Roadmap de Estudos para se Tornar um Profissional de Segurança

Governança de Segurança – É o time que governa ou planeja as ações de Segurança para a empresa. Confunde um pouco com gerenciamento de segurança, mas cuida dos planos, dos projetos, escolhe ferramentas, define controles, organiza o time.

- Confidencialidade, Integridade e Disponibilidade
- Definição de Métricas
- Definição de Roadmap
- Levantamento de Requisitos de Negócios
- Privacidade

Gestão de Risco – Avalia os riscos que a empresa tem, risco de fraude, risco de incêndio, risco de mercado... E depois com a Governança, vai implementar controles para diminuir ou acabar com o risco.

- Avaliação de Riscos;
- Definição de plano de mitigação;
- Aplicação de controles de risco

Conformidade – Toda empresa tem leis que deve seguir. Por exemplo, toda empresa precisa emitir nota fiscal. Na segurança, algumas empresas têm obrigações de segurança, que estão na lei. A Lei de Privacidade e Marco Civil da Internet é um bom exemplo de leis.

- Normas de Segurança
- Guias de Segurança
- Leis aplicadas à Segurança
- Auditorias

Segurança de Dados – Define os processos e políticas de dados. Como serão armazenados, como serão controlados, como será feito backup, como evitar vazamento de dados.

- Classificação de Dados
- Integridade
- Criptografia e Confidencialidade
- Assinatura Digital
- Certificado Digital e Infraestrutura de Chaves Públicas
- Backup
- Descarte Seguro de Dados

Controle de Acesso – Gerencia o acesso dos colaboradores, clientes, parceiros aos sistemas da empresa e consequentemente aos dados. Define por exemplo a política de senha, quais métodos de autenticação devem ser usados.

- Controle de Acesso
- Auditoria e Federação de Acesso
- Provisionamento de Acesso

- Usuários Privilegiados

Segurança de Redes e Telecom – Se encarrega de avaliar os riscos de segurança na rede cabeada, sem fio, VPN, comunicação de datacenters, internet e também a parte de telefonia.

- Segurança de Redes e Infra
- Recursos de Proteção de Redes
- Segurança de Infraestrutura de Tecnologia
- Serviços de Rede

Segurança de Software – Avalia softwares desenvolvidos internamente e os softwares adquiridos no mercado. Também gerencia a atualização dos softwares, para evitar vulnerabilidades conhecidas.

- Segurança de Software
- Software Desenvolvido
- Segurança de Dados em Softwares e Testes
- Gerenciamento de Patches

Segurança de Endpoints – fica responsável pela segurança de dispositivos dos usuários, desktops, laptop, celulares, tablets e qualquer outro equipamento de ponta. Algumas cuidam de impressoras, scanners também e os dispositivos IOT. Internet das coisas.

- Segurança de Endpoints
- Mobile Device Management
- Atualização de Softwares e Firmwares
- Segurança de Desktops

Segurança Física – gerencia os riscos de ambientes físicos. Incêndios, danos elétricos, alagamento, furtos, roubos, invasão, vandalismo e tudo associado com informações da empresa nestes meios.

- Segurança Física
- Segurança de Datacenters
- Riscos Físicos
- Segurança Física de Dados
- Monitoramento de Segurança Física

Cloud Security – vai gerenciar todas as aplicações que rodam em nuvem publica, como por exemplo Office 365, Salesforce e os sistemas que rodam em nuvens como AWS, Google, Azure.

- Cloud Security
- Controlando acessos em Cloud Security
- Diferenças entre Cloud Security
- Proteções e Conformidade de Cloud Security

Inteligência de Segurança – neste ponto algumas pessoas confundem com inteligência artificial na segurança. Não é o caso aqui. Em inteligência de segurança é o monitoramento dos ambientes e o tratamento de eventos de segurança. É aqui nesta

parte por exemplo, que atuam os hackers éticos, engenheiros sociais, forense computacional.

- Inteligência e Operação de Segurança
- Preparando e Detectando Ataques
- Anatomia de Ataques
- Controles Operacionais de Segurança

Resposta a incidente – é a área que vai cuidar dos planos de emergência caso um evento de segurança ocorra. Por exemplo um incêndio no Datacenter. Como você deve fazer para resolver esta emergência. Tudo tem plano, ensaio, testes....

- Resposta à Incidentes
- Demais Planos de Resposta
- Outras Ferramentas de Apoio
- Testes e Ensaios de Segurança
- Reciclando Planos

Ética Profissional – Bom, não é apena o hacker que deve ser ético. Existem algumas regras da nossa profissão, que devem ser seguidas. Por exemplo, aqui você precisa conhecer o que é um documento de Confidencialidade, como você deve tratar informações sigilosas.