edgescan™

SMART VULNERABILITY MANAGEMENT™

2022 Vulnerability Statistics Report

Table of Contents

Introduction

For our 7th Year running, welcome to the Edgescan Vulnerability Stats Report 2022. This report aims to demonstrate the state of full stack security based on thousands of security assessments and penetration tests performed globally, as delivered by the Edgescan SaaS during 2021.

Compiling this report and delving into the underlying data is still a joy as it let us understand the true state of cyber posture based on thousands of assessments and penetration tests. It gives unique insight into what's going on from a trends and statistics perspective and indeed a snapshot of the overall state of cyber security.

The Edgescan report has become a reliable source for truly representing the global state of cyber security vulnerability management. This is becoming more evident as our unique dataset is now also part of other annual security analysis reports, such as the Verizon DBIR (we are happy contributors for many years now).

This year we examined vulnerability metrics from a known vulnerability (CVE), Malware, Ransomware and visibility standpoint (exposed services), coupling both internal and public Internet-facing systems. We also take a look at how quick we are fixing various vulnerabilities based on risk.

We still see high rates of known (i.e. patchable) vulnerabilities, which have working exploits in the wild, used by known nation state and cyber criminal groups.

We also decided to look at the state of cyber posture from an ASM (Attack Surface Management) standpoint. Exposed services are a real risk. Statistically some of the exposures have a very low percentage but many of them would result in a breach.

Remote access exposures across the attack surface are a worrying trend and accounted for 5% of total exposures in 2021.

So yes, patching and maintenance is still a challenge, demonstrating that it is not trivial to patch production systems. The MTTR (Mean Time to Remediation) stats also reflect on this issue. Detection on a constant basis needs improvement and as I've always said, visibility is paramount. The web application layer is where the majority of risk still resides, but some lower layer (Host/Operating system/Protocol) issues, if discovered, could also present headaches if exploited. CVE's as old as 2015 are being used by ransomware and malware toolkits to exploit systems within "the perimeter".

Attack Surface Management (Visibility) is a key driver to cyber security and based on our continuous asset profiling, we discuss how common sensitive and critical systems are exposed to the public Internet. The assumption here is that enterprises simply did not have the visibility or systems in place, to make them aware of, or inform them of the exposure.

This report provides a glimpse of a global snapshot across dozens of industry verticals and how to prioritize on what is important, as not all vulnerabilities are equal. We call out which threat actors are leveraging discovered vulnerabilities, which should be food for thought.

This year we included a section on API security based on the assessment of thousands of API's in 2021. We list the Top API vulnerabilities and frequency of such.

Best Regards

Eoin Keary

2021 Year in Review
Breaches of note and root causes of 2021

Log4j:

(CVE-2021-44228 – CVSS Score: 10) A zero-day vulnerability in the Log4j Java library, a remote code execution (RCE) flaw, has now been actively exploited in the wild since December 2021. The vulnerability is known as Log4Shell and is now being weaponized by botnets, including Mirai, CONTI, Konsari, and TellYouThePass groups, currently leveraging it in their campaigns. See https://www.edgescan.com/log4shell-quick-script/ for technical guidance. – **Root cause: Remote Code Injection**

Bitmart:

In December, Bitmart said a security breach permitted cyberattackers to steal circa $150 million in cryptocurrency, with total losses including damages, to reach $200 million. Criminals stole various crypto tokens on December 4, after using a stolen privacy key to gain access to one of BitMart's hot wallets. – **Root cause: Stolen authentication credentials**

Robinhood:

Number Of Individuals Impacted: 7 million. Robinhood disclosed a data breach impacting five million users of the app. Email addresses, names, phone numbers, and more were accessed via a customer support system. For the vast majority of affected customers, the only information obtained was an email address or a full name. For 310 people, the information taken included their name, date of birth, and ZIP code. Of those, 10 customers had "more extensive account details revealed," Robinhood said in a statement. - **Root cause: customer-service reps were socially engineered into sharing information**

UC San Diego Health:

UC San Diego Health said employee email accounts were compromised by criminals, leading to an exposure. Patient, student and employee data potentially including medical records, claims information, prescriptions, treatments, Social Security numbers, were exposed. - **Root cause: Phishing attack**

Kaseya:

A vulnerability in a platform developed by IT services provider Kaseya was exploited in order to hit an estimated 800 - 1500 customers, including MSPs. It is believed that attackers carried out a supply chain ransomware attack by leveraging a vulnerability in Kaseya's VSA software against multiple managed service providers (MSP) and their customers. – **Root Cause: Supply chain attack**

"Many attacks in 2021 were attributed to weaknesses such as exposed remote login or exposed data stores."

2021 Year in Review
Breaches of note and root causes of 2021

Volkswagen, Audi:

The car manufacturers disclosed a data breach impacting over 3.3 million customers, the majority of which were based in the United States. It occurred between August 2019 and May 2021. Audi and Volkswagen customer data was being sold on a hacking forum after being stolen from an exposed Azure BLOB container. – **Root Cause: Exposed Database**

Colonial Pipeline:

The fuel pipeline operator was struck by ransomware, via the DarkSide cyber criminal collective. This resulted in fuel delivery disruption and panic buying across the United States. The company paid a ransom. The weakness was an exposed legacy VPN service, with only single-factor authentication. – **Root Cause: Exposed Remote Access Service**

Facebook:

A data dump of information belonging to over 550 million Facebook users was published online. Facebook IDs, names, dates of birth, genders, locations, and relationship statuses were included in the logs, of which Facebook (now known as Meta) said was collected via scraping in 2019. – **Root Cause: Unprotected personal data.**

CNA Financial:

75,000 individuals impacted. CNA Financial employees were unable to access corporate systems and were locked out following a ransomware attack which also involved the theft of internal data. The company paid a $40 million ransom. They were attacked via Phoenix Cryptolocker Ransomware. - **Root Cause: Exposed Remote Access Service**

Microsoft Exchange Server:

Over 30,000 organizations across the United States impacted. Widespread compromise of Microsoft Exchange servers caused by a set of zero-day vulnerabilities known as ProxyLogon leveraging CVE-2021-26855,. Microsoft became aware of the flaws in January and released emergency patches in March. - **Root Cause: Remote Code Execution / Server Side Request Forgery**
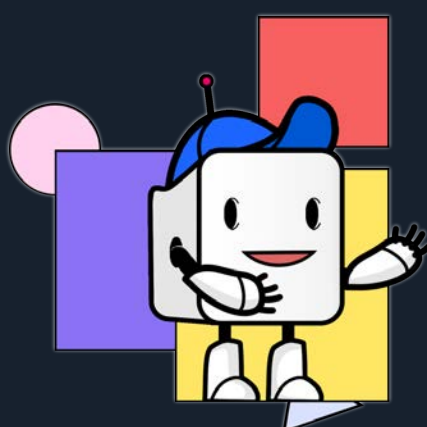
OneMoreLead:

Number of individuals impacted 63 Million. OneMoreLead used an exposed database to store the personal and professional information for to at least 63 million people. – **Root Cause: Exposed Database**

How we get the numbers

The statistics below are based on the full stack assessment of tens of thousands of individual assets during 2021.

This included over **40,000** web application and API assessments, **3 million Network Endpoint assessments** and circa **1000 penetration tests** delivered in 2021 by the edgescan team.

40% of Edgescan clients leverage on-demand Penetration Testing as a Service (PTaaS)

65% of clients regularly request "Retest on-demand" to rapidly validate and close code, configuration and patching fixes.

Clients **save an average of 4 hours per application per month** in time saved with this approach resulting in more rapid mitigation.

40,000 Web Application and API Assessments	+	3,000,000 Network Endpoint Assessments	+	1000 Penetration Tests	=	4 Hours* Saved on average per application per Month
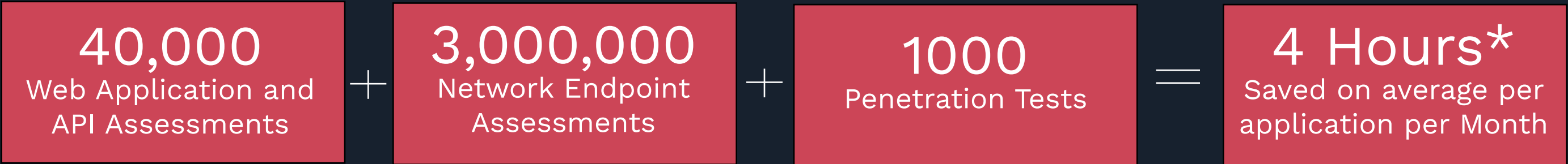
*Based on an average Enterprise customer

"We have observed that the convergence of Attack Surface Management (ASM), Full stack vulnerability management and Penetration Testing as a Service (PTaaS) into a singular platform, has resulted in better visibility and increased response rates to discovered vulnerabilities." – Ciaran Byrne, Head of Operations.

