tech + people

RESPOSTA A INCIDENTES BLACKBOX:

O BÁSICO NÃO FEITO

SOOW SIGMA

TLP:CLEAR

Alencar Silva

Bacharel em ciências da computação
Pós graduado em segurança defensiva
Gestão de equipe - CSIRT Sigma

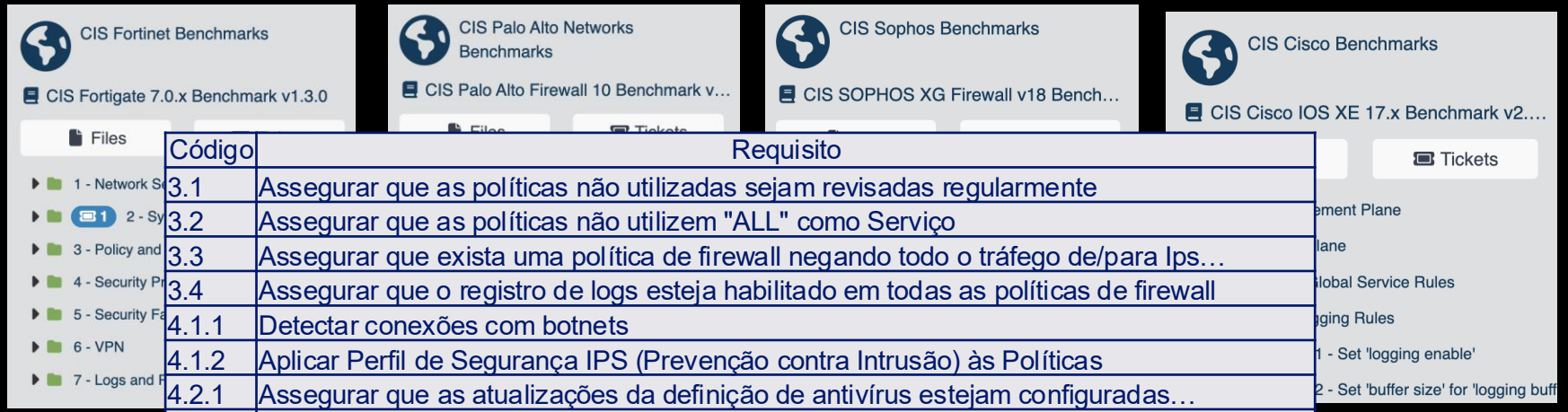
Felipe Schiel

Bacharel em Cibersegurança
Mestrando em segurança de redes
Analista de Malware – CSIRT Sigma

E AGORA?
RECOMENDAÇÕES...

