

Monitoramento e observabilidade

Paulo Henrique Nazaré



PUC Minas
Virtual

Application Performance Management (APM)

Application Performance Management

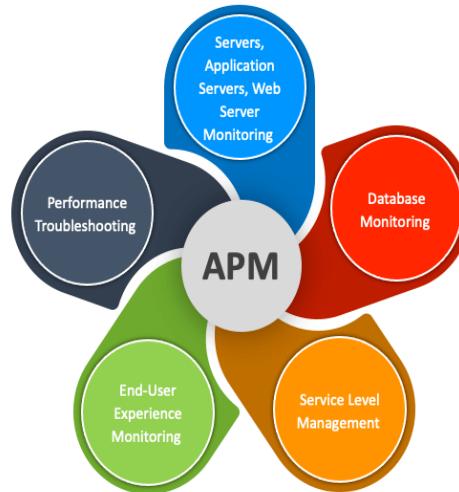
Também conhecido como Application Performance Management, o APM é um tipo de software, ou até serviço, que se certifica se os softwares estão com o desempenho e performance adequada. Ele monitora a velocidade e a linearidade de transações digitais dos mais variados tipos: softwares, sistemas, infraestruturas de rede, etc. Por meio de testes de carga, monitoramento da experiência real de usuários, desempenho web, prevenção de erros e bugs e até instrumentalizando a aplicação, o APM é um tipo de solução muito adequada para auxiliar empresas que possuem sistemas desenvolvidos **internamente ou possuem grandes desafios relacionados a infraestruturas complexas**. O resultado alcançado por isso, deve ser uma boa experiência final para o usuário.

Observabilidade – Como medir

Dimensões serviços de APM

APPLICATION PERFORMANCE MANAGEMENT

Solução de problemas



End user experience (Experiência do usuário final)

O monitoramento da experiência do usuário final pode ser realizada de duas maneiras: sintética/proativa ou real. A mais comum é a sintética/proativa, que é feita via robôs emuladores, que simulam o comportamento do usuário na forma real, por meio de logs de aplicação ou plugins de softwares especializados em APM. Nos dois tipos a monitoração é utilizada para gerar dashboards e disparar alarmes, caso ocorra alguma violação de tempo ou SLA.

Runtime application architecture (Arquitetura do aplicativo e tempo de execução)

O uso do runtime application architecture para conhecer o fluxo das transações é de extrema importância, pois cada vez mais as aplicações se encontram distribuídas e descentralizadas. Ter um desenho transacional atualizado de forma automática, faz parte da entrega de algumas das muitas ferramentas de APM do mercado.

Deep Dive Component Monitoring(Monitoramento de componentes de mergulho profundo)

O uso do runtime application architecture para conhecer o fluxo das transações é de extrema importância, pois cada vez mais as aplicações se encontram distribuídas e descentralizadas. Ter um desenho transacional atualizado de forma automática, faz parte da entrega de algumas das muitas ferramentas de APM do mercado.

Analytics/Reporting(Análise/Relatórios)

Normalmente, após a coleta de dados diretamente nas aplicações e infraestruturas que as sustentam, as soluções de APM fornecem ferramentas para analytics e reporting. Nesse caso, dados brutos são coletados para uma posterior análise acerca do desempenho, capacidade ou custos (caso em cloud) de uma aplicação.

Analytics/Reporting(Análise/Relatórios)

Normalmente, após a coleta de dados diretamente nas aplicações e infraestruturas que as sustentam, as soluções de APM fornecem ferramentas para analytics e reporting. Nesse caso, dados brutos são coletados para uma posterior análise acerca do desempenho, capacidade ou custos (caso em cloud) de uma aplicação.

APPLICATION PERFORMANCE MANAGEMENT

APM Service Offerings





PUC Minas
Virtual

Elementos da monitoração

Network Performance Monitor

O Network Performance Monitor é um de monitoramento de rede avançado e acessível que permite detectar, diagnosticar e resolver rapidamente problemas de desempenho e falhas de rede, permite que os usuários se conectem a dados de aplicativos, de servidor, virtuais e correlacionem esses dados para diagnosticar e resolver problemas de desempenho complexos da rede híbrida.

Network Performance Monitor

Por meio de integrações profundas com produtos, permite unir silos de domínios para executar a análise de causa raiz rapidamente com ferramentas detalhadas e Mapas , permitindo que os usuários obtenham insights de dados correlacionados historicamente e em tempo real.

Network Performance Monitor

Permite criar uma central de mensagens compartilhada na qual é possível ver eventos e alertas na sua rede em uma única visualização, além de mecanismos de escalabilidade e insights de dispositivos avançados para solucionar problemas. O Network Performance Monitor é um processo de monitoramento de rede avançado e acessível que permite detectar, diagnosticar e resolver rapidamente problemas de desempenho e falhas de rede.

Analise de Trafego

O Analisador de tráfego é um processo complementar que permite que ferramentas analisem fluxos de vários fornecedores afim de reduzir proativamente o tempo de inatividade da rede. A análise de tráfico fornece insights que podem ser colocados em prática para ajudar os profissionais de TI a solucionar problemas e otimizar o consumo de largura de banda. Esses insights indicam quem e o que consome tráfego e onde o tráfego é consumido.

Analise de Trafego

Na analise de trafego utilizamos infraestruturas modulares para facilmente integrar e detectar dados . Por meio de integrações profundas e com base na analyses produtos, como uma central de mensagens compartilhada na qual é possível ver eventos e alertas na sua rede em uma única visualização para solucionar problemas rapidamente em toda a plataforma.

