HARMONY PURPLE

Ferramenta para gestão de vulnerabilidades e riscos aliada a pentest whitebox

2023

DESCRIÇÃO E DIFERENCIAIS

- Harmony Purple é uma ferramenta poderosa para gestão e priorização de vulnerabilidades e riscos através de Testes de Penetração WhiteBox contínuos e automáticos da infraestrutura de rede e Web
- Conta com tecnologia patenteada APS que, através de inteligência artificial, simula um ataque hacker humano mapeando todos os possíveis caminhos de movimentação dentro da rede
- Focado nas regras de negócio especificas do cliente
- União de Blue e Red Teams para economia de tempo e recursos

Foco e priorização são fatores chaves para a Validação de Segurança

O nosso Mercado (pelo Gartner Group)

Escaneamento Tradicional de Vulnerabilidades

Processo operacional de segurança clássico exigido pela maioria das organizações, bem como por padrões como NIST, PCI e outros.

- Soluções: Nessus, Qualys, Tenable, Rapid7, etc...

Ferramentas de Simulação de Ataques e Localização de Brechas (BAS Tools)

O BAS é implantado em várias partes do ambiente e usa agentes e / ou VMs para testar ativamente o ambiente em busca de problemas, simulando métodos comuns usados por atacantes. Essas ferramentas são posicionadas como ferramentas de teste de penetração automatizadas ou como ferramentas de avaliação de controles de segurança, fornecendo uma "visão do atacante".

- Soluções: AttackIQ, SafeBreach, XM Cyber, Cymulate, Pcysys, Verodin etc...

Tecnologia de Priorização de Vulnerabilidades (VPT)

Prioriza as vulnerabilidades de ativos críticos e destaca os ativos vulneráveis com maior probabilidade de serem atacados. Organizações se concentram em consertar os maiores riscos, melhorar a eficiência do gerenciamento de patches e reduzir o TCO.

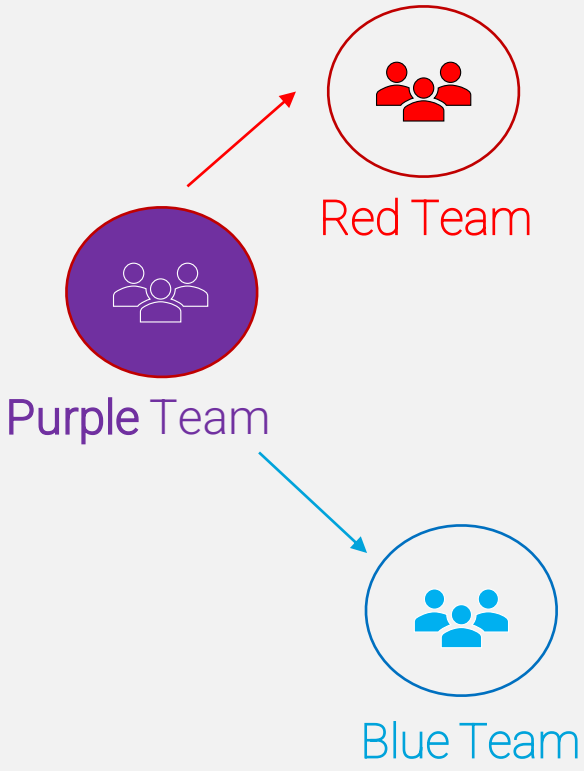
Solução: Harmony Purple

O Purple é uma Tecnologia de Priorização de Vulnerabilidades (VPT)

Teste de penetração whitebox 24x7 automatizado que une Blue e Red Teams, utilizando tecnologia única de priorização de vulnerabilidades e gerenciamento de riscos, focado nas regras de negócio

- As organizações conseguem avaliar seus riscos cibernéticos baseados na criticidade e análises avançadas de seus ativos
- Permite que as organizações invistam seu tempo e recursos nas vulnerabilidades que ameaçam seus ativos críticos e processos de negócios
- Mostra o poder da Tecnologia patenteada "Attack Path Scenario™", onde o Sistema cria uma lista priorizada de vulnerabilidades
- Permite às organizações reduzir substancialmente a superfície de ataque com o menor tempo e esforço e com o mais eficiente uso de seus recursos da equipe

Purple garante Eficácia dos Controles de Segurança



As Capacidades do Red Team"

- Simula como o seu Red Team atuaria em seu ambiente
- Busca vulnerabilidades e as usa para movimentação em seu ambiente diretamente sobre seus recursos críticos
- Usa "cenários de caminhos de ataques - APS" para criar uma lista priorizada de riscos cibernéticos para seus ativos, aplicativos e dispositivos (servidores, terminais e dispositivos móveis)

As Capacidades do Blue Team

- Aproveita "cenários de caminhos de ataque-APS" para **recomendar controles eficazes** ou onde os controles são limitados por considerações de negócios, **compensando estes controles**

