



Desafios e melhores práticas na Gestão de Cibersegurança

Conhecimento e Compliance em tempo real

Lorena Freitas – Security Engineer

José Irapuan – Security Engineer

Maio de 2024



YOU DESERVE THE BEST SECURITY

Agenda

- Estudos de Mercado
- O que é a Compliance Blade?
- Demo
- Informações Adicionais
- Perguntas

“95% das falhas de Segurança poderiam ser **evitadas** pela **configuração correta** dos equipamentos de segurança”

Gartner



Os desafios de nossos clientes

De acordo com o Gartner, 99% das falhas de Segurança em nuvem até 2025 estarão relacionadas a erros de configuração.

27%

of corporates with “Any Any Accept” rules

75%

of corporates had not implemented Anti-Spoofing

77%

of corporates had not fully documented their FW rules

>80%

of the corporates with unused or expired rules



<https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we>

<https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/what-is-a-cloud-security-misconfiguration/>

Os desafios de nossos clientes

Advocating for Proactive Cybersecurity with Continuous **Risk-Based Posture Assessment**

“Com os ambientes de TI cada vez mais complexos e as exposições a riscos cada vez mais numerosas, as organizações precisam pensar em usar uma plataforma holística e proativa de gerenciamento de segurança cibernética que reúna todas as exposições a riscos cibernéticos em um só lugar, para que sejam pontuadas da mesma maneira. Uma plataforma de gerenciamento também simplifica a priorização e a geração de relatórios.”

Michelle Abraham, research director, Security and Trust, IDC

<https://blogs.idc.com/2023/04/03/advocating-for-proactive-cybersecurity-with-continuous-risk-based-posture-assessment/>

Smart Security



Compliance

Avaliação dos clientes

“Compliance Blade is a **second set of eyes** for security administrators”

Tim Bulu, Information Security Office, USF Health

“A Compliance Blade is an **incredible resource-saver**”

Aleksandr Nositsh, Network Security Office, Swedbank

“ A Compliance Blade trouxe **mais Segurança** ao nosso ambiente.”

Bill Dippel, Networking and Data Security Manager, DRI

Ideias Principais



Melhores Práticas em Segurança

Garantir que o ambiente está operando de acordo com as recomendações da Check Point.



Alertas de Segurança em Tempo Real

Simular o impacto das alterações antes que sejam implementadas.



Relatórios de Auditoria

Fácil acesso à relatórios de auditoria para variados padrões e regulamentos.