Gestão dos Endereços de IP

Uma grande parte de ter de lidar com as redes e os desafios complexos da rede atual começa com o gerenciamento do inventário de endereços IP e de recursos essenciais de DNS e DHCP. Você pode criar acesso ao gerenciamento centralizado de endereços IP, pois ele atua com a administração unificada de DHCP e DNS e ajuda as equipes a encontrar e configurar endereços disponíveis em sistemas DHCP e DNS.

Gestão dos Endereços de IP

- Crie e mantenha grupos de IP e utilize-os em todos para caracterizar o tráfego entre grupos e definir aplicativos personalizados.
- Personalize alertas quando houver conflito de IPs e acelere a resolução de conflitos de endereços IP com o ferramentas para identificar a causa raiz por endereço MAC, fornecedor, porta de switch, SSID Wi-Fi e usuário.
- Visualize todos os eventos e alertas na sua rede de uma só vez para solucionar problemas de dispositivos avançados em toda a plataforma de monitoramento e obeservabilidade.

User Device

Controle automatizado de usuários e dispositivos, juntamente com recursos avançados de gerenciamento de porta de switch para que você possa controlar quem ou o que se conecta à sua rede. Localize rapidamente um computador ou usuário e rastreie dispositivos perdidos ou invasores com uma simples busca pelo nome de usuário, endereço IP, nome do host ou endereço MAC.

- Oferece informações sobre aumento de largura de banda do usuário e localização da porta de switch, permitindo que você reduza o uso de largura de banda ou remova-a da rede.
- Simplifica e acelera a resolução de conflitos de IP ao permitir que usuários identifiquem um problema, recebam alertas em caso de conflito e desativem a causa remotamente.

Não deixe que aplicativos lentos e tempos de inatividade afetem os usuários finais e os serviços de sua empresa. Identifique a causa raiz de problemas de aplicativos em várias camadas da pilha de TI. Descubra automaticamente o ambiente do seu aplicativo e comece a monitorar em apenas uma hora.

- Para ver o desempenho, o tempo de atividade, a capacidade e a utilização de recursos em toda a pilha de TI(lista de softwares, estruturas, tecnologias, linguagens de programação etc).
- Certifique-se de que os problemas de configuração não estão afetando o desempenho dos sistemas e aplicativos.

Configuração de Servidores

Quando as configurações começam a perder o rumo, o impacto pode ser grave: interrupções, lentidão e violações de segurança e conformidade. As ferramentas de monitoramento podem revelar rapidamente quando as configurações do servidor, aplicativo ou banco de dados mudarem, quem as está mudando, o que mudou e qual o impacto para o desempenho. Isso ajudará você a ter a visibilidade necessária para solucionar problemas mais rápido, melhorar a segurança e demonstrar conformidade.

Configuração de Servidores

Quando as configurações começam a perder o rumo, o impacto pode ser grave: interrupções, lentidão e violações de segurança e conformidade. As ferramentas de monitoramento podem revelar rapidamente quando as configurações do servidor, aplicativo ou banco de dados mudarem, quem as está mudando, o que mudou e qual o impacto para o desempenho. Isso ajudará você a ter a visibilidade necessária para solucionar problemas mais rápido, melhorar a segurança e demonstrar conformidade.

Configuração das Virtualizações

O gerenciamento de desempenho, o planejamento de capacidade e a otimização entre ambientes VMware vSphere, Microsoft Hyper-V e Nutanix AHV.

- Identificar se a lentidão é causada por um aplicativo, servidor virtual, host ou repositório de dados.
- Recomendações de desempenho ativas e preditivas e leve as métricas básicas de desempenho de VM disponíveis.
- Visibilidade de seu desempenho de ambiente virtual VMware, Hyper-V e Nutanix no VMAN (além do monitoramento de hosts físicos) para identificar e resolver problemas mais rápido.

Performance Web

Monitorar a experiência do usuário e avaliar as transações de sites internos e externos e aplicativos baseados na Web – em qualquer local. Você pode identificar rapidamente elementos que apresentam lentidão ou falhas e solucionar os problemas até a infraestrutura de suporte, do servidor da Web e do banco de dados até o hardware de armazenamento:

- Veja a experiência do usuário final, além das métricas de rede e sistemas para identificar e entender o escopo dos problemas.
- Use o mecanismo de alertas inteligentes para criar alertas personalizáveis em um só lugar, definir critérios de notificação, acionar scripts externos e integrar-se aos sistemas de emissão de tíquetes do Service desk .

Analise do Logs

Com a coleta, análise e visualização de logs em tempo real, você obtém visibilidade pronta para uso do desempenho e da disponibilidade de sua infraestrutura e aplicativos de TI:

- Visualize os dados de log e o desempenho de rede e sistemas facilmente para acelerar a solução de problemas com integração total de dados de logs e eventos.
- Colete, consolide e analise os eventos de rede, sistemas, Windows e VMware, juntamente com dados de desempenho e disponibilidade .

