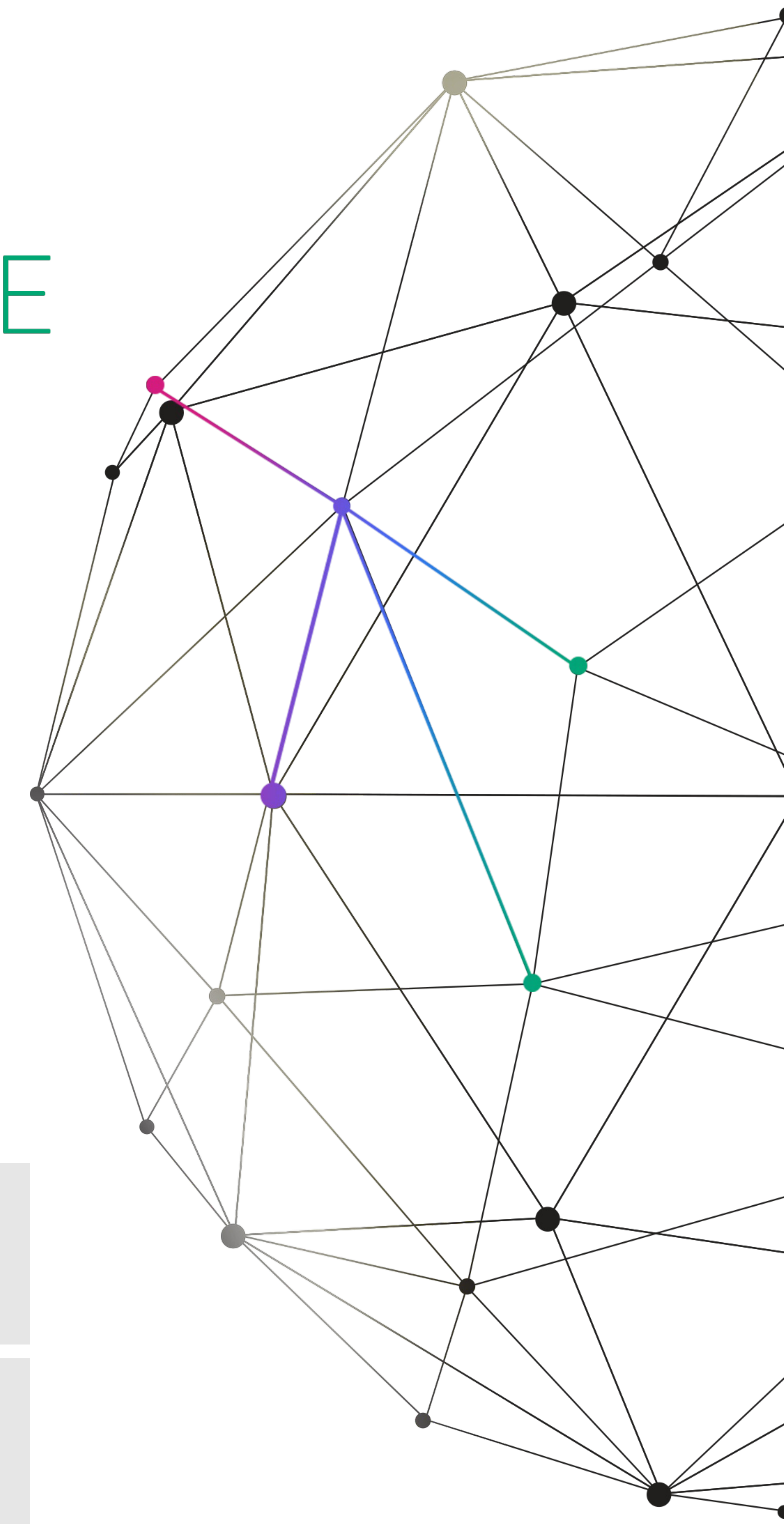
February 12, 2019

CYBOT PRO EXECUTIVE REPORT

Last Data update:
Jul. 31, 2018



CyBot product suite by Cronus is CVE compatible

cve.mitre.org

Cronus is a CREST-Certified Penetration Testing vendor

