Segurança Cibernética

SERPRO
Soluções digitais que conectam governo e sociedade

SERPRO

Agenda

01 **Realidade**

02 **Segurança Operacional SERPRO**
Times de segurança nos dias de hoje

03 **Incidentes Recentes**

04 **SOC – Centro de operações de segurança**

05 **Destaques**

Segurança Cibernética

“Segurança da Informação é quase sempre vista como excessiva, até o dia em que não é suficiente”

Segurança Operacional

Áreas de atuação

SOC

Coordenar o tratamento de incidentes
Efetuar a monitoração de segurança
Buscar por novas ameaças
Gestão de Vulnerabilidades Infraestrutura

Pentest, Forense & Patch

Gestão de patchs
Segurança Ofensiva
Forense Computacional

Eng. Arquitetura de Segurança &Cloud

Desenvolvimento de análise de arquiteturas de segurança.
Atuação em proteção de ambiente em Cloud

Gestão de FW & IPS

Configuração e sustentação de FIREWALL e IPS

Segurança no Desenvolvimento

Padrão de desenvolvimento seguro
Análise de vulnerabilidade Aplicação (Caixa Preta)
Análise de vulnerabilidade código (Caixa Branca)
Gestão de WAF

VPN & EndPoint

VPN
Proteção de Endpoint

Demandas de Segurança

Atendimento de tickets
Sustentação de regras de Firewall
Sustentação de demandas de outras áreas da empresa

Incidentes Recentes

Data of 143 million Americans exposed in hack of credit reporting agency Equifax

EQUIFAX – dados vazados de mais de 143 milhões de americanos - falha principal Apache Struts (CVE-2017-5638).

Incidentes Recentes

Hacked: 92 Million Account Details for DNA Testing Service MyHeritage

Uber concealed massive hack that exposed data of 57m users and drivers

Incidentes Recentes

Banco X – 40 gb de dados de clientes. nomes, endereços, senhas, cpf, rg, IRPF, catões/cvv e etc. Além das chaves de criptografia, chaves SSH, e código fonte do core Banking.

Hacker: "O grande recado que quero deixar nesse artigo é, quando for para a nuvem, não esqueça o que você sabia sobre segurança. Ao Contrário, é preciso implementar mais controles, não apenas controles diferentes."

Fonte: Tecmundo

SERPRO
SOC


Planejamento e reconhecimento
Ocultação de rastros
Scanning
Metodologia Pentest
Manter acesso
Enumeração
Exploração

Planejamento SOC

Domínio de ferramentas

Domínio de ferramentas de SIEM
Domínio de coleta de eventos.

CTI & Investigações

Inteligência de ameaças
Investigações mais aprofundadas

Machine learning

Aplicar machine learning as correlações do SOC
Testar funcionalidade

SOAR – Automação de resposta

Adquirir e implantar ferramenta de automação, triagem e investigação

User Behavior

Correlação baseada em comportamento

SERPRO

Atividades diárias de um SOC

01

Monitoração

- ✔ Desenvolvimento de casos de USO
- ✔ Prática de Monitoração
- ✔ Bloqueio atividades maliciosas

02

Manutenção SOC

- ✔ Melhoria de ferramentas
- ✔ Coleta de eventos
- ✔ Buscar Automação

03

Tratamento de incidentes

- ✔ Tratar incidentes de segurança
- ✔ Padronizar tratamento de incidentes
- ✔ Ferramenta de fluxo de tratamento de incidentes.

04

Vulnerabilidades

Fazer a gestão de vulnerabilidades.

Ferramentas

Ter ferramentas adequadas para a execução da atividade:

Falta ferramenta de fluxo de tratamento de incidentes

Evolução SOAR

Processos

Ter os processos bem documentados e de conhecimento da equipe aderente as atividades e com cumprimento de requisitos legais

Pessoas

Equipe bem qualificada e motivada para a execução das atividades.

Aspectos importantes

Situação ideal

Aspectos importantes

Engajamento da empresa
Como todos devem se unir para cumprir essa atividade?

Segurança
Como a segurança será afetada nos próximos anos? IoT, Cloud, API, APP, Home Office.

Mudança de políticas e normas e contratos
Alguma adaptação será necessária?

Incidentes
Eles continuarão existindo e a Resposta será fator crítico de sucesso

Tiago Iahn

Cargo: Gerente de Cibersegurança
E-mail: tiago.iahn@serpro.gov.br

/serprobrasil
@serprobrasil
@serpro
/serpro
serpro.gov.br

SERPRO
Soluções digitais que conectam governo e sociedade