Aplicabilidade

É aconselhável ter um APM se:

- Sua organização desenvolve aplicativos do zero
- Sua receita depende das aplicações desenvolvidas
- Você possui vários sistemas que interagem ou dependem de outras aplicações
- As operações de negócios dependem das aplicações desenvolvidas internamente
- A aplicação depende do suporte regular de um fornecedor e você depende dos membros internos da equipe de TI para apoiá-la



PUC Minas
Virtual

Data Observability

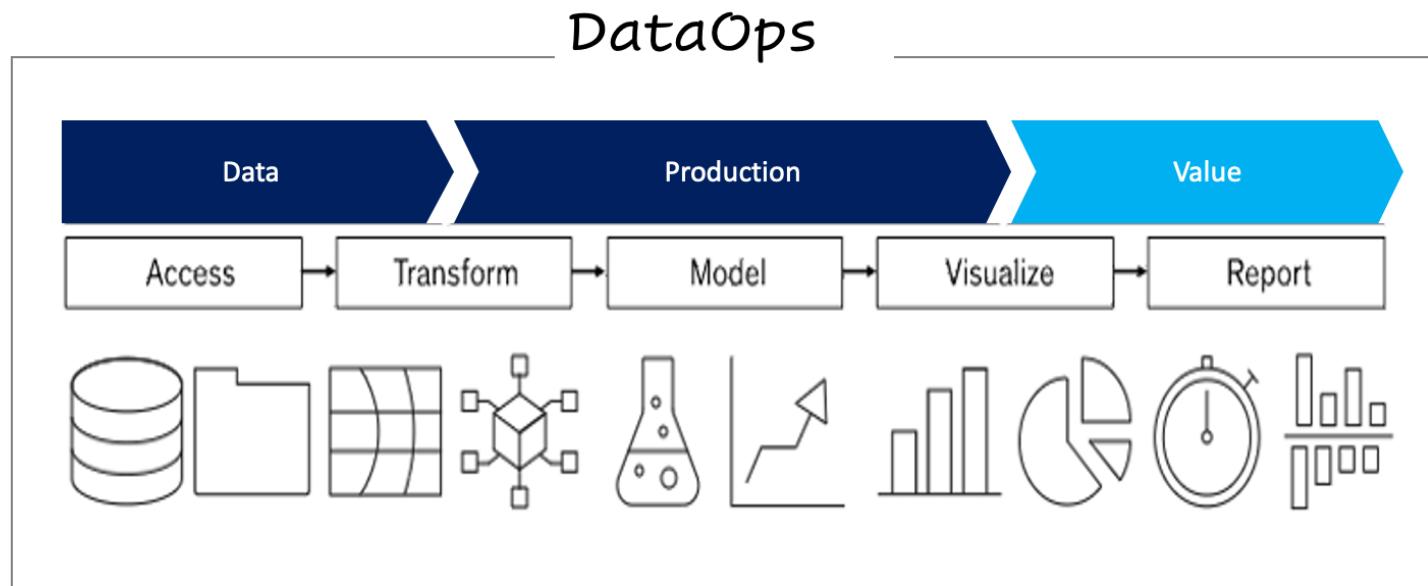
Observabilidade dos dados

A observabilidade de dados (Data Observability) refere-se à capacidade de coletar e analisar dados para entender e otimizar o desempenho de um sistema. Os dados se tornaram um dos ativos mais valiosos dos tempos modernos. À medida que mais empresas dependem de insights de dados para conduzir decisões críticas de negócios, os dados devem ser precisos, confiáveis e de alta qualidade.

Observabilidade dos dados

Um aspecto fundamental da observabilidade de dados é a capacidade de acessar e analisar dados de todas as partes do sistema. Isso inclui dados de aplicações, da infraestrutura e dos usuários do sistema. Ao coletar dados de todas essas fontes, é possível obter uma visão completa do sistema e identificar áreas de melhoria. Outro aspecto importante da observabilidade de dados é a capacidade de identificar e solucionar problemas em tempo real. Ao monitorar constantemente os dados, é possível detectar e resolver problemas antes que eles se tornem críticos.

Observabilidade dos dados





PUC Minas
Virtual

Estudos

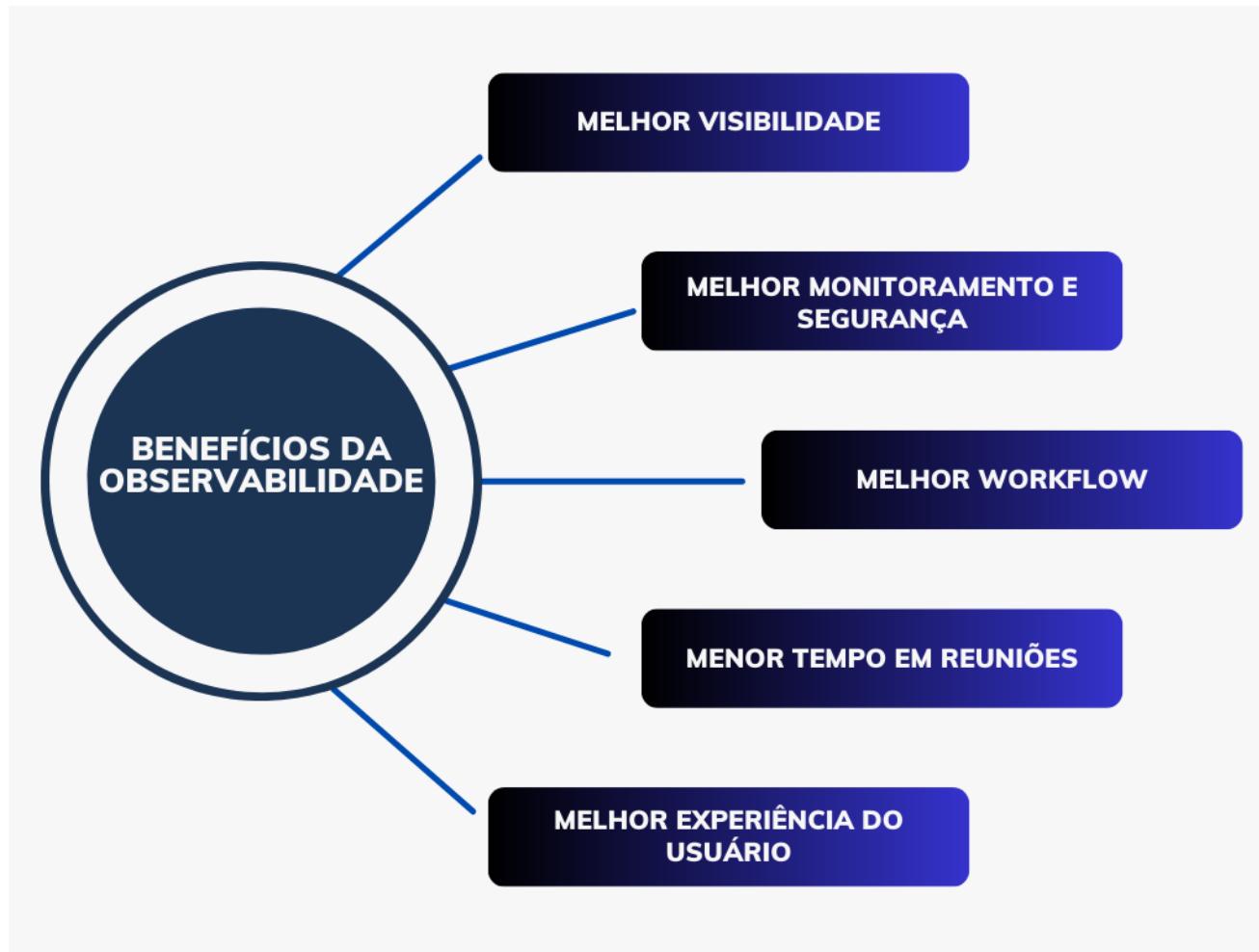
Estudos mostram que 78% dos clientes desistem de uma compra devido a uma experiência insatisfatória.

