February 12, 2019

CRONUS REPORT

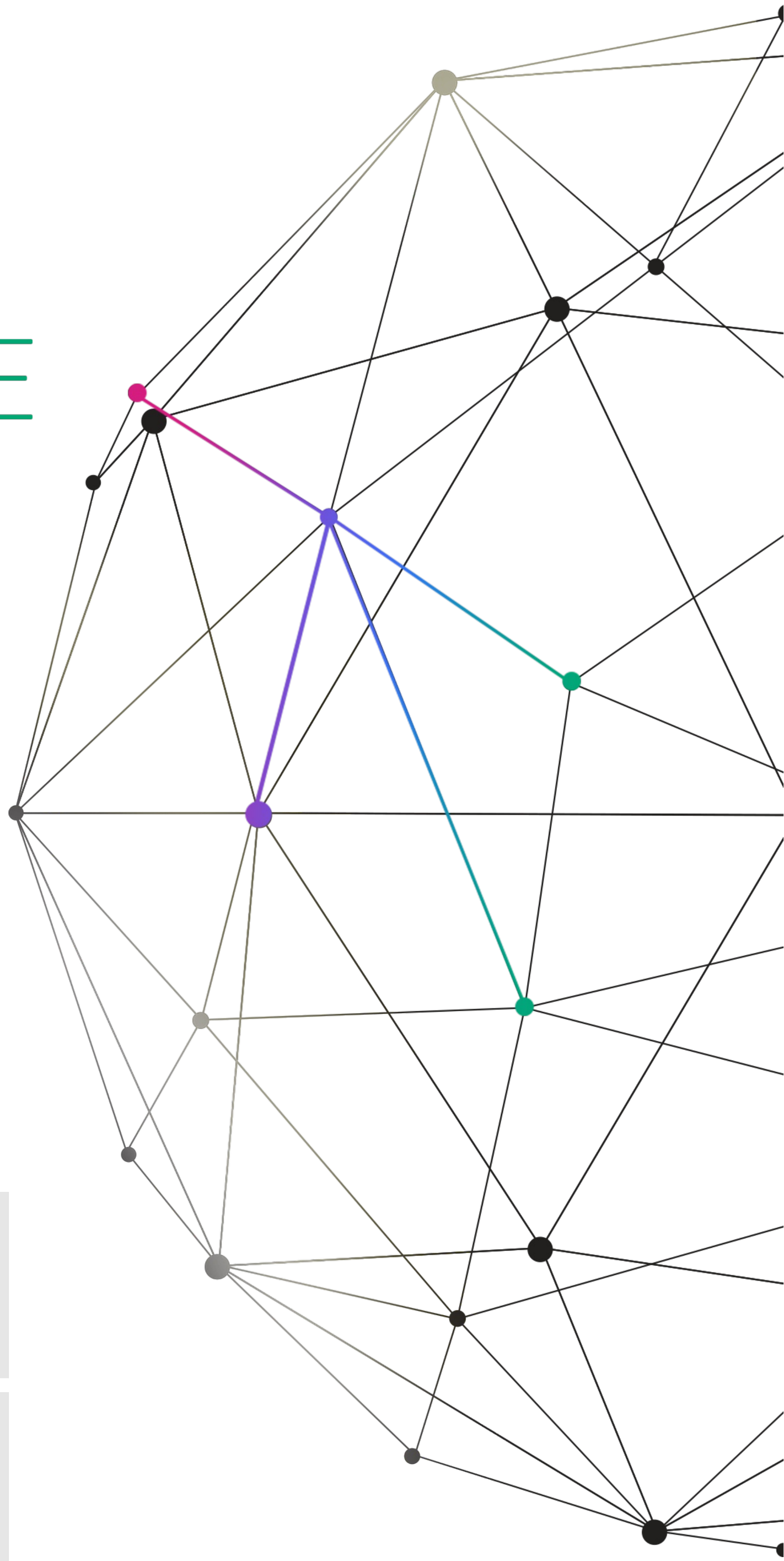
EXECUTIVE REPORT

Last Data update:
Feb. 11, 2019

