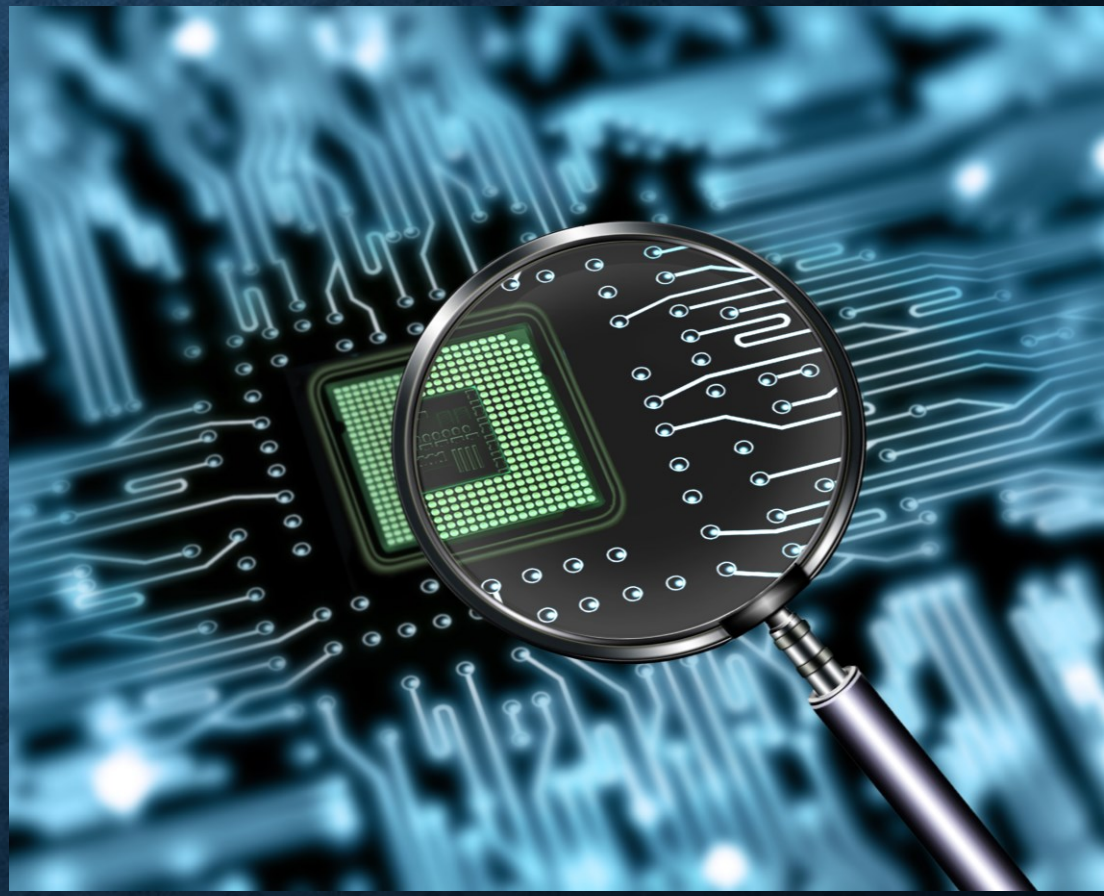
8º Fórum Brasileiro de CSIRTs

FORENSE COMO SERVIÇO

Um estudo preliminar sobre métodos, técnicas e seus desafios.



Willian Bitencourt
São Paulo, 09/09/2019.

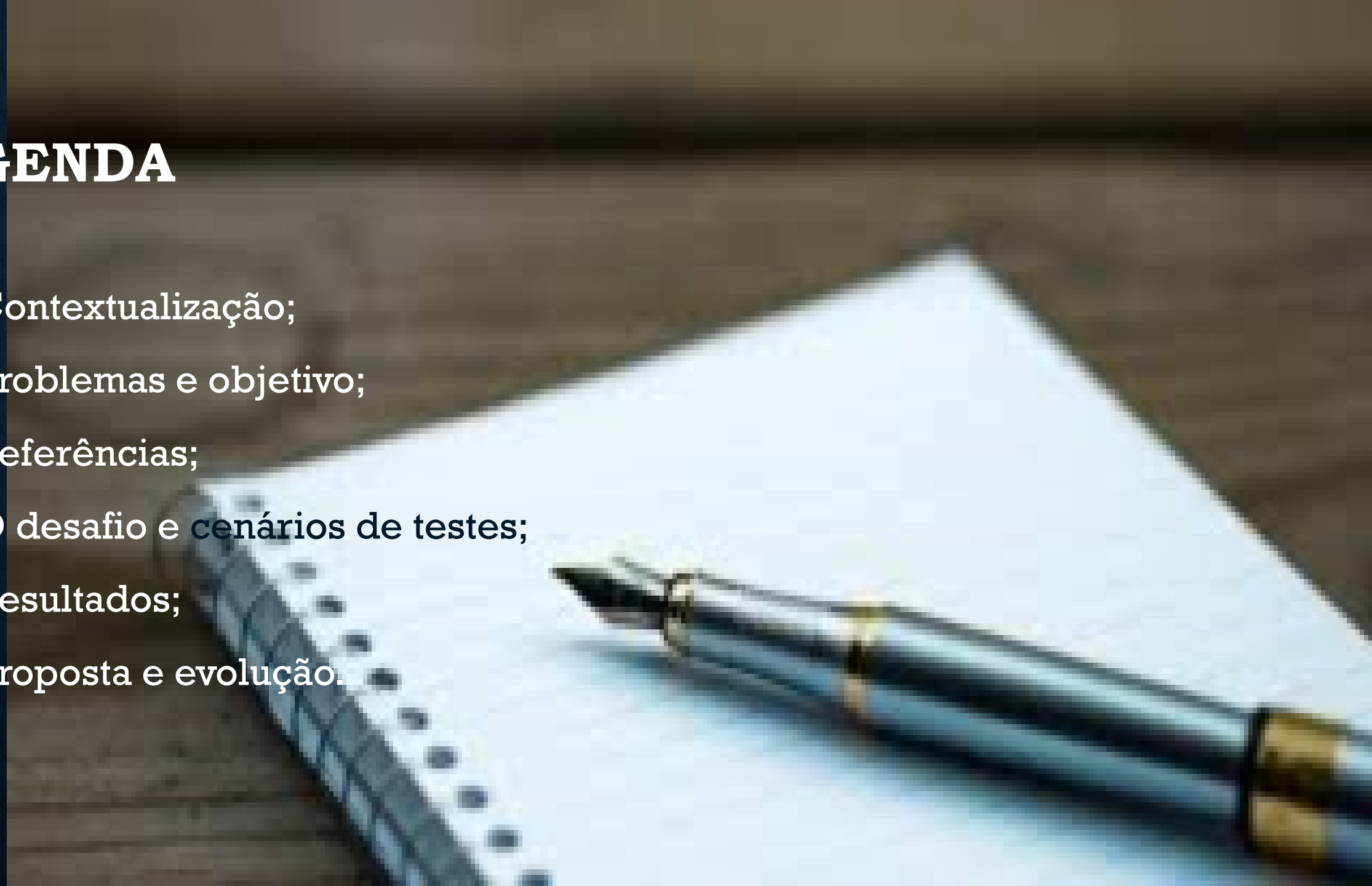
APRESENTAÇÃO

Willian Lopes Bitencourt

- Experiências:
  - Especialista em Segurança da Informação - Santander Getnet;
- Formação:
  - Graduado em Segurança da Informação – Universidade do Vale do Rio dos Sinos;
  - Especialista em Forense Computacional e Perícia Digital – IPOG/RS;
- Certificações:
  - CCNA;
  - LPIC-1;
  - ITIL v3;
  - Cobit4.1.