Provided by:
Digital Pathways LTD. **www.digpath.co.uk**

CYBOT PRO EXECUTIVE REPORT

February 12, 2019

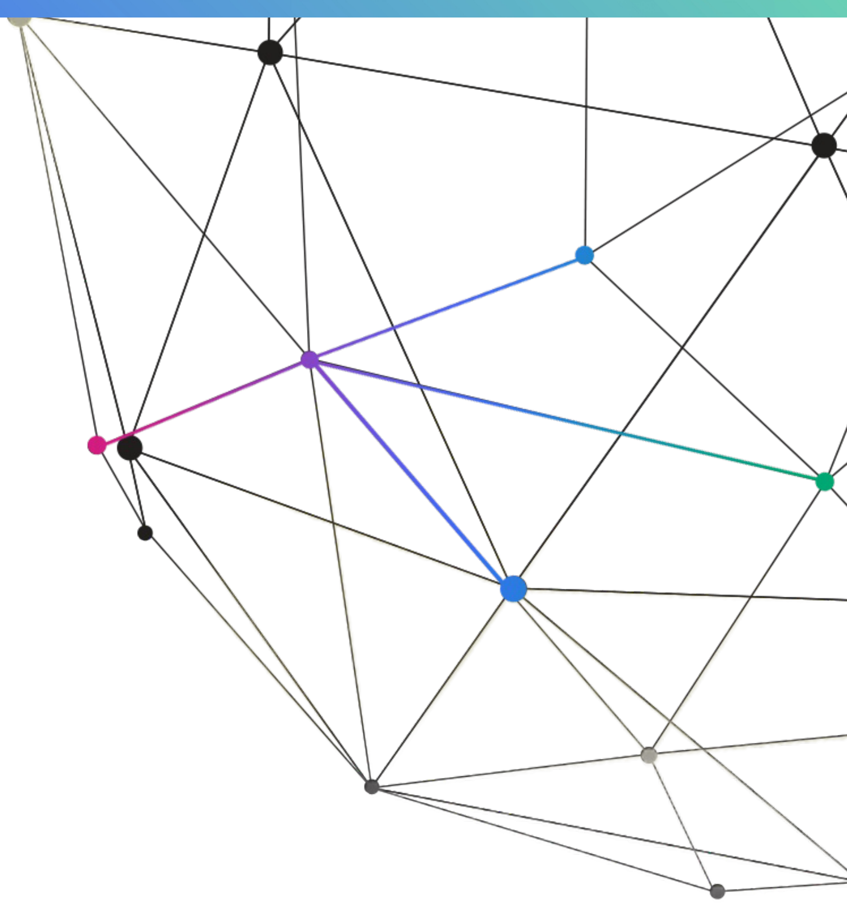
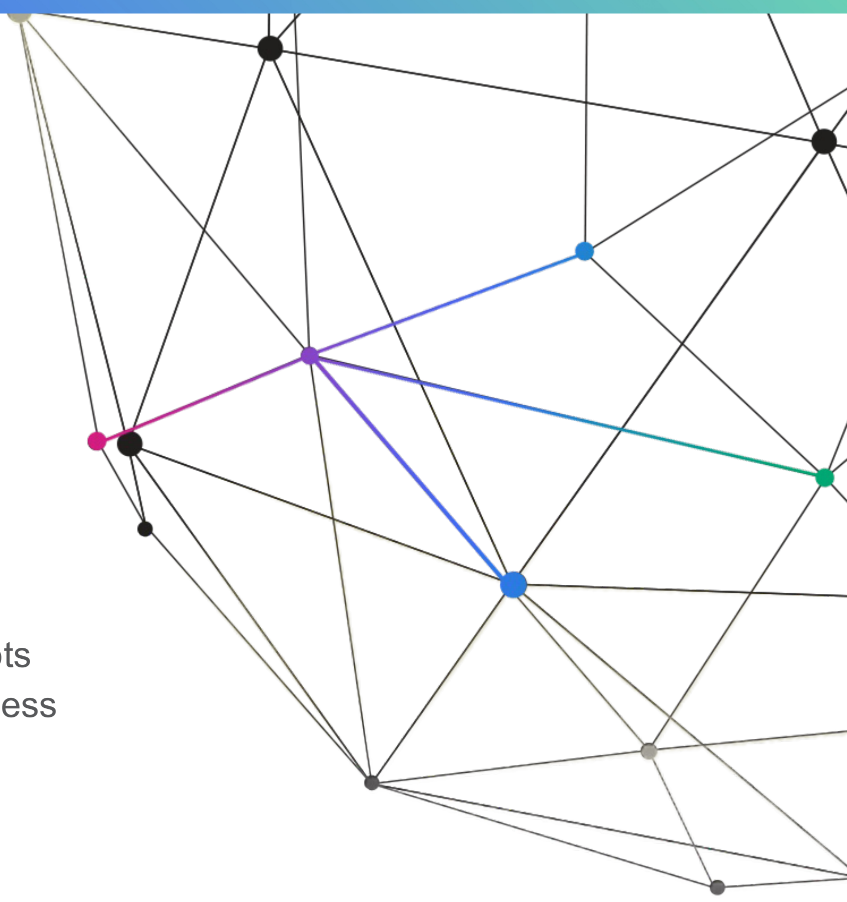