- Por exemplo, o Purple pode recomendar o patch para um servidor de alto risco para diminuir o risco ou compensar esses controles com base no ambiente e nas considerações de negócios

Visibilidade

- Visibilidade contínua de todos os ativos, incluindo endpoints, aplicativos e servidores
- Mapeamento de rede e validação de conectividade

Avalia e Prioriza vulnerabilidades, processos de negócios e risco

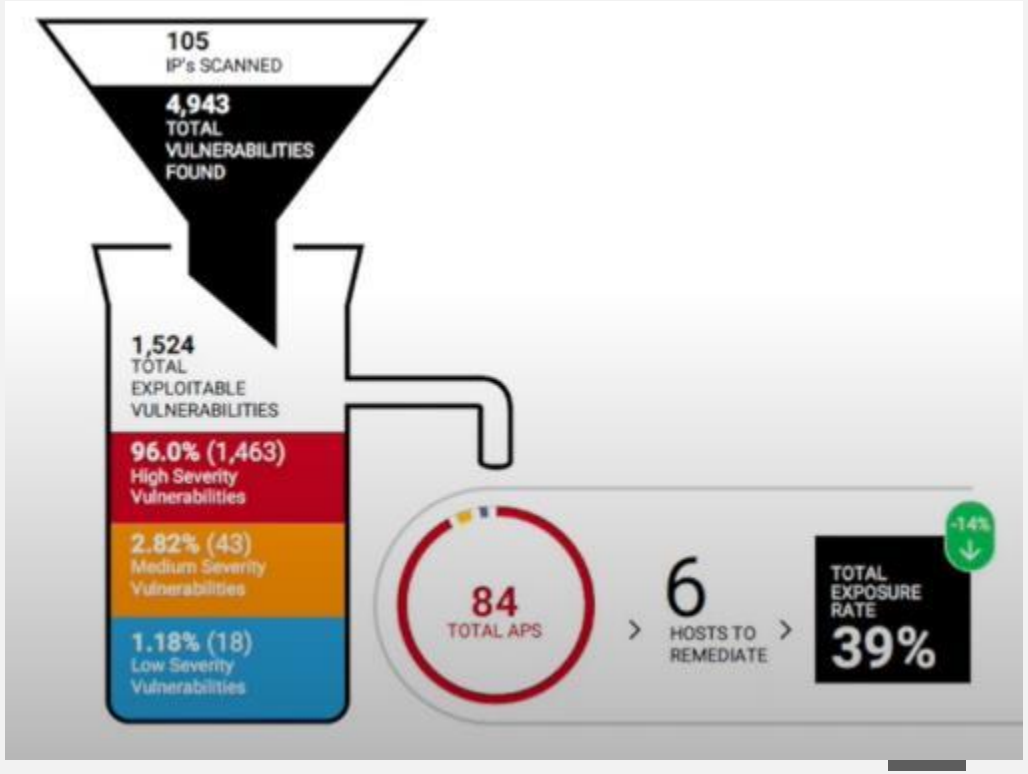
- Lista explorável que ameaça os processos de negócios
- OVAL® analysis – (Open Vulnerability and Assessment Language)

Attack Path Scenarios ™

- Redes Multi site
- Visualise todos os "attack path scenario" e foque no que mais importa
- Valide continuamente os controles críticos em ativos "joias da coroa"

