Evolução dos Riscos de Cibersegurança: Da Gestão Tradicional à Abordagem Holística

O cenário de cibersegurança está em constante evolução, e atualmente exige abordagens dinâmicas para a gestão de vulnerabilidades e identificação de riscos. Tradicionalmente, a gestão de riscos era realizada através de métodos estáticos, que não conseguiam acompanhar a complexidade crescente do panorama de ameaças.

As Limitações da Gestão Tradicional

1 Visão Passiva

O método tradicional foca-se essencialmente em varreduras de rede (scanning), com ou sem estrategia ou periodicidade, mais ainda passivo. Passivo porque não permite uma visão completa e continua da gestão e postura de segurança dos riscos associados aos seus ativos.

2 Análise e Priorização Manual | Dependencia Humana

A análise manual dos resultados da varredura ou scanning gera relatórios passivos, não permitindo a priorização eficaz e continua dos riscos, assim como a identificação de ações urgentes.

3 Foco em Riscos Conhecidos

Scans tradicionais apenas identificam vulnerabilidades conhecidas, deixando um espaço enorme para riscos desconhecidos e tráfego anômalo na rede.

4 Desalinhamento entre Detecção e Correção

O MTTD (tempo médio para detecção) e o MTTR (tempo médio para correção) nunca se alinham, pois a análise de vulnerabilidades é feita p uma área diferente da que realiza o patching.

O processo passivo e reativo de gestão e identificação de riscos

1

Identificar

Configuração dos perfis e sensores de varredura ou scan de acordo com o contexto, estrategico ou não.

2

Configurar

identificação dos endereços ou gamas de IP para fazer o scan.

3

Iniciar

Iniciar o scan e aguardar os resultados conforme o perfil definido.

4

Analisar

Analisar os resultados do relatório sobre as vulnerabilidades descobertas e recomendar ações de remediação de acordo.

5

Relatório

Entregar relatório ao departamento de IT para as devidas ações de remediação.

O que pode ser melhorado?

Qualys Um agente, um Dashboard, uma solução, vários módulos.

Definimos riscos como sendo tudo aquilo que potencialmente impeça uma empresa de atingir os seus objetivos estratégicos. "Tudo aquilo" é propositadamente vago para lembrar que os riscos podem ser conhecidos ou desconhecidos, internos ou externos, podem ser colaboradores ou prestadores de serviço. Who Knows!

Visão Abrangente

A gestão holística de riscos considera todos os fatores dentro do contexto de gestão de riscos que possam impedir uma empresa de atingir seus objetivos estratégicos, dentro ou fora da apetite de risco.

Riscos Conhecidos e Desconhecidos

A abordagem holística engloba riscos conhecidos, como vulnerabilidades identificadas por scans, e riscos desconhecidos, como ameaças emergentes ou comportamento anómalo.

Abordagem Interna, Externa e Redes isoladas

Riscos internos, como falhas de configuração ou erros humanos, e riscos externos, como vulnerabilidades exploraveis externamente assim como resposta a ataques cibernéticos.

O processo ativo de gestão, priorização e remediação continua dos riscos.

Um agente, um dashboard, varios modulos...