Organisations
Risks & Remediations

"Continuous improvement is better than delayed perfection"
Mark Twain

Risk Density
Risks Across the Full Stack

The following is a breakdown of the risks discovered across the full stack, Web applications and Network/Hosts. It also depicts the risks associated with potential PCI (Payment Card Industry) failures – Not every vulnerability results in a PCI fail. Across the full stack, 20.4% of all discovered vulnerabilities in 2021 were either High or Critical risk weaknesses. 9% of all Web Application vulnerabilities were either High or Critical Weaknesses. In the end, 16.8% of all Network/Host vulnerabilities were either High or Critical Risk.

Full Stack

Vulnerability Risk

PCI Failures: 86.3%

5.5% Critical — 14.9% High — 15.4% Low — 64.1% Medium

6.1% Critical — 16.4% High — 3.6% Low — 72.9% Medium
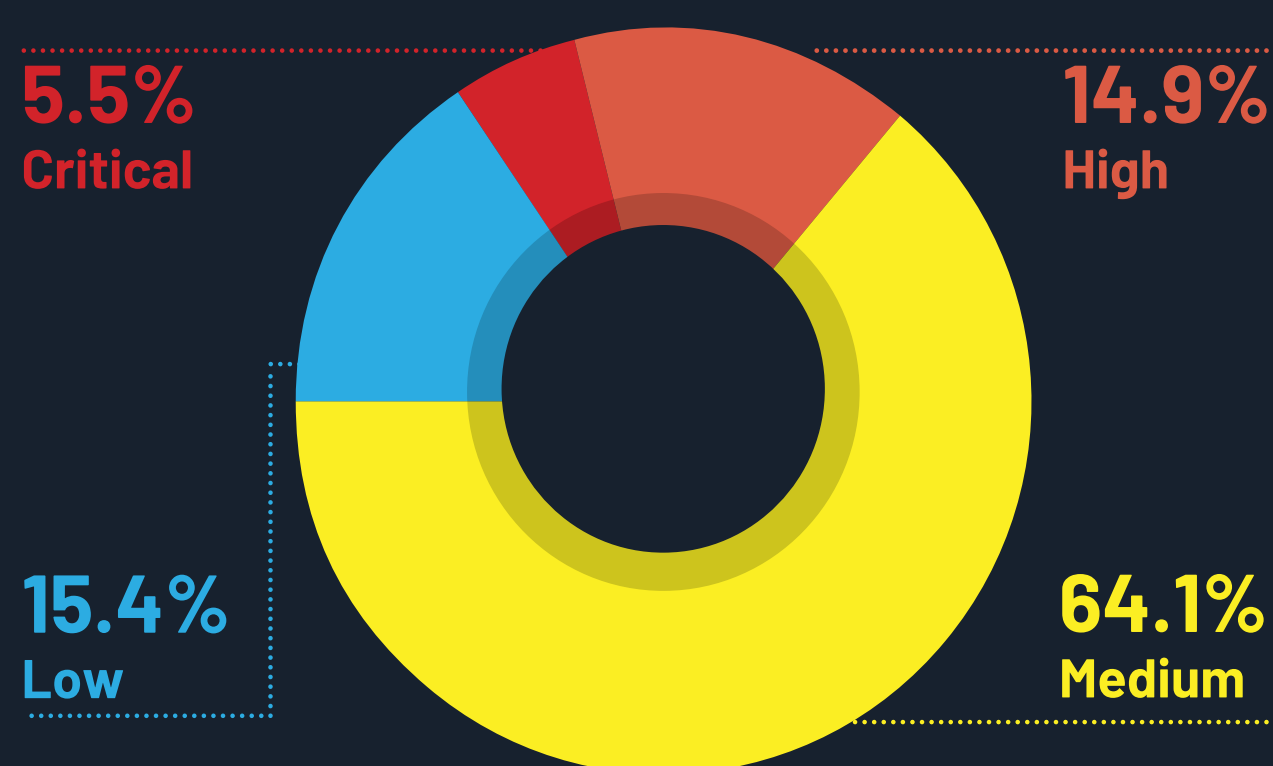
The "Full stack" includes both web application, API & Network vulnerabilities discovered. We don't believe in silos of risk given cyber criminals don't either.
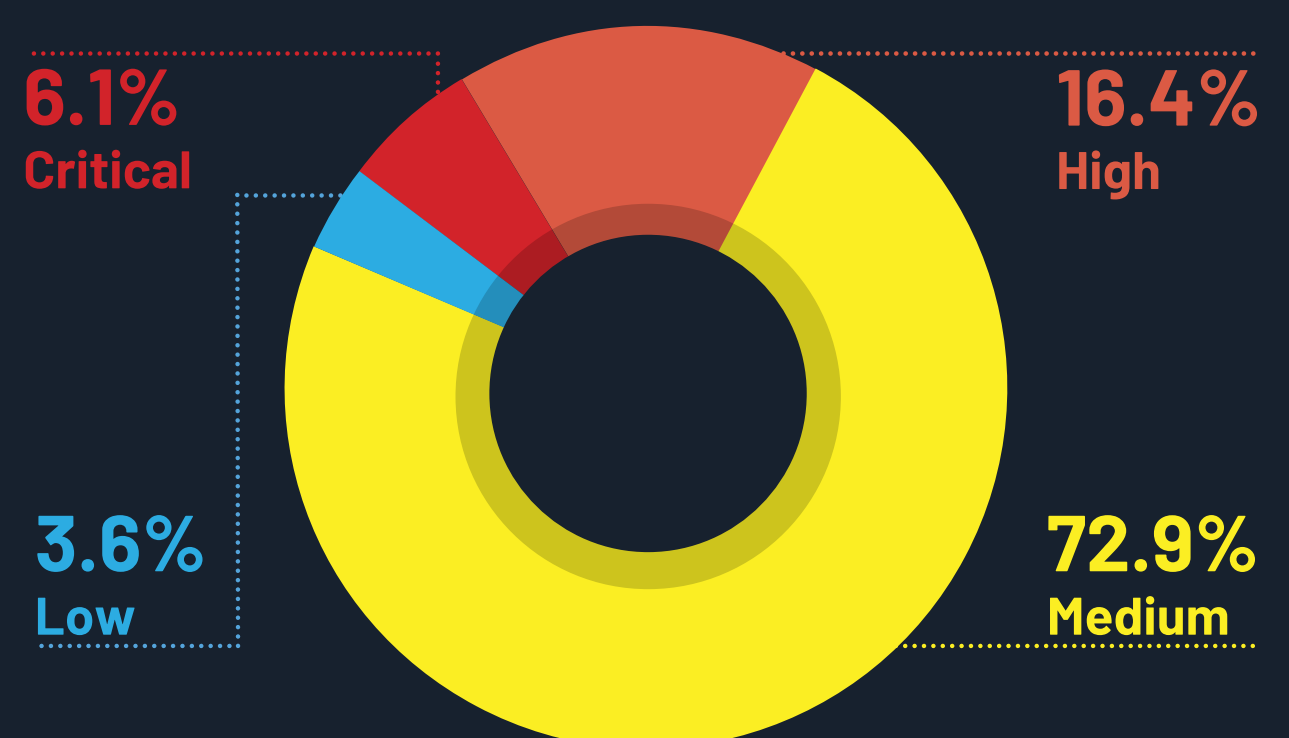
Out of all vulnerabilities found on the full stack, 86.3% resulted in PCI Failures.

How we measure Risk

Definition of a Critical Risk Vulnerability: "Exploitation of the vulnerability likely results in complete compromise of services or data. Exploitation is relatively trivial in the sense that the attacker does not need any special authentication credentials or knowledge about the system to initially exploit a system. Likelihood of exploitation is generally very high"

Definition of a High Risk Vulnerability: "Exploitation of the vulnerability likely results in significant compromise of services or data. Exploitation takes expertise in the sense that the attacker may need to be experienced. Likelihood of exploitation is generally high

Edgescan depicts risk via the typical **"Info/Low/Medium/High"** risk nomenclature (similar to the OWASP Risk Rating Methodology) and also via CVSS Score. CVSS scores may not always be accurate due to not taking the context of a vulnerability into account.