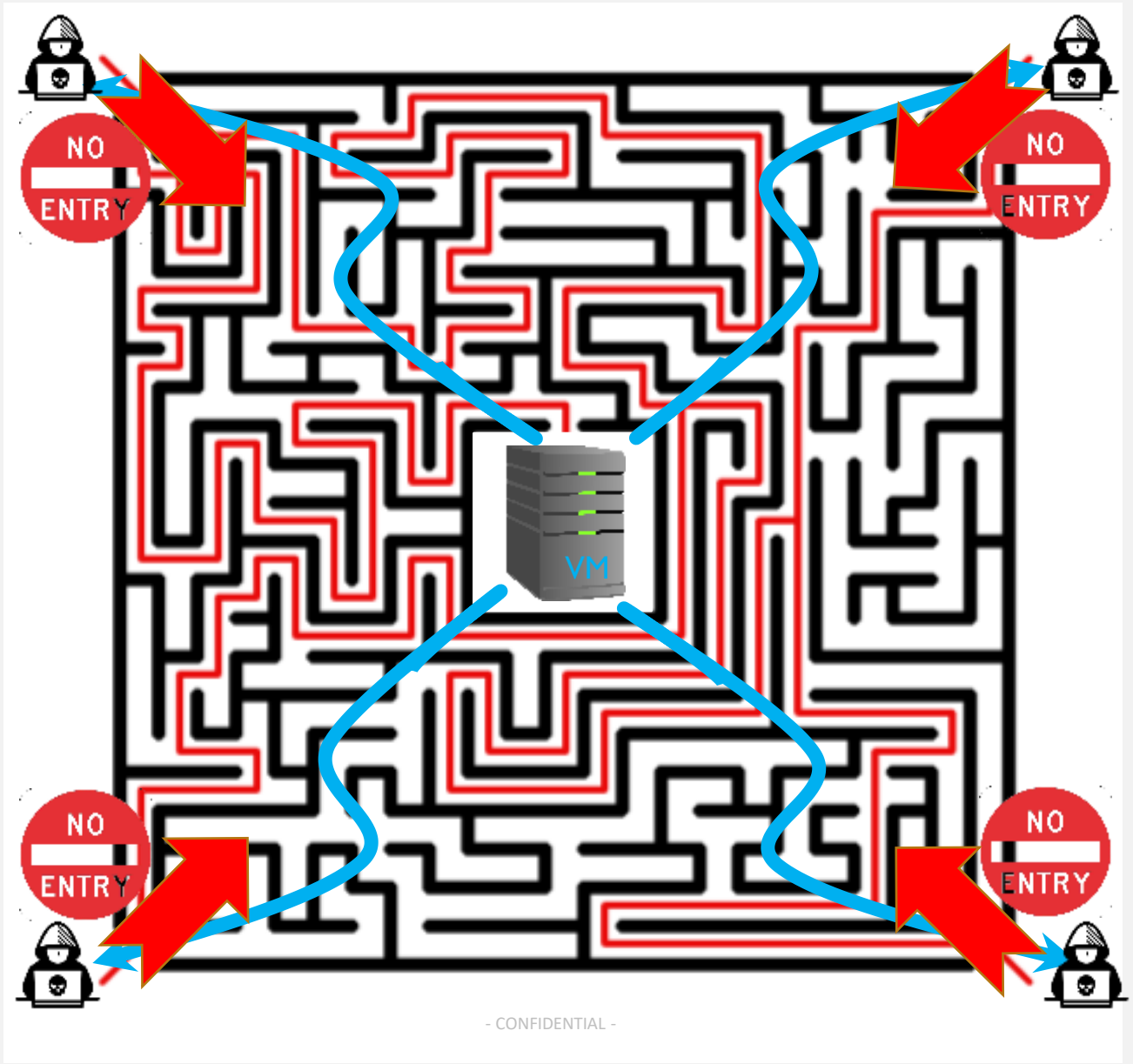
Relatórios, Correções e Automação

- Estratégia de controle de compensações
- Principais riscos de negócios e ativos
- Relatórios
- Remediações e Mitigações