BENCHMARK EQUIPAMENTOS DE BORDA

Analise as configurações do seu FW, WAF, CDN, etc

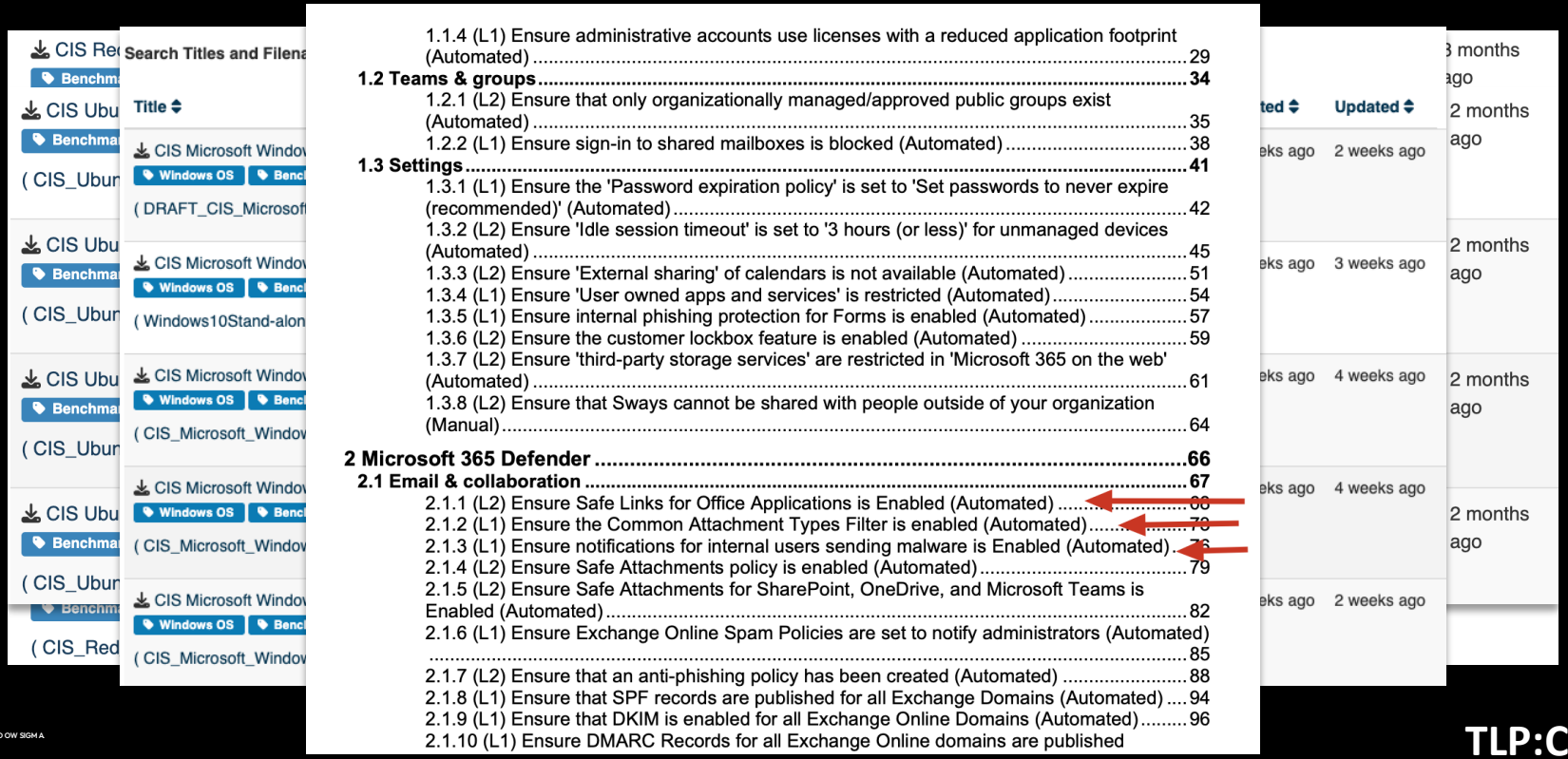


Código	Requisito
3.1	Assegurar que as políticas não utilizadas sejam revisadas regularmente
3.2	Assegurar que as políticas não utilizem "ALL" como Serviço
3.3	Assegurar que exista uma política de firewall negando todo o tráfego de/para Ips…
3.4	Assegurar que o registro de logs esteja habilitado em todas as políticas de firewall
4.1.1	Detectar conexões com botnets
4.1.2	Aplicar Perfil de Segurança IPS (Prevenção contra Intrusão) às Políticas
4.2.1	Assegurar que as atualizações da definição de antivírus estejam configuradas…
4.2.2	Aplicar Perfil de Segurança de Antivírus às Políticas
4.2.3	Habilitar o banco de dados de Prevenção Outbreak(Outbreak Prevention Database)

https://workbench.cisecurity.org/

BENCHMARK SERVIDORES (HARDENING)