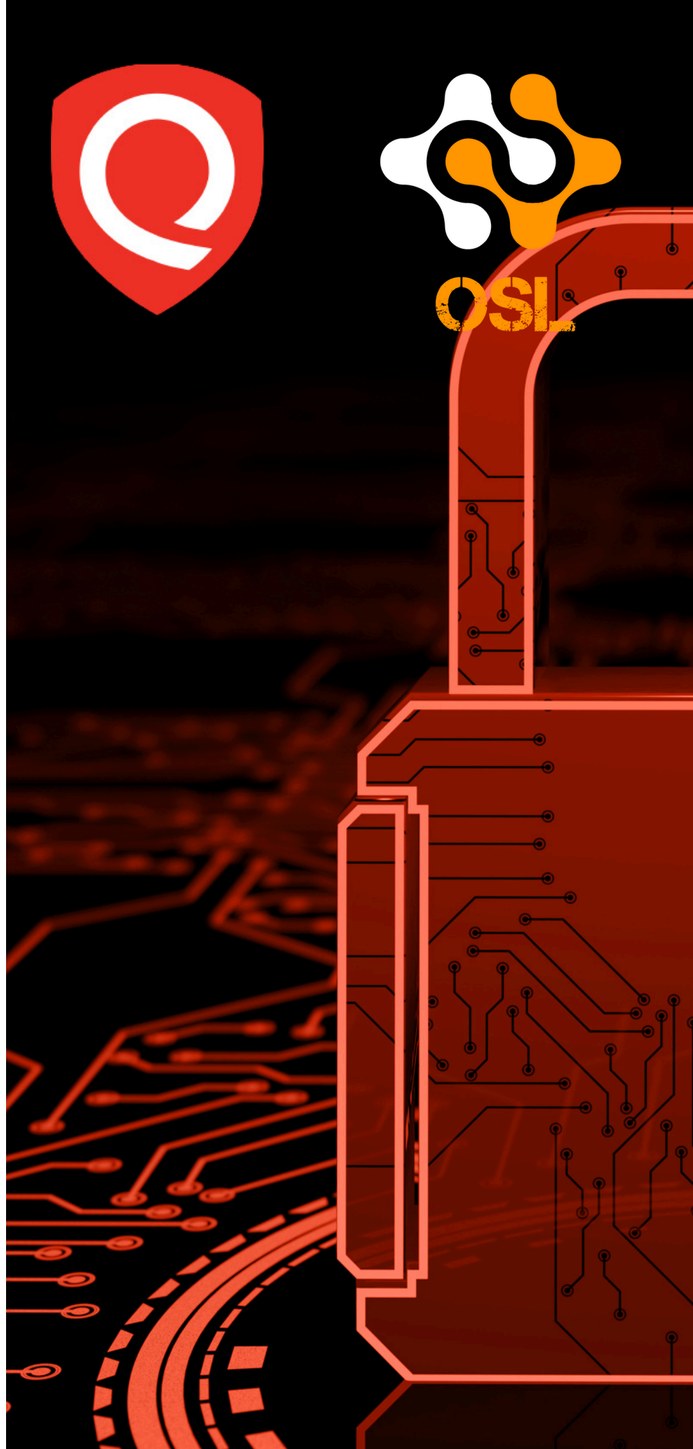
Descubra todos os seus ativos
Gestão de ativos com dados internos e externos

Detete todas as Vulnerabilidades
Detete todas as vulnerabilidades em todo o seu ambiente

Priorize as ameaças
Avaliar e medir de acordo ao contexto do negocio

Remedie com Automação
Patching sem códigos e workflows

Detetar & Responder continuamente
Anti-Malware - Endpoint Detection & Response



O que 95% dos frameworks recomendam, e o que as Empresas estão a procura.

Operacionalização
Otimizar os Workflows e melhorar a colaboração entre as Infraestruturas de TI, liderança e as equipes de segurança

Visualização
Visibilidade 360° sobre as ameaças, conhecidas ou desconhecidas, associadas a ativos de caracter interno ou externo, domínios/subdomínios aplicativos e muito mais.

