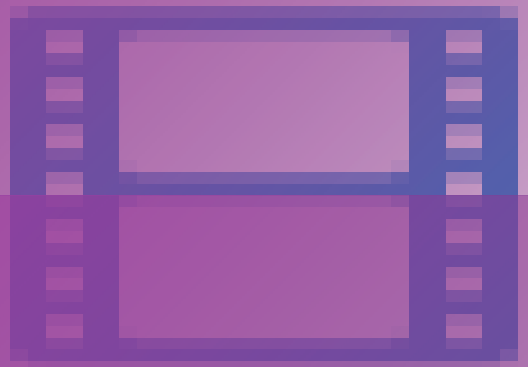
Cyber Security Services



Joas Antonio

SERVICES TYPES

PenTest

- Realização de Testes de Invasão, focando também em compliances como ISO27K, LGPD e PCI-DSS;
- Utilizar como principal framework e metodologia para os testes de invasão o PTES, NIST SP 800-15, OWASP-TOP 10;
- Os tipos de Testes oferecidos:
  - Black Box: Sem conhecimento nenhum do ambiente
  - Gray Box: Conhecimento Parcial do Ambiente
  - White Box: Conhecimento pleno do Ambiente

*Ponto focal: Criar modelos de documentos de Assessment e montar uma estrutura de Testes de invasão, sobre como é feito cada tipo de teste fornecido.

Analise de Vulnerabilidade

- Realizar Scanners de Vulnerabilidades em nossos clientes
- Podendo dar uma amostra grátis, realizando um Scanner em um site, servidor ou outra aplicação
- Categorias de Scanner:
  - Scanner Básico: Realizar uma varredura em alguns endereços IPs escolhidos pelo cliente e realizar uma varredura não muito profunda;
  - Scanner Completo: Realizar um Scanner completo em toda rede da empresa, até nas estações de trabalho;
  - Scanner apenas em servidores: Realizar a varredura apenas nos servidores da empresa;
  - Scanner voltado a Compliance: Varredura voltada a PCI-DSS como exemplo, para validar se está em compliance ou não o ambiente;

  *Ponto focal: Escolher uma boa solução para isso e estruturar um documento de assessment especifico

Teste de Phishing

- Podemos fornecer um primeiro Teste de Phishing de graça até 100 usuários;
- Após os testes podemos gerar um relatório ou criar um relatório e apresentar para o cliente e mostrar nosso cardápio de serviços;
- Realizar campanhas bimestrais ou semestrais de Phishing, ou campanhas voltadas ao ramo de negócio da empresa, simulado um Spear Phishing;
- Basear nossas campanhas conforme o Mitre Att&ck, utilizando em referências as técnicas que os grupos APTs trabalham;

*Ponto focal: Solução como Phishix

Security Awareness

- Poderia colocar o teste de phishing dentro desse serviço, mas vamos ir além;
- Após o teste ou não, conforme o NIST 800-50, podemos estruturar uma campanha de conscientização de segurança para os clientes, da seguinte forma;
  - Teste de Phishing
  - Auditoria de senhas: Verificar como é gerenciado a senhas, como os usuários criam suas senhas e etc..
  - Segurança nos navegadores: Estudar soluções, técnicas e métodos para proteger seus navegadores;
  - Teste de Engenharia Social: Famoso PenTest Físico, isso podemos alinhar depois com mais maturidade;
  - Segurança em dispositivos mobiles corporativos: Procurar soluções que auxiliam na segurança de dispositivos mobiles;
  - Treinamentos: Fundamental os treinamentos de segurança, podemos usar como base a certificação CSCU ou trazer parceiros para auxiliar;
  - Segurança no trabalho remoto: Propor soluções para auxiliar no trabalho remoto, algo a ser estruturado

Adversary Emulation

- O objetivo é verificar a eficácias dos componentes de defesas implementados, assim modelando e criando indicadores para melhor identificar um adversário, ou seja, um cibercriminoso;
- Utilizando como base o Mitre Att&ck e ferramentas para nos auxiliar como Infectmonkey e o Atomic Red Team;
- Pode ser vendido para empresas que já tem maturidade com segurança e precisam ter seus ambientes testados, indo além de um PenTest;

