ALGOSYSTEMS
THE PATH FORWARD

Exposed

The Ugly truth behind your Vulnerable Digital Existence

Data Breaches Insights

3x

The number of data breaches more than tripled between 2013 and 2022

95%

In the 2023 IBM Cost of a Data Breach Report, 95% of breached organizations surveyed experienced more than one data breach. According to a 2022 study by Forrester, nearly 75% of surveyed organizations were victims of a data breach in the prior 12 months.

98%

98% of organizations have a relationship with a vendor that experienced a data breach within the last two years.

60%

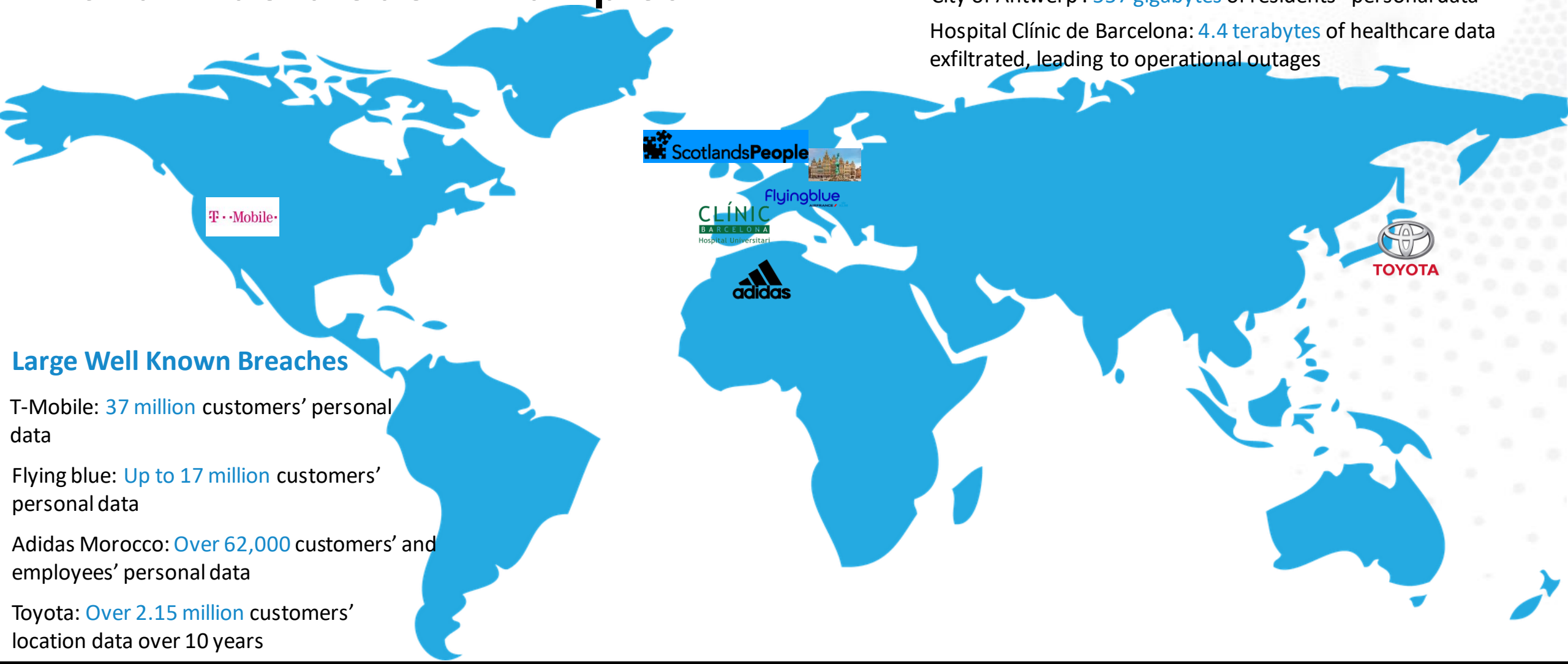
Up to 60% of data breaches are caused by failing to patch known vulnerabilities. The rest include Social Engineering and Phishing Attacks, Misconfigurations, Insider Threats, Zero-Day Attacks

Impact of Breaches

- $ Based on the latest reports the global average cost of Data Breach regarding a Cybersecurity or Ransomware attack span to ~ **$4.5B**