AGENDA

1. Contextualização;
2. Problemas e objetivo;
3. Referências;
4. O desafio e cenários de testes;
5. Resultados;
6. Proposta e evolução.



CONTEXTUALIZAÇÃO

A nuvem e a forense...

COMPUTAÇÃO EM NUVEM

Vantagens da nuvem:

- A nuvem é linda!
- Recursos ilimitados...
- Escalabilidade conforme sazonalidade;
- Pública, privada, híbrida;
- IaaS, SaaS, Paas, etc;

Tendências (...ou realidade):

- Cada vez maior adesão pelos negócios;
- Cada vez mais tipos de negócios migram;
- Cada vez mais dinheiro circula pela nuvem;

https://news.microsoft.com/pt-br/santander-fecha-parceria-com-a-microsoft-como-provedor-de-nuvem-estrategico-para-impulsionar-a-transformacao-digital-do-banco/

Santander fecha parceria com a Microsoft como provedor de nuvem estratégico para impulsionar a transformação digital do banco

30 abril , 2019 | Microsoft News Center Brasil

Contrato plurianual prevê utilização dos recursos de inteligência artificial e nuvem da Microsoft para ajudar o Santander a melhorar o atendimento ao cliente e sua eficiência operacional

O Banco Santander fechou parceria com a Microsoft Corp. como provedor de nuvem estratégico na transformação digital do banco. As duas empresas anunciaram hoje a parceria global de longo prazo, que ajudará o banco a impulsionar a inovação digital e aumentar sua eficiência operacional, utilizando diversas soluções em nuvem, incluindo Microsoft Azure, Dados, Inteligência Artificial e Serviços Cognitivos.

O Santander está fazendo a transição de sua infraestrutura de TI para um ambiente multinuvem, com plataformas globais apoiadas em metodologias ágeis, que ajudam a acelerar a transformação tecnológica do Grupo.

"Acreditamos firmemente que, por meio de inovações bem-sucedidas e focadas no cliente, podemos ganhar fidelização com a melhoria e a personalização das experiências dos clientes, além de nos tornarmos mais ágeis e eficientes. A tecnologia é um facilitador essencial para o sucesso de nossos negócios, e a Microsoft é uma forte parceira que nos ajudará a alcançar nosso objetivo", disse Dirk Marzluf, diretor de Tecnologia e Operações do Banco Santander.

Tom Keane, vice-presidente corporativo de Azure Global na Microsoft afirma que a parceria com o Santander vem em um momento de transformação para os serviços financeiros, que estão se tornando rapidamente digitais em resposta às mudanças em todo o setor. "Estamos ansiosos para aprofundar nosso envolvimento na nuvem com o Santander, à medida que a instituição impulsiona a inovação digital em suas operações globais", concluiu.

Sede do Santander em Boadilla del Monte, Madri, Espanha

Nuvem como alavanca para acelerar a inovação

Como parte da parceria, a Microsoft trabalhará com o Santander para estender os recursos de nuvem do banco em seus mercados, impulsionando a criação de aplicativos nativos na nuvem e o desenvolvimento de soluções bancárias inovadoras, ao mesmo tempo que aprimora os aplicativos atuais com novos recursos inteligentes. Além disso, a Microsoft apoiará programas de treinamento e certificação do Azure para os funcionários.

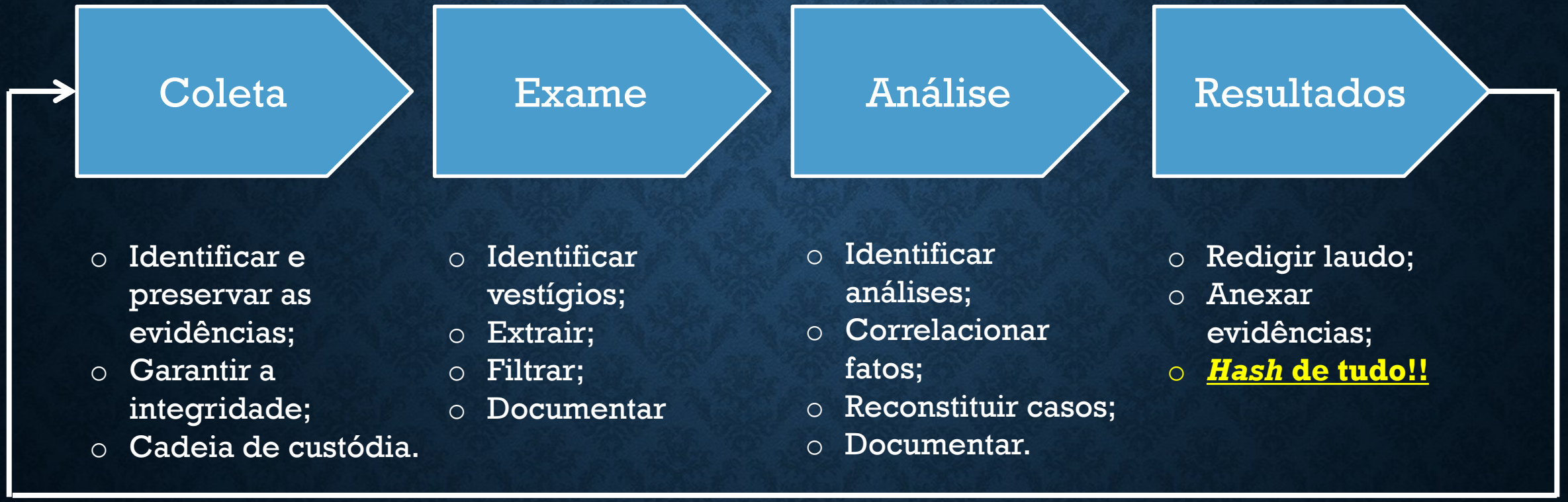
O Microsoft Azure fornece ao Santander agilidade, escala e tecnologia inteligente necessárias para levar novos produtos ao mercado mais rapidamente e atender às necessidades dos clientes com maior flexibilidade por meio de canais de distribuição e operações internas otimizadas.