Indisponibilidade do sistema: Sem a observabilidade adequada, é difícil identificar problemas que possam estar causando a indisponibilidade do seu sistema, como problemas de recursos, falhas de hardware ou problemas de software. Isso pode resultar em períodos de inatividade e interrupções no negócio.

Problemas de segurança: Sem informações detalhadas sobre o comportamento de um sistema, é difícil identificar e corrigir problemas de segurança, como vulnerabilidades, ataques de rede ou invasões. Isso pode resultar em danos aos dados ou a reputação da empresa.

Problemas de escalabilidade: Sem informações sobre o comportamento de um sistema, é difícil identificar pontos de gargalo ou limitações que possam estar impedindo o crescimento ou a escalabilidade do sistema. Isso pode resultar em perda de oportunidades de negócios e dificuldades para atender às demandas dos usuários.

Estudos



A Observabilidade Aplicada (Applied Observability) possui 3 elementos-chave: democratização dos dados, múltiplas camadas de dados simultâneas e implementação. Ao analisarmos esses três elementos, vemos que a maioria dos fornecedores já estão adotando a abordagem de que quanto mais dados observados, melhor o resultado da correlação. No entanto, penso que o maior desafio é a implementação, pois ela envolve estratégia e vários stakeholders. Juntamente a isso, um grande desafio que profissionais de observabilidade tem encontrado é levar a mensagem de que monitoramento e observabilidade andam juntos, mas são conceitos diferentes. Isso também vale outro post.

Gartner.

3 Key Elements of Applied Observability

The diagram consists of three horizontal grey boxes stacked vertically, each containing an orange icon and text. To the left of the boxes is a large orange number '3' followed by the text 'Key Elements of Applied Observability'. The first box contains an orange icon of a central processing unit (CPU) and the text 'Democratized opportunity'. The second box contains an orange icon of four squares with arrows indicating data flow between them and the text 'Multiple concurrent data layers'. The third box contains an orange icon of a gear inside a square frame and the text 'Implementation'.

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved.



PUC Minas
Virtual

Produto

Modelo

Ambiente de produção é, de longe, a parte mais importante e, surpreendentemente, menos discutida do Ciclo de Vida do Modelo. É aqui que o modelo atinge o negócio. É onde as decisões que o modelo toma realmente melhoram os resultados ou causam problemas para os clientes. Ambientes de treinamento do modelo, onde os Cientistas de Dados passam a maior parte de seu tempo, consistem em apenas uma amostra do que o modelo verá no mundo real. Em um ambiente de desenvolvimento de software bem controlado, um engenheiro tem controle de versão, análise de cobertura de teste, teste de integração, testes executados em check-ins de código, revisões de código e reproduzibilidade.

Validação

Os modelos são construídos e avaliados usando vários conjuntos de dados. O conjunto de dados de treinamento é usado para ajustar os parâmetros do modelo. O conjunto de dados de validação é usado para avaliar o modelo durante o ajuste de hiperparâmetros.