Table of contents:



1. Introduction:

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

How does it work?

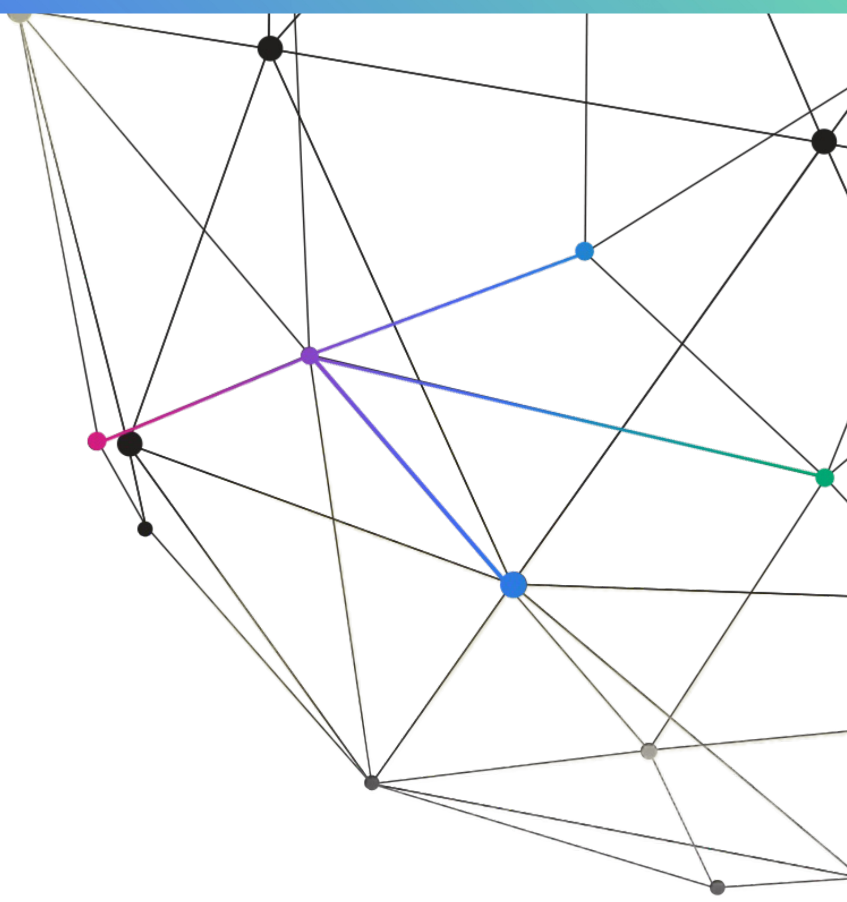
CyBot Pro scanned the network and detected Attack Path Scenarios^{TM} (APS) which threaten critical assets in the organisation.
The APS detected were either Global APS (APS between organisational networks, or branch offices) or Web APS (APS originating from a web application), or both, as detailed below.