Risk Density
Risks Across the Web Application and Network Layer

Looking at both the Web Application and Network Layer, we can see that web applications have more critical vulnerabilities but also have more lower risk vulnerbilities. On the Network layer, the focus is mainly around both High and Medium risk vulnerabilities which are more common.

Web Application

Vulnerability Risk

4.6% Critical

4.4% High

53.7% Low

37.4% Medium
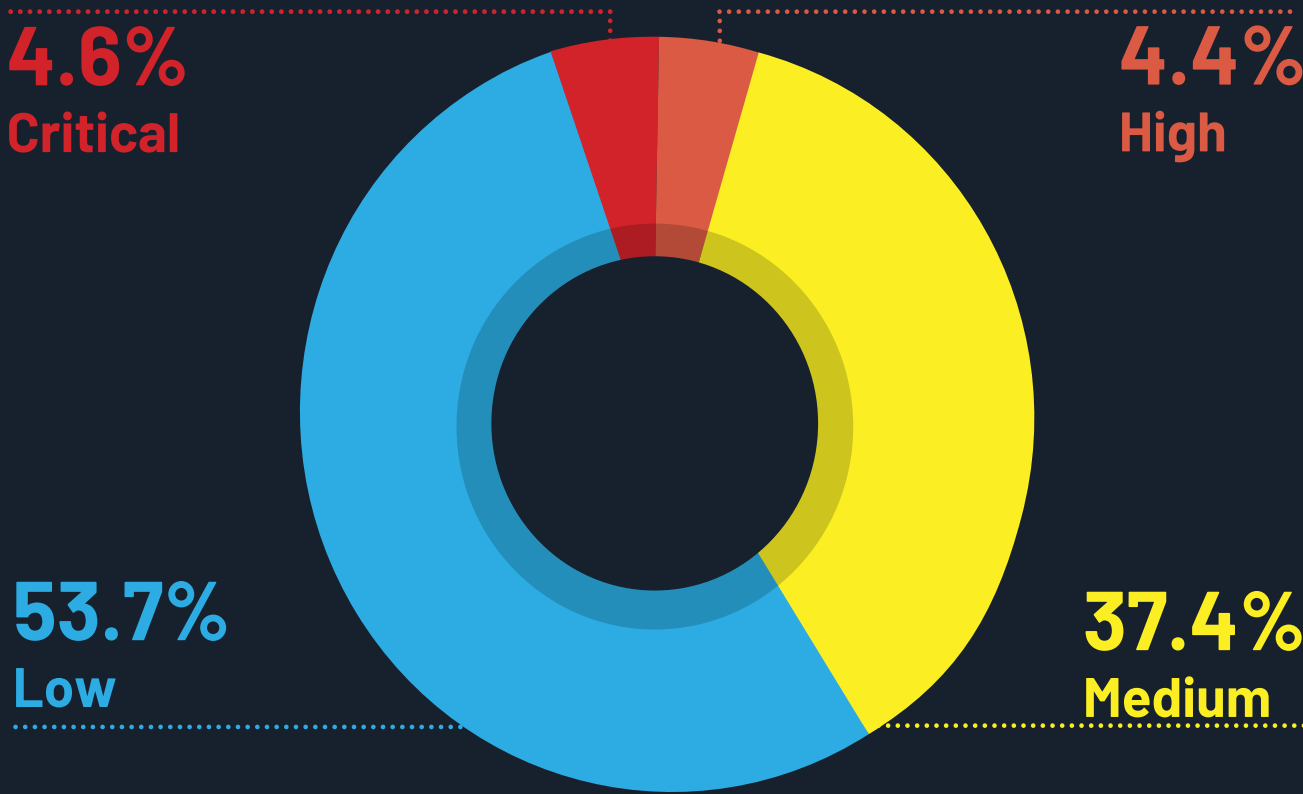
Web Application Layer risks cover Web applications, API's, Mobile apps and systems developed by bespoke development teams. The risks are primarily due to coding bugs. They generally have a CWE but not a CVE as the systems are not commodity items.

PCI Failures: 59%

8% Critical

7% High

85% Low

62% Medium

Out of all vulnerabilities found on the Web Application layer, 59% resulted in PCI Failures.

Network

Vulnerability Risk

4.3% Critical

12.5% High

8% Low

52% Medium
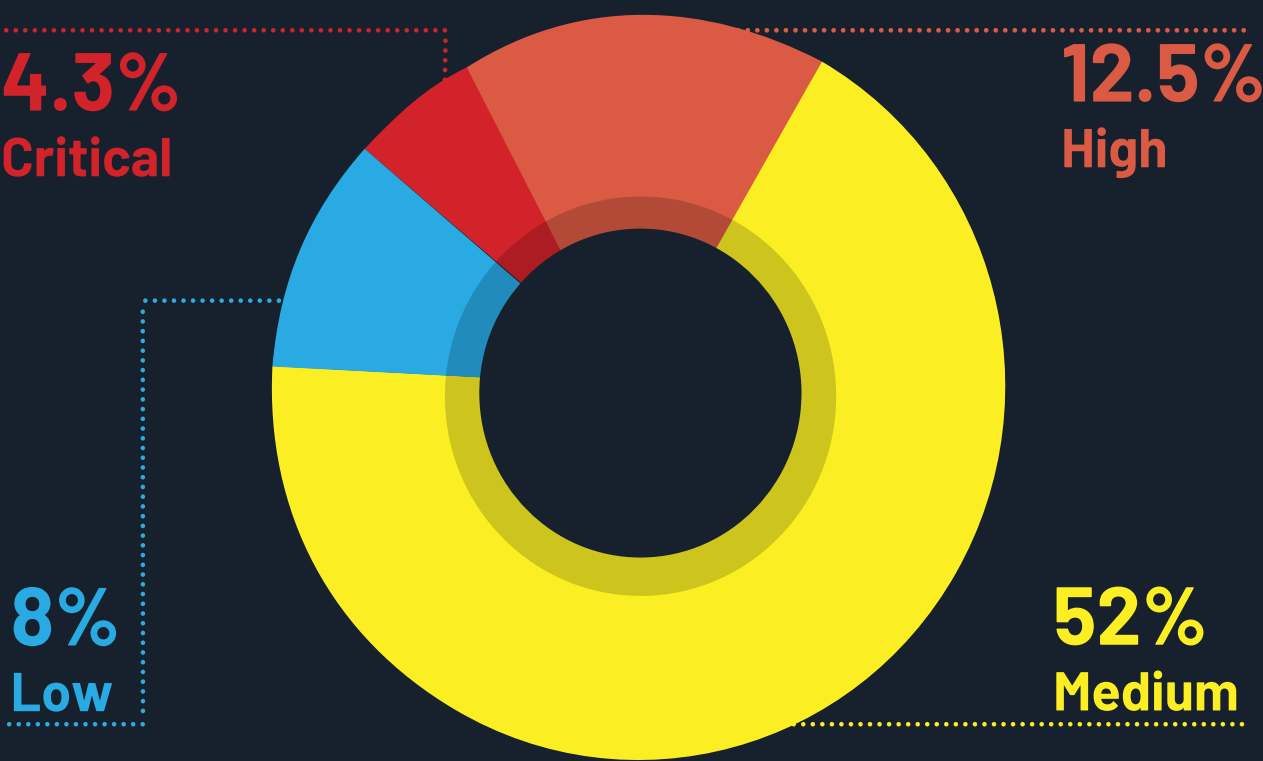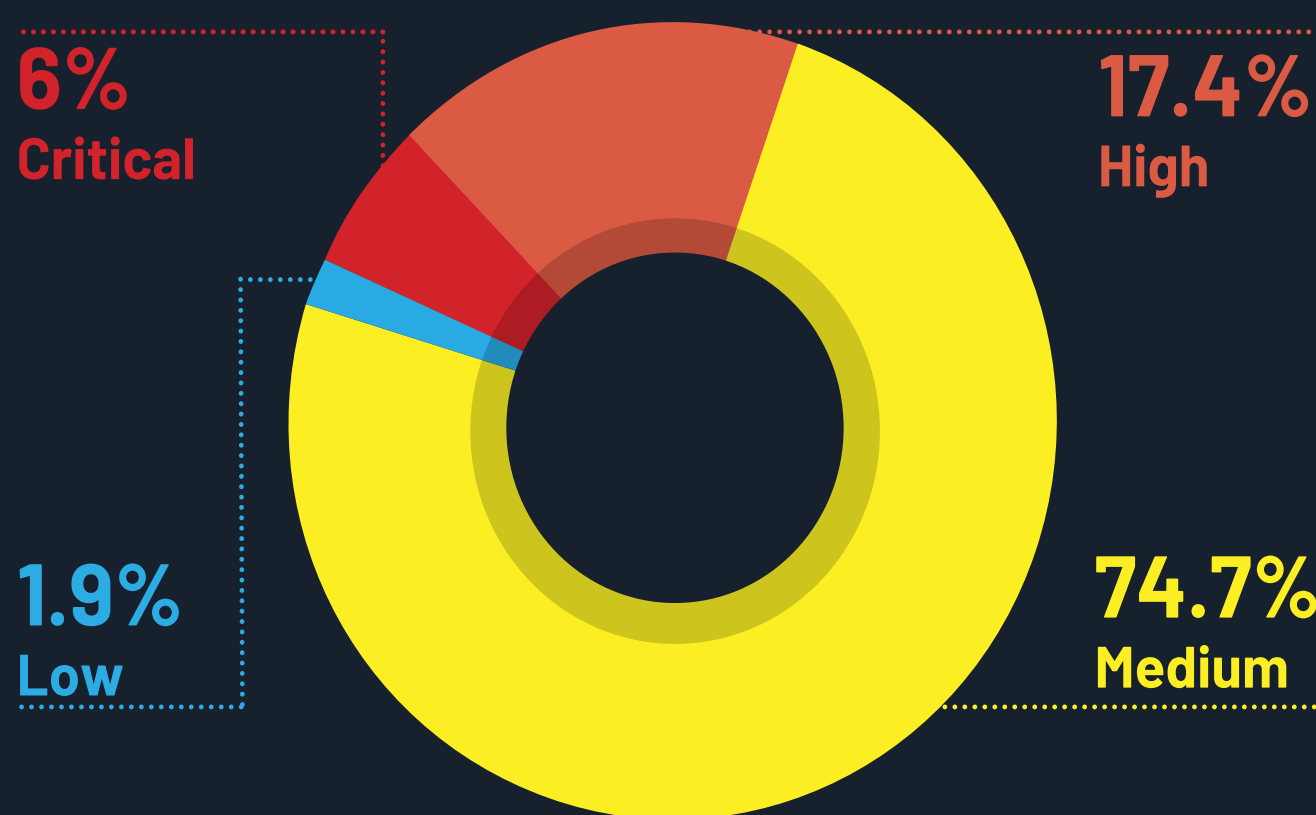
When we talk about "Network" risks we really mean device, servers and systems which require patching or confirguration. Most issues raised have an associated CVE or known configuration fix and are not "developer" code related issues (even though ultimately everything is just software!).