Validação

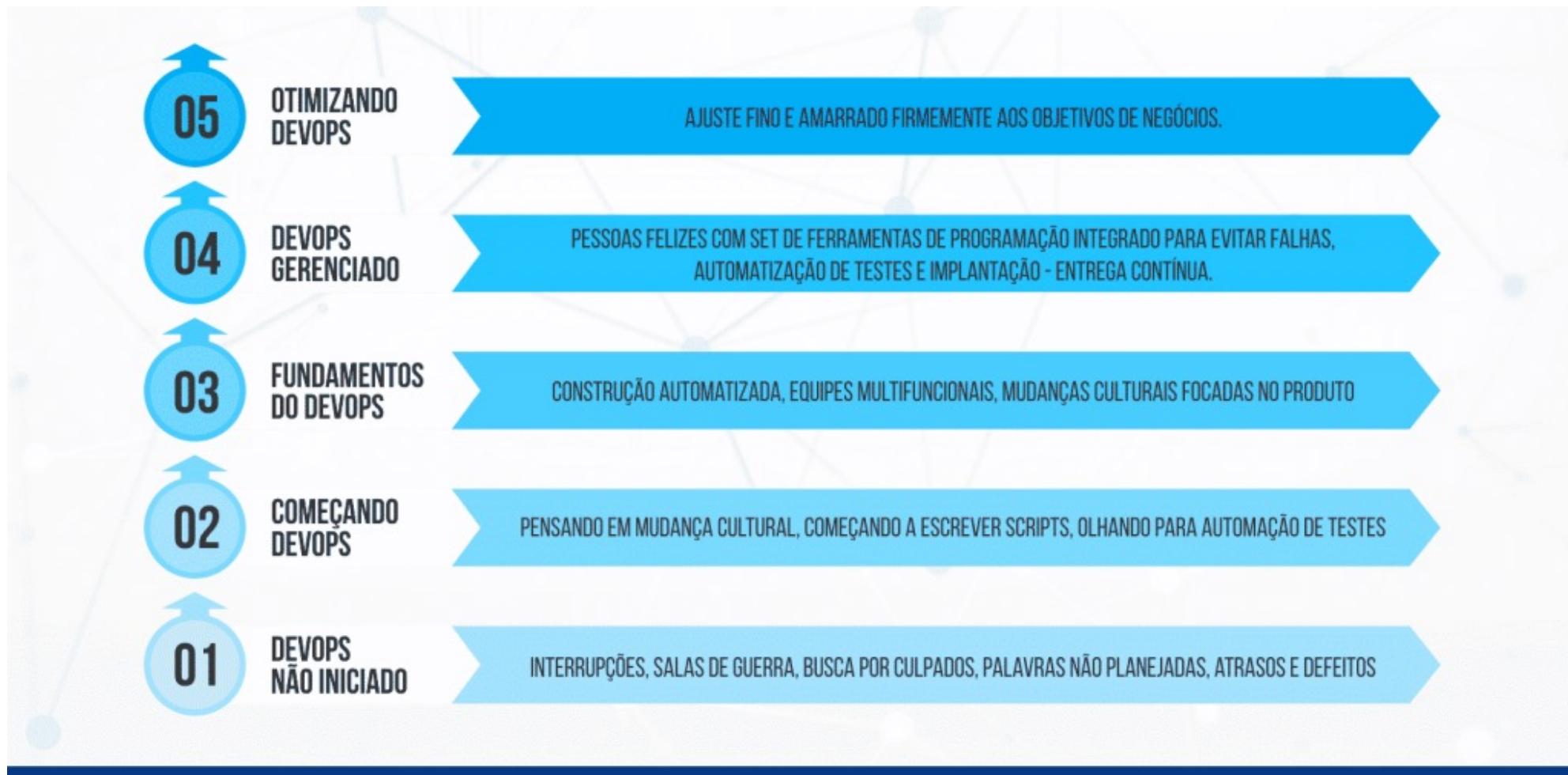
Independentemente do setor, há certas verificações a serem feitas antes de implantar o modelo na produção. Essas verificações incluem (mas não estão limitadas a):

- Testes de avaliação de modelo (precisão), tanto no geral como por fatia.
- Verificações de distribuição de previsão para comparar a saída do modelo com as versões anteriores.
- Verificações de distribuição de recursos para comparar recursos altamente importantes com testes anteriores.

Validação

- Análise de importância de recursos para comparar mudanças em recursos que estão sendo usados para decisões.
- Análise de sensibilidade para ruído de entrada aleatório e extremo.
- Teste de estresse do modelo.
- Viés e Discriminação.
- Erro de rotulagem e verificações de qualidade de recursos.
- Verificações de vazamento de dados.
- Verificações de ajuste excessivo e insuficiente.
- Dados históricos para comparar e avaliar o desempenho.
- Testes de pipeline de recursos que garantem que não haja quebra de recurso entre pesquisa e produção.

