Controles importantes LGPD

Check Point SOFTWARE TECHNOLOGIES LTD

Vertente	Controles	Proteções	Produto
INFRA TRADICIONAL	Monitoramento de atividades baseado na autenticação de usuário	App Ctrl + Identity Awareness	
	Prevenção de ameaças baseada em assinaturas e comportamentos	AV + IPS + SandBlast	
	Verificação de conformidade dos controles com regulamentações	Blade Compliance	
	Classificação de dados, evitando o vazamento de informações internas Monitoramento de dados sendo enviados para fora da empresa Prevenção de vazamento de informações, levando em consideração dados pessoais e sensíveis	Blade DLP	
	Prevenção a ataques relacionados a aplicações e de indisponibilidade de serviço	Blade IPS	
	Alerta/Notificação de acesso de usuários contrariando as políticas definidas Análise de riscos Criacao de camadas de seguranca por meio de segmentacao de rede Criptografia de dados pessoais e sensiveis Opções de alta disponibilidade, prevenindo pontos únicos de falha (single points of failure) Resiliencia para lidar com situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados	Gateways Check Point	
	Logs gerados pelas ferramentas de segurança devem ser encriptados e possuir mecanismos a evitar perdas ou adulterações de registros durante a transmissão e armazenamento	Gateways Check Point + SmartLog/SmartEvent	
	Gerenciamento de ameaças e prevenção de ataques	SandBlast	
	Realizar a verificação de alterações realizadas, aprovando-as ou não Separação de tarefas por usuário	Smart Workflow	
	Controle de acesso em tempo real de acordo com as políticas implementadas	SmartLog	
	Armazenamento de logs e correlação de eventos Produção de relatórios de auditoria mostrando quais usuários acessaram as aplicações	SmartLog + SmartEvent	
	Auditoria de dados	SmartLog + SmartReporter	
CLOUD	Prevenção de ameaças baseada em assinaturas e comportamentos	CloudGuard IaaS	
	Extração de relatórios com o intuito de serem utilizados em possíveis auditorias Logs gerados pelas ferramentas de segurança devem ser encriptados e possuir mecanismos a evitar perdas ou adulterações de registros durante a transmissão e armazenamento	CloudGuard IaaS + Dome9	
	Resiliencia para lidar com situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados Detecção e remediação de anomalias	CloudGuard IaaS + Dome9 + CloudGuard SaaS	
	Visibilidade completa de assets e fluxo de dados em ambientes cloud Redução de falhas de configuração, mitigando brechas de segurança Controle de acesso baseado no nível de permissão definido Bloqueio de acesso baseado em geolocalização	Dome9	
	Auditoria de dados de acordo com os logs coletados Respostas a alertas de rede, logs ou incidentes	Dome9 + CloudGuard IaaS	
	Armazenamento de logs e correlação de eventos	Log.ic + Dome9	
MOBILE	Verificação e bloqueio de URLs maliciosas em mensagens Análise de aplicativos instalados Inspeção de configurações definidas no aparelho Varredura (scan) da rede wifi conectada Verificação da versão das aplicações instaladas Segurança contra ameaças zero-day	SandBlast Mobile Protect	
	Encriptação de dados corporativos Container encriptado utilizado para armazenamento de dados Separação de dados corporativos de dados pessoais	Capsule Workspace	
	Implementar classificação da informação e restrição de acesso à documentos em seu ciclo de vida	Capsule Docs	
ENDPOINT	Bloqueio da comunicação com fontes conhecidas por serem botnets	Anti-bot	
	Bloqueio e restauração de arquivos afetados por ransomware	Anti-ransomware	
	Implementar classificação da informação e restrição de acesso à documentos em seu ciclo de vida	Capsule Docs	
	Definição e verificação de conformidade minimos para estação de trabalho (compliance)	Compliance	
	Encriptação de todos os dados do disco	FDE	
	Análise forense mostrando os principais dados a respeito da ameaça	Forense	
	Encriptação de mídias removíveis e proteção de portas (USB, etc)	Media & Port Encryption	
	Análise comportamental de malwares Emulação de ameaças identificadas Inspeção de malwares em arquivos baixados Bloqueio de phishing e ameaças zero-day	SandBlast Agent	
GERENCIAMENTO	Verificação de conformidade dos controles com regulamentações Extração de relatórios para possíveis auditorias e como documentação	Blade de Compliance	
	Visibilidade completa em diferentes ambientes Dashboards customizados Definição de politicas centralizadas, visando boas praticas e efetividade Resiliencia para lidar com situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados Controle de acesso administrativo a politicas e dados de gerenciamento de acordo com perfis	R80.30	
	Gerenciamento centralizado com controle de logs Logs gerados pelas ferramentas de segurança devem ser encriptados e possuir mecanismos a evitar perdas ou adulterações de registros durante a transmissão e armazenamento	SmartLogs + SmartEvent	