O Santander terá à disposição o compromisso contínuo da Microsoft com segurança, conformidade, privacidade e transparência. Além disso, o programa Microsoft Financial Services Compliance – que permite que empresas bancárias e reguladores examinem sistemas, serviços e processos em nuvem da Microsoft – garante a conformidade das operações em nuvem da companhia com os requisitos regulamentares para permitir que o banco ganhe a flexibilidade necessária para competir, preservando a privacidade e a segurança de seus clientes.

Sobre o Santander

O Banco Santander (SAN SM, STD EUA, BNC LN) é um banco comercial líder de varejo, fundado em 1857 e sediado na Espanha. Tem presença significativa em dez principais mercados na Europa e nas Américas e é o maior banco na zona do euro por capitalização de mercado. No final de 2018, o Banco Santander tinha 981 bilhões de euros em recursos de clientes (depósitos e fundos mútuos), 144 milhões de clientes, 13.000 agências e 200.000 funcionários. O Banco Santander obteve lucro atribuído de 7,810 milhões de euros em 2018, um aumento de 18% em relação ao ano anterior.

E A FORENSE...?



Mas em nuvem? Como se faz?

PROBLEMAS E OBJETIVO

O que fazer?

PROBLEMAS E PERGUNTAS QUE PRECISAM DE RESPOSTAS...

- Falta de integridade do processo de aquisição de evidências em nuvem;
- Ferramentas forenses convencionais não compatíveis ou com limitações à ambientes de nuvem;
- Ataques normalmente acontecem nas camadas de aplicação, enquanto a investigação requer acesso a todas as camadas (IaaS).

Mas e no modelo SaaS e Paas, como fica?

- Além do serviço oferecido pela nuvem, existem serviços que orquestram, monitoram, controlam, sustentam a nuvem.

Que vestígios estes sistemas podem apresentar?

Que funcionalidades eles poderiam disponibilizar para a investigação?

ESCOPO E OBJETIVO

Propor modelos, métodos e técnicas forenses capazes de auxiliar em uma investigação que envolva ambientes sazonais em nuvem.

1) Apresentar pontos de coleta de evidências que poderiam ser utilizados em investigações forenses mesmo antes de serem destruídos pelas alterações de ambiente. Ou ainda;

2) Mesmo que tais evidências sejam destruídas, seja possível buscar vestígios de que algum serviço foi disponibilizado por um período de tempo utilizando determinados recursos no qual se deu o comprometimento e por consequência o crime cibernético.