PCI Failures: 68%

6% Critical

17.4% High

1.9% Low

74.7% Medium

Out of all vulnerabilities found on the Network layer, 68% resulted in PCI Failures.

Mean Time to Remediate (MTTR) Vulnerabilities
Time it takes to fix Vulnerabilities across the Full Stack

The measurements below include remediation and verification that the fixes are robust (including reassessments & retesting). Mean time to Remediate (i.e. acode fix) for a critical risk on the web application/API layer is 47.6 days. Mean time to Remediate (i.e. patch or reconfigure) a device/host layer critical risk is 61.4 days. The quickest remediation on a vulnerability that was found was 0.5 days.

Full Stack

					Average MTTR
51.4 days	63.2 days	59.8 days	56.2 days	60 days	**57.5 days**
Info	Low Risk	Medium	High Risk	Critical	
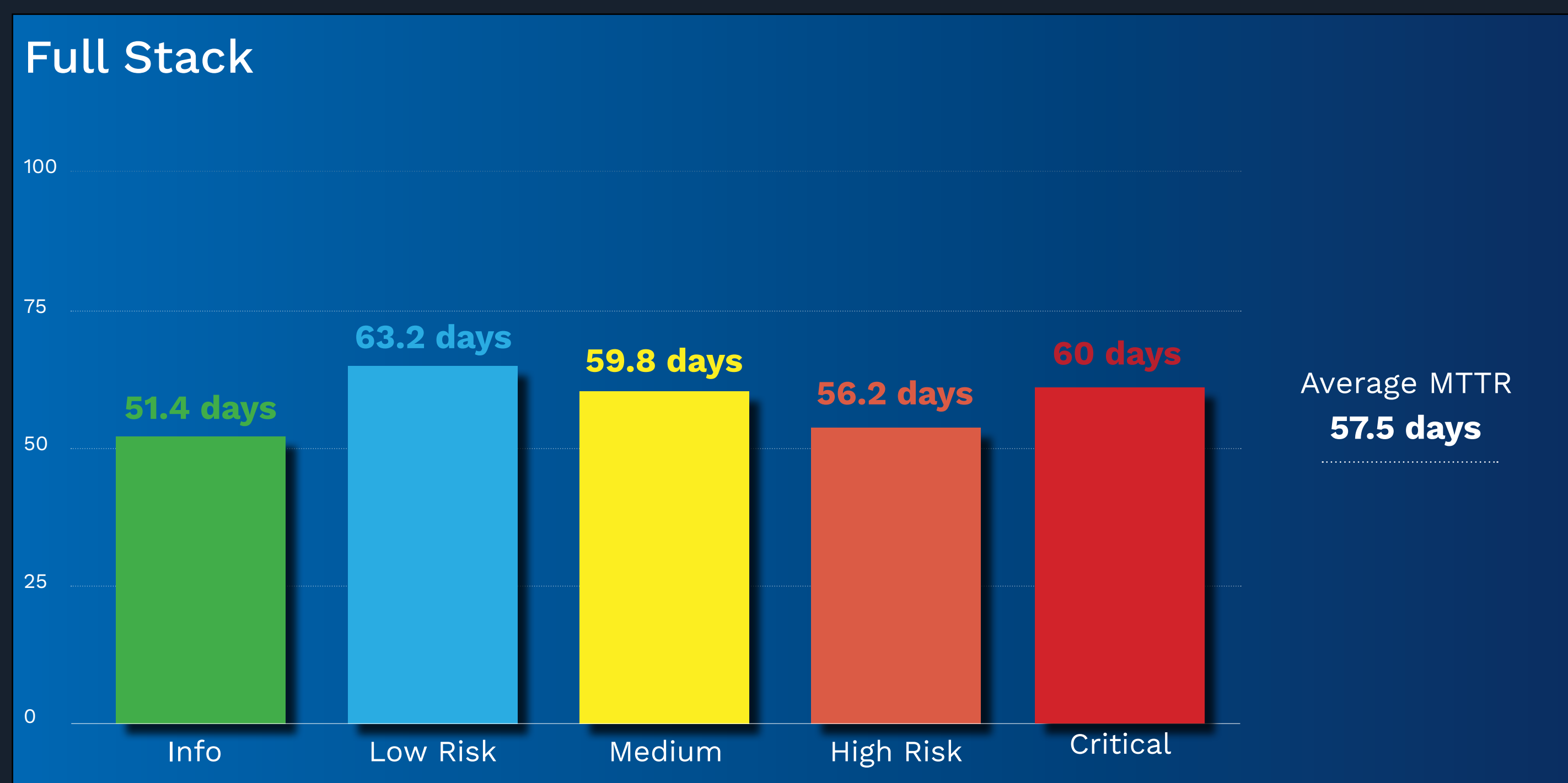
Informational risks are commonly risk accepted resulting in an MTTR of **51.4 days.** As an industry we need to improve the MTTR for high and critical risks.

Mean Time to Remediate (MTTR) Vulnerabilities
Looking at Web App/API & Device/Host Layer

Looking now to both the Web App/API & Device/Host layers, we can see a big difference on the web/app layer compared to the Device/Host layer. In particular that the length of time to remediate on the Web App/API layer is 63.8 days compared to the average of 57 days on the Device/Host layer.