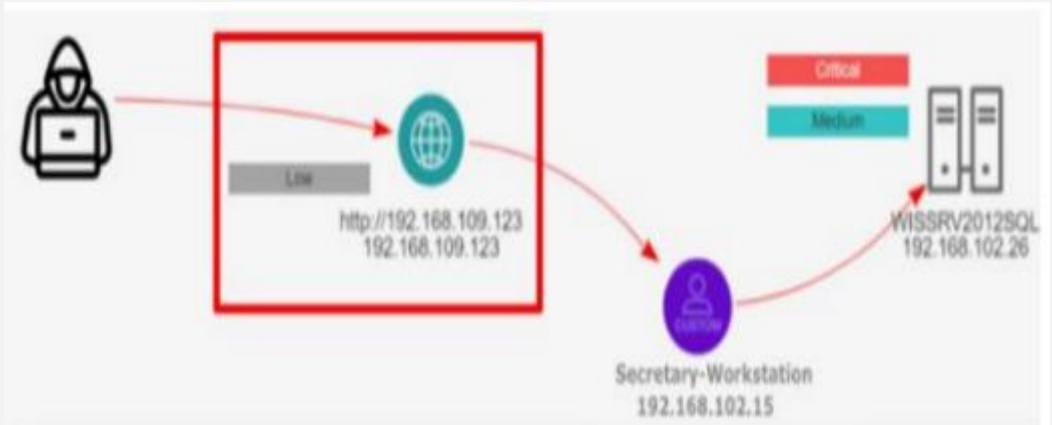


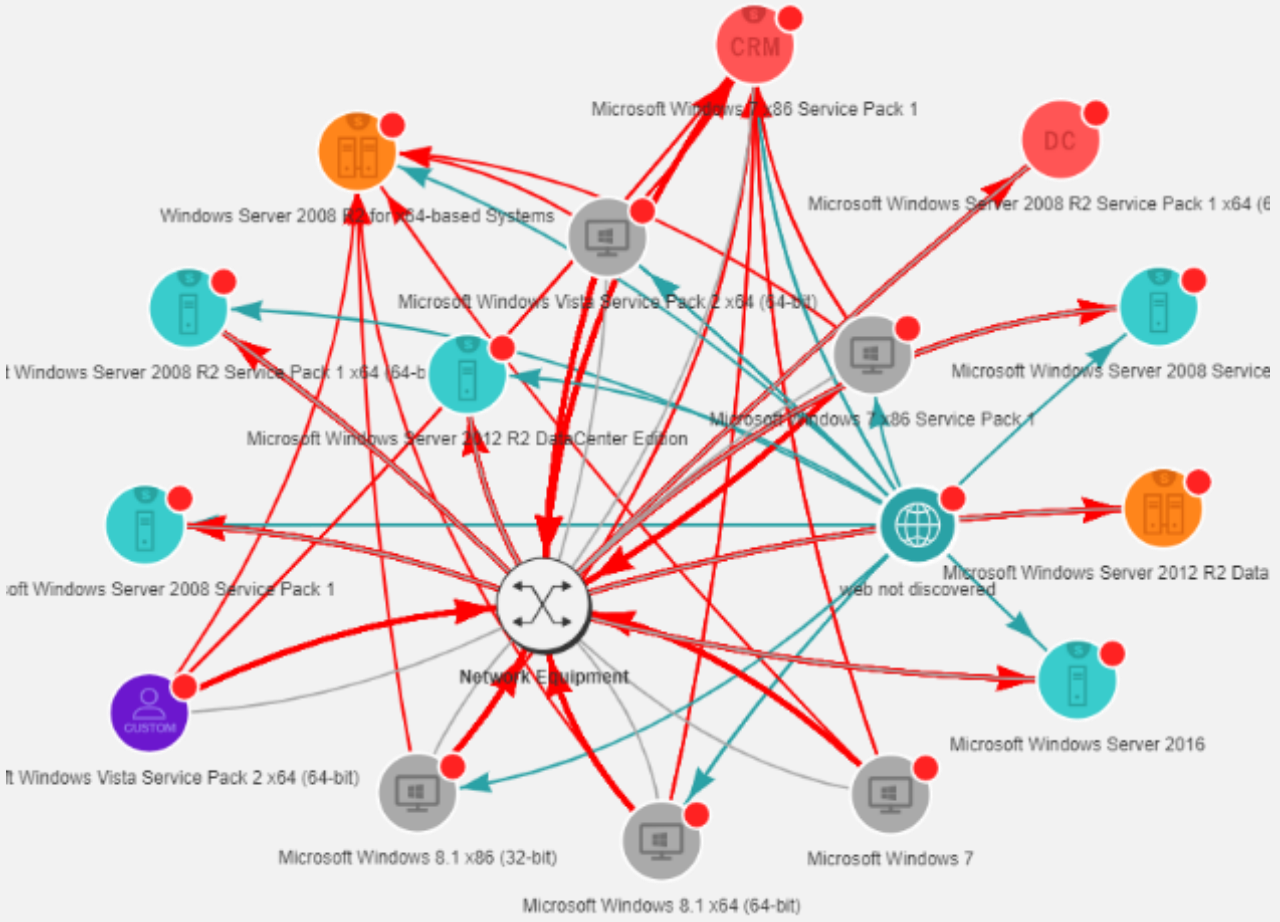
Como o Purple funciona?

Nesse exemplo, vemos que se fecharmos apenas essas 4 portas de entrada, toda a rede estará protegida.



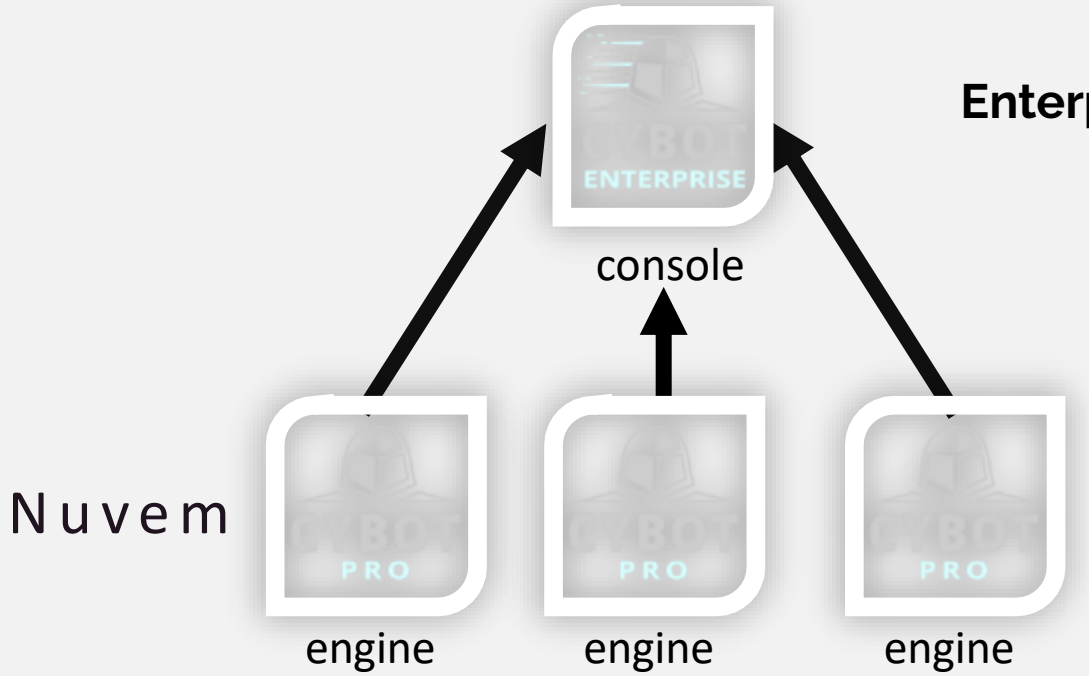
O Purple detecta múltiplos vetores de ataque que podem ser explorados contra o mesmo alvo 24x7