THE CUSTOMER

CyBot product suite by
Cronus is CVE compatible

Cronus is a CREST-Certified
Penetration Testing vendor



CYBOT PRO EXECUTIVE REPORT

February 12, 2019

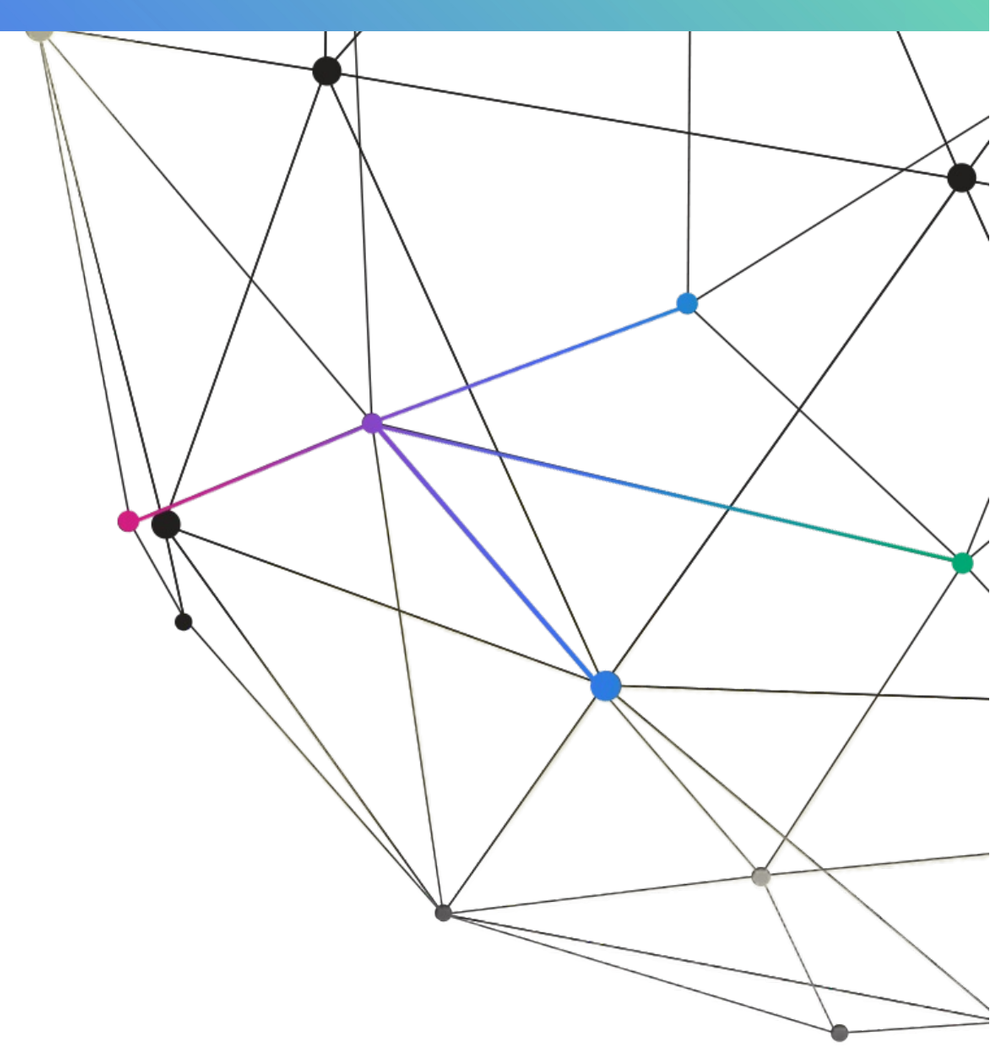
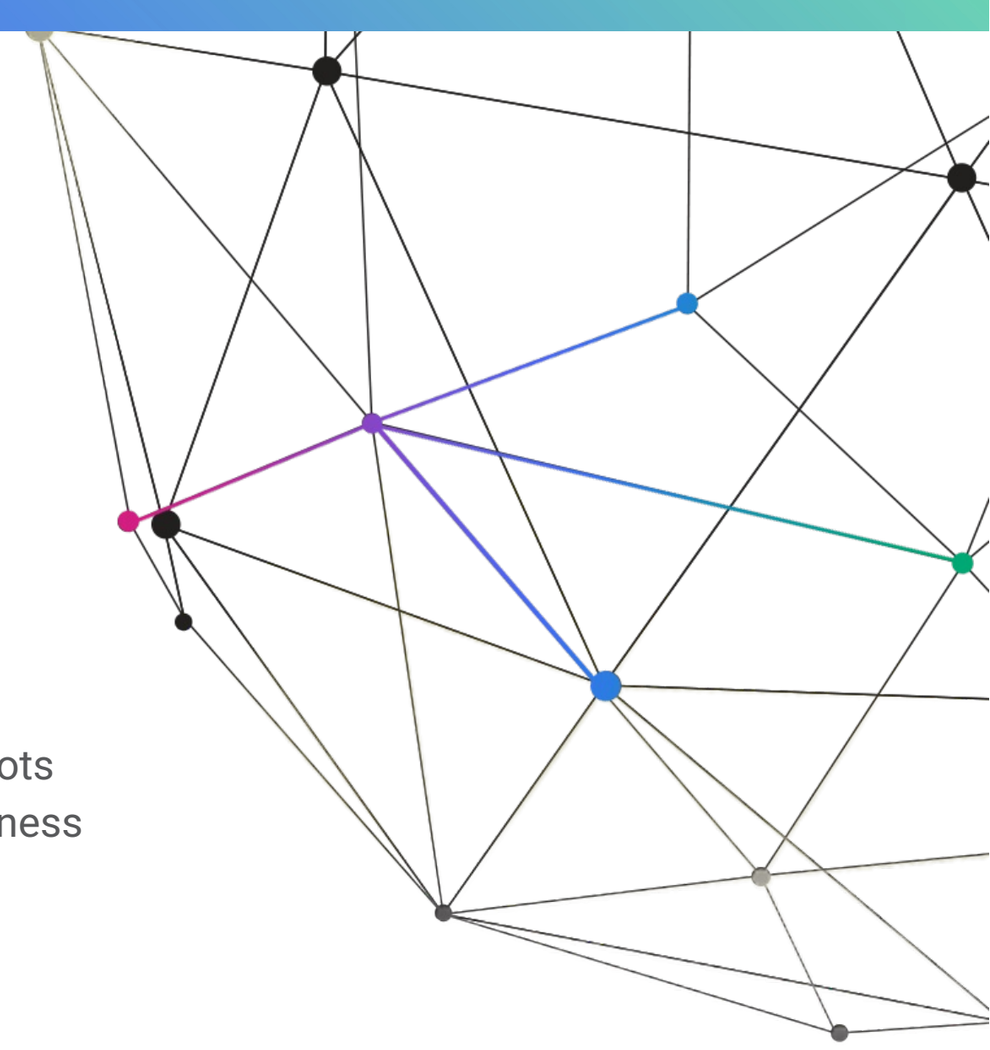