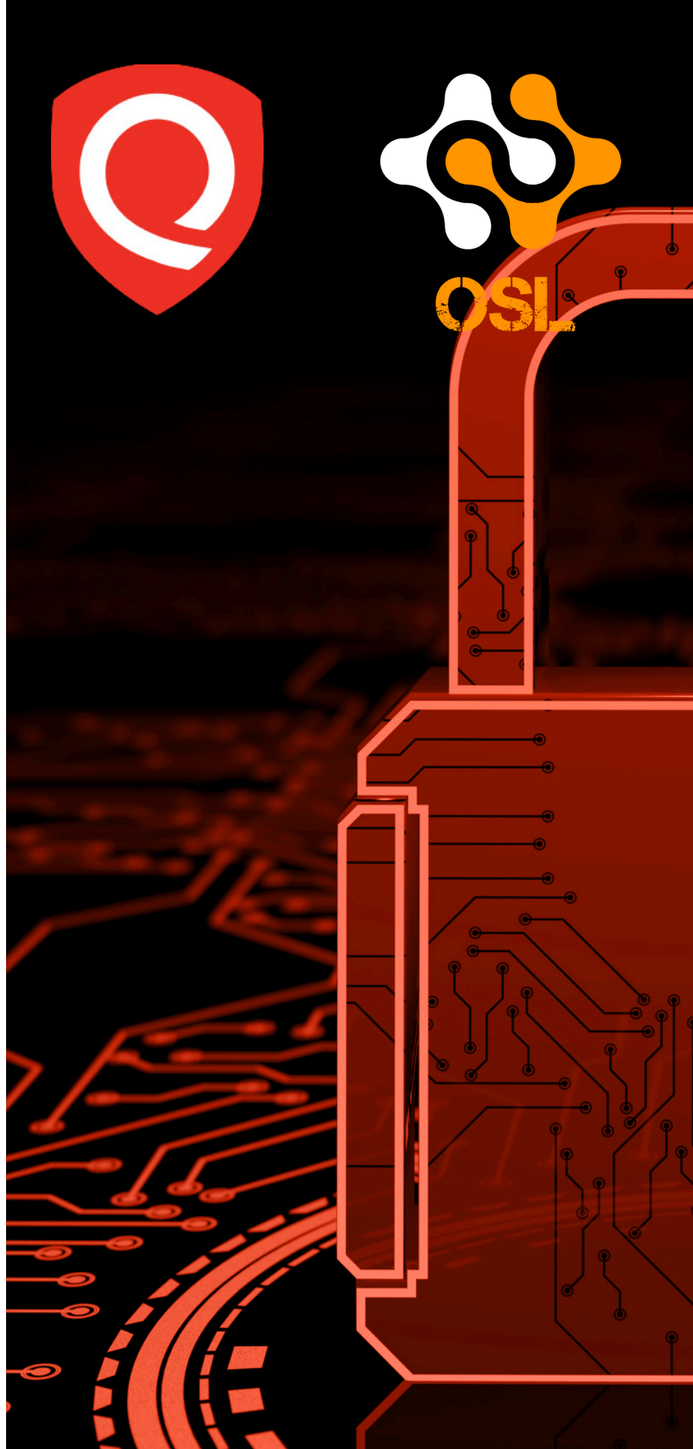
Inventario
Inventario automatizado e preciso com gestão automática de EOL/EOS

Unificação
Integração-bidirecional entre gestão de ativos, superfície de ataques, analise e otimização do tempo médio para recuperação MTTR

Alguns benefícios sobre a abordagem holística

Qualys ajuda a reduzir o risco de segurança com uma abordagem holística a cyber segurança

- Visibilidade 360 sobre todos os seus ativos, incluindo as redes isoladas
- Priorização estratégica focando em riscos criíicos e ações urgentes
- Identificação e resposta proativa dos riscos
- Remediações com base em recomendações automáticas
- Detecção e resposta contínua dos riscos



Onde Diferenciar o Qualys

Poderoso e Simples
40% Mais rápido em remediações para vulnerabilidades criticas com sistema de gestão de patches nativamente integrado

Redução rápida de Riscos
Auditorias aceleradas com painéis unificados que agregam centenas de órgão reguladores, incluindo FedRAMP, PCI, SOX, HIPAA, FINRA, GDPR, NYDFS, CCPA e outros

Uma Única Plataforma de Orquestração
Nativamente Integrado com todas as soluções da Qualys, assim como integrações com sistemas SIEM/ticketing

Ações Automáticas
Nativamente-integrado com gestão da superfície de ataque externa, patching, compliance, endpoint security e muito mais

Obrigado!

OSL COMERCIAL, LDA
Rua Antonio Feliciano de Castilho Nº72, Vila Alice - Luanda
www.osl-itservice.com
+ 244 929 735 666 | quote@osl-itservice.com