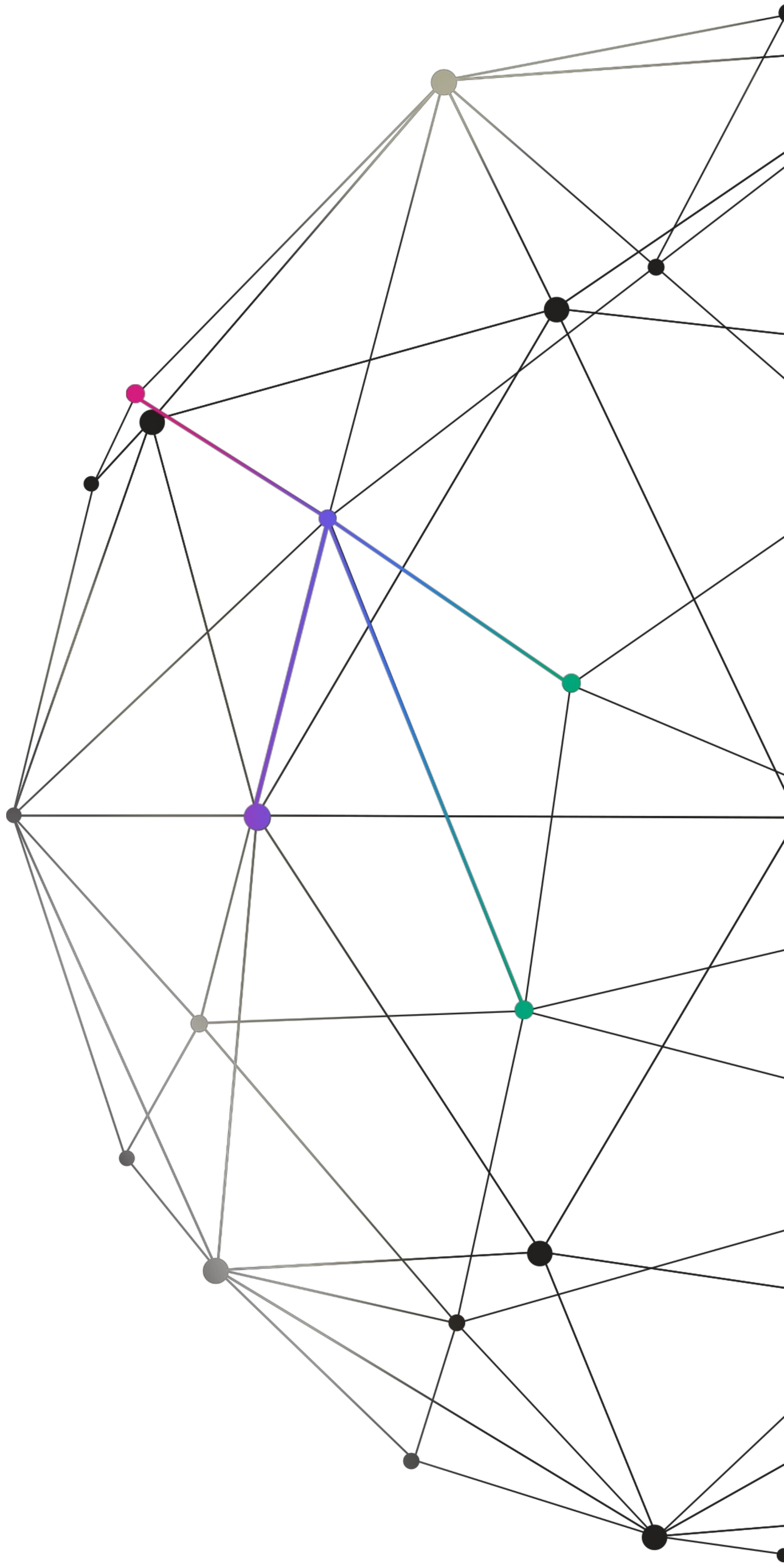
October 11, 2022

HARMONY PURPLE

EXECUTIVE REPORT

HARMONY
PURPLE
PRO

ORCHESTRA



Harmony Purple Product Suite by Orchestra Group Is CVE Compatible

Table of Contents

1. Introduction

The purpose of this report is to provide succinct, actionable information, summarizing the main risks, the threats to business processes, and the vulnerabilities that have the potential to harm critical systems, workstations, server applications, web applications, and business scenarios.

How does it work?

Harmony Purple scans the network and detects the Attack Path Scenarios ™ (APSs) that threaten critical assets in the organization. The APSs detected were either Infrastructure APSs or Web APSs, or both, as detailed below.