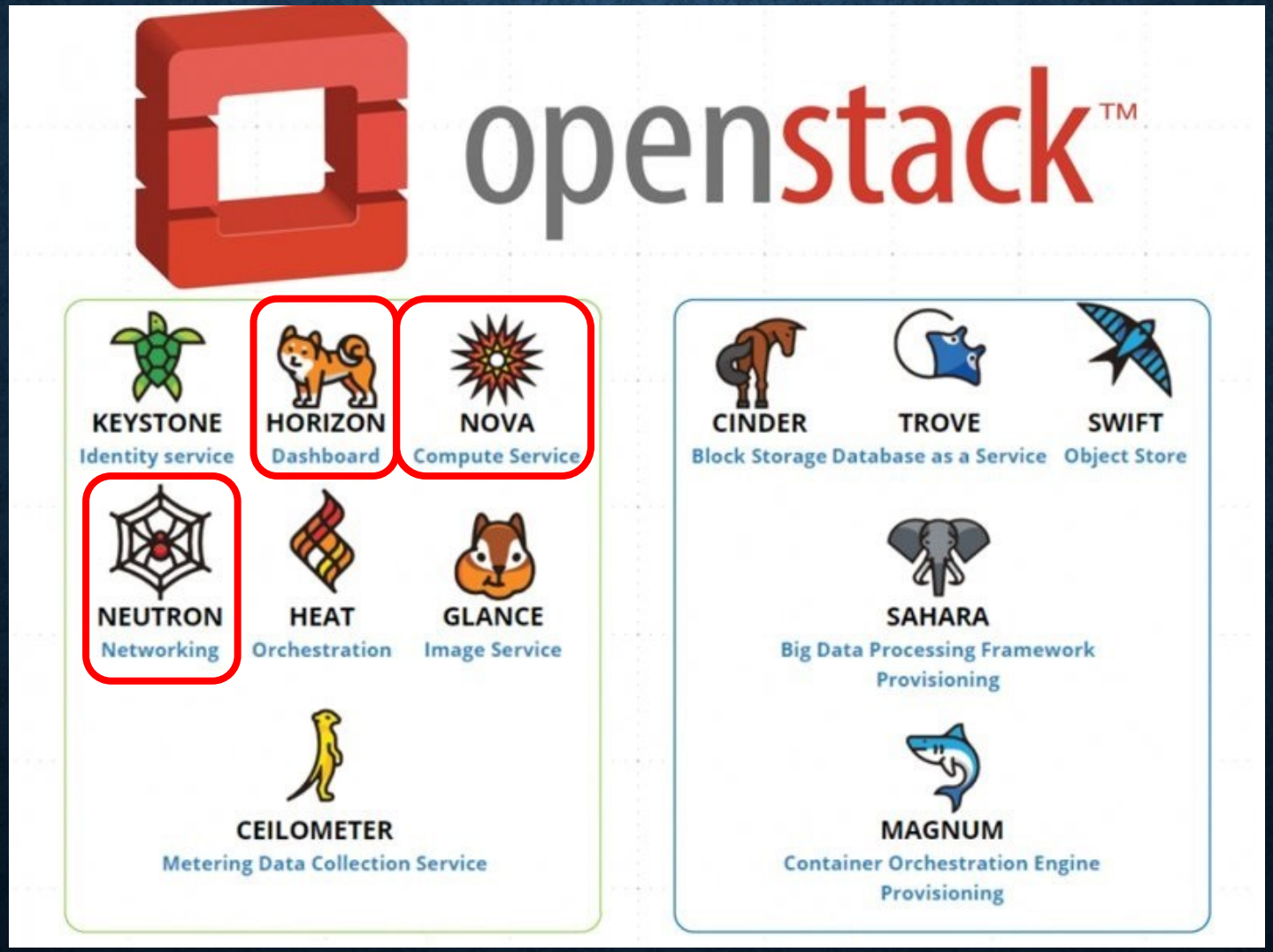
Plataformas privadas

Vs

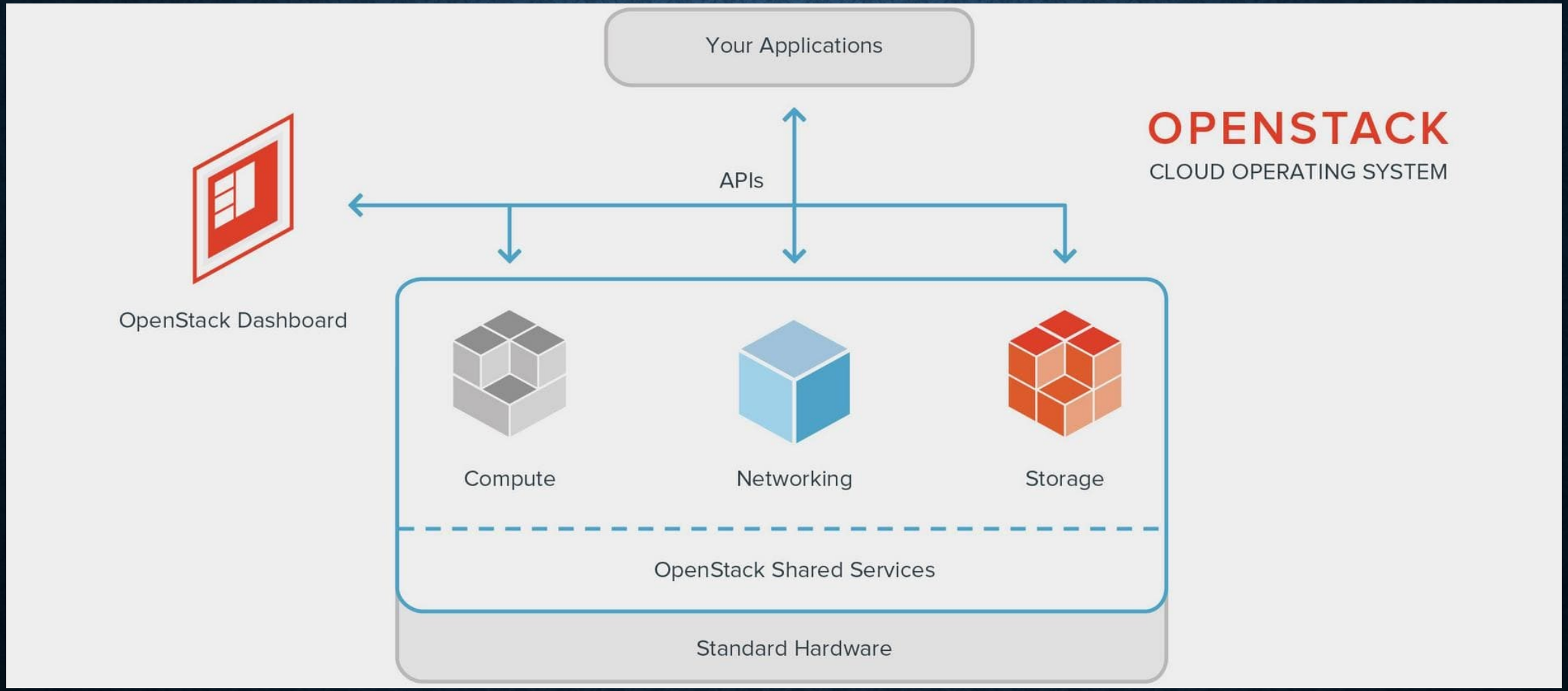
Plataformas *Opensource*

IaaS? SaaS? PaaS?

A PLATAFORMA OPENSTACK



A PLATAFORMA OPENSTACK



REFERÊNCIAS

O que já foi estudado e proposto.

REFERENCIAL TEÓRICO

1) Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques

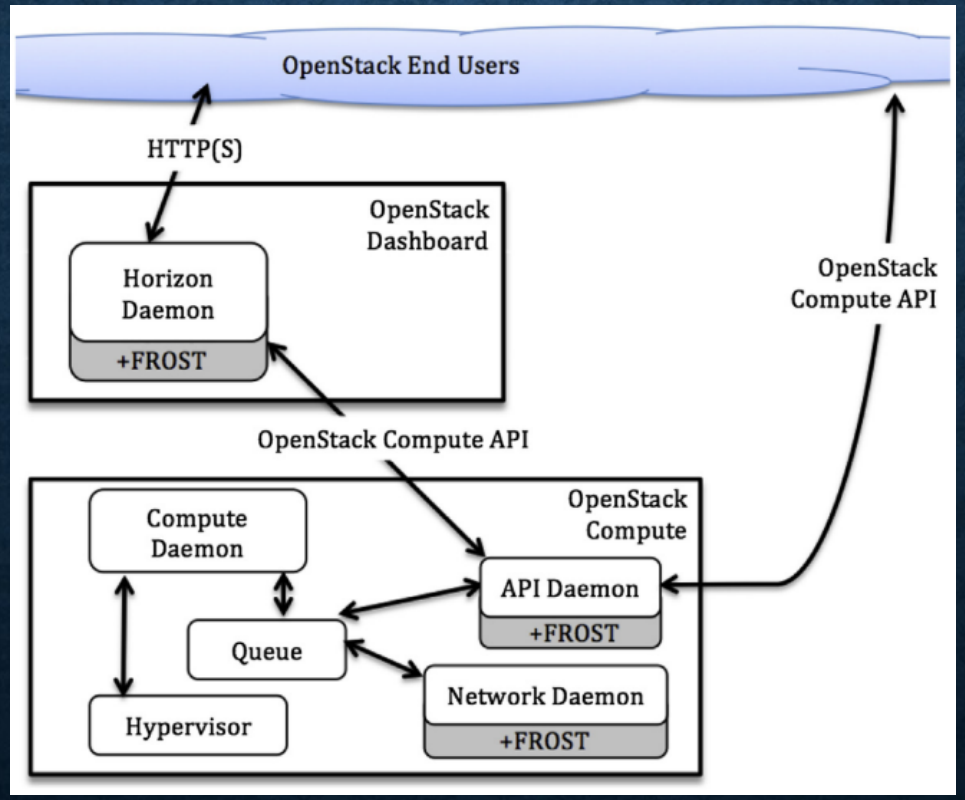
DYKSTRA, Josiah e Sherman, Alan T (2012)

Experiment	Tool	Evidence collected	Time (hrs)	Trust required
1	EnCase	Success	12	OS, HV, Host, Hardware, Network
1	FTK	Success	12	OS, HV, Host, Hardware, Network
1	FTK Imager (disk)	Success	12	OS, HV, Host, Hardware, Network
1	Fastdump	Success	2	OS, HV, Host, Hardware, Network
1	Memoryze	Success	2	OS, HV, Host, Hardware, Network
1	FTK Imager (memory)	Success	2	OS, HV, Host, Hardware, Network
1	Volume Block Copy	Success	14	OS (imaging machine), HV, Host, Hardware, Network
2	Agent Injection	Success	1	HV, Host, Hardware, Network
3	AWS Export	Success	120	AWS Technician, Technician's Host, Hardware and Software, AWS Hardware, AWS Software