Validação



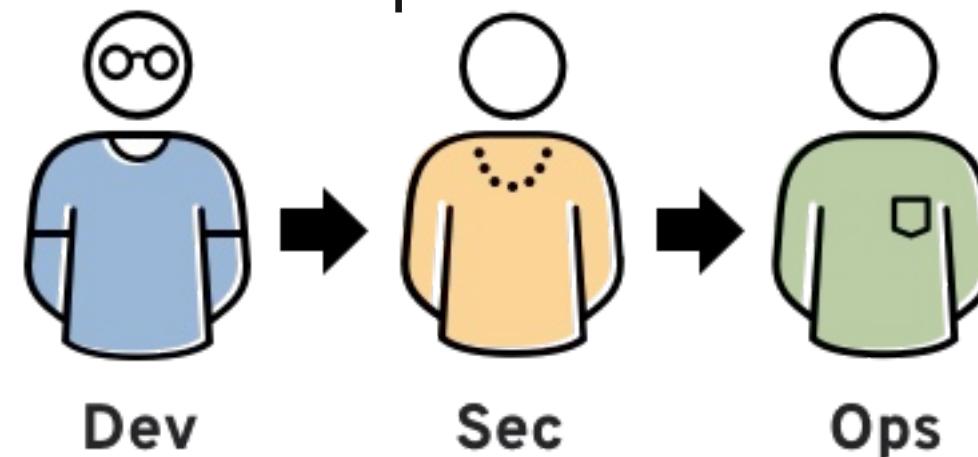


PUC Minas
Virtual

DevSecOPS

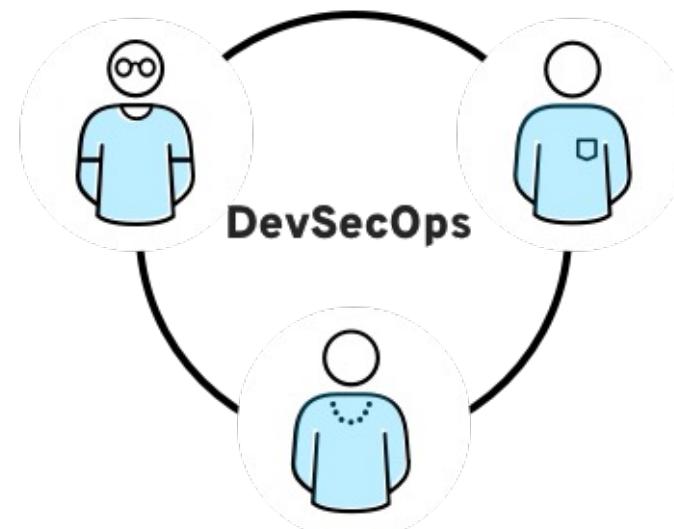
DevSecOps significa desenvolvimento, segurança e operações. É uma abordagem à cultura, automação e design da plataforma que integra segurança ao DevOps como uma responsabilidade compartilhada em todo o ciclo de vida da TI.

A metodologia DevOps não envolve apenas as equipes de desenvolvimento e de operações. Se você quiser aproveitar ao máximo a agilidade e a capacidade de resposta proporcionadas pela abordagem DevOps, também será necessário que a equipe de segurança da TI desempenhe um papel integrado em todo o ciclo de vida das aplicações da sua empresa.



DevSecOps

Agora, no framework colaborativo do DevOps, a segurança é uma responsabilidade compartilhada e integrada do início ao fim. É uma mentalidade tão importante que resultou na criação do termo "DevSecOps" para enfatizar a necessidade de criar uma base de segurança para sustentar as iniciativas de DevOps.



Segurança automatizada

O que é preciso fazer: manter os ciclos de desenvolvimento curtos e frequentes, integrar as medidas de segurança com mínima interrupção das operações, acompanhar o ritmo das tecnologias inovadoras (como containers e microserviços) e, acima de tudo, estimular a colaboração entre equipes que normalmente trabalham isoladas, uma tarefa complicada em qualquer organização. No entanto, o elemento facilitador dessas mudanças no aspecto humano do framework de DevSecOps é a automação.



Segurança para ambientes e dados

- **Padronize e automatize o ambiente:** cada serviço deve ter o mínimo possível de privilégios para reduzir as conexões e os acessos não autorizados.
- **Centralize os recursos de controle de acesso e identidade de usuários:** ter um controle rígido do acesso e usar mecanismos de autenticação centralizados são fatores essenciais para a segurança dos microsserviços, já que a autenticação é iniciada em vários pontos.
- **Isole os containers que executam microsserviços um dos outros e da rede:** isso inclui dados em trânsito e em repouso, já que ambos os tipos podem ser alvos de ataques.
- **Criptografe os dados trocados entre aplicações e serviços:** uma plataforma de orquestração de containers com funcionalidades de segurança integradas ajuda a minimizar a chance de ocorrerem acessos não autorizados.
- **Introduza gateways de API seguros:** APIs seguras aumentam a visibilidade de autorização e roteamento. Ao diminuir a quantidade de APIs expostas, as organizações podem reduzir as superfícies de ataque.