- $ CNBC reports that cyberattacks cost for US-Based SMEs an average of **$200K - $300K**, with some pushed to closure

World Wide breach Examples



Large Well Known Breaches

T-Mobile: 37 million customers' personal data

Flying blue: Up to 17 million customers' personal data

Adidas Morocco: Over 62,000 customers' and employees' personal data

Toyota: Over 2.15 million customers' location data over 10 years

Smaller Less Known Breaches

Scotland's People: Birth, death, and adoption records going back up to 100 years

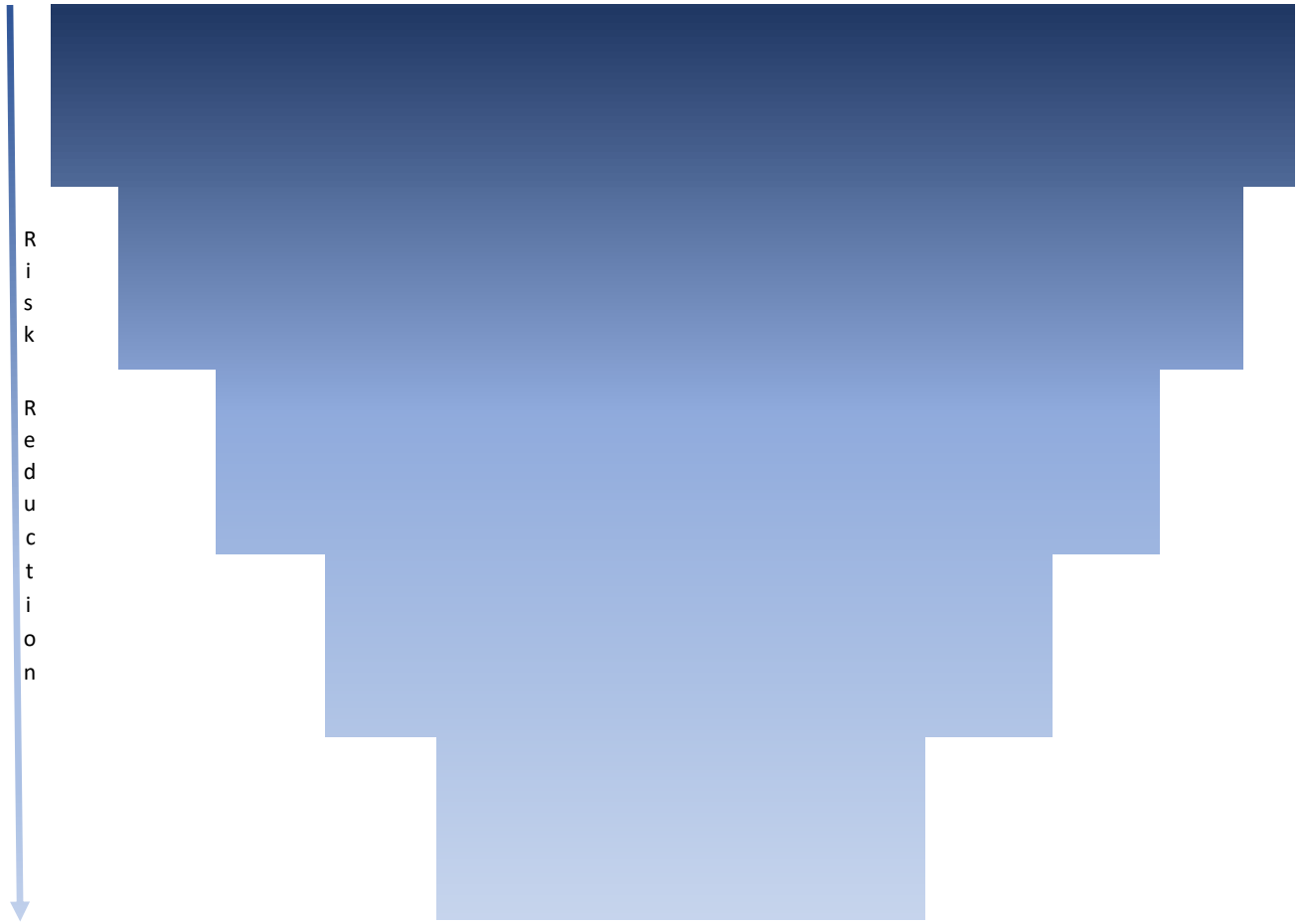
City of Antwerp : 557 gigabytes of residents' personal data

Hospital Clínic de Barcelona: 4.4 terabytes of healthcare data exfiltrated, leading to operational outages

I have a Firewall, some would say!