2. Harmony Purple Scan Summary

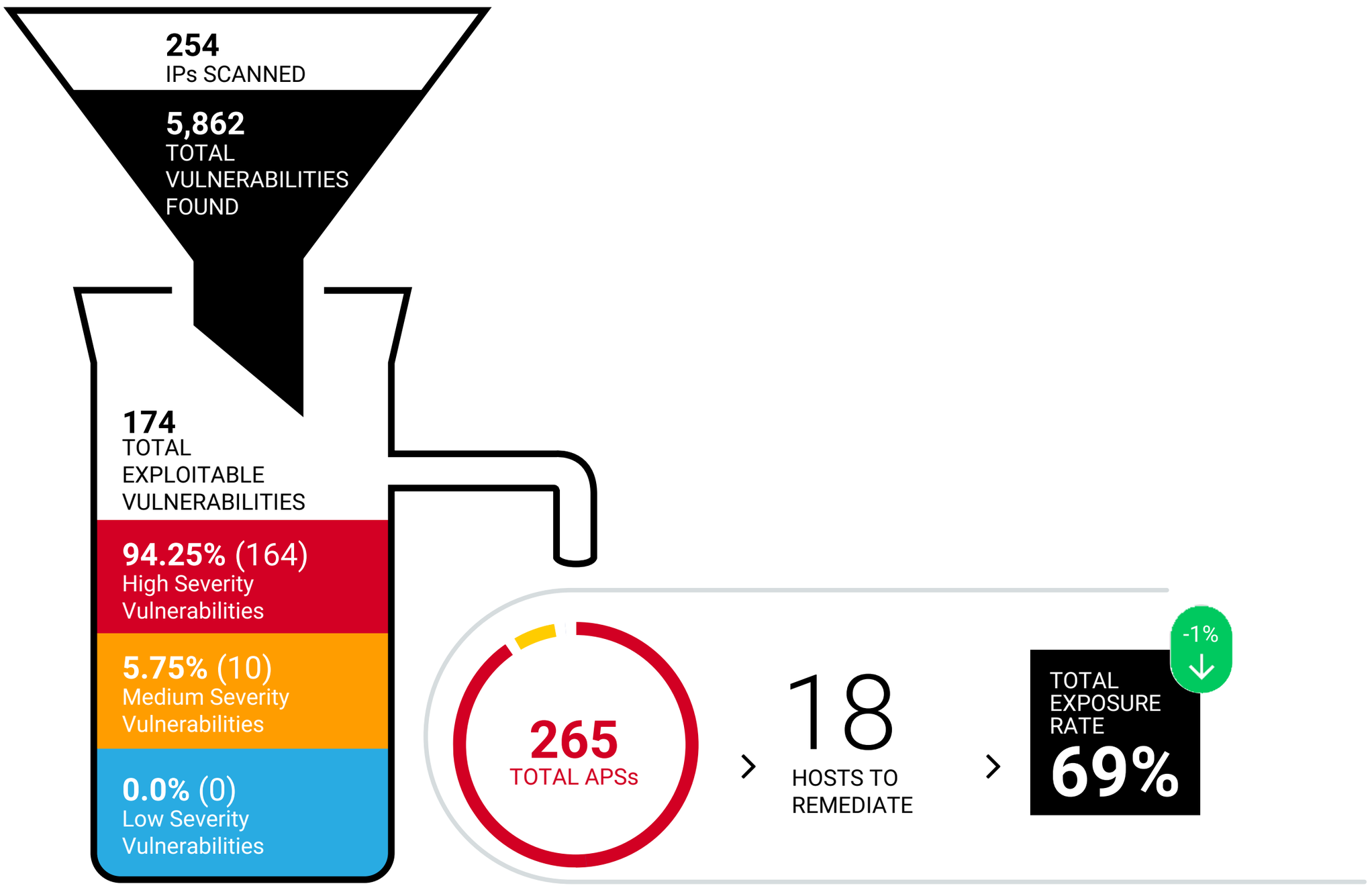
	Current			Previous	
As of	**17 March 2021 14:46**			17 March 2021 13:29	
Infrastructure	TOTAL	NEW	APSs	TOTAL	APSs
Total Assets scanned	**200**	27	265	187	225
Total assets at risk	**32**	0	265	32	225
Member servers	**19**	0	158	19	132
Standalone servers	**4**	0	8	4	8
Domain controllers	**1**	0	11	1	9
Other	**8**	0	88	8	76

As of	**08 November 2020 14:15**			-	
Web application	TOTAL	NEW	APSs	TOTAL	APSs
Total domains scanned	**3**	3	2	0	0
Total domains at risk	**2**	2	2	0	0

Harmony Purple Scan Summary

This diagram illustrates the total number of IPs scanned and the exploitable vulnerabilities found, going through the Harmony Purple analysis and prioritization funnel, producing a prioritized list of the most probable Attacks Path Scenarios (APSs) that hackers may use, and a recommended list of hosts to remediate.