Web App/API Layer

Risk	Days
Info	79.4 days
Low Risk	58.3 days
Medium	68.4 days
High Risk	61.4 days
Critical Risk	47.6 days

Average MTTR
63.8 days
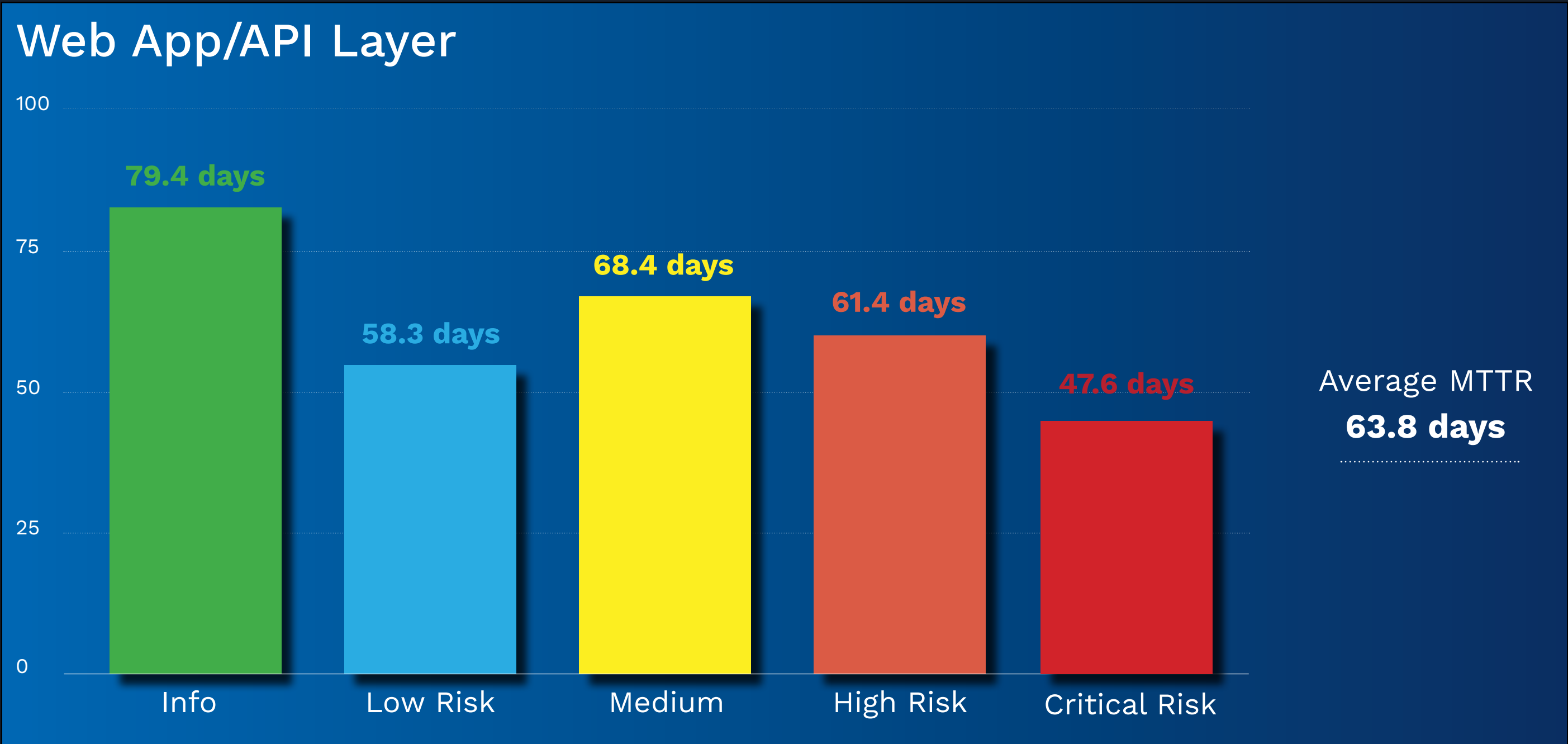
The average time to fix a Critical Risk issue, comes in at only **47.6 days**, which shows that organisations are focusing on prioritising fixing vulnerabilities in the application layer. This is overshadowed however by both the Medium and High Risks which come in at **68.4 Days** and **61.4 Days** respectfully.

Device/Host Layer

Risk	Days
Info	50.7 days
Low Risk	65.4 days
Medium	59.4 days
High Risk	56 days
Critical Risk	61.4 days

Average MTTR
57 days
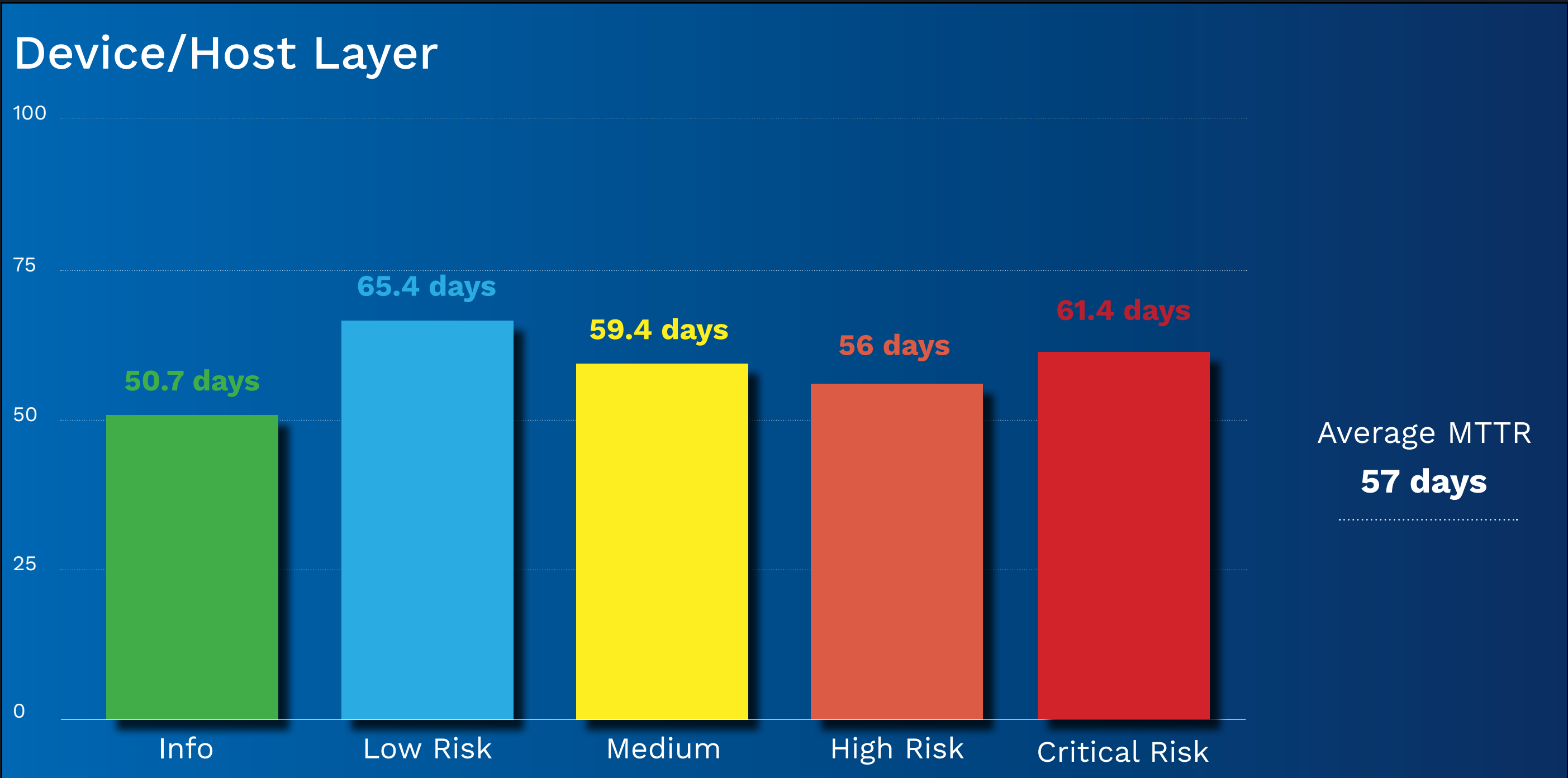
The Device/Host layer has the lowest average MTTR of **57 days,** but it also has the highest MTTR for Critical risks of **61.4 Days**.