Table of contents:



1. Introduction:

The purpose of this report is to provide succinct, actionable information, summarizing the main risks, the threats to business processes and the 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™ (APS) which threaten critical assets in the organization.
The APS detected were either Global APS (APS between organizational networks, or branch offices) or Web APS (APS originating from a web application), or both, as detailed below.

2. Data summary:

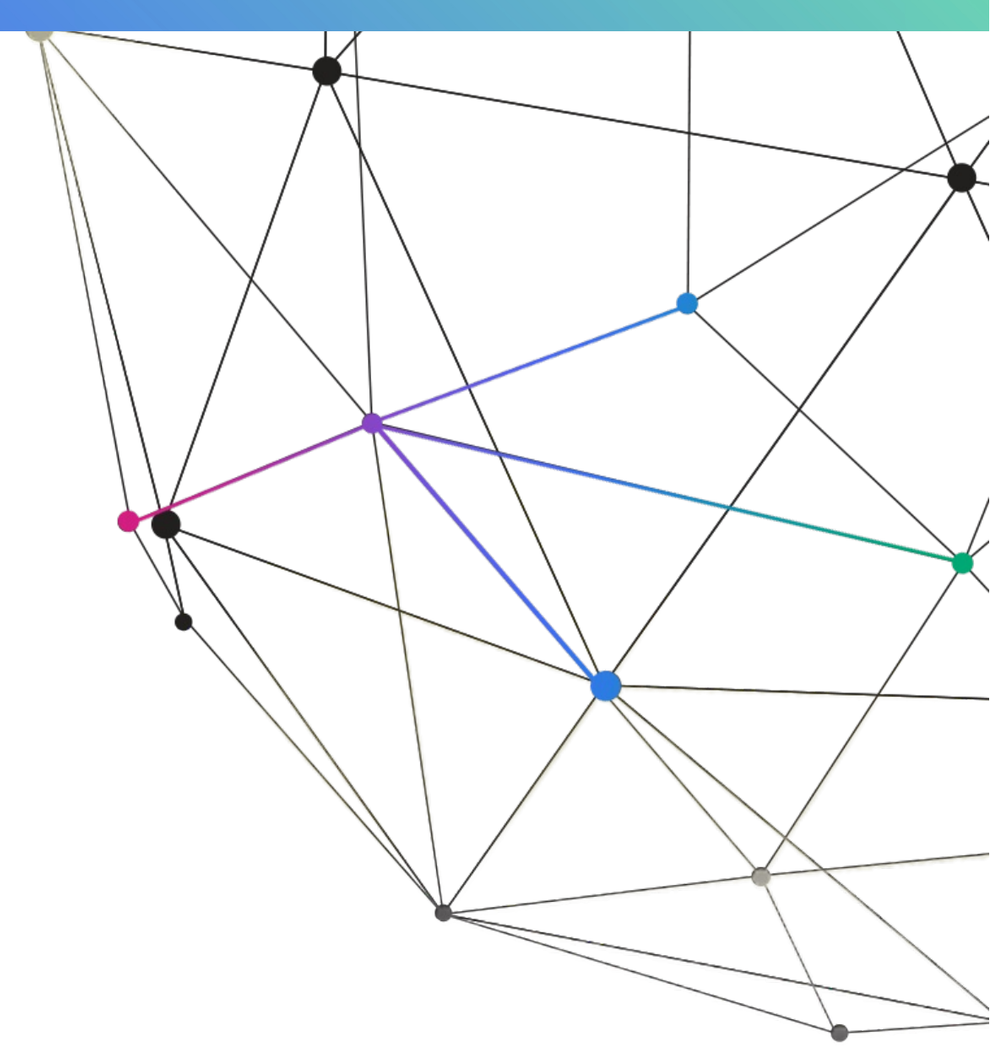
Total Assets at Risk	**42 from 198 (0 New)**
Member Server	38 from 173 (Exposure Rate 19%)
Domain Controller	2 from 4 (Exposure Rate 50%)
Other	2 from 21 (Exposure Rate 5%)