Harmony Purple's threat prioritization reduces false-positive alerts to the bare minimum, optimizing the effectiveness of your blue team, reducing time to path and operational costs, while dramatically improving your overall security posture.



3. Attack Path Scenarios Summary

Harmony Purple's Attack Path Scenarios (APSs) represent possible attack steps through exploitable vulnerabilities that hackers can take to penetrate the network and reach critical assets in the organization.

Each APS starts with a Source host and ends with a Target host. The table below summarizes the total APSs found across all scans vs the system's state prior to the latest scan, and provides a breakdown of the total APSs found by Target host significance.

Assets	Current			Previous		
Total APSs	265 (136 new)			225		
Total exposure rate	69.0%			70.0%		
Exposure severity	**HIGH**			**HIGH**		
Source Hosts	18 (3 new)			16		
Target Hosts	32 (0 new)			33		
Target host significance	MEDIUM	HIGH	CRITICAL	MEDIUM	HIGH	CRITICAL
	4	**26**	**2**	4	26	2

Exposure severity

Critical	Range from 75% to 100%
High	Range from 50% to 74%
Medium	Range from 25% to 49%%
Low	Range from 0% to 24%

4. Recommended Remediation

4.1 Top Assets at Risk

The purpose of this section is to highlight the most critical assets in your organization at risk, the risk severity, its duration, and if the asset has a confirmed Attack Path Scenario (APS). For each asset, Harmony Purple offers several recommended remediations to choose from that fit your critical asset risk, significance, and operational needs.

Critical High Medium Low

	Host name	IP	Role	APS	At risk since	Host significance	Severity
1	LABDC3	192.168.100.65	BackupDomainController	YES	17 March 2021 11:06		
2	WIN-YN9G899Q9FZ	192.168.100.57	Web Server - Internal	YES			
3	WIN-J1XJ0X4DSTA	192.168.100.39	MemberServer	YES	16 March 2021 18:44		
4	SERVER201268-71	192.168.100.71	MemberServer	YES	16 March 2021 18:45		
5	WINSER2003SP1X6	192.168.100.51	Terminal Server	YES	16 March 2021 18:43		
6	WIN-3VNE20HDQSG	192.168.100.210	Honey Pot	YES	17 March 2021 12:31		
7	WIN-KOCGCVB8KKV	192.168.100.8	Network Equipment - VPN	YES	16 March 2021 18:45		
8	SRV2019EN_DSKTP	192.168.102.11	MemberServer	YES			
9	SRV2019RU_DSKTP	192.168.102.34	MemberServer	YES			
10	WIN-YN9G899Q9FZ	192.168.100.59	Database Server	YES	16 March 2021 18:45		

4. Recommended Remediation

4.2 Hosts on APS

Harmony Purple's approach to mitigating the risk to a critical asset with a confirmed Attack Path Scenario (APS) is to cut the attack path by remediating the attack entry point used for initial access. The table below lists hosts that have one or more Attack Path Scenarios and the total number of APSs that will be mitigated if the host is remediated. These hosts should be patched according to Harmony Purple's recommended remediation, provided for each host.

