Sobre o Time de Product Security

O time ProdSec da Dock é responsável por garantir a segurança dos ambientes de produção, implementando controles de segurança avançados, monitorando continuamente as operações em busca de possíveis ameaças e respondendo de maneira rápida e eficaz a vulnerabilidades. A equipe trabalha incessantemente para garantir a integridade, a confiabilidade e a continuidade das operações críticas da organização, promovendo um ambiente digital seguro.

Missão: Assegurar um ambiente digital protegido para todas as operações da empresa.
Visão: Ser referência global em segurança da informação, promovendo inovação contínua e proteção intransigente.
Valores: Segurança, integridade, inovação, colaboração e transparência.

Nossas Frentes de Atuação:

- **RedTeam (Offensive):** Conduzimos testes de penetração para identificar e explorar vulnerabilidades em sistemas, aplicando técnicas de ataque para antecipar possíveis riscos.
- **AppSec:** Realizamos revisões de código e implementamos controles de segurança para proteger nossas aplicações, promovendo uma abordagem de segurança desde o início do ciclo de desenvolvimento.

Guia de Segurança da Informação para Fornecedores e Parceiros

Na Dock, a segurança da informação é uma prioridade estratégica para proteger nossos dados, operações e, especialmente, as interações com nossos fornecedores e parceiros. Abaixo, destacamos as práticas e expectativas de segurança que devem ser adotadas para fortalecer a proteção de nossas operações em conjunto.

1. A Importância da Segurança da Informação

A segurança é fundamental para proteger os dados e ativos da Dock e de nossa cadeia de fornecimento. A crescente ameaça de ciberataques, como ransomware e violações de dados, pode afetar toda a rede de parceiros. Portanto, a adoção de práticas de segurança eficazes e a vigilância constante são essenciais para proteger todos os envolvidos.

Os fornecedores e parceiros devem estar plenamente cientes do atual cenário de ameaças, que vai desde ataques cibernéticos sofisticados até falhas humanas. A colaboração mútua é imprescindível para assegurar a proteção de todos os elos da cadeia de fornecimento.

2. Red Teaming: Simulando Ameaças para Proteger

O Red Teaming é uma técnica avançada que simula ataques cibernéticos reais para avaliar a resiliência da organização e identificar pontos fracos nos sistemas, processos e na

equipe. Esse processo é fundamental para antecipar e mitigar riscos antes que possam ser explorados por invasores.

- **Simulação de Ameaças Internas e Externas:** O Red Team testa tanto as ameaças internas (como agentes desonestos) quanto as externas (como hackers e outras ameaças vindas de fora).
- **Testes de Invasão (Penetration Testing):** Realizamos testes de penetração para identificar e corrigir vulnerabilidades em sistemas e aplicativos antes que possam ser exploradas por cibercriminosos.
- **Engenharia Social:** Avaliamos a vulnerabilidade humana através de simulações de ataques, como phishing, para testar como os colaboradores reagem a tentativas de manipulação.
- **Uso de Táticas, Técnicas e Procedimentos (TTPs):** O Red Team utiliza as mesmas táticas, técnicas e procedimentos empregados por cibercriminosos reais para avaliar a eficácia das defesas da empresa.

3. Segurança de Aplicações (AppSec)

Aplicativos de terceiros utilizados pela Dock devem aderir aos mais altos padrões de segurança. Espera-se que nossos fornecedores implementem práticas como:

- **Segurança no Ciclo de Desenvolvimento (SDLC):** A segurança deve ser integrada desde as primeiras fases do ciclo de desenvolvimento, minimizando riscos e vulnerabilidades desde a concepção até a entrega do software.
- **OWASP Top 10:** Recomendamos que as equipes de desenvolvimento priorizem a mitigação das vulnerabilidades mais críticas listadas pelo OWASP Top 10.
- **DevSecOps:** A prática de integrar segurança ao fluxo de trabalho DevOps é essencial para garantir que a segurança seja parte de cada etapa do desenvolvimento e deployment de software.
- **Requisitos de Segurança para Softwares de Terceiros:** Todos os softwares de terceiros utilizados na organização devem atender aos padrões de segurança estabelecidos pela Dock para proteger o ambiente corporativo.

4. Compliance e Regulamentações

A Dock é certificada pelas normas ISO 27001, ISO 27701 e PCI DSS, evidenciando nosso compromisso com as melhores práticas de segurança e compliance. Para uma parceria segura, é fundamental que fornecedores também cumpram com padrões compatíveis de segurança e regulamentações, garantindo a proteção dos dados e a continuidade segura das operações. O alinhamento com essas normas é essencial para a proteção mútua e a minimização de riscos ao longo da cadeia de fornecimento.

5. Treinamentos e Capacitação

Na Dock, oferecemos treinamentos anuais sobre desenvolvimento seguro e segurança cibernética para garantir que todos os colaboradores estejam atualizados sobre as melhores práticas e os novos desafios no cenário digital. Esses treinamentos abordam desde a segurança no desenvolvimento de software até a proteção contra ataques cibernéticos. É

fundamental que fornecedores e parceiros também capacitem suas equipes, garantindo que todos estejam preparados para identificar e mitigar ameaças.

6. Ferramentas e Boas Práticas de Segurança

A Dock adota ferramentas avançadas para garantir a segurança de nossos sistemas e dados, incluindo softwares de verificação de vulnerabilidades, monitoramento de redes e gestão de identidade. Além disso, promovemos boas práticas de segurança que devem ser seguidas por todos os colaboradores e fornecedores, como o uso de senhas fortes, a atualização regular de sistemas e a conscientização sobre ataques de phishing. A adesão a essas práticas é vital para garantir a proteção não apenas dos ativos da empresa, mas de toda a cadeia de fornecimento.

Para mais informações sobre as políticas e práticas de segurança da Dock, acesse nossa página de Segurança da Informação.