PERFIL

Profissional C-Level, Executivo, com visão estratégica para negócio atua no Comitê e ativo no Board. com 12 anos de experiência. Lider nato, com larga experiência, em missão crítica de empresas de portes variados , atuando em áreas estratégicas, Risco, Análise de Vulnerabilidade, Resposta a Incidente de Segurança, Análise de Vazamento de Informação, Gestão de Crises, Análise de Riscos governança corporativa, SOC, SIEM, Frameworks, IAM, gestão de identidades, IA.
Experiência internacional: Morou no Japão durante o período aproximado de 4 anos, onde desenvolveu linguagem e escrita para expandir novos horizontes no mercado de trabalho onde conheceu novas culturas, diversidades e ensinamentos.

CONTATO

11 91618-5591

EMAIL:
diego.tajima@gmail.com

LinkedIn
www.linkedin.com/in/diego-tajima

PORTIFÓLIO:
https://cyberbrasil.site/portfolio

CERTIFICADOS
https://cyberbrasil.site/certificacoes-e-eventos

FORMAÇÃO ACADÊMICA

Setembro 2022
Estácio
MBA Executivo Gestão Cyber Segurança Empresarial
Status: Concluído

DIEGO TAJIMA

IDADE 35 ANOS - 19/12/1989 - BRASIL

| C-Level | MBA Cyber Security | Incident Response | Security Operation Center | CSO | CISO | CTO | CIO

- Profissional com 12 anos de experiência. Gestor de Segurança da Informação há 8 anos, com larga experiência em missão crítica e empresas de portes variados, atuando em áreas estratégicas, risco, governança corporativa, SIEM, Frameworks, gestão de identidades, AD e gestão de incidentes. C-Level, Executivo, com visão estratégica para o negócio atua no Comitê e ativo no Board.
- Segurança da informação, security office, projetos processos de negócio, inteligência operacional, gestão conhecimento e serviços e operacionais, especialista em risco e TI, administrador, analista Hardware, Software, AD, Rede e Cloud, SIEM e SOC.
- Especialidades: gestão de risco, governança, tecnologia e segurança da informação, meio de pagamento eletrônico. Sólida experiência PCI, ITIL, COBIT, NIST, SANS, MITRE, defender Lean IT, PMBOK (PMI), ITSM; SCRUM, BSC, SOX. SIEM, normas e padrões de Segurança da Informação e Tecnologia (ITIL, ISO27001, ISO 27002, COBIT, MITRE, SANS, CIS e NIST), ISA/IEC 62443 e cofre de senhas (Cyberark e Senha Segura).
- Gestão de equipes planejar executar projetos em Risco e Tecnologia TI. Segurança da Informação baseline, patching, hardening, cybersecurity, pentest/vulnerabilidade, classificação informação, descarte e retenção mídia e backup, controle de acesso físico/lógico; SIEM, WAF, DAM, FIM, EDR; resposta a incidente, gestão de crise. Administração de NGFW, WAF e NAC, segmentação de VLANs, microsegmentação, roteamento, regras de firewall, IPS/IDS, VPN e SDWAN;
- Gestão risco operacional (análise crítica, modelagem, grau e tipificação, tratamento de risco; estabelecer, testar ,monitorar controles). - Monitora eventos (serviço, antifraude – Dev/Homologação/Produção); - Implantação gestão serviço (SLA/TI/Service Desk); - Processos negócio: análise/map/modelagem.
- Atuação conformidade, auditoria (interna/externa), fraude (coleta, organização, análise prevenção, detecção).
- Continuidade negócio (plano contingência e continuidade, análise impacto BIA) -contrato fornecedor; CAPEX/OPEX; Comitê Executivo e ativo no board da empresa.

EXPERIÊNCIA DE TRABALHO

Dezembro 2024 – Atual
Unidas - São Paulo, Brasil
Gestor de segurança da informação Blue, Red Team e Vulnerabilidases

Gestão de Políticas, Normas e Procedimentos, contemplando as melhores práticas utilizadas internacionalmente e realizar as devidas considerações de Si ao Negócio;
Competência e Habilidade para trabalhar de forma colaborativa com múltiplos times técnicos e multidisciplinar;
Experiência em Elaborar relatórios técnicos e gerenciais de investigações, avaliações realizadas e indicadores;
Elaborar, sugerir e conduzir planos de ação contemplando a mitigação das vulnerabilidades identificadas, para um curto, médio e a longo prazo;
Experiência com gestão de contratos e fornecedores de segurança.

Maio 2022
Harvard
Pós Ciências da Computação

Setembro 2021
Anhanguera
Graduação Analise e Desenvolvimento de Sistemas

IDIOMAS

Inglês Avançado C1
Espanhol Proficiente C2
Japonês Avançado C1
Português Proficiente C2

CERTIFICAÇÕES

Formação e Liderança

AWS IA Generativa.