Compliance: Seu Consultor Automatizado



**Aumento dos scores
de Segurança**



**Detecção de Erro
Humano**



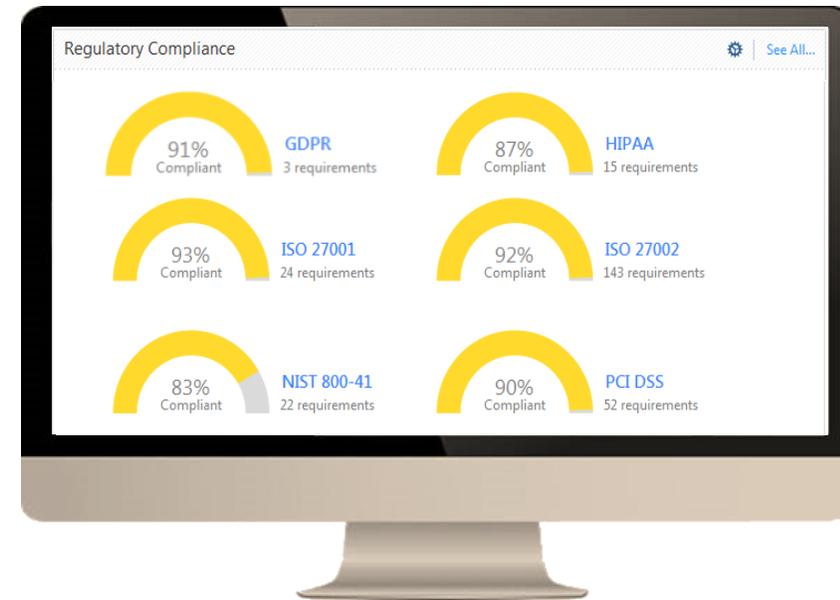
**Compliance de
Segurança**

Compliance



- Analisa Security Gateways Blades, Políticas e configurações em tempo real
- Detecta má configuração considerando 300+ Check Point Security Best Practices para garantir o mais alto nível de segurança
- Compliance de Segurança incluindo GDPR e LGPD, traduzindo milhares de requisitos complexos de compliance em melhores práticas de Segurança simpliadas

Utilize todo o potencial de seus produtos Check Point. Detectando erro humano em Tempo real



Exemplos de Melhores Práticas



Firewall Policies

- Clean-up Rule exists
- Stealth Rule exists
- Any Any Drop doesn't exist
- All rules have Name defined
- All rules have defined Track setting



VPN Settings

- Authentication Timeout
- Secure Encryption
- Password Caching Disabled
- Re-authentication Frequency
- DNS Traffic Encrypted



Firewall Settings

- TCP Session Timeout
- Anti-Spoofing Activated
- Firewall Logs being Saved
- NAT / PAT Enabled
- Hit Count Enabled



IPS Settings

- Protections are Updated
- Default set to Prevent
- Protections activated by Policy
- Gateways perform IPS Inspection
- Critical Protections Enabled

Regulamento de Compliance

- Regulamentações Check Point
- Regulamentações de Mercado

PCI DSS v4.0



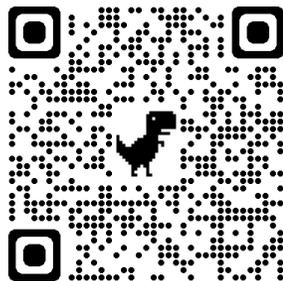
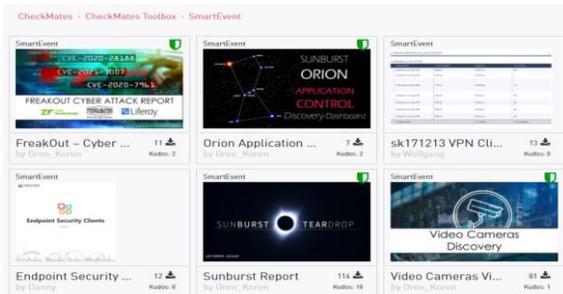
DEMO



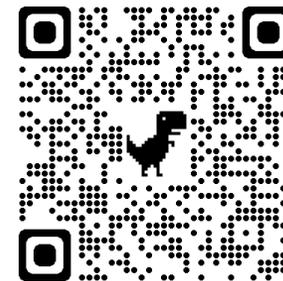
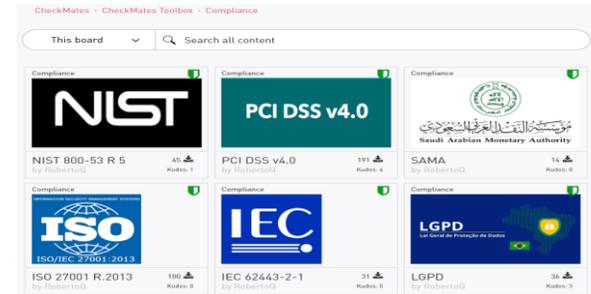
Recursos Adicionais



SmartEvent



Compliance Blade



Como melhorar operação com a Compliance Blade



- Aumenta a eficiência operacional e reduz drasticamente os eventos que precisam ser resolvidos;
- Utiliza integralmente o potencial de todos os produtos Check Point e mantém o ambiente em conformidade;
- Evita erros humanos e reduz a complexidade do gerenciamento da segurança cibernética;



Obrigado!

YOU DESERVE THE BEST SECURITY