2. Data summary:

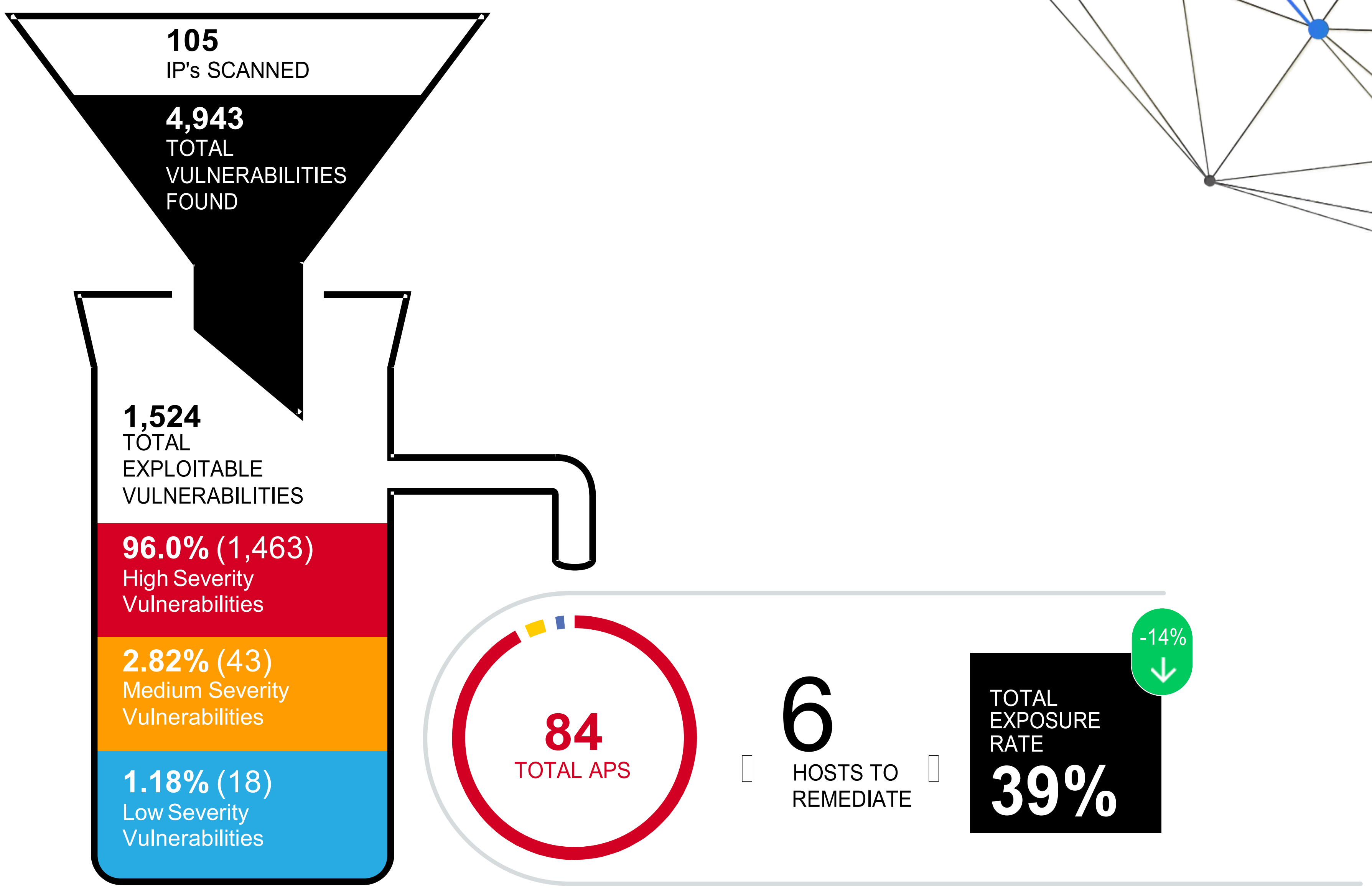
Total Assets at Risk	**19 from 27 (0 New)**
Member Server	2 from 3 (Exposure Rate 60%)
Domain Controller	1 from 1 (Exposure Rate 80%)
Other	16 from 23 (Exposure Rate 35%)