Benchmarks para diversas soluções - https://workbench.cisecurity.org/

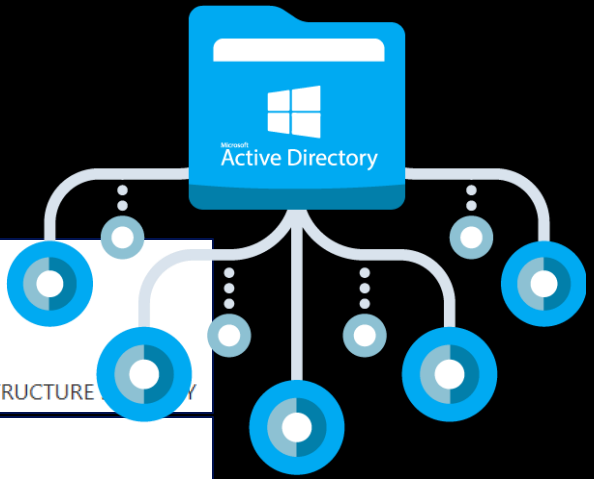


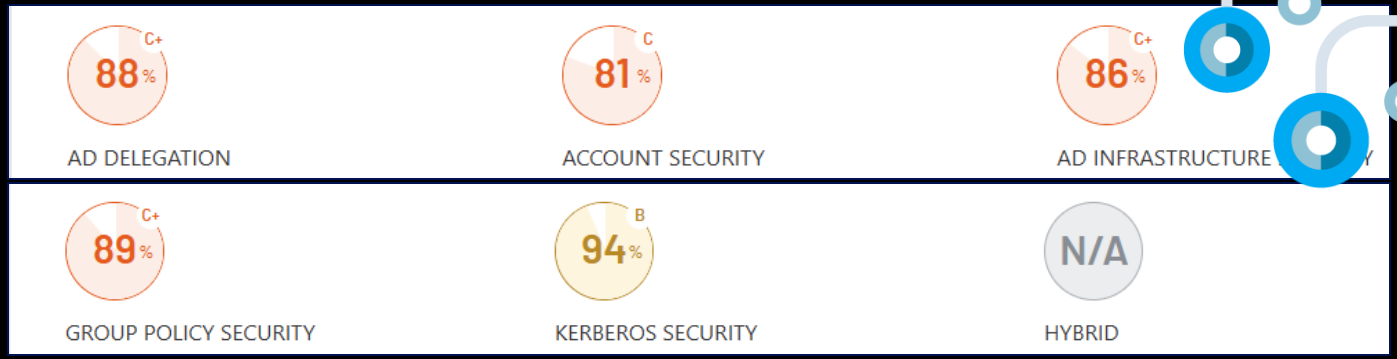
SOOW SIGMA

ACTIVE DIRECTORY: CUIDE DELE

Auditoria de AD

- Gerenciamento de Contas e Privilégios;
- Políticas de Segurança e Autenticação;
- Configurações de GPOs;
- Identificação de fragilidades;