REFERENCIAL TEÓRICO

2) Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform

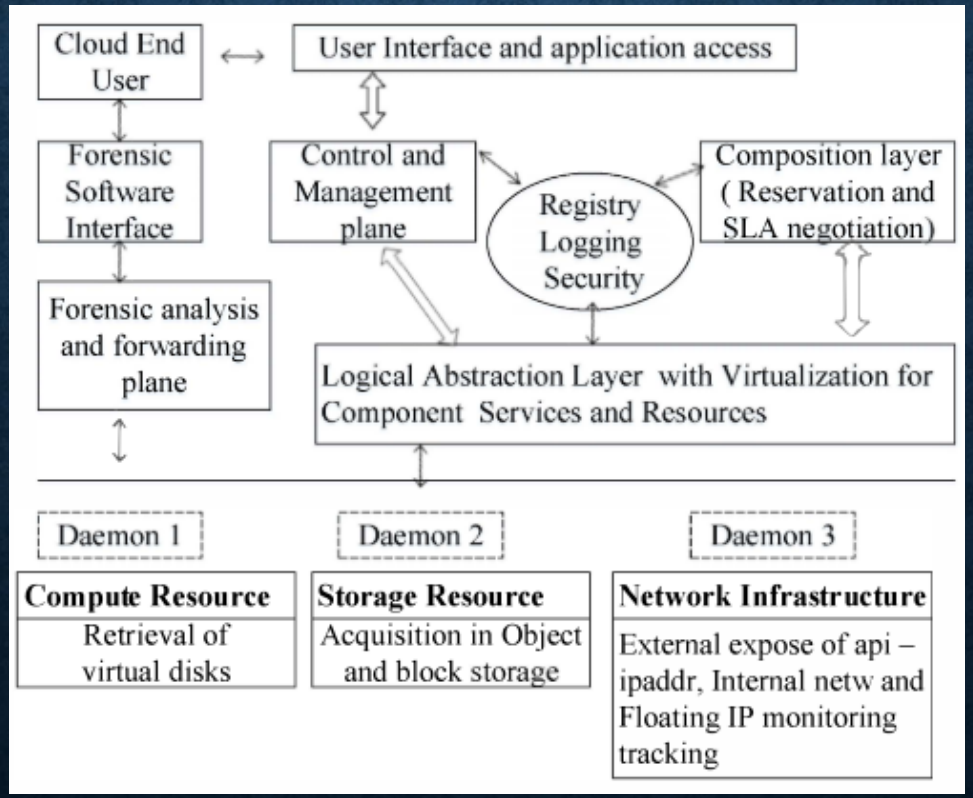
DYKSTRA, Josiah e Sherman, Alan T (2013)



REFERENCIAL TEÓRICO

3) Design and Implementation of a forensic framework for Cloud in OpenStack cloud platform

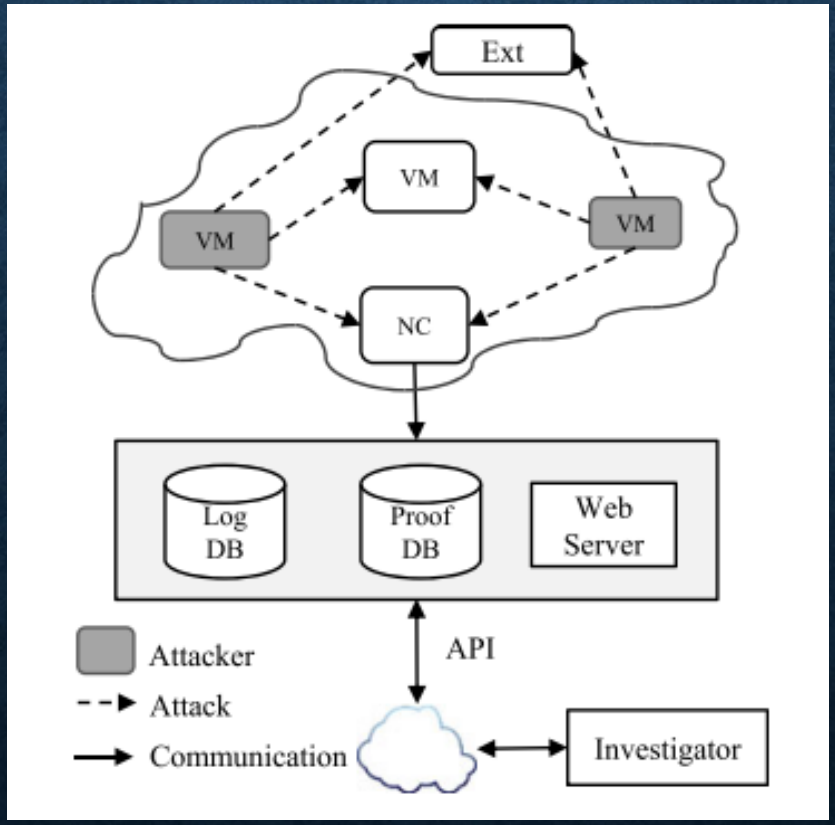
SAIBHARATH, S. e Geethakumari, G. 2014



REFERENCIAL TEÓRICO

4) Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service

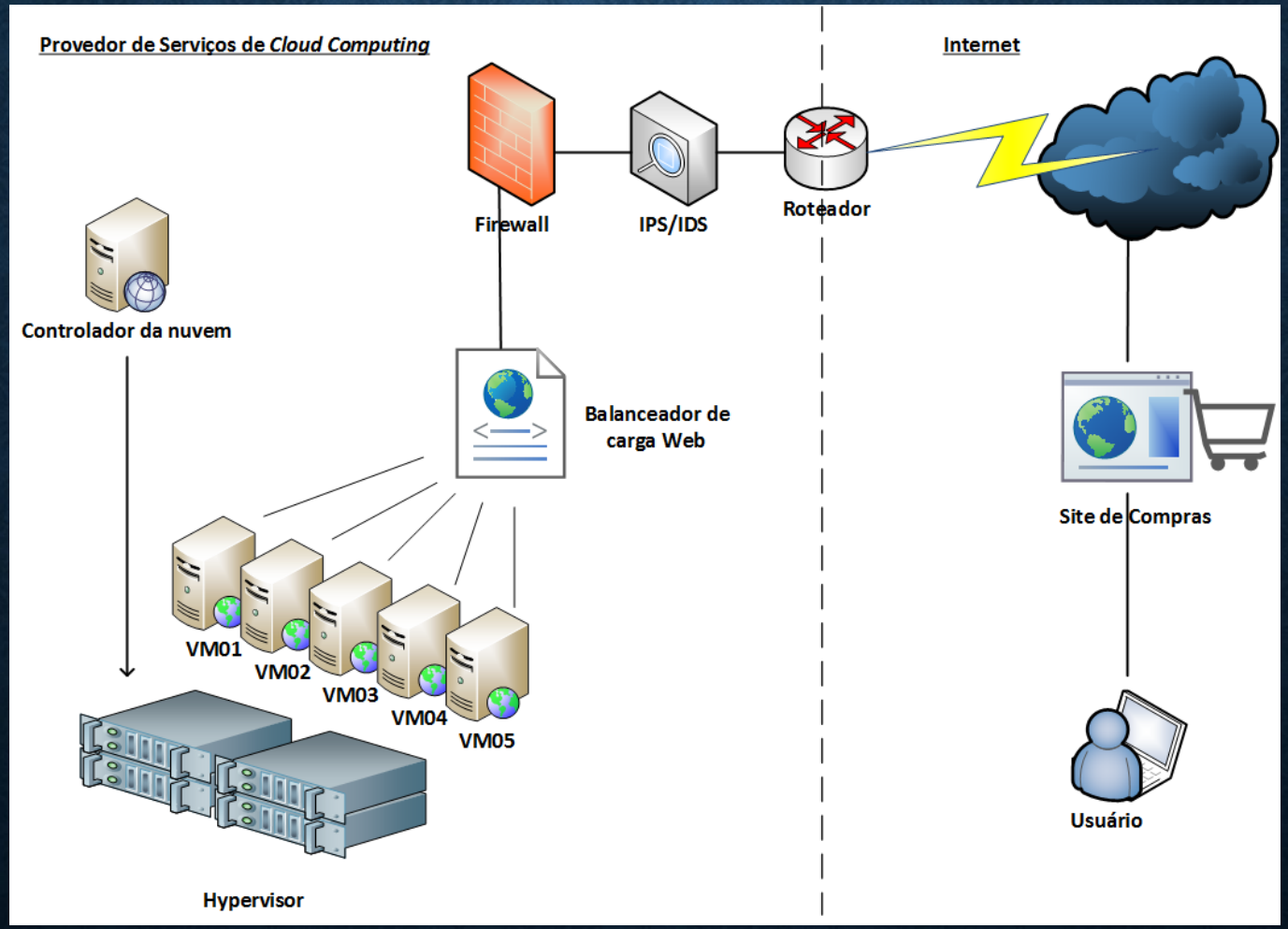
ZAWOAD, Shams et al (2016)