But do you assess and patch regularly??

Who does it affect?



Not performing any Vulnerability Assessment

Performing single annual Vulnerability Assessment to identify some risks

Performing regular Vulnerability Assessment / Management and introduce Patching processes

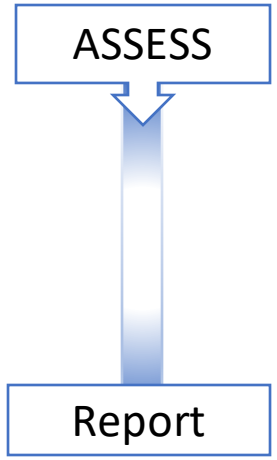
Performing regular Vulnerability Assessment / Management and introduce Patching and Vulnerability Mitigation processes

Performing continuous Vulnerability Assessment / Management and utilize continuous Patching and Vulnerability Mitigation processes

Mandate for a shift in Mindset

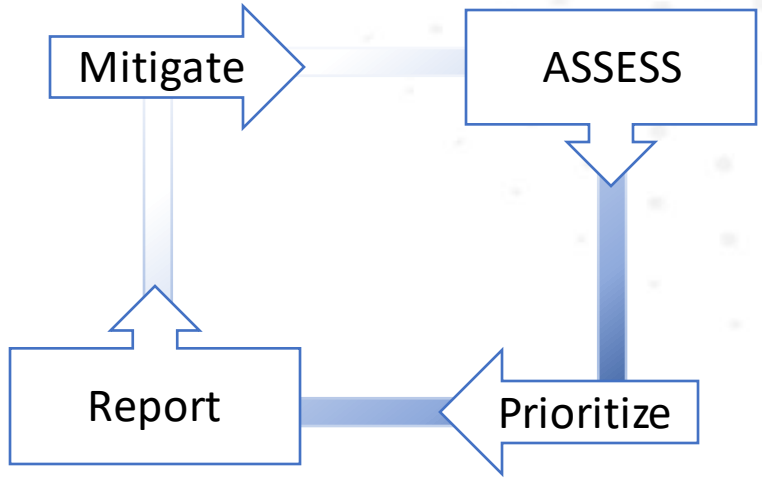
Vulnerability Assessment

- Goal: Identify vulnerabilities
- Approach: Point-in-time evaluation
- Frequency: Usually once a year
- Outputs: Vulnerability report (usually huge)



Vulnerability Management

- Goal: Manage vulnerabilities through assessment, prioritization, remediation, and retesting
- Approach: Ongoing Process
- Frequency: Continuous or as frequently as possible
- Outputs: Summarized Report with remediation action plan and recommendations