Formação de Liderança C – Level

Competência Transversal Tecnologia da Informação e Comunicação

Curso de CTO

Curso de DPO

Curso de LGPD

Curso de GRC

Curso de SOC

ISO/IEC 27001 - Dynamics of Information Security Management System (ISMS)

MITRE&ATTACK

NIST

COBIT

SANS

ISO/IEC 27005:2022 Start: Gestão de Riscos de Segurança da Informação

IBM QRADAR

Microsoft AZ- 900

CISCO – cyber security

Curso Perito Forense Digital,

Proteção de bancos e finteches

ISA/IEC 62443

Red Team:
Realiza testes de penetração em sistemas e aplicações, identificando vulnerabilidades e propondo soluções.
Ser responsável pela análise de vulnerabilidades em aplicações (Web e Mobile) e APIs;
Direcionar apoiar tecnicamente os times de desenvolvimento sobre como implantar os controles de segurança;
Elabora documentos e relatórios contendo a análise realizada, a evidência da vulnerabilidade e a sugestão de correção;
Faze especificação de requisitos de Si e atualização de baseline.
Desenvolve e executa ataques simulados para avaliar a postura de segurança da empresa.
Analisa os resultados dos testes, documentar as descobertas e criar relatórios detalhados.

Blue Team:
Monitora continuamente os sistemas e redes em busca de atividades suspeitas e incidentes de segurança.
Analisar logs e alertas de segurança para identificar e responder a ameaças.
Implementa e manter sistemas de detecção de intrusão (IDS) e prevenção de intrusão (IPS).
Realizar a correção de vulnerabilidades e incidentes de segurança.
Coordena Time técnico composto de especialistas e analistas de "Cybersecurity
- Blue Team";
Gestão de Projetos e de contratos especializados em SI;
Gestão de avaliação da produtividade e desempenho;
Experiência no direcionamento estratégico das atividades threat intelligence, SOC CSIRT;

Maio 2022 – Novembro 2024
Nava For Business - São Paulo, Brasil
Gerente de segurança da informação Executivo - CISO

Visão estratégica do negócio, adota as melhores práticas para ganhar visibilidade do park, aloca os melhores recursos, tem contatos com fornecedores, serviços e clientes para um melhor network. Tem uma gama de clientes como grandes Bancos, financeiras, Energia nível Brasil e serviços;
Responsável pelo SOC - Tem uma visão aguçada para discernir alertas reais e falso positivo, com isso instrui e dá o melhor direcionamento para a equipe 42 pessoas.
Cuida e desenvolve temas apresentados pelos cliente sempre com resiliência e melhores práticas do mercado;
Desenvolve junto com time de desenvolvedores a IA, inteligência artificial para soluções aos clientes como ChatGPT.
Gestão que exalta a liderança ao Invés de imposição, tem um mindset para novas tendências e tecnologia;
Visão de melhoria contínua com suas equipes de 42 pessoas N1, N2 e N3 operacionais consultores e especialistas, equipe de GRC, blueteam e redteam, gestão de acessos e Compliance, WAF, tendo foco SOC e anti-fraude. Realiza entrevistas, alocação de recuso em clientes, redireciona e desligamentos;
Vivencia a parte financeira de projeções, capex e ocapex, métricas e valuation com variável de câmbio estrangeiro e forcast de cada projeto.

Destaque:
Responsável pela BU de segurança da informação dentre as 5 BU da empresa obteve destaque no valuetion triplicando a meta de valores sendo que mais faturou no ano de 2022.

Janeiro 2022 - Junho 2022
Stefanini - São Paulo, Brasil
Coordinator Cyber Security

Coordenação de Incidentes e Defesa Cibernética - Responsável pela resposta tempestiva , contenção de impacto na resposta a incidentes e proteger as informações críticas e as Jóias da Coroa;

AFILIAÇÕES

•Membro do comitê público Associação Nacional de Proteção e Privacidade de dados – ANPD

•Membro do conselho publico Instituto de Defesa Cibernética – IDCIBER

•Membro do Comitê público da Associação Brasileira de CIO's -ABCIS

•Membro do CISO´S CLUBE BRASIL

REALIZAÇÕES

CISO - Diretor de segurança da informação.

Responsável por torre de segurança de informação, BU.

Gestor de Crise Cybernetica.

Domínio em elaboração de relatórios (técnicos e gerenciais) de incidentes e causa raiz, PDI, BIA, PDR, POP, PB ; Coordenar e atuar em ações de melhoria contínuas dos playbooks e runbooks de cenários de ataques cibernético ; Tem resiliência e empatia; Habilidade de construir um bom relacionamento interpessoal e com a equipe, One a One, feedback construtivo e Fastback e sempre gosta de ouvir a opinião da equipe; Realiza controle de horas dos colaboradores, faz ajustes de horas e escalas, faz planilhas de horas de cada funcionário;

Coordenar a revisão de controles internos e externo para acompanhamento de métricas SOC. Atuar na revisão de processos , controles e procedimentos de operação de segurança da informação, Anti-Fraudes e Proteção de Dados; documenta as ações das equipes ; Apoiar na construção e desenvolvimento de políticas, normas e procedimentos; Acompanha a qualidade das entregas nos atendimentos da equipe de 14 pessoas, 24x7, visando a melhoria contínua ; Monitora e traçar planos de melhoria para a performance da equipe com metodologias ágeis Scrum master e Kamban. Atua para que as entregas sejam realizadas dentro dos prazos; Manter comunicação proativa e consultiva com os clientes internos e externos ; Realizar reuniões de status e acompanhamento de serviços prestados ;