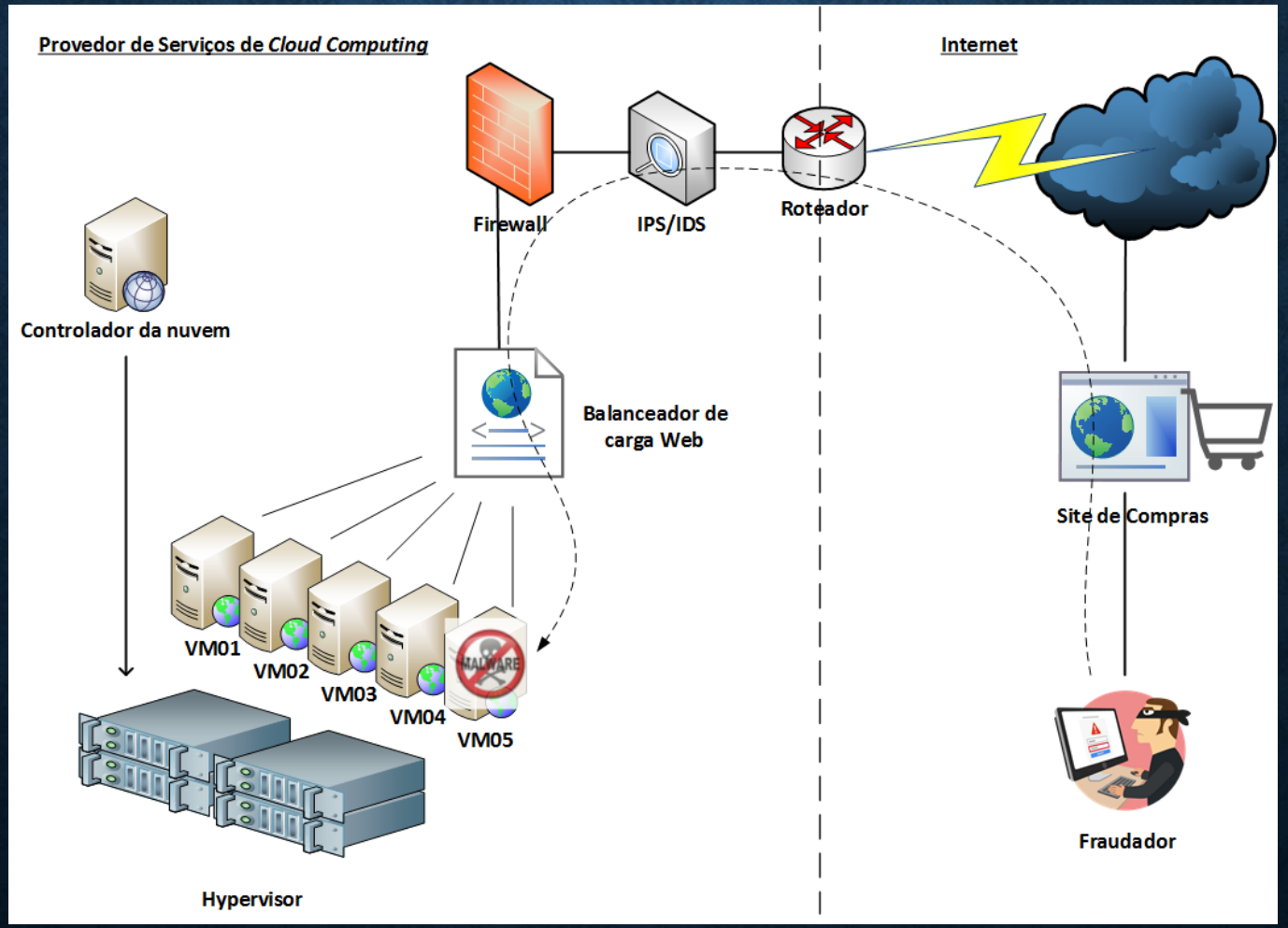
O DESAFIO

Cenário de teste.

