Elite Voip, Lda

Departamento Comercial

www.elitevoip-ao.com
comercial@elitevoip.co.ao
TLF: +244 **226 434 570**

“Vulnerability Management” para resultados económicos

21/03/2021

Elite Voip, Lda

Departamento Comercial

www.elitevoip-ao.com
comercial@elitevoip.co.ao
TLF: +244 **226 434 570**

- **GESTÃO ABRANGENTE DA VULNERABILIDADE COMO UM SERVIÇO**

Nenhuma organização possui os recursos necessários para tomar decisões totalmente informadas sobre a priorização de vulnerabilidades. Os objectivos de metas mudam diariamente com a descoberta de novas vulnerabilidades e um universo crescente de explorações tomando vantagem deles. A nossa empresa aborda o imperativo de gerenciar a exposição à vulnerabilidade dos nossos clientes, obtendo a solução mais eficaz, permitindo-lhes obter ainda mais valor das suas operações de segurança IT.

"***RiskSense Comprehensive Vulnerability Management as a Service***" é um novo modelo de produtos para empresas que disponibilizamos, combinando nossos serviços especializados e a Vulnerabilidade baseada em risco "**RiskSense**" Plataforma de gerenciamento (RBVM) para priorização de vulnerabilidade, atribuição e rastreamento de remediação e segurança relatórios de risco. Nós permitimos que as organizações corrijam o risco de segurança cibernética e tomem medidas rápidas com os negócios transparência que imensuravelmente fazem a diferença.

Com a nossa colaboração no apoio à segurança das organizações, as mesmas serão capazes de liberar recursos para se concentrar em itens de maior prioridade e melhorar sua postura de segurança em toda a rede informática.

O nosso serviço abrangente determina a capacidade de exploração de vulnerabilidades de rede e aplicativos da web. Fornece-mos o "scanning da rede", avaliação de vulnerabilidade, contextualização de ameaças integradas, criticidade de negócios e aumento do risco de exposição a ameaças ativamente usadas por natureza. Assim sendo, permite que a equipe se concentre estritamente em ações de remediação, reduzindo e / ou eliminando as ameaças aos sistemas. Por sua vez, o nosso serviço permite a monitorização continua à sua postura de risco de segurança com base na exposição ao risco adversário.