Algosystems Vulnerability Management As a Service

VMaaS
AlgoVaas

Solving today's industry issues

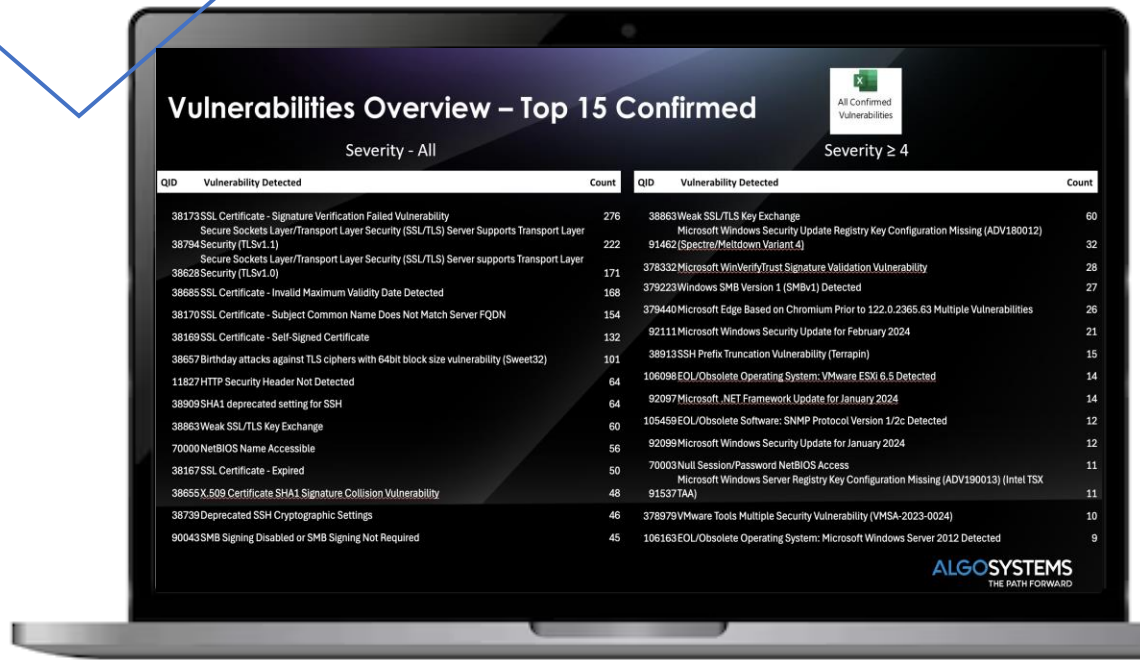
- Algo consultants provide refined summarized reports
- Algo consultants provide provide information on V M process Including guidance on mitigation process
- Algosystems can manage the VM process end-2-end

Algosystems Vulnerability Management As a Service

VMaaS
AlgoVaas

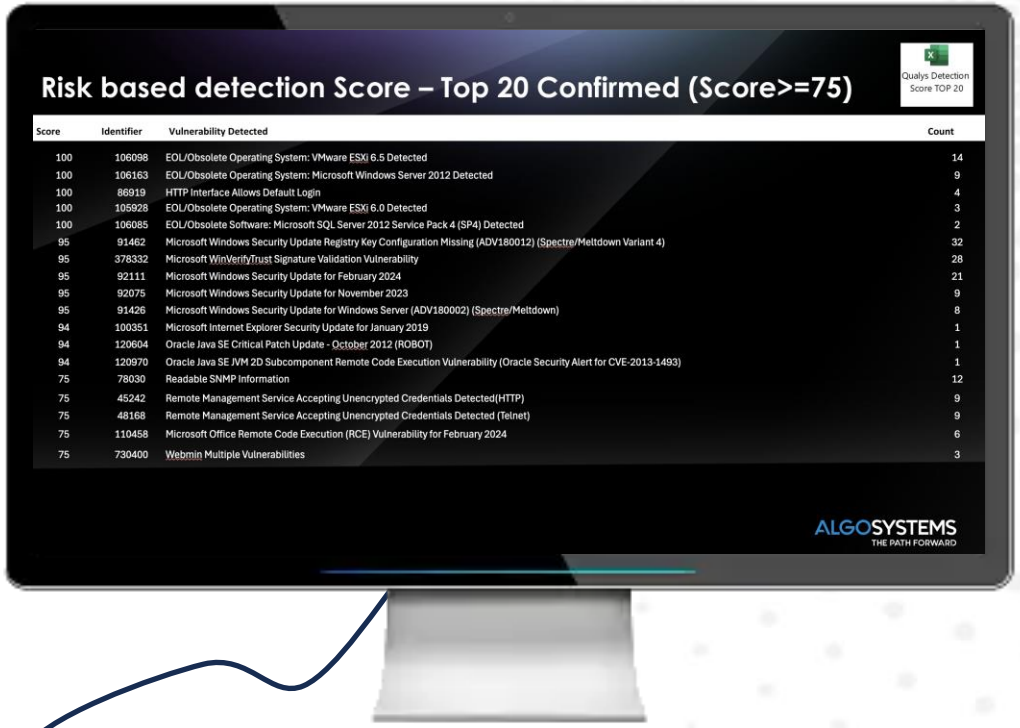
Algosystems Vulnerability Management As a Service