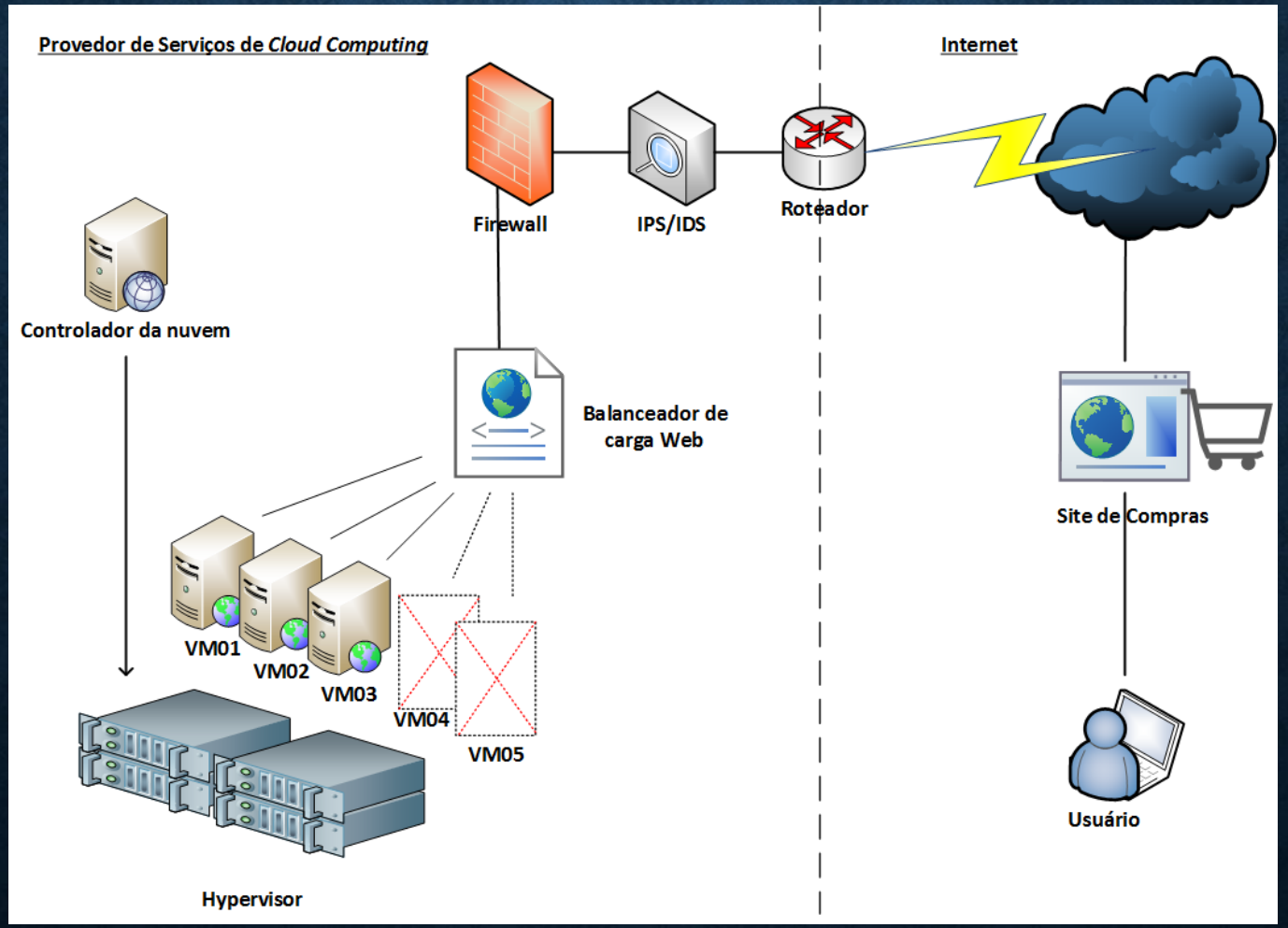
CENÁRIO DE TESTE



CENÁRIO DE TESTE



CENÁRIO DE TESTE



RESULTADOS

... e algumas proposições.

COMPARATIVO E RESULTADOS

Teste	Ferramentas	Funcionalidade	Aplicabilidade
01	FROST	Logs, aquisição de disco virtual	Insucesso
02	*Forensic Framework*	Logs, aquisição de disco virtual	Insucesso
03	SecLaaS	Logs	Sucesso Parcial
04	*Cloud Trail*	Logs	Insucesso

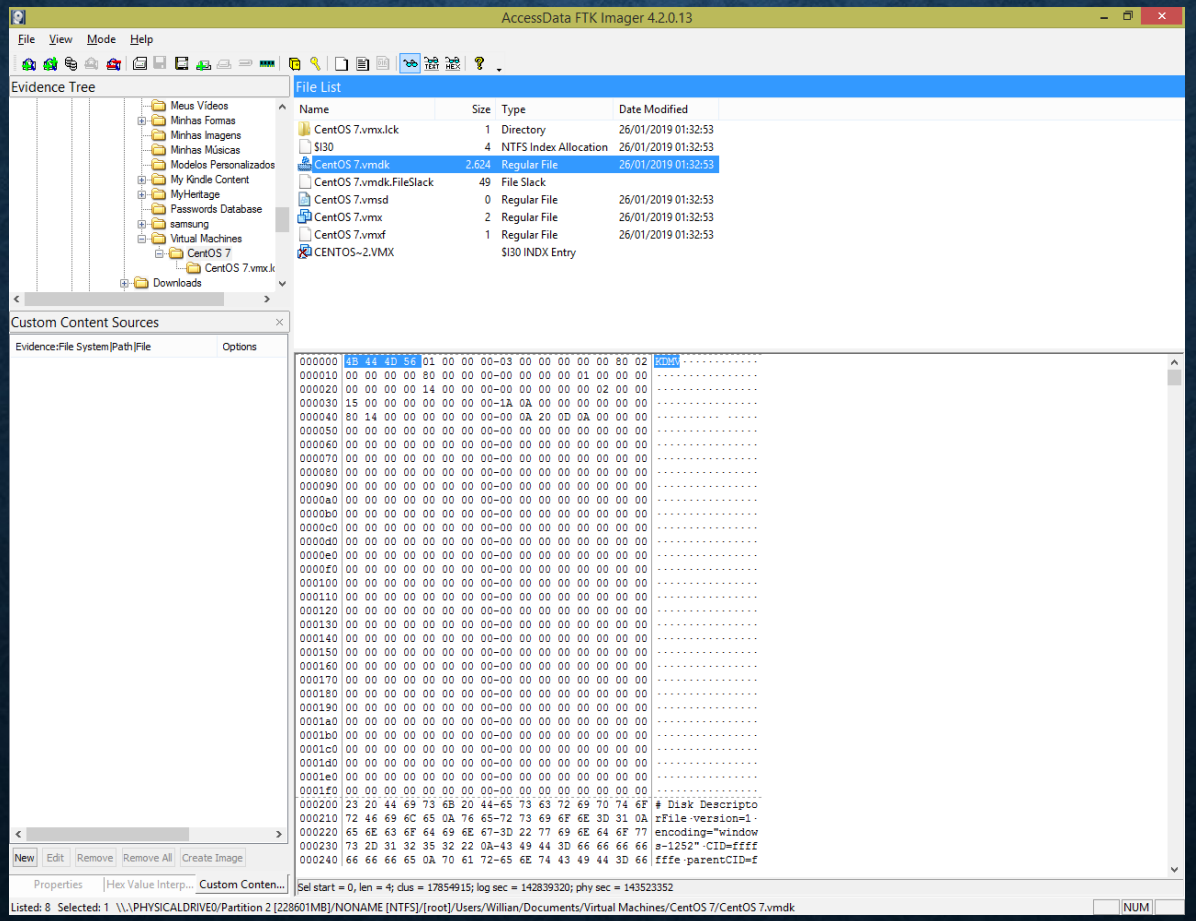
Tabela 2 – Consolidado dos resultados.
Fonte: Autoria própria.

Combinação	Ferramenta Principal	Demais Ferramentas	Aplicabilidade
01	SecLaaS	FROST	Sucesso
02	SecLaaS	*Forensic Framework*	Sucesso
03	SecLaaS	*Cloud Trail*	Insucesso

Tabela 3 – Combinação de técnicas.
Fonte: Autoria própria.