Vulnerability Management

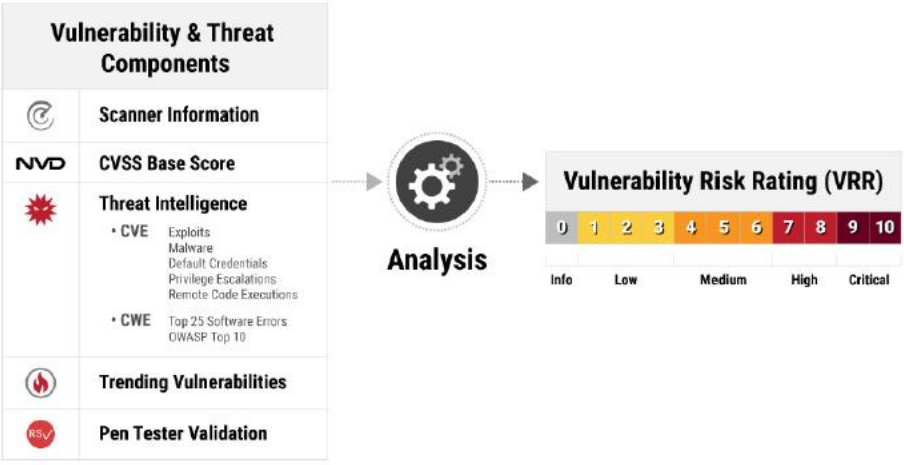
Elite Voip, Lda

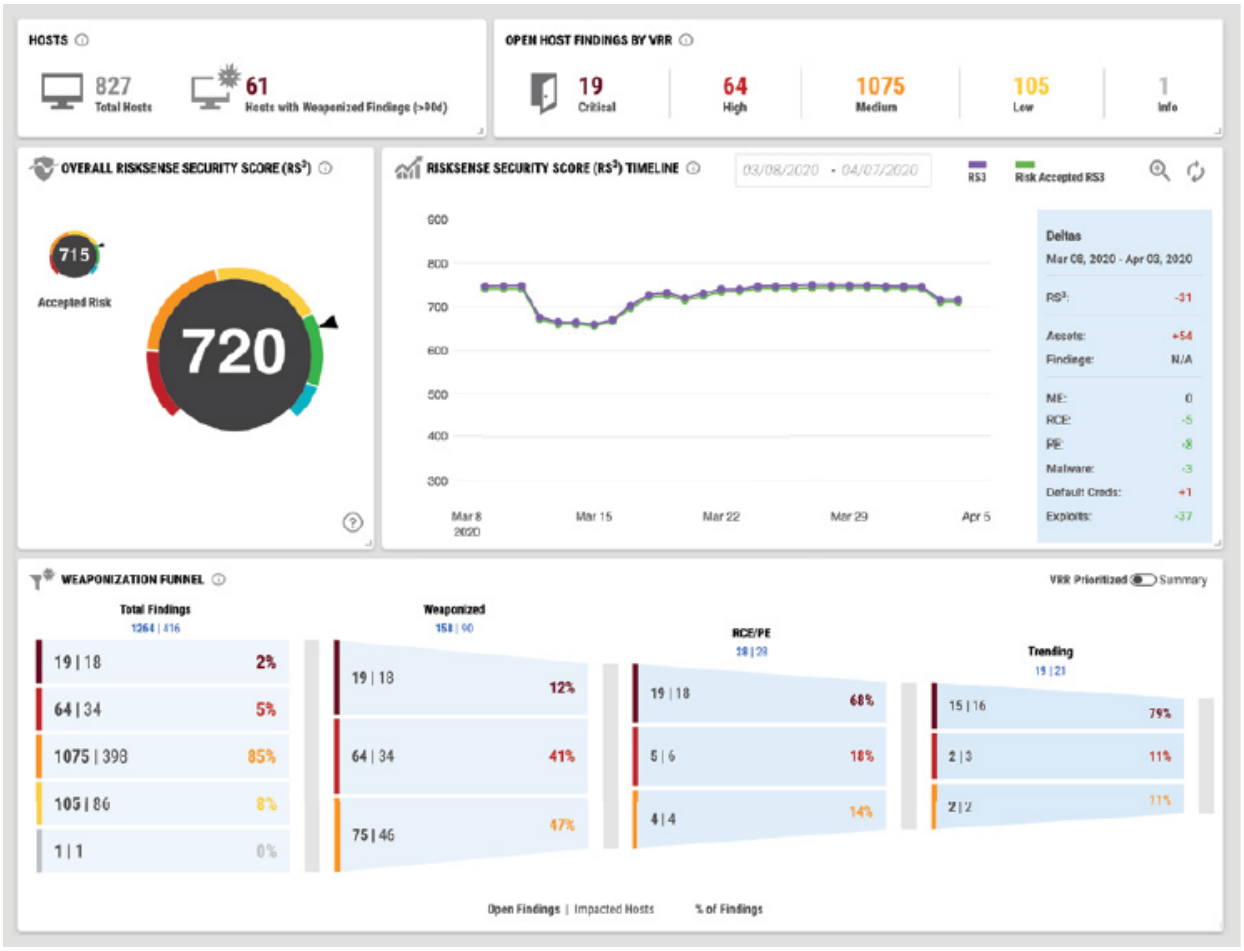
Departamento Comercial

www.elitevoip-ao.com
comercial@elitevoip.co.ao
TLF: +244 **226 434 570**

Novas vulnerabilidades de rede e aplicativos surgem diariamente, e as empresas devem detetá-las e mitigar vulnerabilidades antes que os adversários cibernéticos possam explorá-las. A quantidade e diversidade de vulnerabilidades é difícil de gerenciar com segurança a exposição ao risco.

Nossa equipe de analistas de segurança especializados usa as melhores ferramentas e processos de “scanning”, fornecendo a supervisão humana e controle de qualidade necessários para garantir a avaliação das vulnerabilidades na rede da empresa.





www.elitevoip-ao.com
comercial@elitevoip.co.ao
TLF: +244 **226 434 570**

- **Teste de penetração para validar as pontuações de risco com base nas condições do mundo real e controles de compensação.**

O teste de penetração, ou teste de caneta, é muitas vezes tratado como um atividade autónoma, realizada por um grupo de especialistas que não precisam interagir com o resto da organização de TI.

O teste de caneta pode identificar vulnerabilidades que parecem ser graves, mas representam um risco relativamente pequeno para a organização. Ele pode apontar outras pessoas que podem parecer inócuas por si mesmas, mas que podem ser exploradas em sequência para atingir o alvo de um invasor.