VMaaS
AlgoVaas



QID	Vulnerability Detected	Count
38173	SSL Certificate - Signature Verification Failed Vulnerability	276
38794	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	222
38628	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	171
38685	SSL Certificate - Invalid Maximum Validity Date Detected	168
38170	SSL Certificate - Subject Common Name Does Not Match Server FQDN	154
38169	SSL Certificate - Self-Signed Certificate	132
38657	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	101
11827	HTTP Security Header Not Detected	64
38909	SHA1 deprecated setting for SSH	64
38863	Weak SSL/TLS Key Exchange	60
70000	NetBIOS Name Accessible	56
38167	SSL Certificate - Expired	50
38655	X.509 Certificate SHA1 Signature Collision Vulnerability	48
38739	Deprecated SSH Cryptographic Settings	46
90043	SMB Signing Disabled or SMB Signing Not Required	45

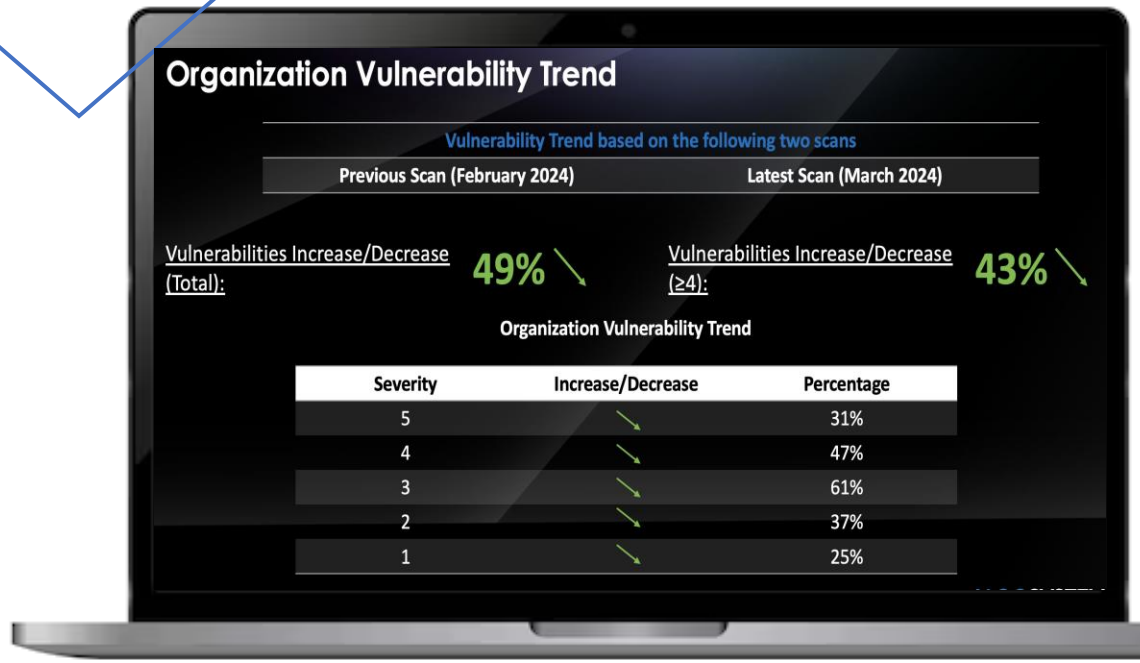
QID	Vulnerability Detected	Count
38863	Weak SSL/TLS Key Exchange	60
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4)	32
378332	Microsoft WinVerifyTrust Signature Validation Vulnerability	28
379223	Windows SMB Version 1 (SMBv1) Detected	27
379440	Microsoft Edge Based on Chromium Prior to 122.0.2365.63 Multiple Vulnerabilities	26
92111	Microsoft Windows Security Update for February 2024	21
38913	SSH Prefix Truncation Vulnerability (Terrapin)	15
106098	EOL/Obsolete Operating System: VMware ESXi 6.5 Detected	14
92097	Microsoft .NET Framework Update for January 2024	14
105459	EOL/Obsolete Software: SNMP Protocol Version 1/2c Detected	12
92099	Microsoft Windows Security Update for January 2024	12
70003	Null Session/Password NetBIOS Access	11
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) (Intel TSX TAA)	11
378979	VMware Tools Multiple Security Vulnerability (VMSA-2023-0024)	10
106163	EOL/Obsolete Operating System: Microsoft Windows Server 2012 Detected	9

