C Library like glibc or libstd before version 2.25, when DNS support is enabled, will add long long unsigned int to name servers, potentially exposing user DNS spoofing attacks due to IP fragmentation.									
Source	CVE ID: NVD , CWE , Linux , cve-uses , bugtraq , Exploit-DB , Metasploit , Find 0day , Libraries , Gentoo , SUSE , Debian , Ubuntu , Mages , Gentoo contributors , what security , medium [patch range: bugfixes]									
NVD severity	8.7 (base)									
Debian bug	870600									
Vulnerable and fixed packages										
The table below lists information on source packages.										
Package Name	Release	Version	Status							
glibc (PTG)	whisky	2.13-38-ubuntu10	vulnerable							
glibc (PTG)	whisky	2.13-38-ubuntu12	vulnerable							
glibc (PTG)	jessie	2.13-38-ubuntu1	vulnerable							
	etch	2.13-11-ubuntu3	vulnerable							
	etch	2.13-11-ubuntu1	vulnerable							
	butler, sid	2.27-3	fixed							
The information below is based on the following data on fixed version.										
Package Type	Release	Fixed Version	Upgrade	Origin	Debian Bug					
glibc	source (unstable)	(unfixed)	medium							
glibc	source	2.25-1	medium		870600					
glibc	source	experimental	2.25-Debianexperimental	medium						
Notes										
[patchlist] = glibc (Klaus Leiser)										
[patchlist] = glibc (Klaus Leiser)										
[patchlist] = glibc (Klaus Leiser)										
https://sourceware.org/libc/news_blog.cgi?id=131461										
https://newsroom.debian.org/cgi-bin/bugreport.cgi?bug=870600										
https://xrlan.org/bugfix/13951_601.pdf										

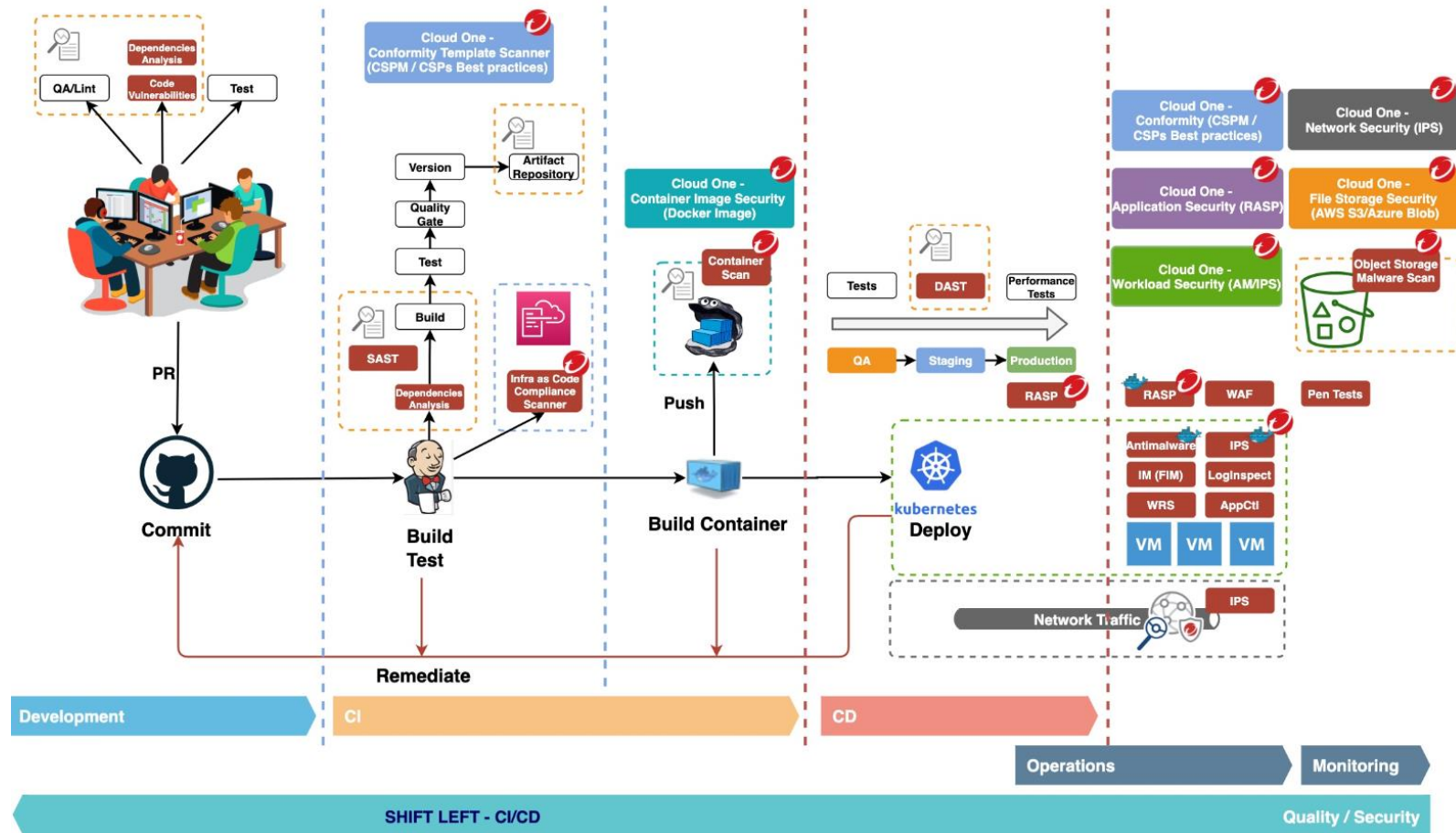
- Existe correção?
- Qual é a correção?
- Quais pacotes/
bibliotecas possuem vulnerabilidades altas?
- Quais são as vulnerabilidades?
- Qual o impacto no meu ambiente?

Não tem remediação e agora?



DEMO!

Use case



Concluindo...



Melhoria contínua

Não reivente a roda – Entenda o modelo de responsabilidade compartilhada



Automação

Utilize Frameworks já existentes – NIST – CIS - PCI DSS



```
"name": "string",  
"type": "scan-for-open-ports",  
"scheduleDetails": {  
  "timeZone": "string",
```

Vulnerabilidades (Bugs)

O que é aceitável?



“Segurança, teste, desenvolvimento, operações, integração - seja qual for o seu pipeline contínuo, certifique-se de que o pipeline completo de código de qualidade é para fazer o cliente feliz no tempo mais rápido possível.” — Almodena Rodriguez Pardo

4 etapas para integrar a segurança ao DevOps

Shift Left





THE ART OF CYBERSECURITY

Automated hybrid cloud workload protection via calls to Trend Micro APIs. Created with real data by Trend Micro threat researcher and artist **Jindrich Karasek**.

Vamos juntos nesta trilha!



linkedin.com/groups/8984009



youtube.com/c/InovacaoComDadosEmNuvem



anchor.fm/inova-dados-nuvem



github.com/taborda-cbip/inovacao-com-dados-em-nuvem



Inovação com dados em nuvem

COMO FAZER UMA JORNADA
PARA NUVEM (QUASE)
SEM TURBULÊNCIA



Como fazer uma Jornada para nuvem (quase) sem turbulência

Tales Casagrande

Trilha Inovação com dados em nuvem



Este trabalho está licenciado sob uma Licença Creative Commons Atribuição-Compartilhual 4.0 Internacional. Para ver uma cópia desta licença, visite <http://creativecommons.org/licenses/by-sa/4.0/>.