MTTR by Industry
Industry Mean Time to Remediate Vulnerabilities

Public Administration (NAICS* 92)
92 days
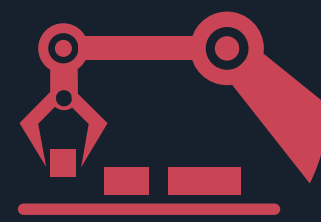
Manufacturing (NAICS 31-33)
78 days
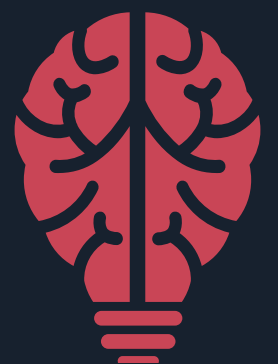
Professional, Scientific & Technical Services (NAICS 54)
68 days

Accomindation & Food Services (NAICS 72)
64 days
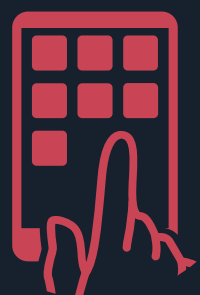
Information (NAICS 51)
61 days
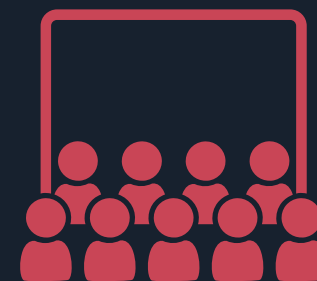
Arts, Entertainment and Recreation (NAICS 71)
58 days

Education Services (NAICS 61)
51 days

Financial & Insurance (NAICS 52)
48 days

Retail (NAICS 44-45)
47 days

Healthcare (NAICS 62)
44 days

Through the Edgescan platform, we examined ten different industries to report on their average rates of MTTR within that industry. We can see that the shortest MTTR can be seen in Healthcare (NAICS 62) while the longest is Public Administration (NAICS 92). The second longest MTTR is seen to be manufacturing (NAICS 31-33) with an average of 78 days. This means that both Public Administration and Manufacturing take approximately double the length of time compared to the Healthcare industry, to fix vulnerabilities.

*The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. - https://www.naics.com/

MTTR by Region
Region Mean Time to Remediate Vulnerabilities
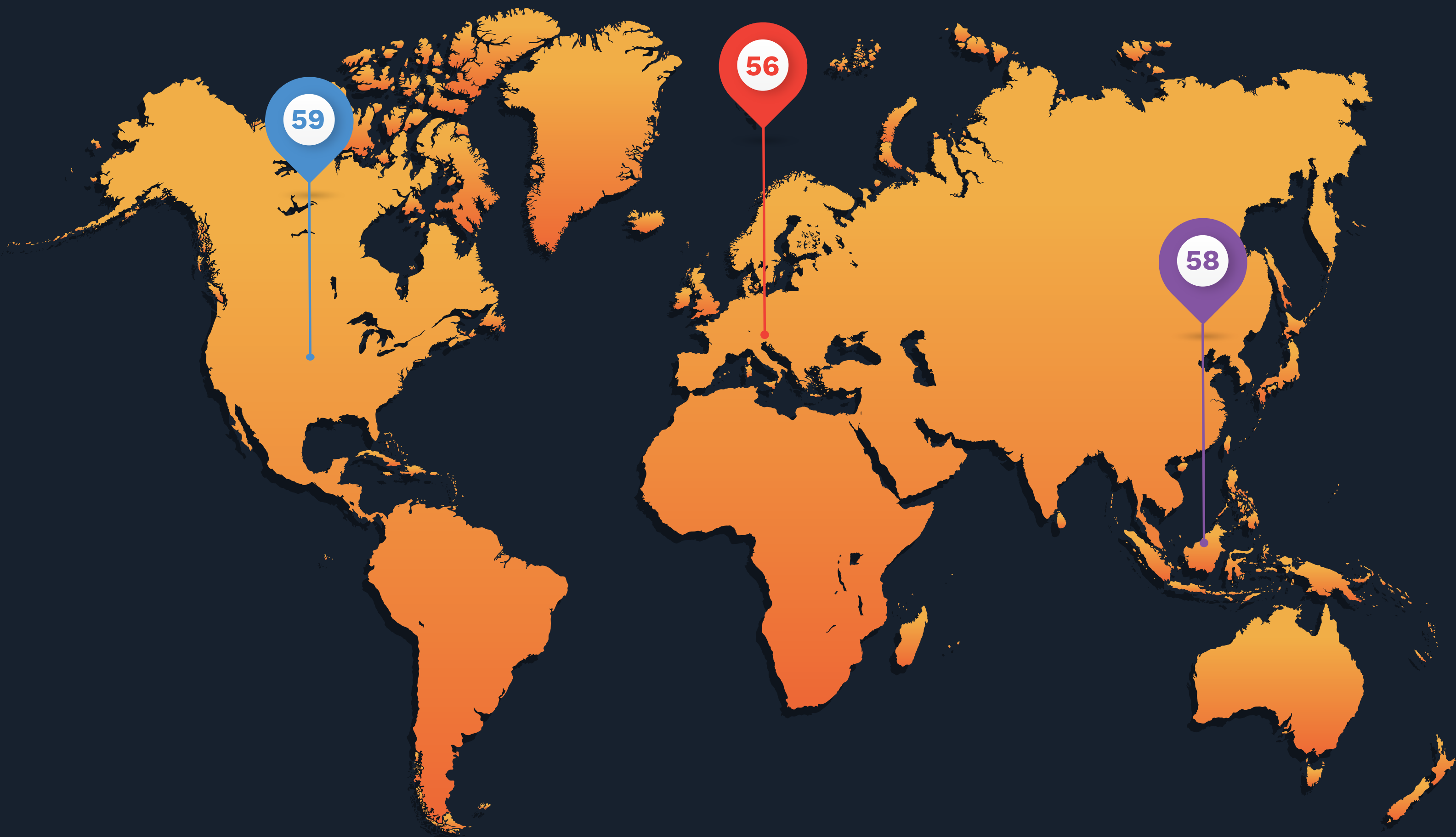
North America
59 Days

Europe (EMEA)
56 Days

Asia-Pacific
58 Days

As we can see from the above figures, the North America region has the highest MTTR for companies with an average of **59 days** while Europe (EMEA) has an average of **56 days**.

This gives us a global MTTR average of **57.5 Days** for companies to fix their vulnerabilities.

MTTR Based on Company Size
Company Mean Time to Remediate Vulnerabilities

We believe the size of an organization does not impact speed of security.

It appears that company size generally has little or no impact in relation to the time it takes to fix vulnerabilities, similar to the 2021 report. We measured time-to-fix for critical risk vulnerabilities for a number of company sizes and the average is much the same across these organizations.

IT and Information Security generally does not grow linearly with the size of a business.

Larger organizations have more to secure, more data and systems, but generally not relatively more security staff!

Staff Count: 11-100

68 Days

Staff Count: 101-1000

61 Days

Staff Count: 1001-10000

75 Days

Staff Count: 10000+

84 Days
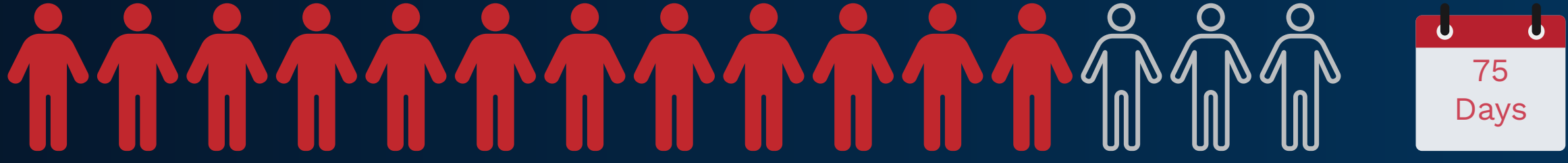
Vulnerabilities
Growing threats to orgs

"If you always do what you've always done, you'll always get what you've always got"

Henry Ford

Vulnerability Age
Full Stack

One common theme that we find each year, is the prevalence of 'older' known vulnerabilities that are found. This section highlights the age of known vulnerabilities that were found in a system during 2021. All of these issues already have patches available to address them. We can see 57% of such issues could be considered old – issues that range from being first discovered back in 1999, right up to recent years!