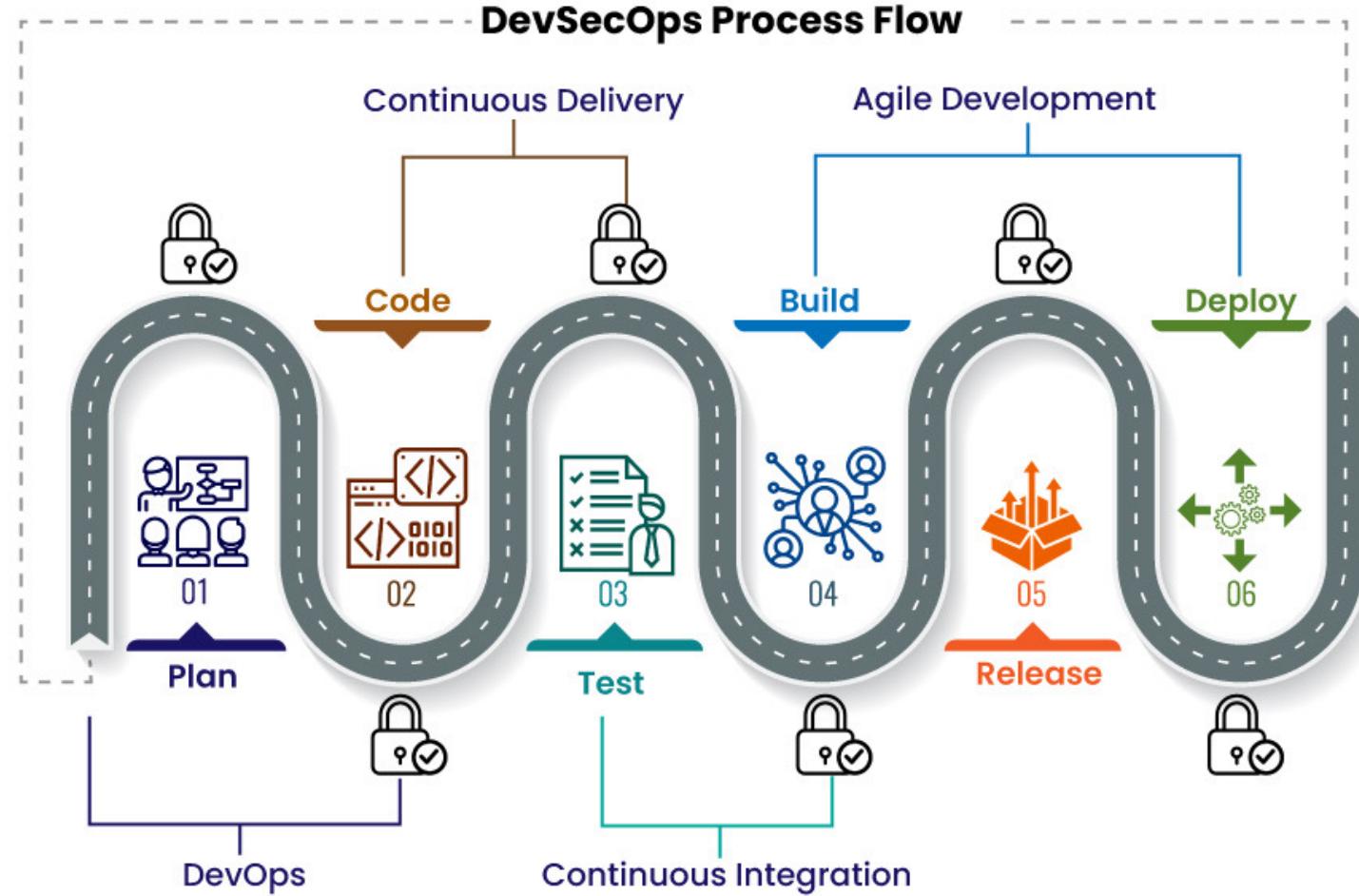
Segurança do processo de CI/CD

- **Integre verificadores de segurança para containers:** isso deve fazer parte do processo de inclusão de containers no registro.
- **Automatize os testes de segurança no processo de integração contínua:** isso inclui executar ferramentas de análise estática de segurança como parte das compilações, bem como verificar quaisquer imagens de container criadas anteriormente para encontrar vulnerabilidades de segurança conhecidas conforme elas são inseridas no pipeline de criação.
- **Adicione testes automatizados para os recursos de segurança no processo de teste de aceitação:** automatize os testes de validação de entradas e os funcionalidades de autorização e autenticação da verificação.

Segurança do processo de CI/CD

- **Automatize as atualizações de segurança, como patches, para identificar vulnerabilidades conhecidas:** faça isso por meio de um pipeline DevOps. Essa medida deve eliminar a necessidade de administradores se conectarem aos sistemas de produção, a mesmo tempo que cria um log de alterações rastreáveis e documentadas.
- **Automatize os recursos de gerenciamento das configurações de serviços e sistemas:** com isso, é possível manter a conformidade com as políticas de segurança e eliminar os erros manuais. As tarefas de auditoria e correção também devem ser automatizadas.

Segurança do processo de CI/CD





PUC Minas
Virtual

ITSM

Gerenciamento de Serviços de TI

Uma ferramenta de ITSM pode executar várias funções, como gerenciamento de incidentes, gerenciamento de solicitações de serviço, gerenciamento de problemas e gerenciamento de mudanças, apenas para citar algumas. Uma ferramenta de ITSM geralmente também consiste também de um CMDB.

Gerenciamento de Serviços de TI

Information Technology Service Management – em português “Gerenciamento de Serviços de TI” – ou somente a sigla ITSM é um processo de gerenciamento indispensável para o ciclo de vida do TI, tão essencial na interligação de tantos setores de uma empresa.

Através do ITSM, gerenciar a definição e implementação de processos, criar estratégias de melhoria contínua para os serviços e servidores e acompanhar o cumprimento de normas e valores em uma empresa tornam-se mais fáceis. O ITSM transforma o TI em um sistema integrado a todas as atividades da empresa, e permite uma abordagem mais focada nos clientes e nos serviços de TI voltados para o cliente, como o suporte, sempre priorizando o melhor caminho.

Como funciona o ITSM?

O ITSM possibilita a integração de aspectos tecnológicos de diversos setores de uma empresa, como marketing, finanças e recursos humanos, facilitando a identificação de informações, a identificação de problemas e consertando falhas. Geralmente o gerenciamento de nível de serviços de TI na prática acontece seguindo as seguintes estratégias:

- Mapeamento e inventário da infraestrutura de TI da empresa;
- Avaliação sobre os serviços de TI, equipamentos e outras ferramentas tecnológicas que podem auxiliar o negócio;
- Análise e interação com outras áreas da empresa, podendo tornar o projeto mais consistente;
- Definição de cronograma e metas de reestruturação, respeitando as prioridades e custos;
- Monitoramento e avaliação dos resultados constantemente.

Como realizar o gerenciamento de serviços de TI

O gerenciamento de serviços de TI na prática envolve alguns passos fundamentais. Confira abaixo quais são eles:

- Tenha um plano estratégico de TI – esse plano estratégico pode seguir as mesmas normas do planejamento estratégico corporativo da empresa;
- Tenha um catálogo de serviços de TI – quais os principais serviços que a área de TI da sua empresa cobre?;
- Estabeleça metas de níveis de serviço (SLA) – que condições os serviços precisam ter para atingir as expectativas dos clientes?;
- Gerencie os incidentes – sempre que houver uma interrupção, queda de qualidade ou indisponibilidade de internet, é preciso estar preparado;

Como realizar o gerenciamento de serviços de TI

- 1.Gerencie os problemas – quais os sintomas causados pelos incidentes? Como gerenciar?;
- 2.Gerencie os projetos de TI – siga as melhores práticas mundiais, e tenha um portfólio de projetos;
- 3.Melhore os serviços de TI – avalie os serviços com frequência para detectar a necessidade de mudanças;
- 4.Gerencie a capacidade do serviço – qual a capacidade máxima de atendimentos que seu negócio consegue realizar?