Experiência em soluções de segurança (Firewall , IPS , Antivírus , DLP , EDR , AntiSpam , WAF; AntiDDOS , NAC , GRC , HSM , Criptografia , Scan de Vulnerabilidades e SIEM; Conhecimento dos frameworks de segurança como NIST , CIS , família 27000 ; ISO 27001 , MITRE ATT & CK , ISO27005, ISA/IEC 62443 , PCI / DSS; CIS Control ; ITIL Foundation para gerenciamento de serviços em TI, Conhecimento da LGPD (Lei Geral de Proteção dos Dados) ; Conhecimento em Segurança de Perímetros , segurança de infra - estruture , equipamente aplicações.

Destaque:
Elaborou e Implementou a ISO2701 em uma grande rede de moda empresa multinacional Arezzo. Realizou o projeto da PM São Paulo onde desvincula o nome da função e dados pessoais dos agentes públicos tanto na deep web, dark web e surface. Utilizou da normativa ISA/IEC 62443 em uma empresa de Mineração Vallourec.

Julho 2021 - Janeiro 2022
Italtel - São Paulo, Brasil
Consultor SR

Gestor de crise de uma grande financeira, elaboração mitigação e lições apreendidas elaboração de playbooks, runbooks, Pops, fluxogramas das áreas; Implementação de frameworks de segurança como ITIL, COBIT, MITRE e Sans. Realizou a maturidade das áreas com a ISO27001 e compliance LGPD e no segmento industrial a normativa ISA/IEC 62443. Elaborou treinamentos de segurança da informação para diversas áreas da empresa para conscientização dos colaboradores melhores práticas e resiliência dos temas atuais de malwares, vazamento de informações e evasão de dados;
Atuou full part em um grande Banco e realizou projetos com uma grande empresa multinacional de telecomunicações onde coletava cves, hardening e patching e realizava suas atualizações.
Realiza o controle de horas dos alocados e projetos , faz ajustes de horas e escalas, faz planilhas de horas do projeto. Realiza entrevistas, alocação de recuso em clientes, redireciona e desligamentos. Cuidava dos custos envolvendo alocados, projetos e faz o ponto focal com o cliente.

Destaque:
Gestor de Crise de uma grande financeira onde era responsável por liderar a equipe de segurança da informação e anti fraude, orquestrar as war room's onde mitigou dois ataques de Ramsonware importantes.

Novembro 2018 - Julho 2021
UnitedHealth Group - São Paulo, Brasil
Coordenador de segurança da Informação

Coordenador de Segurança da informação acompanhamento da alta gestão na visão estratégica. 12 pessoas sob sua gestão.
Direcionamento do setor N1,N2 e N3 participação atividades como reuniões e apresentações e autonomia de gestão de acessos ao cofre de senhas da empresa; Representou área de direct de segurança da informação; Principais atividades Análise de relatórios para liberação de acesso ou alteração de Atua

com SAP e Protheus e outras ferramentas TOTVS, Sistemas operacionais (ambiente de servidores de rede e ambiente de estações de trabalho) AD e JIRA. Certificações em sistemas operacionais e produtos de segurança, Protocolos de rede (TCP/IP), Produtos de segurança de rede, como endpoint protection, firewalls, prevenção de intrusão, gestão de segurança Service Now, SAP e Rundeck, Portal Colaborador, AD, Redes entres outras atribuições.

Realizou toda parte documental juntamente com o time de GRC e compliance atualizando políticas e procedimentos voltados a segurança da informação.

Destaque:
Deixou toda área de segurança informação em compliance com as diretrizes de todos os hospitais onde foi visto com bons olhos todo trabalho realizado.

Março 2015- Novembro 2018
Toyota Motor Corporation - Aichi-ken, Japan
Auditor de Qualidade
Auditor de qualidade de produtos, técnico de solo. Interação com clientes e funcionários. Realizava auditoria em sistemas e gerenciamento de tarefas. Metodologias Kanban, Scrum e metodologias ágeis. 5S, normativa ISA/IEC 62443 e processos de conformidade destinadas a cada país de exportação. Voltado a qualidade interna e externa Toyota.

Agosto de 2012 - janeiro de 2015
Itaú Unibanco - São Paulo, Brasil
Analista de Segurança da Informação JR.

Analista de de segurança da informação - Verifica fluxo de projetos em andamento, implantação, desenvolvimento, finalização, prazos, gestão de equipe e apresentação. Voltados a segurança da informação

Habilidades e competências

Conhecimentos na área de segurança da informação
Rapidez na resposta a situações de crise
Habilidade de desenvolver gestores para gerar equipes de alta performance

Domínio da Lei Geral de Proteção de Dados (LGPD)
Proteção de dados confidenciais
Visão aguçada para identificação de riscos à segurança.