Total IP's Count	**476**
New IP's discovered	**0**

Web Applications at Risk	**0**

CYBOT PRO EXECUTIVE REPORT

February 12, 2019



2.1 CyBot graphic visualization

476
IP's SCANNED

1,663
TOTAL VULNERABILITIES FOUND

24
TOTAL EXPLOITABLE VULNERABILITIES

100.0% (24)
High Severity Vulnerabilities

0.0% (0)
Medium Severity Vulnerabilities

0.0% (0)
Low Severity Vulnerabilities

55
TOTAL APS

3
HOSTS TO REMEDIATE

+1%
TOTAL EXPOSURE RATE
18%

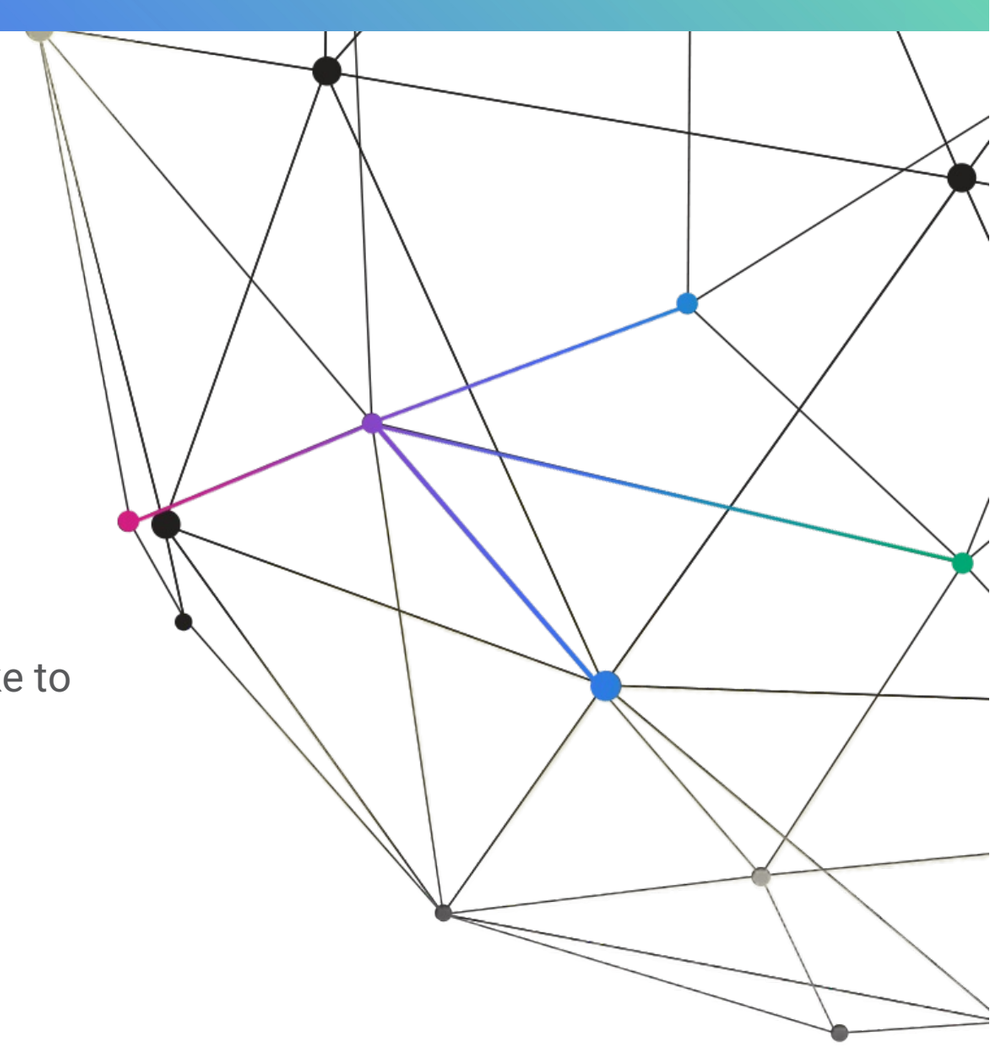
2.2 Network risk trends:

0%
APS HOSTS
8%

-8%
INFO. LEAKAGE THREATS
92%

+1%
ASSETS AT RISK
8%

+7%
MAJOR THREATS APS
7%



3. Attack Path Scenarios™ Summary:

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

3.1 Exposure Rate Summary:

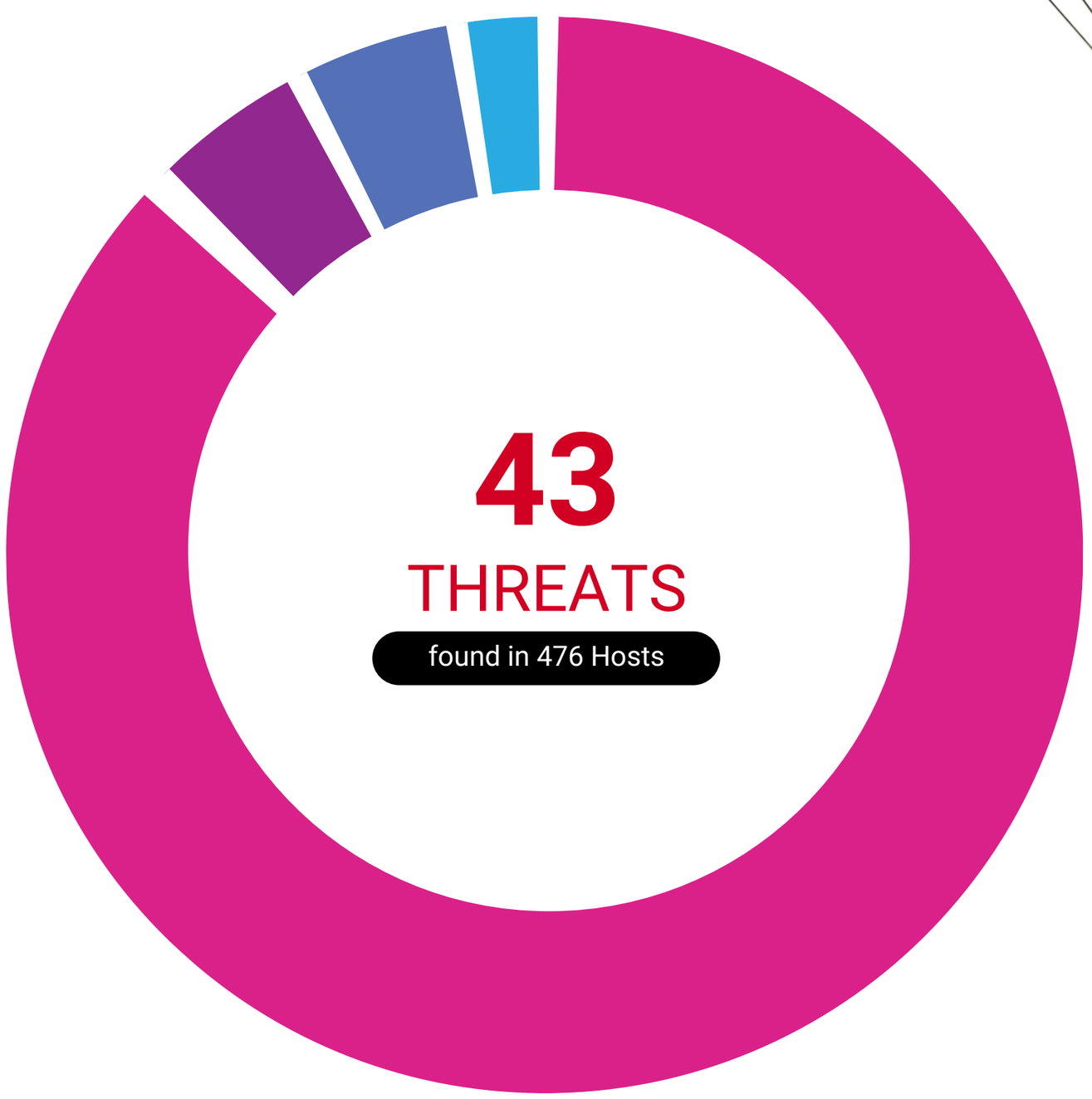
	INFRASTRUCTURE	APPLICATIVE
Attack Path Scenarios™	55	0
Total APS	**55**	
Total Exposure Rate	18%	
Total Severity	LOW	

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

- 88.37% - Business Information Leakage (38)
- 4.65% - General Information Leakage (2)
- 4.65% - Credentials Theft (2)
- 2.33% - Service Interruption (1)