Total IP's Count	**105**
New IP's discovered	**1**

Web Applications at Risk	**1**



2.1 CyBot graphic visualisation



105
IP's SCANNED

4,943
TOTAL VULNERABILITIES FOUND

1,524
TOTAL EXPLOITABLE VULNERABILITIES

96.0% (1,463)
High Severity Vulnerabilities

2.82% (43)
Medium Severity Vulnerabilities

1.18% (18)
Low Severity Vulnerabilities

84
TOTAL APS

6
HOSTS TO REMEDIATE

TOTAL EXPOSURE RATE
39%
-14%

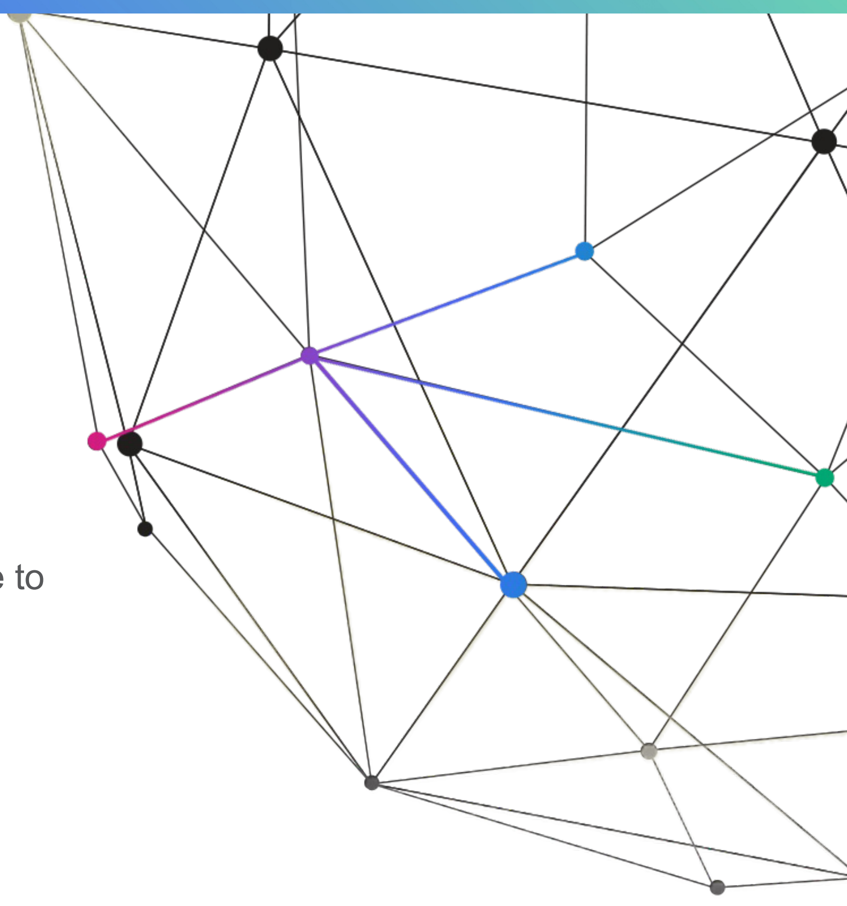
2.2 Network risk trends:

APS HOSTS
23%
-2%

INFO. LEAKAGE THREATS
93%
-7%

ASSETS AT RISK
4%
0%

MAJOR THREATS APS
6%
+6%



3. Attack Path Scenarios™ Summary:

Attack Path ScenariosTM (APS) is the exploitable paths that hacker can take to reach critical assets in the organisation.
APS can be either Infrastructure or Web (originating in a web application)

3.1 Exposure Rate Summary:

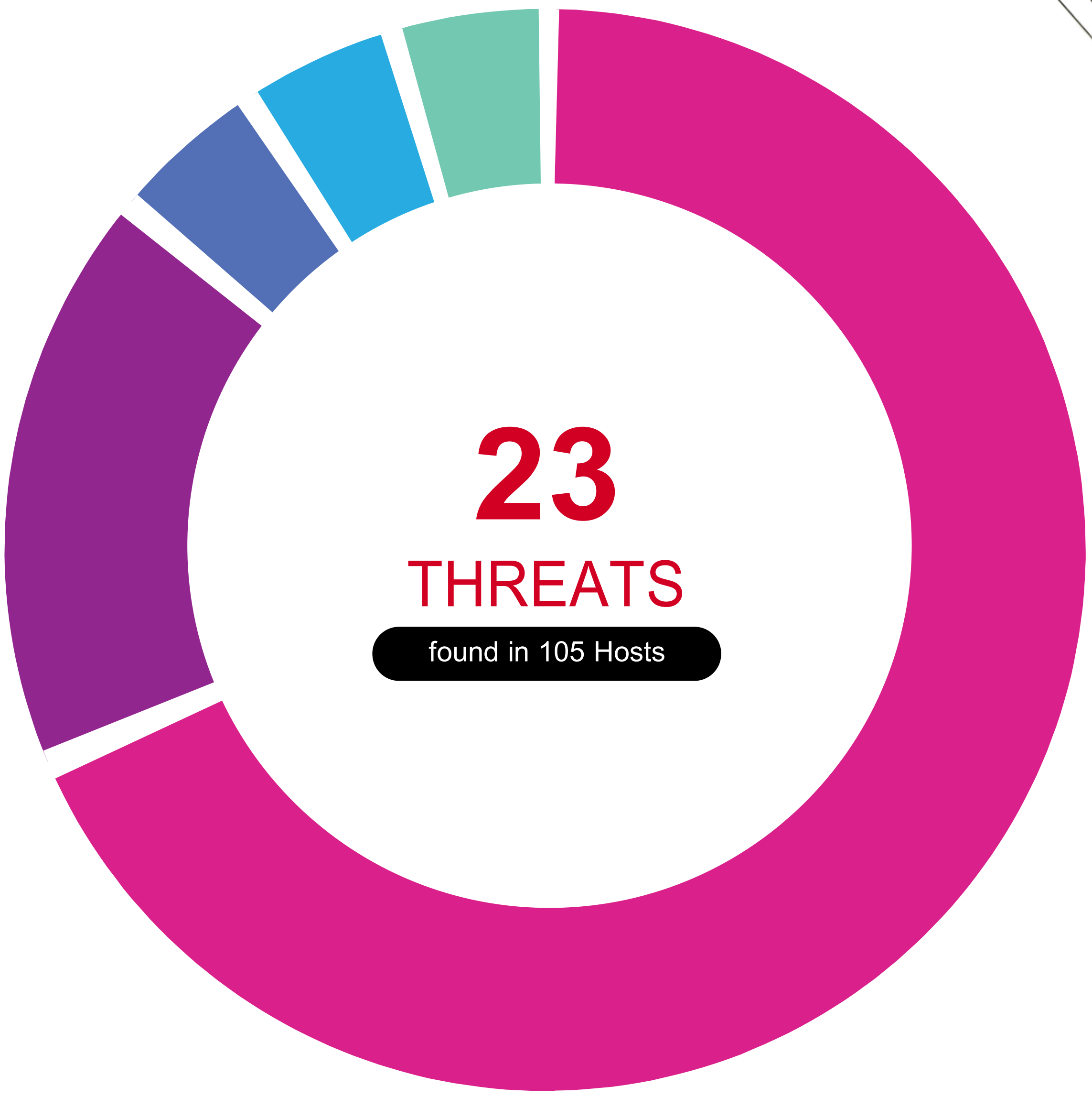
	INFRASTRUCTURE	APPLICATIVE
Attack Path ScenariosTM	80	4
Total APS	**84**	
Total Exposure Rate	**39%**	
Total Severity	MEDIUM	