% of all discovered CVE's
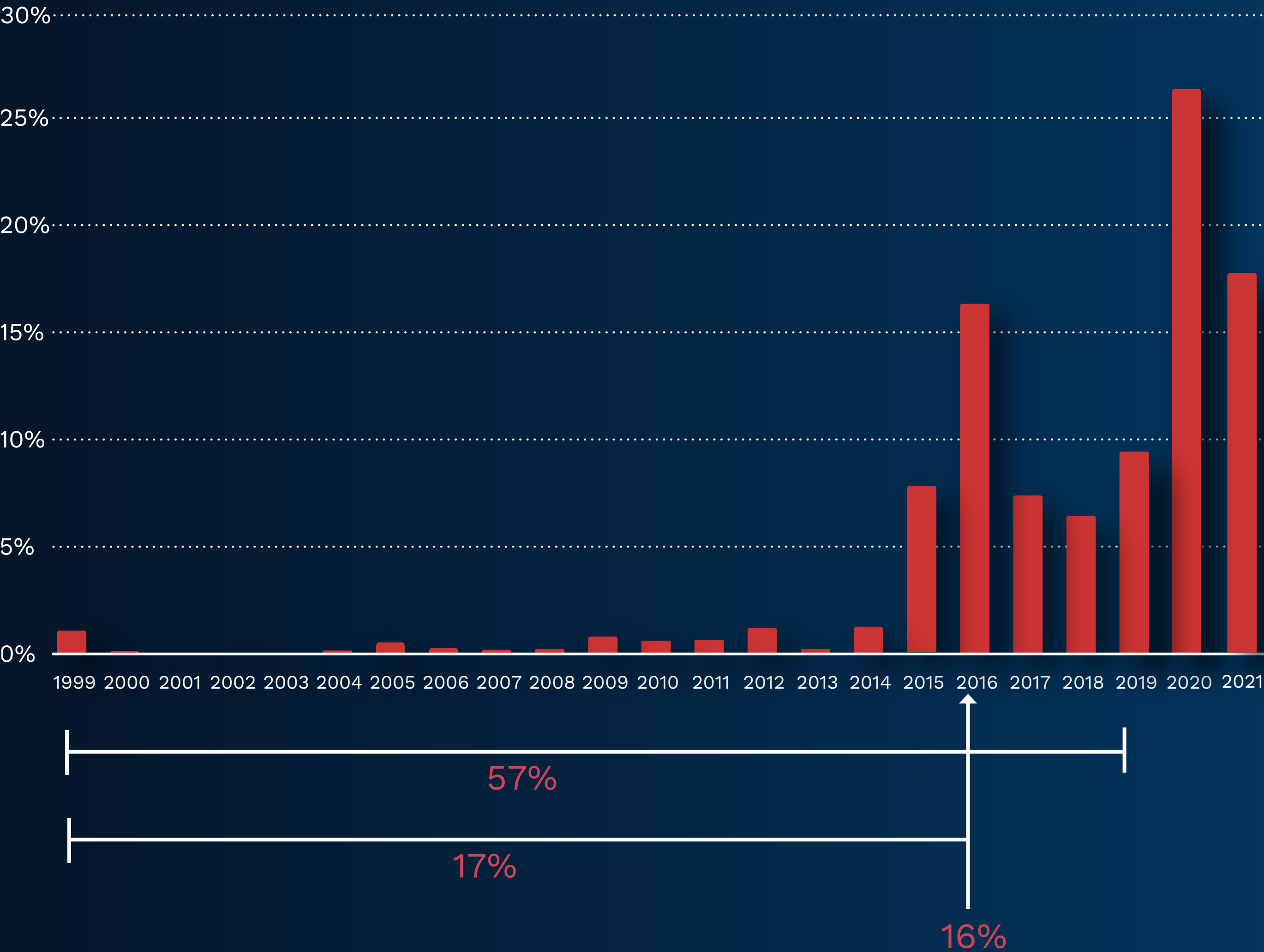
Over 16% of discovered vulnerabilities are from 2016. Circa 17% of vulnerabilities are older than 5 years old with 57% of discovered vulnerabilities are more than 2 years old. We can see that most common CVE in 2021: **CVE-2015-4000** at **8.25%** is **"Logjam"** while the most common CWE in 2021: **CWE-310** at **21.31%** is **"Cryptographic Issues"**
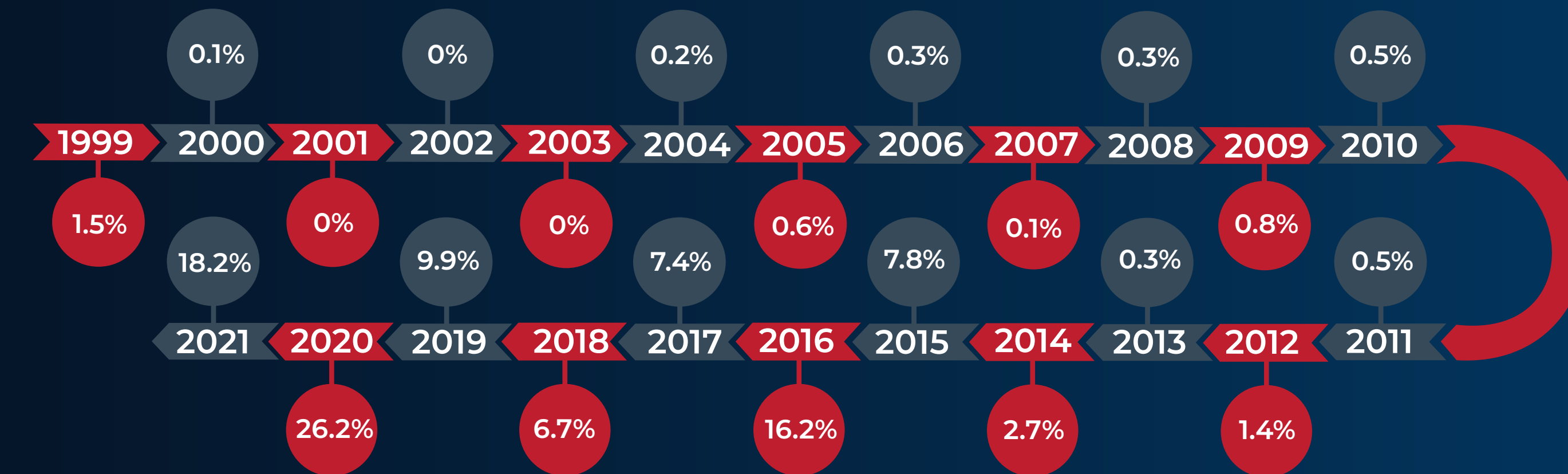
Most Common Critical & High Risk API Vulnerabilities

This examines the most common high and critical risk API issues discovered in 2021 – those with a CVSS score of 7.0 and above. The percentage stated is the rate of occurrence compared to all critical risk vulnerabilities discovered in 2021.

Edgescan validates vulnerabilities based on context of the unique issue and does not always tally with CVSS scoring.

Many API vulnerabilities are similar to Web application vulnerabilities but the devil is in the detail; It appears to be more common to have issues regarding Rate Limiting requests, Direct object access (IDOR) and Authorization issues.

When developing API's it's assumed the "client" is not a person directly but another piece of software (e.g. website, app etc). This may give rise to a false sense of security because users do not directly interact with the API and the exposed features are hidden.