4. Vulnerability Type Breakdown

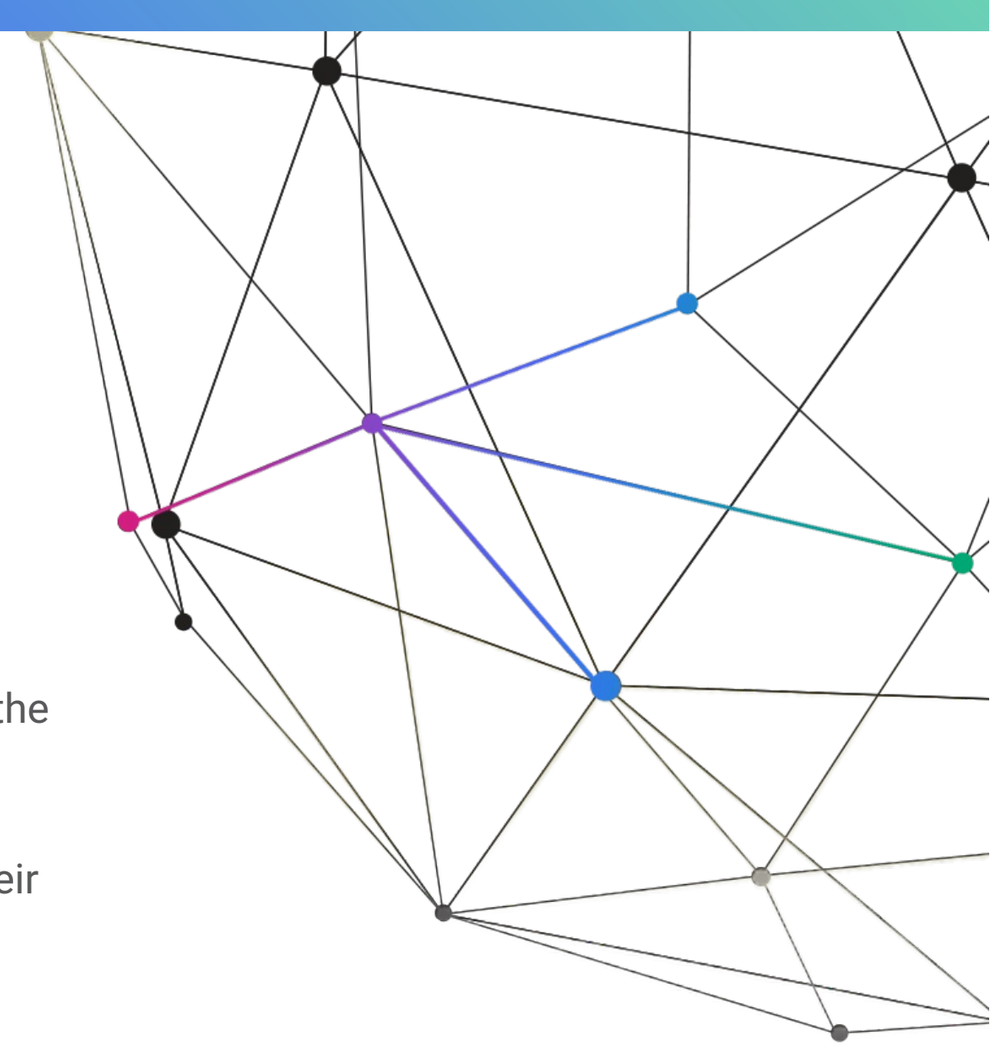
OS Related
51.16% (992)

Application Related
48.63% (943)

Hardware Related
0.21% (4)

4.1 CyBot Risks:

Total Pivots	3
Total APS	55
Total Assets at Risk	42
Max. Exposure Rate	18%
Max. Significance	CRITICAL



5. Total Business Scenarios:

Business Scenarios are organizational business processes, configured by the user, which CyBot looks for.
If an APS meets a Business Scenario Rule, it will be displayed, providing organizations 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 - C-Level WS**	**0**	CRITICAL
2	**Default - Critical WS**	**0**	CRITICAL
3	**Default - FW**	**0**	CRITICAL
4	**Default - DC**	**0**	LOW
5	**Default - DHCP**	**0**	LOW
6	**Default - DNS**	**0**	LOW
7	**Default - Router**	**0**	LOW