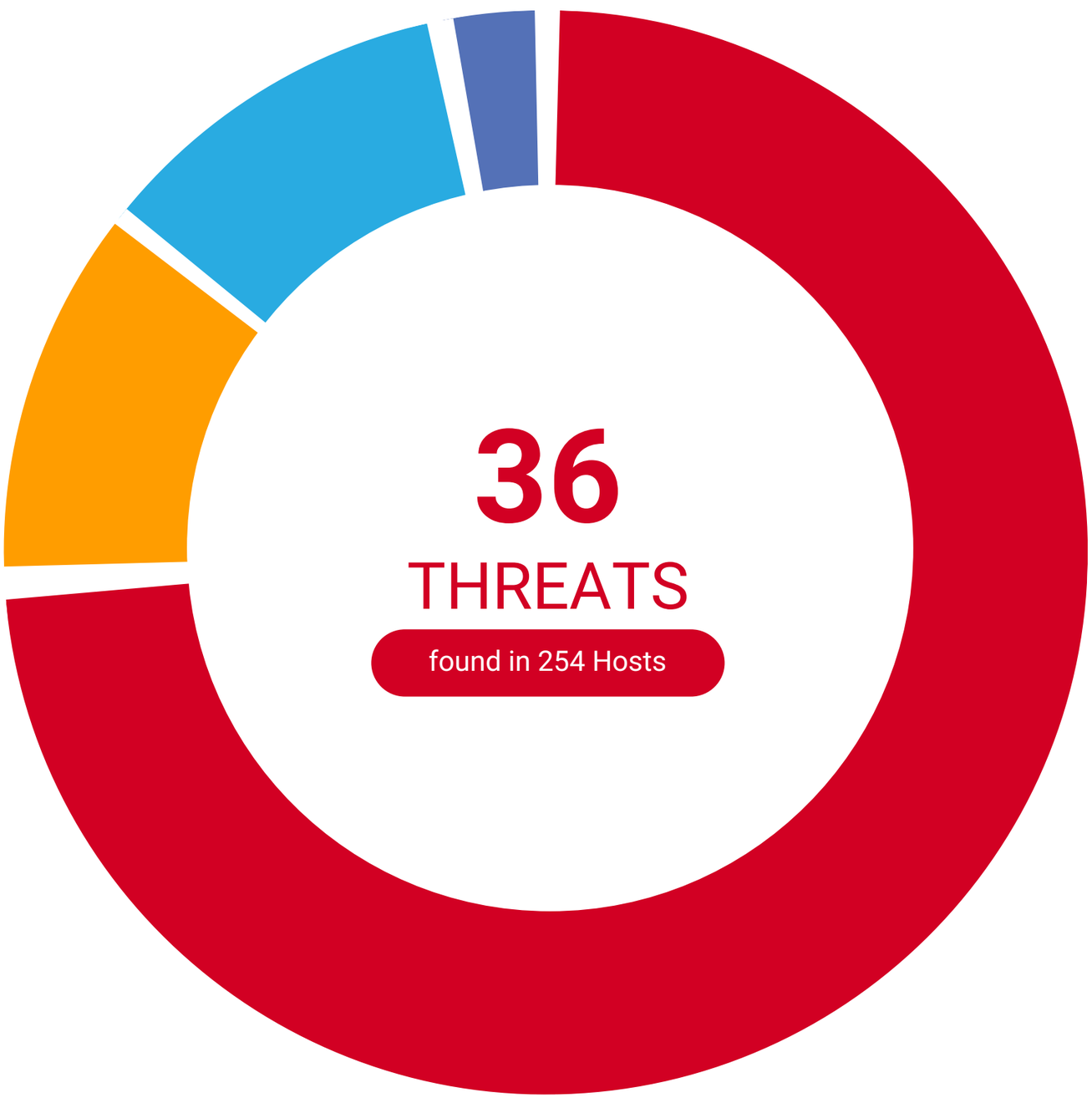
Critical High Medium Low

	Host name	IP	Role	Host significance	Total APSs
1	http://192.168.109.50	192.168.109.50	Web Application		32
2	http://192.168.109.81	192.168.109.81	Web Application		32
3	CLONE7LHNHAC	192.168.101.137	MemberWorkstation		22
4	VISTAX6CLONE	192.168.101.135	Server		22
5	WIN81X64	192.168.101.129	MemberWorkstation		22
6	DESKTOP-TBHFP33	192.168.101.252	MemberServer		22
7	WIN81X64CLONE	192.168.101.97	MemberWorkstation		22
8	WIN7CLONE	192.168.101.104	Storage		22
9	DESKTOP-G1F3BDC	192.168.101.167	MemberWorkstation		22
10	WIN7X64-PC	192.168.101.151	Firewall		21

5. Business Risks

5.1 Business Threats

Harmony Purple allows customers to specify the assets of interest in your organization for closer monitoring, and the potential business threat if such assets get compromised. The chart below lists the total number of assets of interest that were found at risk, broken down by potential business threat.



- 75.0% - Business Information Leakage (27)
- 11.11% - General Information Leakage (4)
- 11.11% - Service Interruption (4)
- 2.78% - Credentials Theft (1)

5. Business Risks

5.2 Business Scenarios Summary

Business Scenarios are organizational business processes of interest configured by the user, which Harmony Purple monitors closely against potential Attack Path Scenarios (APSs). If an APS meets a Business Scenario Rule, it will be displayed below, providing the total number of APSs found for each business scenario together with its significance level.

Critical High Medium Low

Business scenario name	Significance	Total APSs

6. Time to Patch

This section measures the effectiveness of your patch management process by tracking the total number of hosts missing an available patch recommendation.

This analysis is broken down by host significance over two time frames--30 days and 100 days. (Note: The host count in 100 days also includes the host count in 30 days.) The lower the number of unpatched hosts indicates that your patch process is more effective.

6.1 Number of Unpatched Hosts over Time

Critical High Medium Low

Over 30 days				
Host significance	Low	Medium	High	Critical
Number of hosts	**9**	**3**	**9**	**1**
Over 100 days				
Host significance	Low	Medium	High	Critical
Number of hosts	**12**	**4**	**14**	**1**

6.2 Average Time to Patch

Host significance	Low	Medium	High	Critical
Days	**35**	**30**	**15**	**9**