

RESPOSTA A
INCIDENTES
BLACKBOX:

O BÁSICO NÃO FEITO

SOOW SIGMA

TLP:CLEAR



tech people



Alencar Silva ✓

CSIRT Sigma - SCFE | ECIH | CHFI | SecurityX | CRTP
Curitiba, Paraná, Brasil ·

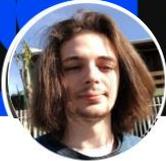
Soow Sigma
Centro Universitário
Campos de Andrade

Alencar Silva

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




tech people



Felipe Schiel ✓ · 1º

Bacharel em Cibersegurança | SCFE | Malware Analysis| DFIR Analyst
| Digital Forensics| Thread Intel | ISO 27001

Soow Sigma
Pontifícia Universidade
Católica do Paraná

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

The screenshot displays the CIS Security Workbench interface with four benchmark categories: CIS Fortinet Benchmarks, CIS Palo Alto Networks Benchmarks, CIS Sophos Benchmarks, and CIS Cisco Benchmarks. A table of requirements is overlaid on the interface, listing various security checks and their corresponding codes.

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/>

Search Titles and Filenames	Title	Updated
CIS Red Hat Enterprise Linux 7 (RHEL7) Benchmark		3 months ago
CIS Ubuntu 16.04 LTS Benchmark		2 months ago
CIS Microsoft Windows Server 2012 R2 (DRAFT_CIS_Microsoft_Windows_Server_2012_R2) Benchmark		2 weeks ago
CIS Ubuntu 14.04 LTS Benchmark		2 months ago
CIS Microsoft Windows 10 Stand-alone (Windows10Stand-alone) Benchmark		3 weeks ago
CIS Ubuntu 16.04 LTS Benchmark		4 weeks ago
CIS Microsoft Windows Server 2012 R2 (CIS_Microsoft_Windows_Server_2012_R2) Benchmark		4 weeks ago
CIS Microsoft Windows Server 2012 R2 (CIS_Microsoft_Windows_Server_2012_R2) Benchmark		4 weeks ago
CIS Microsoft Windows Server 2012 R2 (CIS_Microsoft_Windows_Server_2012_R2) Benchmark		2 weeks ago
CIS Microsoft Windows Server 2012 R2 (CIS_Microsoft_Windows_Server_2012_R2) Benchmark		2 weeks ago

1.1.4 (L1) Ensure administrative accounts use licenses with a reduced application footprint (Automated)	29
1.2 Teams & groups	34
1.2.1 (L2) Ensure that only organizationally managed/approved public groups exist (Automated)	35
1.2.2 (L1) Ensure sign-in to shared mailboxes is blocked (Automated)	38
1.3 Settings	41
1.3.1 (L1) Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' (Automated)	42
1.3.2 (L2) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (Automated)	45
1.3.3 (L2) Ensure 'External sharing' of calendars is not available (Automated)	51
1.3.4 (L1) Ensure 'User owned apps and services' is restricted (Automated)	54
1.3.5 (L1) Ensure internal phishing protection for Forms is enabled (Automated)	57
1.3.6 (L2) Ensure the customer lockbox feature is enabled (Automated)	59
1.3.7 (L2) Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web' (Automated)	61
1.3.8 (L2) Ensure that Sways cannot be shared with people outside of your organization (Manual)	64
2 Microsoft 365 Defender	66
2.1 Email & collaboration	67
2.1.1 (L2) Ensure Safe Links for Office Applications is Enabled (Automated)	68
2.1.2 (L1) Ensure the Common Attachment Types Filter is enabled (Automated)	70
2.1.3 (L1) Ensure notifications for internal users sending malware is Enabled (Automated)	75
2.1.4 (L2) Ensure Safe Attachments policy is enabled (Automated)	79
2.1.5 (L2) Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled (Automated)	82
2.1.6 (L1) Ensure Exchange Online Spam Policies are set to notify administrators (Automated)	85
2.1.7 (L2) Ensure that an anti-phishing policy has been created (Automated)	88
2.1.8 (L1) Ensure that SPF records are published for all Exchange Domains (Automated)	94
2.1.9 (L1) Ensure that DKIM is enabled for all Exchange Online Domains (Automated)	96
2.1.10 (L1) Ensure DMARC Records for all Exchange Online domains are published	