Criar um programa de gestão de reports de vulnerabilidades

- Algo interessante e que esta em alta é o bug bounty. É aquela questão, o que vem depois do PenTest? Preciso esperar 6 meses para um novo teste?
- Por isso, auxiliar o cliente a ingressar no ramo de Bug Bounty ou criarmos uma própria estrutura para isso é bastante interessante, no caso a nossa função poderia ser tanto como caçador como colaborador;
- Ajudar a implementar um programa de recompensa, definir escopo, auxiliar na comunicação entre empresa e pesquisador, realizar a triagem dos relatórios e auxiliar na correção;

PenTest SaaS

- Seria um Bug Bounty, mas diferenciado, aonde a empresa paga por mês para que se realize testes de vulnerabilidades em determinados IPS, ai será necessário uma plataforma nossa para oferecer algo do tipo e com resultado o cliente vai ter:
- 1) Descrição detalhada e prova de conceito para cada descoberta
- 2) Plano de correção acionável e feedback em tempo real
- 3) Mapeamentos de gravidade de risco e percepção do nível de esforço necessário para remediar as descobertas
- 4) Descobertas positivas que indicam quais controles de segurança você possui que são eficazes
- 5) Descrições, capturas de tela e correções sugeridas para vulnerabilidades

SOCaaS

- SOC como serviço? Exatamente, oferecer todo processo do NIST para nosso cliente
- Realizar um monitoramento 24 horas com nosso SOC, ajudando a identificar, proteger, detectar, responder e recuperar;
- Posso englobar também o SIEM SaaS como alternativa, onde o cliente poderá receber eventos através de protocolos e serviços como OSSEC, Snare, Snort, Nessus e por ai vai.
- Gerar automaticamente tickes de incidentes, acompanhando e registrando as atividades para contenção e mitigação;
- Usar indicadores KPI alinhados com a manutenção e registros dos logs para auditorias;
- Trabalhar com inteligência cibernética para fornecer relatórios mensais ou anual de ameaças detectadas;
- E claro, para ofertar o serviço precisa estar em compliance com PCI-DSS, ISO27K, LGPD, BACEN e entre outras normas;

SOCaaS

SOC Avançado: Recursos Técnicos

Recursos de coleta de dados e benefícios de conformidade do gerenciamento de logs

Informações sobre o tráfego de rede e o conteúdo de aplicativos fornecidos pelo Network Forensics

Recursos de correlação, normalização e análise do SIEM (gerenciamento de eventos e informações de segurança)

Automação da resposta a incidentes por Threat Intelligence / Runbook

Visibilidade da rede e detecção avançada de ameaças do NBAD (detecção de anomalia de comportamento da rede) e detecção de anomalias de comportamento do usuário pelo aprendizado de máquina - User Behavior Analytics

Gerenciamento de IOC / VM por Threat Intelligence

Capacidade de reduzir violações e garantir a conformidade fornecida pelo Gerenciamento de Riscos

Relatórios e visualização fornecidos pela camada de apresentação

https://inmetricscorp.sharepoint.com/:w:/s/CyberSecurity2/ERnRdrAtcxxOrgiOr_vuQqUBs8WCBLLIWwICJaIkpi4v2w?e=gV6zKq

SOCaaS

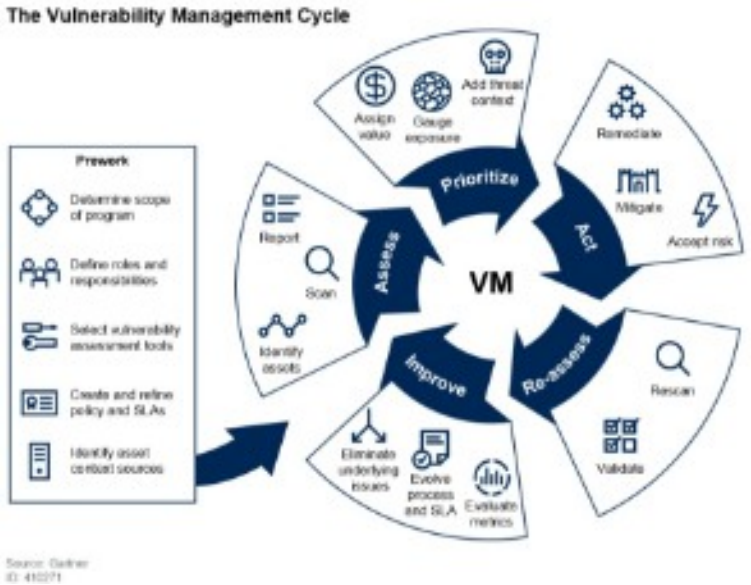
Os problemas que o SOCaaS irá *evoluir para resolver* são os seguintes:

- Simplifique a coleta de dados em qualquer lugar.
- Consolide a pilha de segurança.
- Transforme dados em métricas.
- Fornece orientação simples e real que permite a conformidade e fornece operações de segurança
- Eliminar ameaças de segurança automaticamente para que os clientes não precisem fazer isso.
- Um provedor SOCaaS terá uma plataforma nativa da nuvem e multilocações, não uma coleção de produtos.
- A plataforma será altamente escalonável e extensível, permitindo que os dados sejam ingeridos de qualquer coisa, mas normalizada facilmente para que os mecanismos de segurança sejam aplicados de maneira consistente.
- A plataforma se estenderá de forma flexível a redes, dispositivos, sistemas e SaaS de clientes.
- O SOC tocará todos os controles implantados em uma infraestrutura com APIs (não necessariamente pessoas).

SOCaaS

• O SOC fornecerá manuais com curadoria, mas interativos, para permitir que os clientes determinem o que é e o que não é importante para eles. (Isso injeta a "personalidade" de um cliente.)
• A plataforma irá automatizar todas as ações possíveis, contando com manuais criados por especialistas, mas inserindo a personalidade de um cliente, permitindo resultados altamente precisos e dados destilados para relatórios precisos. (IA e Machine Learning)
• Fornece métricas e pontuação essenciais que demonstram exatamente quais eventos foram observados e quais resultados foram realizados, juntamente com o impacto e a economia que os cerca.
• Um provedor de SOCaaS ajudará a alinhar o CIO / CISO dos dias modernos à plataforma, demonstrando economia e resultados simples, minimizando o uso de jargão técnico complicado.
• O provedor e a plataforma serão maleáveis, permitindo a rápida implantação de "aplicativos" de segurança.
• Todos os aplicativos da plataforma devem ser perfeitamente integrados aos playbooks, automação, métricas e pontuação.

*Pontos focais: Procurar soluções, investir em processos internos primeiramente e contratar mão de obra para chegarmos nesse patamar, termos nosso SOC bem estruturado e bem implementado para ofertar como serviço



Gestão de Vulnerabilidades

- Uma das maneiras mais comuns de falhar na VM é simplesmente enviar um relatório com milhares de vulnerabilidades para a equipe de operações corrigir. Os programas de VM bem-sucedidos aproveitam técnicas avançadas de priorização e ferramentas de fluxo de trabalho automatizadas para agilizar a transferência para a equipe responsável pela correção.
- As organizações que adotam as práticas de DevOps devem adotar uma abordagem integrada aos ciclos de integração / entrega contínua (CI / CD) e abordar os problemas nos estágios de pré-produção.
- Incluir a identificação de questões subjacentes como um dos principais objetivos do processo de VM. Embora ainda seja importante encontrar e resolver vulnerabilidades individuais, a VM também deve fornecer informações sobre as áreas que precisam ser aprimoradas na postura de segurança da organização.
- [Na frequência de varredura VA] A meta de frequência final deve refletir o valor de fornecer dados de vulnerabilidade atualizados para processos de consumidor, como patching e monitoramento de segurança. Se esses processos não se beneficiarem de verificações mais frequentes, realmente não há sentido em tentar obter uma frequência mais alta.
- A mitigação pode muitas vezes ser a primeira linha de defesa, especialmente se puder ser implementada rapidamente. No entanto, as vulnerabilidades atenuadas não desapareceram. Eles ainda precisam ser consertados eventualmente.
- Todas as exceções devem ter uma data de validade. Não permita exceções indefinidas.