Purple – Visão Geral

Insights globais sobre ameaças cibernéticas aos seus processos de negócios



Enterprise gerencia multiplos **Pros**

The 5 unique stages of Purple

Continuous Scan using Cronus's own scanner

- INFRA, Web
- OWASP, NIST compatible
- CVE certified
- CIS certified

Network mapping, validation of connectivity

- Global network mapping
- No false negative
- Inventory / asset management

Smart Vulnerability management

- Exploitable shortlist that threatens business process
- OVAL analysis
- No false positives

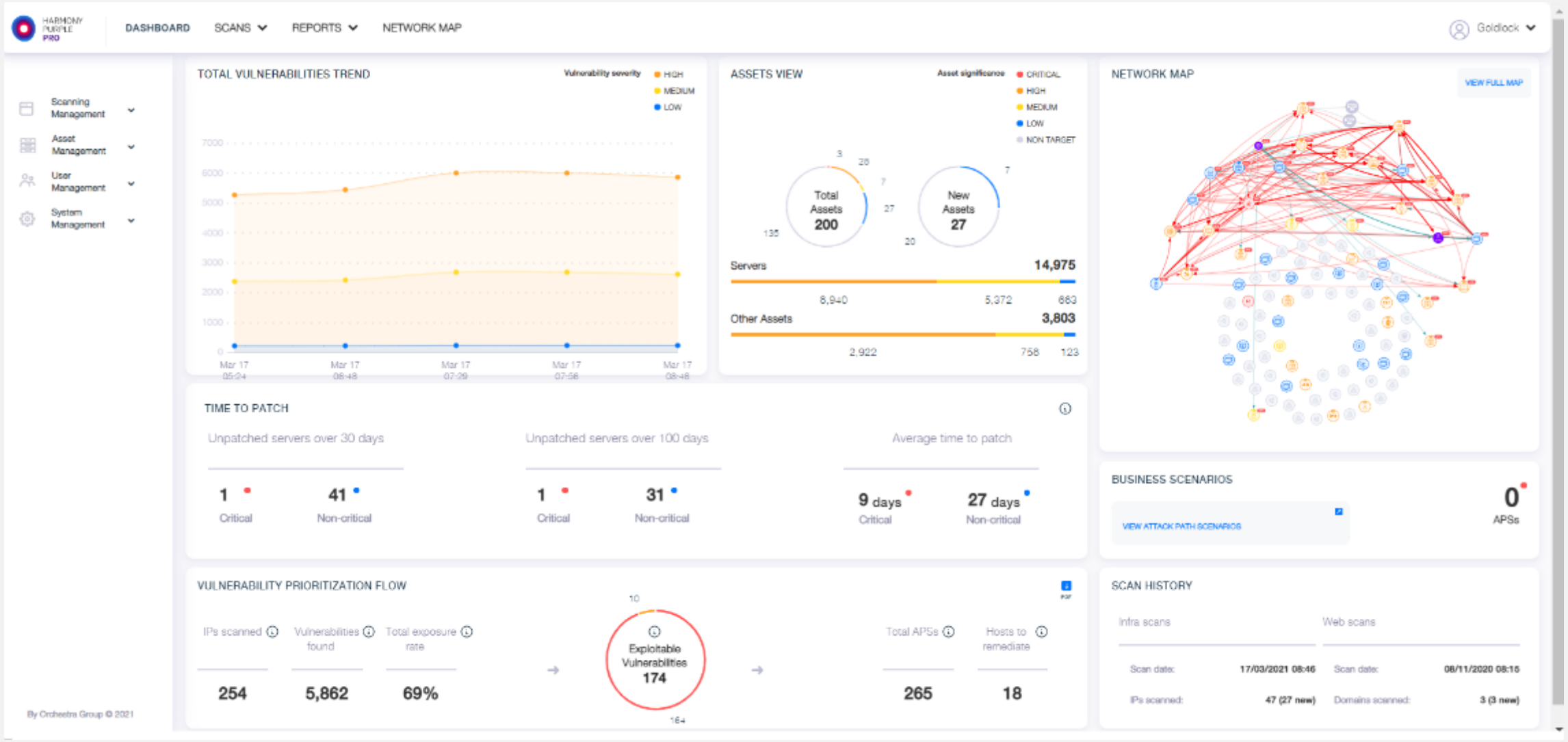
Attack Path Scenarios ™

- Multi site networks
- Visualize ALL attack paths and focus on key scenarios
- Continuous
- Focus on critical assets