Como realizar o gerenciamento de serviços de TI





PUC Minas
Virtual

SIEM

5 exemplos de Gerenciamento de Serviços de TI

O SIEM, ou Gerenciamento de Informações e Eventos de Segurança em português, é a combinação do SEM (*Security Event Manager* - Gerenciamento de Eventos de Segurança) e SIM (*Security Information Management* - Gerenciamento de Informações de Segurança). Essa junção permite:

- Análise em tempo real de alertas de segurança;
- Comparação de eventos nos sistemas com as políticas de segurança para identificar ameaças avançadas;
- Gerenciamento de logs;
- Visão ampla e registros das atividades no ambiente de TI.

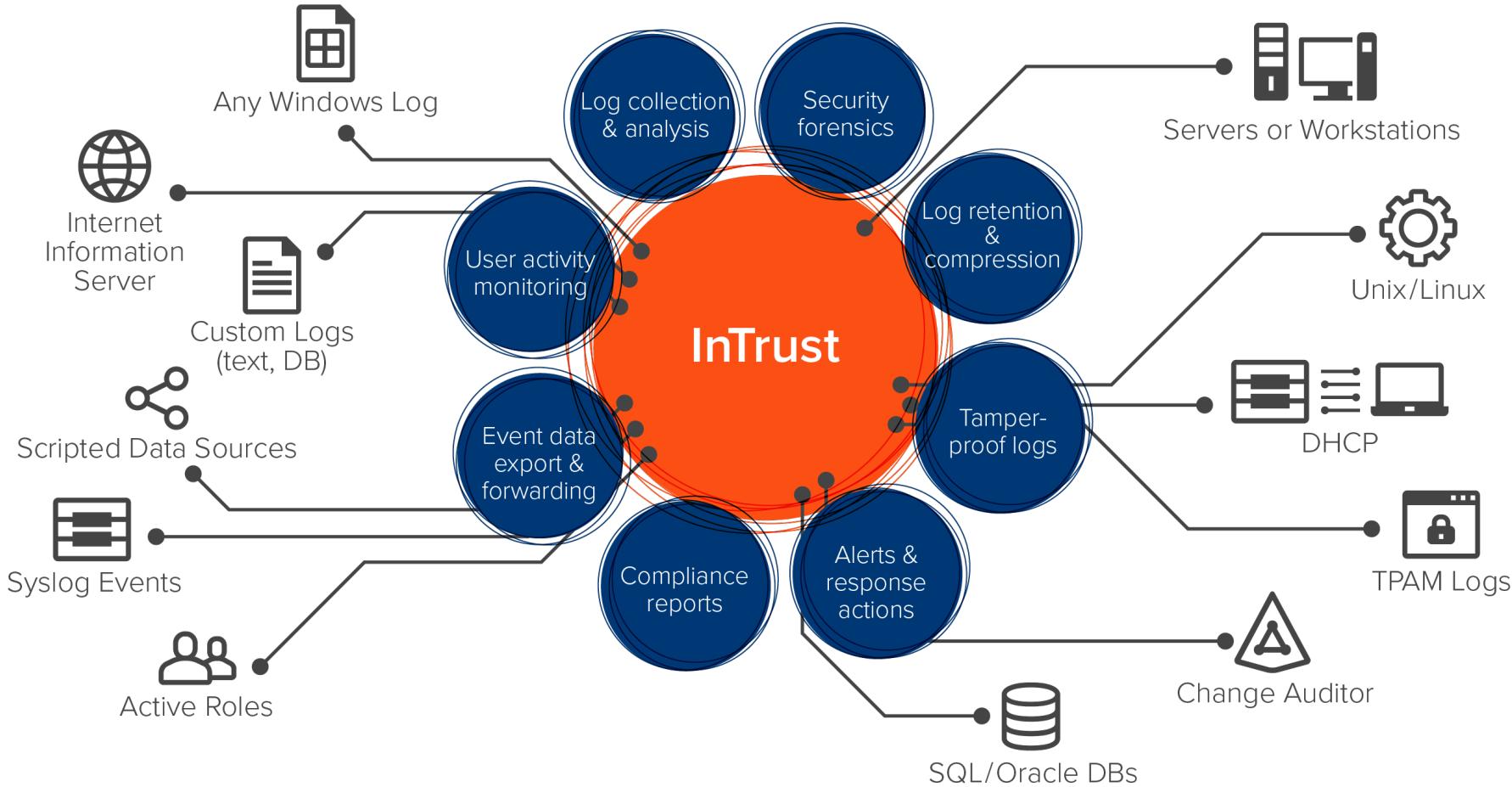
Como funciona o SIEM?

O SIEM coleta dados de diferentes fontes:

- Logs de firewall;
- Eventos gerados por aplicativos (por exemplo, antivírus);
- Dispositivos de segurança;
- Sistemas Host;
- E outros locais.

A partir disso, ele categoriza cada um desses dados. Então, quando o SIEM identifica uma ameaça, ele a classifica em um determinado nível - de acordo com as regras de segurança já pré-estabelecidas - e emite um alerta.

Como funciona o SIEM?





PUC Minas
Virtual