Gestão de Programas de Segurança

- O risco de segurança cibernética afeta organizações e corporações de todos os tamanhos e setores da indústria. Desenvolver e manter uma estratégia de segurança da informação eficaz pode ser difícil sem um talento dedicado à segurança, incluindo liderança. Os recursos internos de uma organização estão em constante mudança. Além disso, as capacidades dos agentes de ameaças estão melhorando continuamente. Como resultado, as empresas estão investindo mais tempo, esforço e recursos para reduzir os riscos para os negócios.
- O objetivo é ajudar as empresas a desenvolver estratégias priorizadas e se concentrar em um processo de melhoria contínua do programa de Segurança da Informação. As iniciativas resultantes reduzem o risco do negócio, melhoram a disponibilidade e permitem que a organização se concentre nas principais atividades de negócios.

Ponto focal: Ter profissionais que conhecem bem de Arquitetura de Segurança da Informação

Resposta a Incidentes e Forense

- A equipe de Resposta a Incidentes da Inmetrics auxilia os clientes a determinar o QUÊ, COMO e QUANDO de uma violação, enquanto desenvolve um plano e processo para conter e remediar o dano.
- As organizações afetadas por incidentes de segurança têm um parceiro confiável no Inmetrics para determinar a extensão do comprometimento e criar etapas acionáveis para manter os danos sob controle. Seja diante de um funcionário insatisfeito, insider mal-intencionado, hackers, uma violação em grande escala ou se você precisar de assistência como uma testemunha especializada para suporte em litígios, o Inmetrics ajuda as organizações de vítimas com contenção e remediação, garantindo que danos e impactos sejam minimizados. O Inmetrics pode ajudar a identificar como os invasores estão acessando seu ambiente, determinar como mitigar o acesso do invasor e ajudar a prevenir ataques futuros. Utilizamos hardware e software aceitos pela indústria e de primeira classe para realizar a Resposta a Incidentes para garantir resultados rápidos e precisos.

Inteligência e Caça de Ameaças

- Usar como base o OSINT Framework e ferramentas complementares para auxiliar na investigação de um incidente, trabalhando ao lado do contexto de Resposta a Incidentes e Forense;
- Além da caça de ameaças, monitorando forums tanto na surface, darkweb, darknet e por ai vai, trazendo métricas e dados que podem auxiliar no plano de reação, além de ingressar em projetos colaborativos como o IST Ransomware Task Force e o MISSP;
- Trabalhar com soluções de mercado como Anomali, Apura e entre outras, como parceira estratégica no fornecimento de serviços e auxiliar tanto no SOCaaS e Resposta a Incidentes;

Segurança de Aplicação

- Oferecer serviços voltado a segurança de aplicação, como analise SAST e DAST, code review e desenvolvimento seguro;
- Englobar com testes de performance da aplicação utilizando o que já temos em casa para trabalhar lado a lado com segurança da informação;

Gestão de Riscos

- **O gerenciamento de riscos envolve a compreensão, análise e abordagem dos riscos para garantir que as organizações atinjam seus objetivos. Portanto, deve ser proporcional à complexidade e tipo de organização envolvida.**
  O Enterprise Risk Management (ERM) é uma abordagem integrada e combinada para gerenciar riscos em uma organização e suas redes estendidas.
- **Como o risco é inerente a tudo o que fazemos, os tipos de funções desempenhadas pelos profissionais de risco são incrivelmente diversificados. Eles incluem funções em seguros, continuidade de negócios, saúde e segurança, governança corporativa, engenharia, planejamento e serviços financeiros.**

Pontos focais: Usar a ISO 27005 + NIST e ter uma plataforma para trabalharmos o

Consultoria em Cibersegurança com foco em GRC

- **Prestar serviços de consultoria, auxiliando as empresas no processo de conformidade em Governança, Risco e Compliance com normas e padrões.**

Pontos Focais

Comentários

- Existem uma gama de serviços e possibilidades, principalmente pegar o nosso modelo de negócio e dar uma repaginada, assim trazendo oportunidades não só para segurança;
- Mas antes de tudo, precisamos investir em mão de obra, procurar parceiros e ter canais de comunicação para nos auxiliar;
- Gerar bastante leads para garantir nosso espaço como parceiros e referência no assunto;
- Ter um centro de capacitação profissional como parceiro, é fundamental para preparar nossos profissionais;
- Pegar o gartner das soluções em alta do mercado e fazer um estudo, marcar reuniões, ver webinars e por ai vai;
- Entre outros fatores que podem ser discutidos;