Reporting and Remediation

- Key business and asset risks
- Interactive Dashboard and live monitoring
- Remediate with one click using SIEM integration

- Exemplo do painel de controle da ferramenta



NETWORK STATUS MAP

DISPLAY ON MAP

- CRITICAL
- HIGH
- MEDIUM
- LOW
- NON TARGET
- APS
- CONNECTIONS

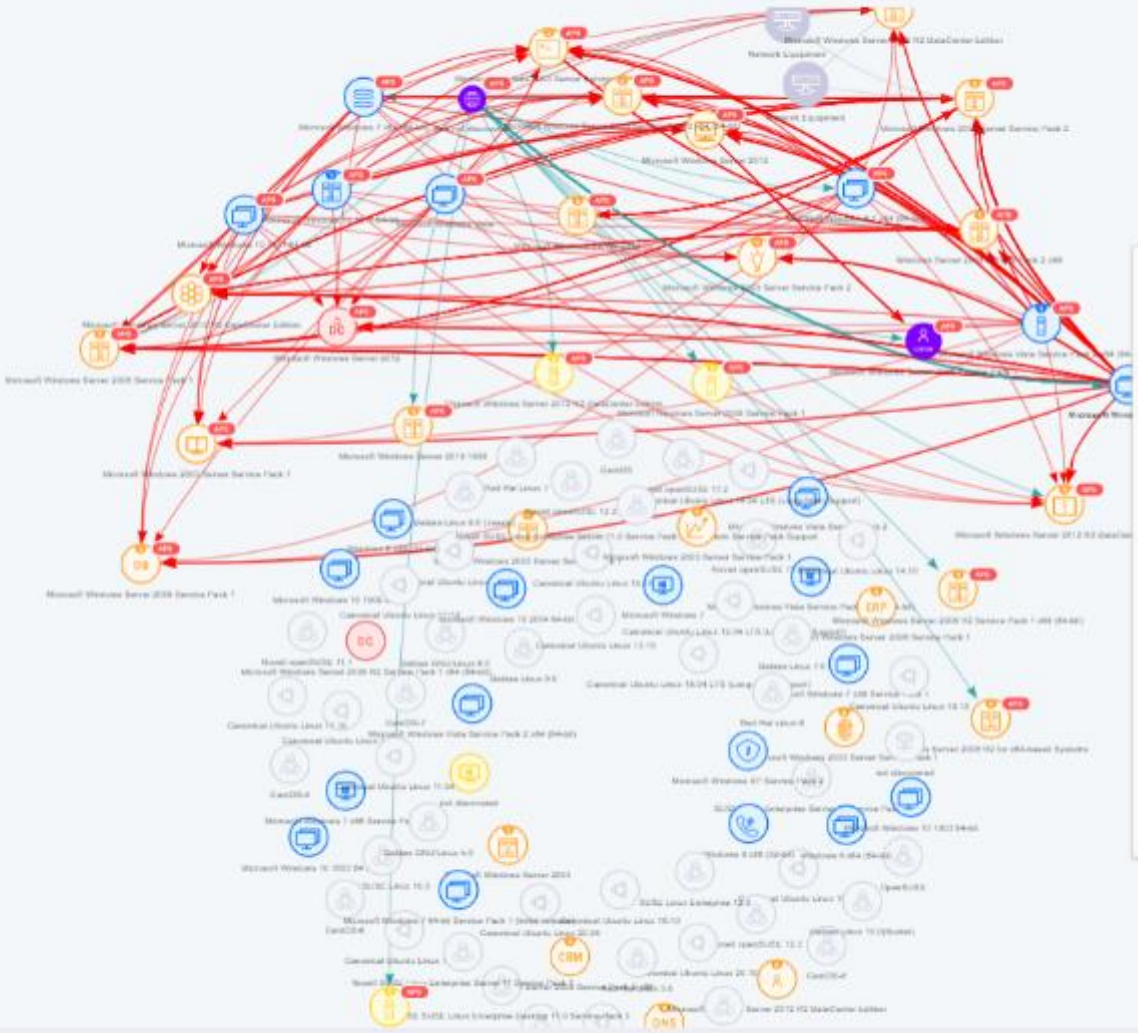
SHOW ONLY HOSTS IN APS

VIEW OPTIONS

FULL VIEW AGGREGATED VIEW

OS

ROLE



Significance Level: Low

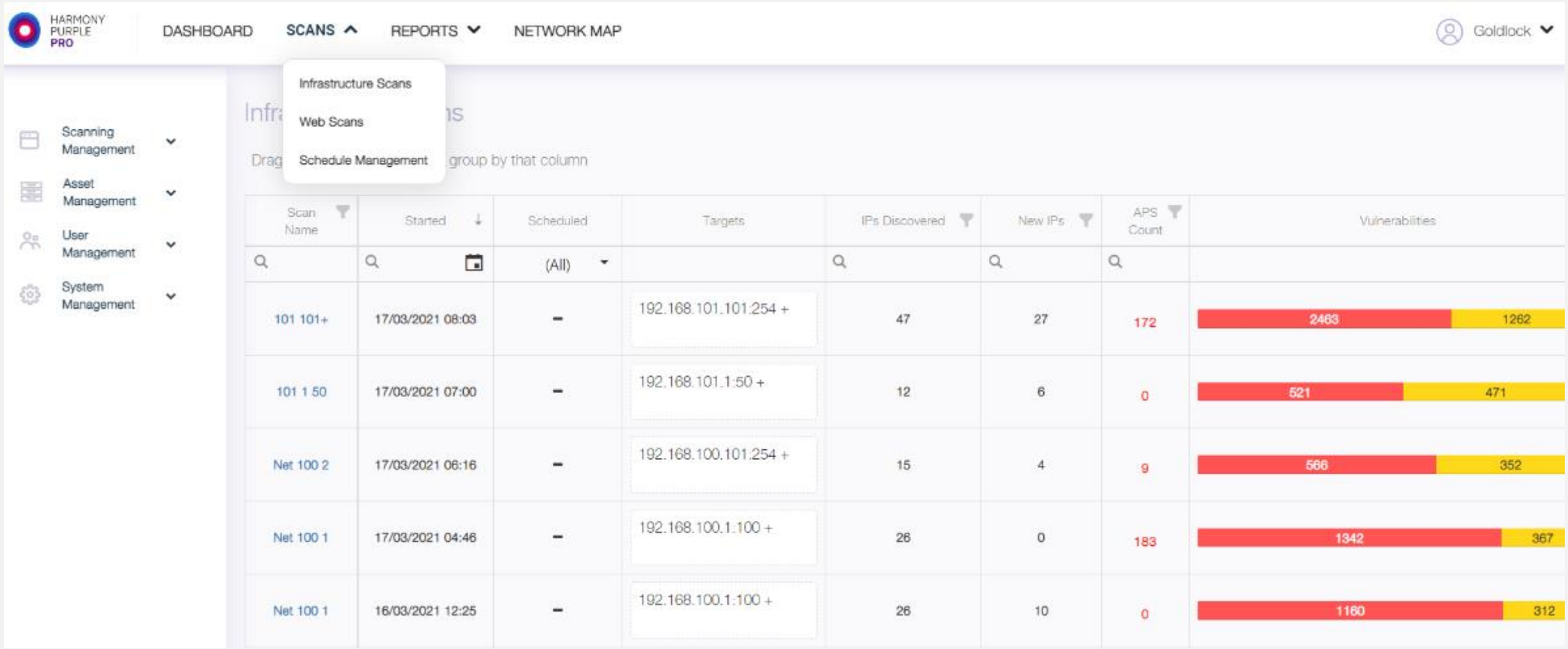
Start: 22

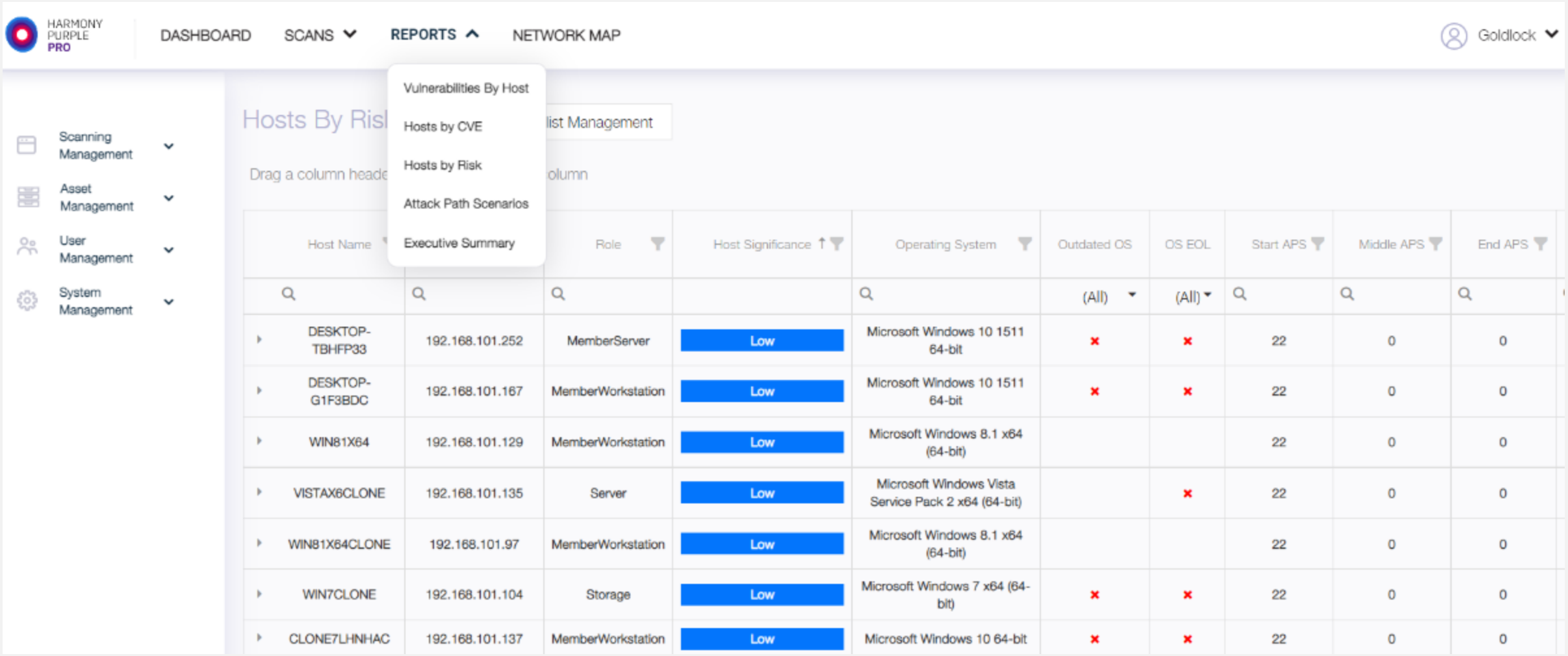
Inbound APS 12

Target 0

Outbound APS 34

Role:	MemberWorkstation
OS:	Microsoft Windows 10 64-bit
Hosts / Urls Count:	4
Vulnerabilities:	84%(129) 16%(25) 0% (0)


HARMONY PURPLE PRO
DASHBOARD
SCANS
REPORTS
NETWORK MAP
Goldlock
Infrastructure Scans
Web Scans
Schedule Management
Scanning Management
Asset Management
User Management
System Management
group by that column