Por exemplo, um testador de caneta pode descobrir que uma vulnerabilidade com uma pontuação de gravidade CVSS alta afeta apenas alguns endpoints que não têm acesso a bancos de dados centrais, enquanto outra vulnerabilidade com uma pontuação mais baixa pode ser explorada por cibercriminosos para a cessar à chave propriedade intelectual. Além disso, a primeira vulnerabilidade pode exigir habilidades extensas para explorar, enquanto a segunda pode ser aproveitada por um hacker menos experiente com um kit.

Portanto, o teste de caneta deve ser tratado como uma parte central do programa moderno de gerenciamento de risco de vulnerabilidade. Informação de varreduras de rede, testes de aplicativos, simulações de phishing e outras fontes de informações de vulnerabilidade devem ser compartilhadas com testadores, que podem então usar essas informações para realizar testes que avaliam o risco real para a organização representado por cada tipo de vulnerabilidade. Além disso, os resultados dos testes devem ser analisados e divulgados aos grupos que priorizam e corrigem vulnerabilidades no curto prazo e aos responsáveis que tomam decisões sobre como fortalecer as defesas de segurança cibernética a longo prazo.

CONCLUSÃO:

Com um serviço moderno de gerenciamento de risco de vulnerabilidade formada por meio da mentalidade SecOps, as organizações podem:

• Aprimorar seu trabalho com a digitalização em rede para incluir visibilidade completa da totalidade da rede, avaliação simplificada e fluxos de trabalho de correção automatizada.

• Abordar melhor as vulnerabilidades de aplicativos da web ao analisar aplicativos mais complexos e adotando Práticas de DevSecOps para acompanhar os aplicativos que podem mudar diariamente ou de hora em hora.

• Mitigar os riscos do usuário vinculando a detecção de incidentes e recursos de resposta com gerenciamento de risco de vulnerabilidade.

• Avaliar o risco geral usando pontuação de risco personalizada e teste de caneta para priorizar vulnerabilidades com base sobre seu risco real para a empresa específica. Evoluir em direção a esse programa requer pensar bem o valor de cada área e encontrar oportunidades de integração às diferentes áreas.

Elite Voip, Lda

Departamento Comercial

www.elitevoip-ao.com
comercial@elitevoip.co.ao
TLF: +244 **226 434 570**

Serviços de Engenharia e Gestão de Sistemas de Informação

Consultoria Cibersegurança - Testes de Penetração

Serviço de "Penetration Testing" parcial, de acordo com o standard PTES (penetration testing execution standard)

- **Estão excluídos testes de:**

(i) "Exploitation";

(ii) "Post Exploitation";

(iii) âmbito disruptivo são sujeitos a acordo mútuo;

(iv) ativos do cliente que residam em infraestrutura de terceiros, são sujeitos a acordo mútuo e respetivas autorizações;

(v) intrusão em instalações físicas e outros casos que possam ser alvo de sanção, criminal ou outra, prevista na lei em vigor, são sujeitos a acordo mútuo e respetivas autorizações.

- Os trabalhos decorrem ao longo de 6 meses de normal actividade comercial do cliente. São previstas entregas parciais do relatório para acompanhamento do cliente, sendo que a informação só poderá ser considerada final na última entrega do relatório.

- As condições comerciais são:
  - 1/3 do valor na adjudicação
  - 1/3 do valor no final do 3º mês
  - 1/3 no final do 6º mês
  - A validade da proposta está sujeita a um levantamento inicial, conforme previsto na fase "Pre-engagement" do PTES.

VALOR TOTAL: 7.500.000,00 Akz

Com impostos incluídos

Elite Voip, Lda

Departamento Comercial

www.elitevoip-ao.com
comercial@elitevoip.co.ao
TLF: +244 **226 434 570**

Serviços de Engenharia e Gestão de Sistemas de Informação

Serviço de "Vulnerability Risk Management" com vista a gerir o risco das vulnerabilidades de software.

As vulnerabilidades são avaliadas do ponto de vista externo no sentido de diminuir a superfície de ataque a partir da internet, assim como do ponto de vista interno, para mitigar a superfície de ataque interna, nas atividades de movimentação lateral.

Para os casos de visibilidade das vulnerabilidades internas, o cliente deve disponibilizar um servidor físico ou virtual, onde será instalado uma sonda.

Consultoria Cibersegurança - Gestão do Risco de Vulnerabilidades

Valor Anual: 7.00.000,00 Akz/ano

OU

Consultoria Cibersegurança - Gestão do Risco de Vulnerabilidades

Valor SETUP (one-time): 2.300.000,00 Akz

Valor Mensal (sem compromisso): 1.000.000,00 Akz