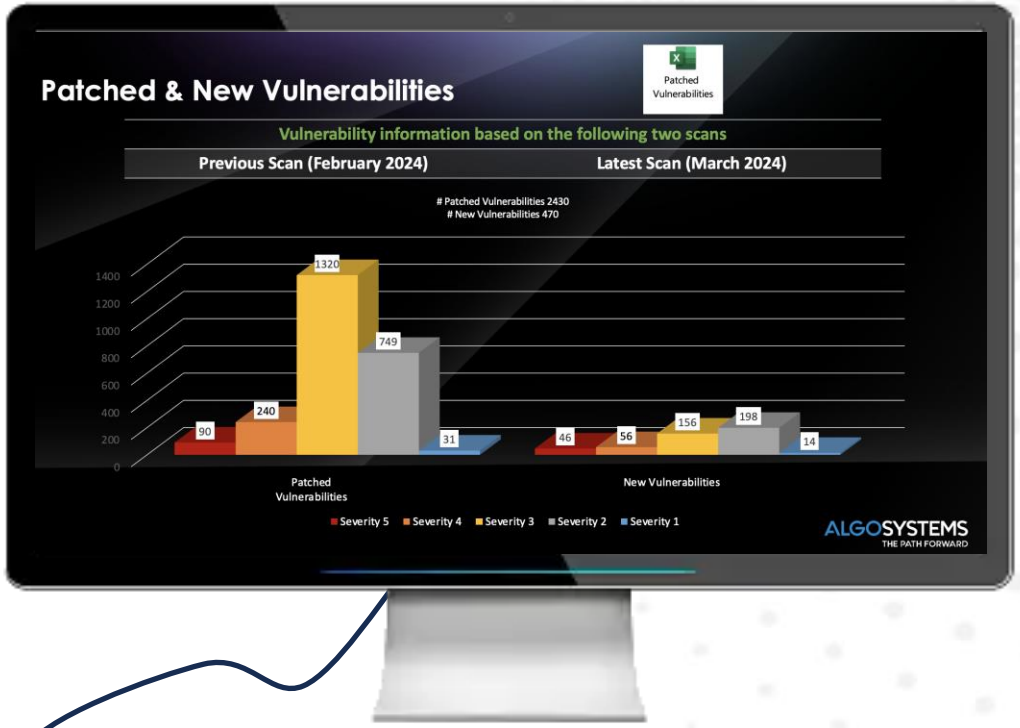


Score	Identifier	Vulnerability Detected	Count
100	106098	EOL/Obsolete Operating System: VMware ESXi 6.5 Detected	14
100	106163	EOL/Obsolete Operating System: Microsoft Windows Server 2012 Detected	9
100	86919	HTTP Interface Allows Default Login	4
100	105928	EOL/Obsolete Operating System: VMware ESXi 6.0 Detected	3
100	106085	EOL/Obsolete Software: Microsoft SQL Server 2012 Service Pack 4 (SP4) Detected	2
95	91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4)	32
95	378332	Microsoft WinVerifyTrust Signature Validation Vulnerability	28
95	92111	Microsoft Windows Security Update for February 2024	21
95	92075	Microsoft Windows Security Update for November 2023	9
95	91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown)	8
94	100351	Microsoft Internet Explorer Security Update for January 2019	1
94	120604	Oracle Java SE Critical Patch Update - October 2012 (ROBOT)	1
94	120970	Oracle Java SE JVM 2D Subcomponent Remote Code Execution Vulnerability (Oracle Security Alert for CVE-2013-1493)	1
75	78030	Readable SNMP Information	12
75	45242	Remote Management Service Accepting Unencrypted Credentials Detected(HTTP)	9
75	48168	Remote Management Service Accepting Unencrypted Credentials Detected (Telnet)	9
75	110458	Microsoft Office Remote Code Execution (RCE) Vulnerability for February 2024	6
75	730400	Webmin Multiple Vulnerabilities	3