Scan Name
Started
Scheduled
Targets
IPs Discovered
New IPs
APS Count
Vulnerabilities
(All)
101 101+
17/03/2021 08:03
192.168.101.101:254 +
47
27
172
2463
1262
101 1 50
17/03/2021 07:00
192.168.101.1:50 +
12
6
0
521
471
Net 100 2
17/03/2021 06:16
192.168.100.101:254 +
15
4
9
566
352
Net 100 1
17/03/2021 04:46
192.168.100.1:100 +
26
0
183
1342
367
Net 100 1
16/03/2021 12:25
192.168.100.1:100 +
26
10
0
1160
312


HARMONY PURPLE PRO
DASHBOARD
SCANS
REPORTS
NETWORK MAP
Goldlock
Vulnerabilities By Host
Hosts by CVE
Hosts by Risk
Attack Path Scenarios
Executive Summary
Scanning Management
Asset Management
User Management
System Management
Hosts By Risk
list Management
Drag a column header
olumn
Host Name
Role
Host Significance
Operating System
Outdated OS
OS EOL
Start APS
Middle APS
End APS
(All)
(All)
DESKTOP-TBHFP33 192.168.101.252 MemberServer Low Microsoft Windows 10 1511 64-bit 22 0 0
DESKTOP-G1F3BDC 192.168.101.167 MemberWorkstation Low Microsoft Windows 10 1511 64-bit 22 0 0
WIN81X64 192.168.101.129 MemberWorkstation Low Microsoft Windows 8.1 x64 (64-bit) 22 0 0
VISTAX6CLONE 192.168.101.135 Server Low Microsoft Windows Vista Service Pack 2 x64 (64-bit) 22 0 0
WIN81X64CLONE 192.168.101.97 MemberWorkstation Low Microsoft Windows 8.1 x64 (64-bit) 22 0 0
WIN7CLONE 192.168.101.104 Storage Low Microsoft Windows 7 x64 (64-bit) 22 0 0
CLONE7LHNHAC 192.168.101.137 MemberWorkstation Low Microsoft Windows 10 64-bit 22 0 0

VULNERABILITY DESCRIPTION

VULNERABILITY

Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)

HARMONY PURPLE REMEDIATION

Please review the following solutions to ensure safety of your network:

Vulnerability Insight

Software Update

Affected Software/OS (13)

CVE's (6)

www.goldlock.com.br - Tel.: (11) 3511-3855

Av. Pacaembu, 1976 - Cep: 01234-000 – SP

Email: info@gold-lock.com.br