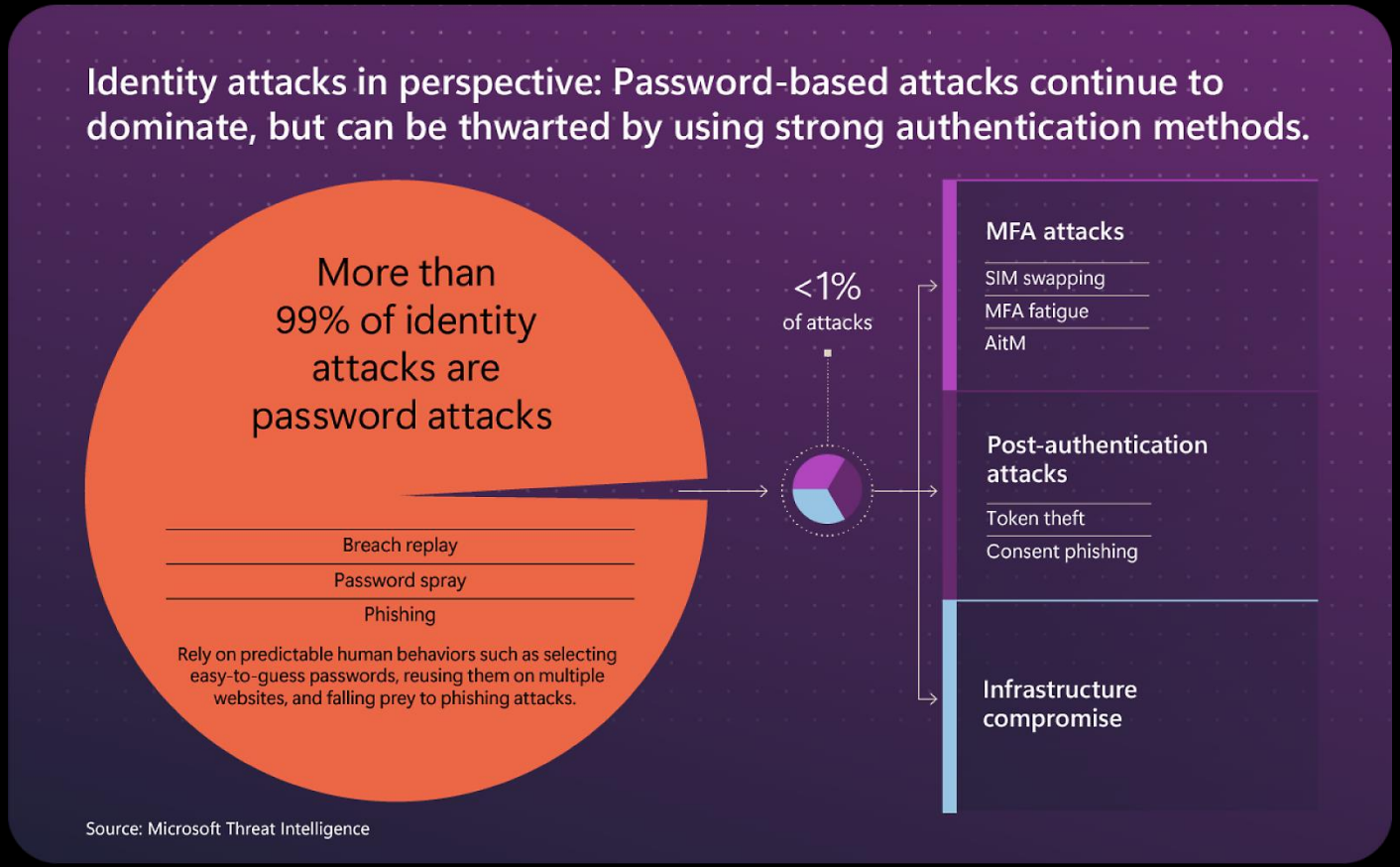


https://www.semperis.com/purple-knight/

TLP:CLEAR

CLÁSSICOS DA LITERATURA: SENHAS

SOOW SIGMA

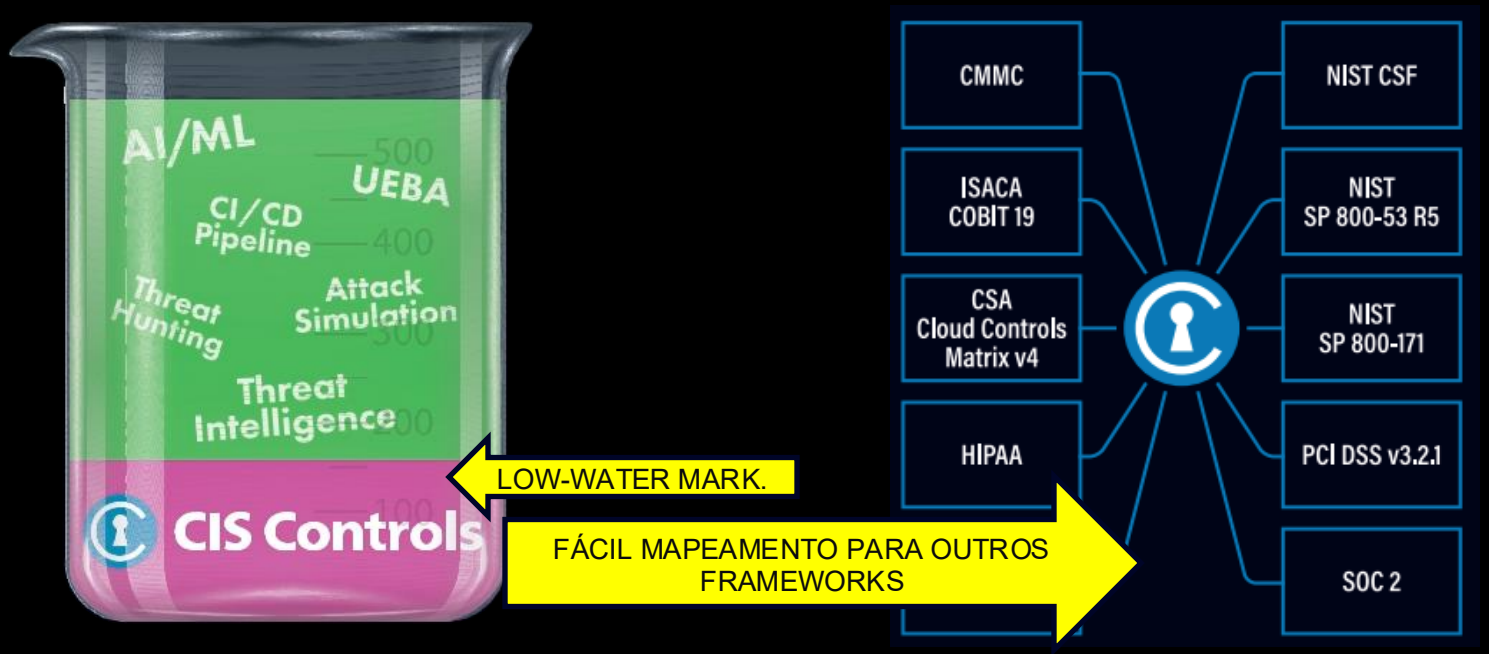


https://www.microsoft.com/pt-br/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

TLP:CLEAR

FRAMEWORK - CIS CONTROLS

O básico que precisa ser feito



REF: https://sansorg.egnyte.com/dl/wuzJBOgziF

SOOW SIGMA

CIS CONTROLS

O básico que precisa ser feito e o essencial que precisa ser desenvolvido

CIS 1	Inventário e controle de ativos corporativos	-
CIS 2	Inventário e controle de ativos de software	-
CIS 3	Proteção de dados	-
CIS 4	Configuração segura de ativos corporativos e software	-
CIS 5	Gestão de contas	-
CIS 6	Gestão de controle de acesso	-
CIS 7	Gestão contínua de vulnerabilidades	-
CIS 8	Gestão de registros de auditoria	-
CIS 9	Proteção de e-mail e navegador Web	-
CIS 10	Defesas contra malware	-
CIS 11	Recuperação de dados	-
CIS 12	Gestão de infraestrutura de rede	-
CIS 13	Monitoramento e defesa da rede	-
CIS 14	Conscientização sobre segurança e treinamento de competências	-
CIS 15	Gestão de provedor de serviços	-
CIS 16	Segurança de aplicações	-
CIS 17	Gestão de resposta à incidentes	-
CIS 18	Testes de invasão	-

TLP:CLEAR

RESUMO DA OPERA

Jóias da coroa

Ativos críticos da organização

Avaliações de risco

Enumerar riscos a organização
Teste de vulnerabilidades

Ferramentas de defesa

Garanta que estejam sendo utilizadas de forma efetiva, o básico bem feito

Logs segurança e acesso

Operacionalize uma gestão de logs eficiente

Patches de segurança

Entenda o que é necessário atualizar

Gestão contínua

Defina um framework de base, CIS Controls, NIST CSF, etc e adapte a sua realidade

Hardening / Baselines

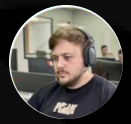
Boas práticas do fabricante;
CIS Benchmarks

Monitoramento

Operacionalize monitoramento no horário onde a infraestrutura fica disponível.

TLP:CLEAR

OBRIGADO!



Alencar Silva

Felipe Schiel

csirt@soow.com.br

www.soow.com.br

SOOW SIGMA