Algosystems Vulnerability Management As a Service

VMaaS
AlgoVaas

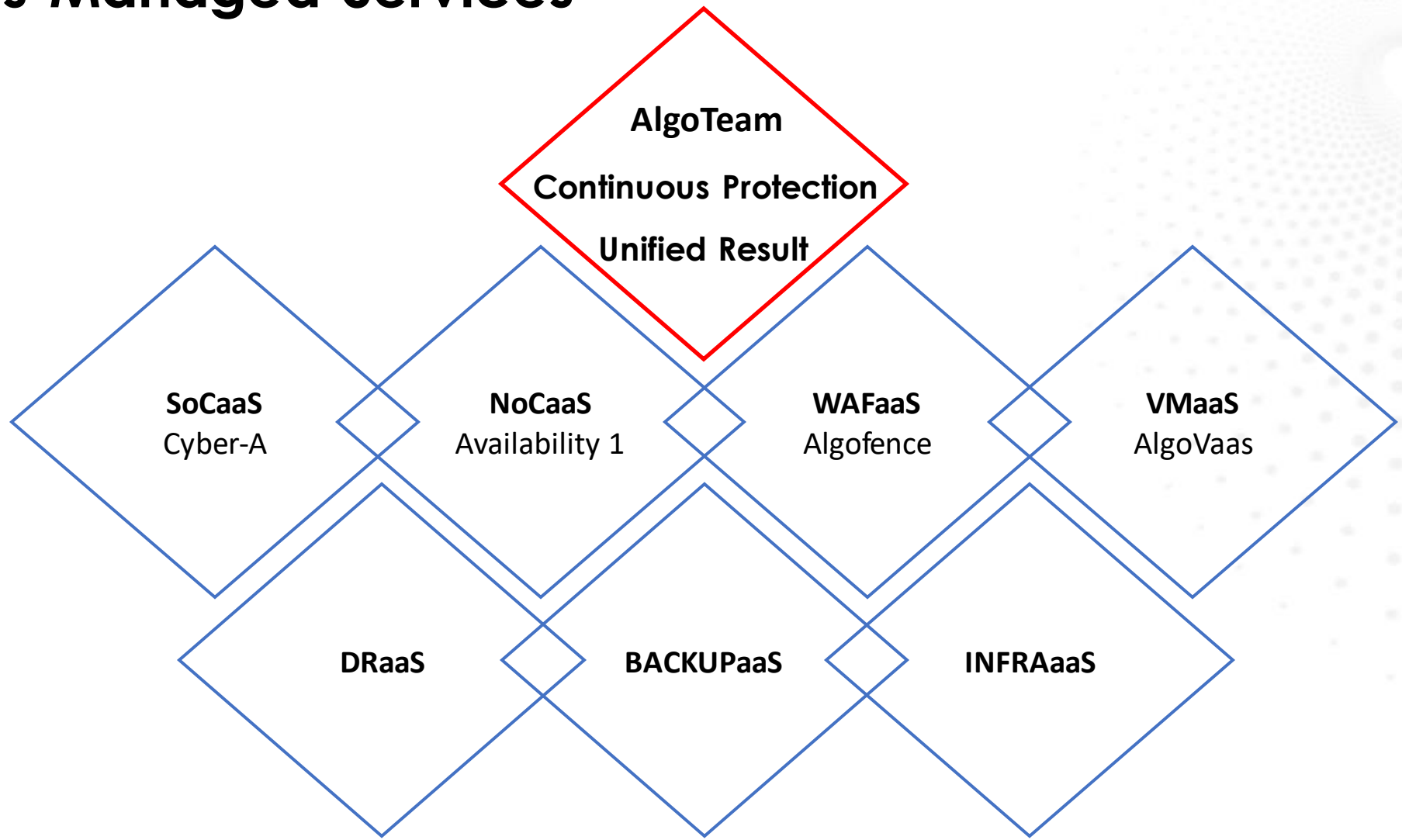




VMaaS by Algosystems

- Assists with continuous evaluation of the organization's security posture
- Provides an expert's point of view on the day-to-day remediation lifecycle
- Improves the vulnerability identification and prioritization
- Reduced Burden on IT Staff as a fully managed service
- Subscription based model eliminates the upfront costs associated with purchasing and maintaining vulnerability management software

Algosystems Managed Services



ALGOSYSTEMS
THE PATH FORWARD

THANK YOU