DESESPERO

DataCarving ajuda, mas não tem garantia de...

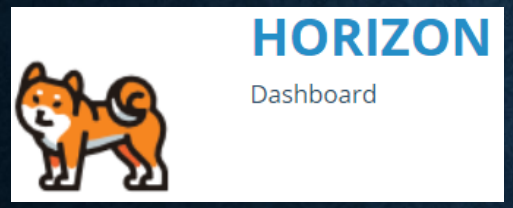


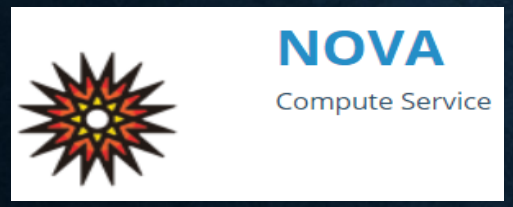
EXPANSÃO DO MODELO

Precisamos evoluir!

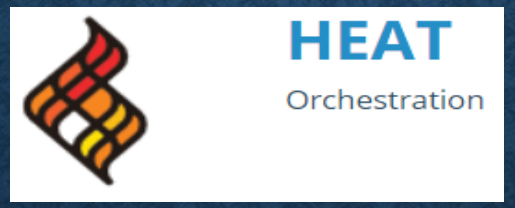
NOVOS REQUISITOS

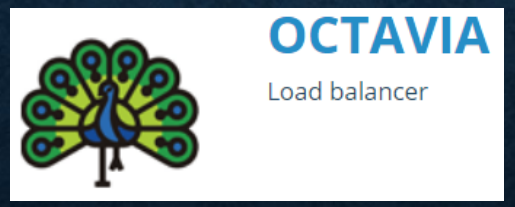
Módulos iniciais:



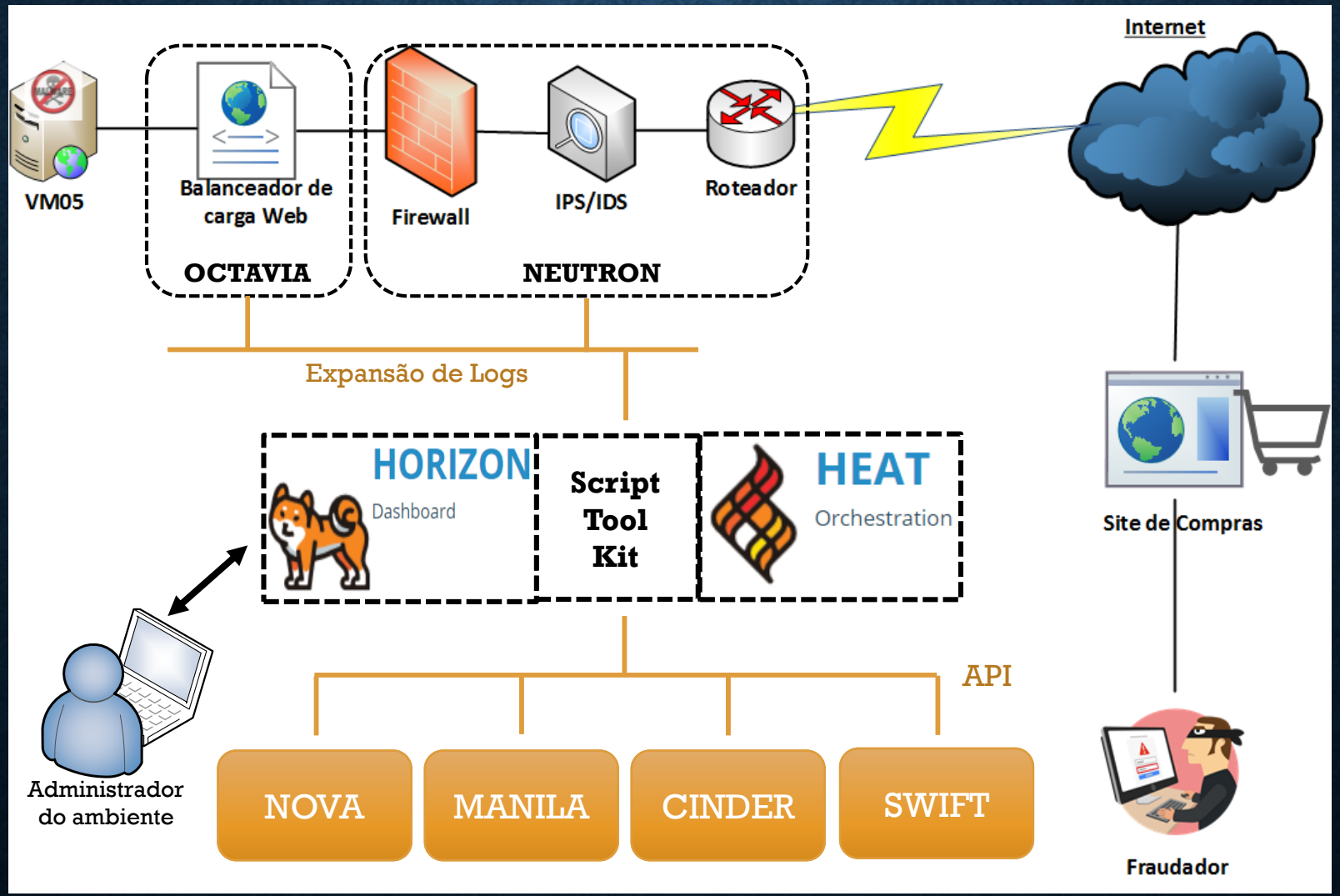


Módulos adicionais:





MODELO PROPOSTO



REFERÊNCIAS

- Referências acadêmicas:

BITENCOURT, Willian. Forense como Serviço: Um estudo preliminar sobre métodos, técnicas e seus desafios. 2018

ZAWOAD, Shams et al. Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service. IEEE Transactions on Dependable and Secure Computing, 2016.

SAIBHARATH, S.; Geethakumari, G. Design and Implementation of a forensic framework for Cloud in OpenStack cloud platform. International Conference on Advances in Computing, Communications, and Informatics - ICACCI, 2014.

DYKSTRA, Josiah; Sherman, Alan T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digital Investigation, 2013.

DYKSTRA, Josiah; Sherman, Alan T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 2012.

- Referências diversas:

OpenStackServices. Disponível em <https://www.openstack.org/software/project-navigator/openstack-components#openstack-services>

https://news.microsoft.com/pt-br/santander-fecha-parceria-com-a-microsoft-como-provedor-de-nuvem-estrategico-para-impulsionar-a-transformacao-digital-do-banco/

WILLIAN LOPES BITENCOURT

Especialista em Segurança da Informação

Santander Getnet

willian.bitencourt@getnet.com.br

lopes.bitencourt@gmail.com

https://www.linkedin.com/in/willianbitencourt/

OBRIGADO!

DÚVIDAS?