+

ACTIVE DIRECTORY: CUIDE DELE

Auditoria de AD

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



AD DELEGATION



ACCOUNT SECURITY



AD INFRASTRUCTURE



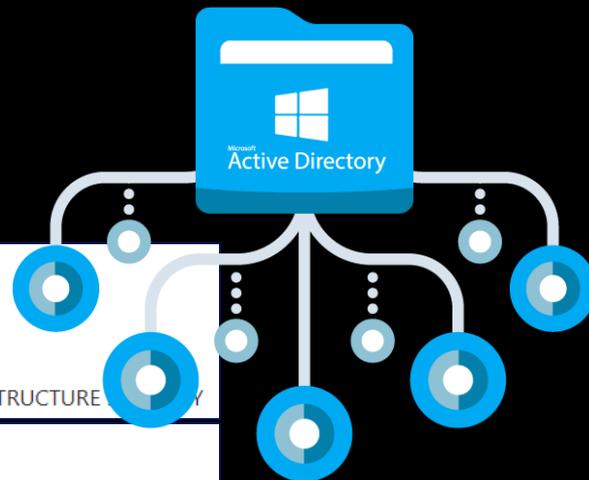
GROUP POLICY SECURITY



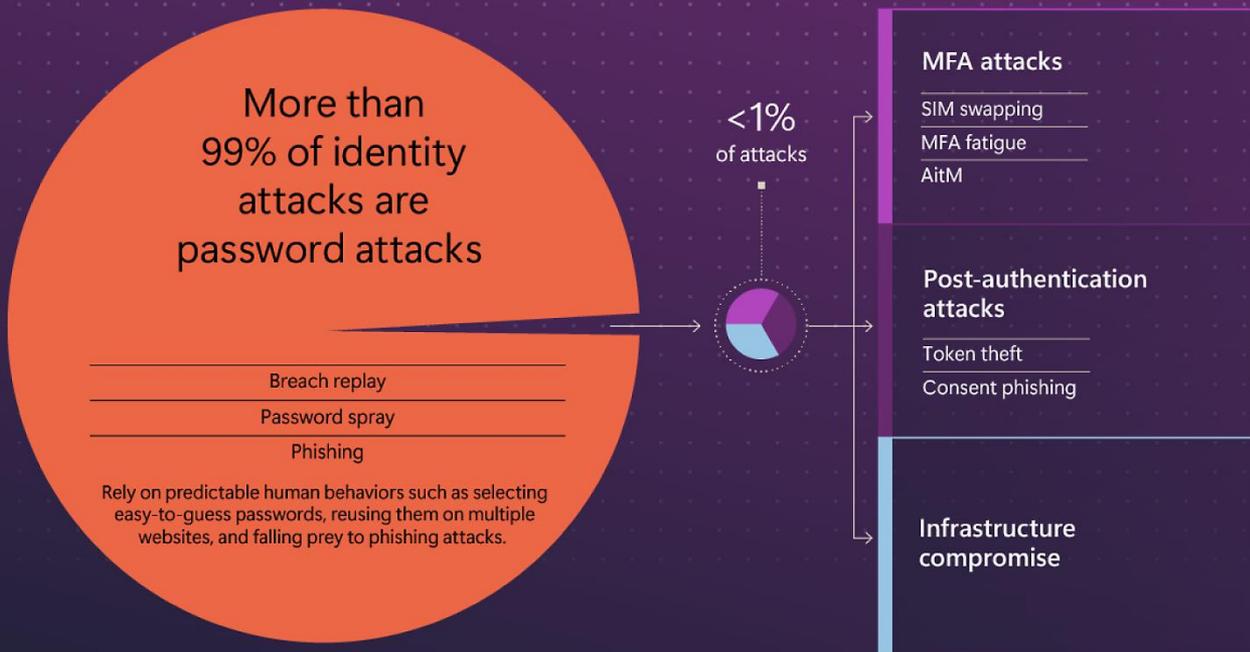
KERBEROS SECURITY



HYBRID



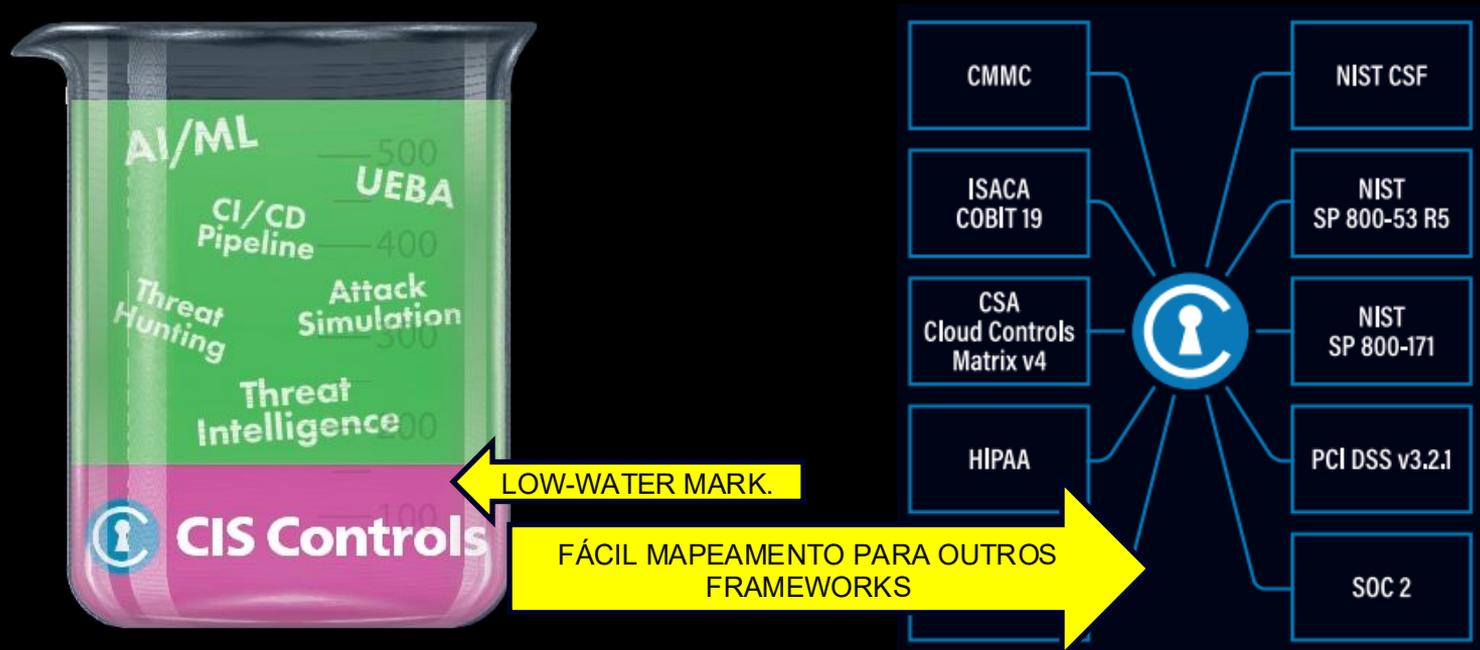
Identity attacks in perspective: Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.



Source: Microsoft Threat Intelligence

+ FRAMEWORK - CIS CONTROLS

O básico que precisa ser feito



+ 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	-

+ 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.

OBRIGADO!



Alencar Silva



Felipe Schiel

csirt@soow.com.br

www.soow.com.br

SOOW'SIGMA

TLP:CLEAR