What is The Exposure Rate?

Exposure Rate is a calculation of multiple factors, which results in a percentage that displays the likelihood and ease of being hacked.
The length of the APS, how many steps it entailed, the Significance and Business Risks of the Asset at Risk, and more, are all included in the calculation.

CRITICAL	Range from 75% to 100%
HIGH	Range from 50% to 74%
MEDIUM	Range from 25% to 49%
LOW	Range from 0% to 24%

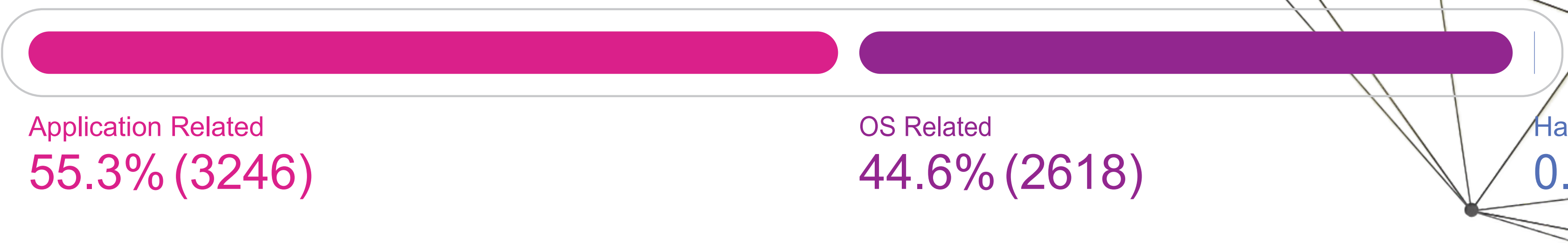
3.2 Business Risks:



LEGEND

- ● 69.57% - General Information Leakage (16)
- ● 17.39% - Business Information Leakage (4)
- ● 4.35% - Clients Information Leakage (1)
- ● 4.35% - Service Interruption (1)
- ● 4.35% - Credentials Theft (1)

4. Vulnerability Type Breakdown



4.1 CyBots by Risk:

Total Pivots	6
Total APS	84
Total Assets at Risk	19
Max. Exposure Rate	39%
Max. Significance	CRITICAL

5. Total Business Scenarios:

Business Scenarios are organisational business processes, configured by the user, which CyBot looks for.
If an APS meets a Business Scenario Rule, it will be displayed, providing organisations with a way to defend their business processes, as well as their systems.

5.1. Business Scenarios Summary:

	BUSINESS SCENARIO NAME	TOTAL FOUND	SIGINIFICANCE
1	**Default - DC**	**5**	CRITICAL
2	**CRM Porocess**	**0**	CRITICAL
3	**db apt**	**0**	CRITICAL
4	**Default - Critical WS**	**0**	CRITICAL
5	**Default - FW**	**0**	CRITICAL
6	**erp**	**0**	CRITICAL
7	**Main DB**	**0**	CRITICAL
8	**From Secretary WS**	**4**	HIGH
9	**DB Server**	**5**	LOW
10	**111**	**0**	LOW
11	**Default - DHCP**	**0**	LOW
12	**Default - DNS**	**0**	LOW
13	**Default - Router**	**0**	LOW