9.9% Broken Function

19.3% Injection Attacks

10.6% Mass assignment

17% Resource Limiting

12.9% Information disclosure

15.0% BOLA

15.3% Broken Authentication
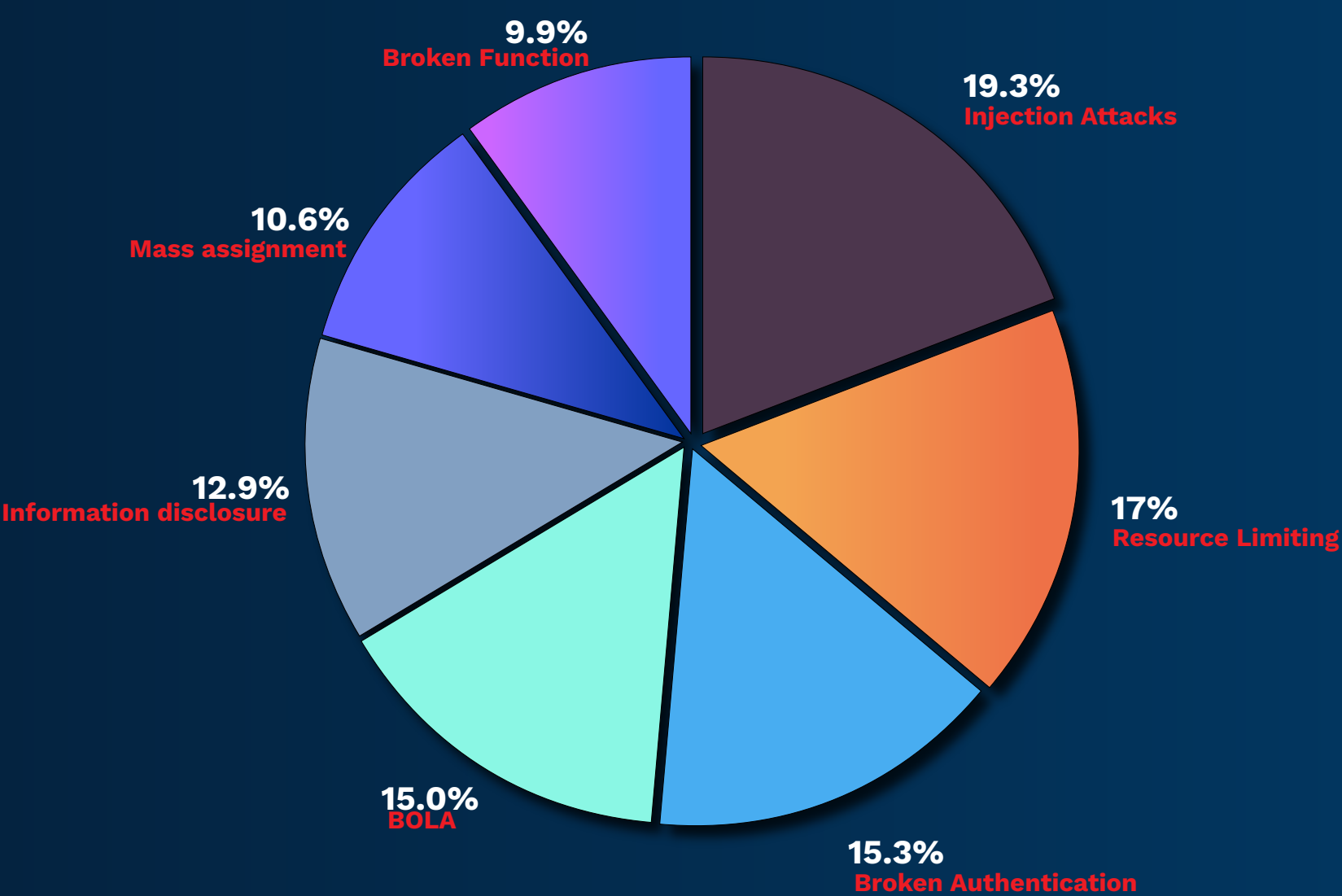
Name	Vulnerability References & Notes	CWE/OWASP	% of Discovered Vulnerabilities
Injection Attacks	SQL, NoSQL, LDAP, OS Injections, Code Injections, ORM based vulnerabilities, Parsers such as XMLTraversal based attacks.	CWE-79, CWE-725, API8:2019	19.3%
Lack of resources and rate limiting	The API does not restrict the number or frequency of requests from a particular API client. This can be abused to make thousands of API calls per second, or request hundred or thousands of data records at once, resulting in a Denial of Service condition. This weakness also enables arbitrary scraping of other parties API's and violate fair usage agreements.	CWE-770 / API4:2019	17.0%
Broken authentication	Weak authentication allowing compromise of authentication tokens or exploitation of common implementation flaws to assume other users identity or bypass authentication completely. Compromising a system's ability to identify the client/user, compromises API security overall.	API2:2019/CWE-287	15.3%
Broken object level authorization (BOLA)	AKA Insecure Direct Object Reference (IDOR). As its name implies, the ability to directly access resources without privileges or authorization.	CWE-639 / API1:2019	15.0%
Excessive data exposure (Information disclosure)	Exposure of all object properties of an API endpoint without consideration for use-case or requirement. Results in the reliance on API clients to perform the data filtering before displaying it to the user.	CWE-22, CWE-23, CWE-200,CWE-269, CWE-250 / API3:2019	12.9%
Mass assignment	API does not control which object attributes can be modified providing the potential for access to opaque data, outcomes or functions. This can be used to create new parameters that were never intended which in turn creates or overwrites new variable or objects in program code.	CWE-915 / API6:2019	10.6%
Broken function level authorization	Admin or sensitive functions exposed in error to unauthorized clients resulting in data disclosure or privileged execution for unauthorized API clients. In effect resulting in an overly large attack surface and unintended exposure risk.	CWE-285 / API5:2019	9.9%

Most Common Critical and High Risk Vulnerabilities
Full Stack View

Pie chart labels:

- **SAP Gateway** 0.08%
- **SAP Message Server** 0.10%
- **SMB** 0.10%
- **OpenBSD OpenSSH** 0.11%
- **MS-NRPC Zerlogon Vuln** 0.11%
- **OS EOL** 0.13%
- **Windows 7/Server EOL** 0.14%
- **jQuery EOL** 0.19%
- **PrintNightmare** 0.19%
- **ChangeCipherSpec** 0.21%
- **SAP internet Graphics** 0.21%
- **SMB Login** 0.23%
- **Dropbear** 0.23%
- **Windows IEpress** 0.24%
- **Microsoft OneDrive - July 2020** 0.25%
- **Microsoft OneDrive - Sep 2020** 0.25%
- **Deprecated SSH-1** 0.31%
- **OpenStage SIP** 0.36%
- **SNMP Agent Default** 0.79%
- **3.09% SSL 64-bit block size cipher**

Vulnerability Name	Risk	Layer (Web/Network)	% of Discovered Vulnerabilities
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	High	Network	3.09%
SNMP Agent Default Community Names	High	Network	0.79%
OpenStage SIP Webinterface Default Password	High	Network	0.36%
Deprecated SSH-1 Protocol Detection	High	Network	0.31%
Microsoft OneDrive Multiple Vulnerabilities - Sep 2020	High	Network	0.25%
Microsoft OneDrive Privilege Escalation Vulnerability - July 2020	High	Network	0.25%
Windows IExpress Untrusted Search Path Vulnerability	High	Network	0.24%
Dropbear < 2020.79 Mishandling Filenames Vulnerability	High	Network	0.23%
Microsoft Windows Unquoted Path Vulnerability (SMB Login)	High	Network	0.23%
SAP Internet Graphics Server Multiple XXE Vulnerabilities	High	Network	0.21%
OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	High	Network	0.21%
Microsoft Windows Print Spooler RCE Vulnerability (KB5005010, PrintNightmare)	High	Network	0.19%
jQuery End of Life (EOL) Detection	Critical	Network	0.19%
Microsoft Windows 7 / Server 2008 End Of Life Detection	Critical	Network	0.14%
OS End Of Life Detection	Critical	Network	0.13%
Microsoft Windows MS-NRPC Zerologon Vulnerability (CVE-2020-1472) - Active Check	Critical	Network	0.11%
OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities	High	Network	0.11%
Server Message Block (SMB) Protocol Version 1 Enabled	High	Network	0.10%
SAP Message Server acl_info Configuration Vulnerability	Critical	Network	0.10%
SAP Gateway ACL Misconfiguration Vulnerability	Critical	Network	0.08%

Most Common Critical Risk Vulnerabilities
Web Applications

The Application Security Critical Risk Top 10 depicts the most common critical risk issues discovered by Edgescan in 2021.

SQL Injection is still the main contender which is interesting to note as we can easily develop code which is not vulnerable to such attacks.

Something which is overlooked quite frequently is malicious file uploads. This can give rise to ransomware, malware and internal network breach pivot points for attackers.

Executable code injection is commonly used by exploit kits to get access to data and the source code of a system. The root cause is due to a system interpreting data as code and executing it.

Authorization issues cover privilege escalation or access to restricted functionality which would result in a data breach.

Excutable Code Injection 2.1%
File Path Traversal 2.5%
OS Command Injection 3.9%
Authorisation Issue 7.0%
4.6%
Server-Side Request Forgery
5.3%
Server-Side Template Injection
7.0%
Malicious File Upload
8.1%
XXE
33.0%
SQL Injection
26.7%
Cross Site Scripting
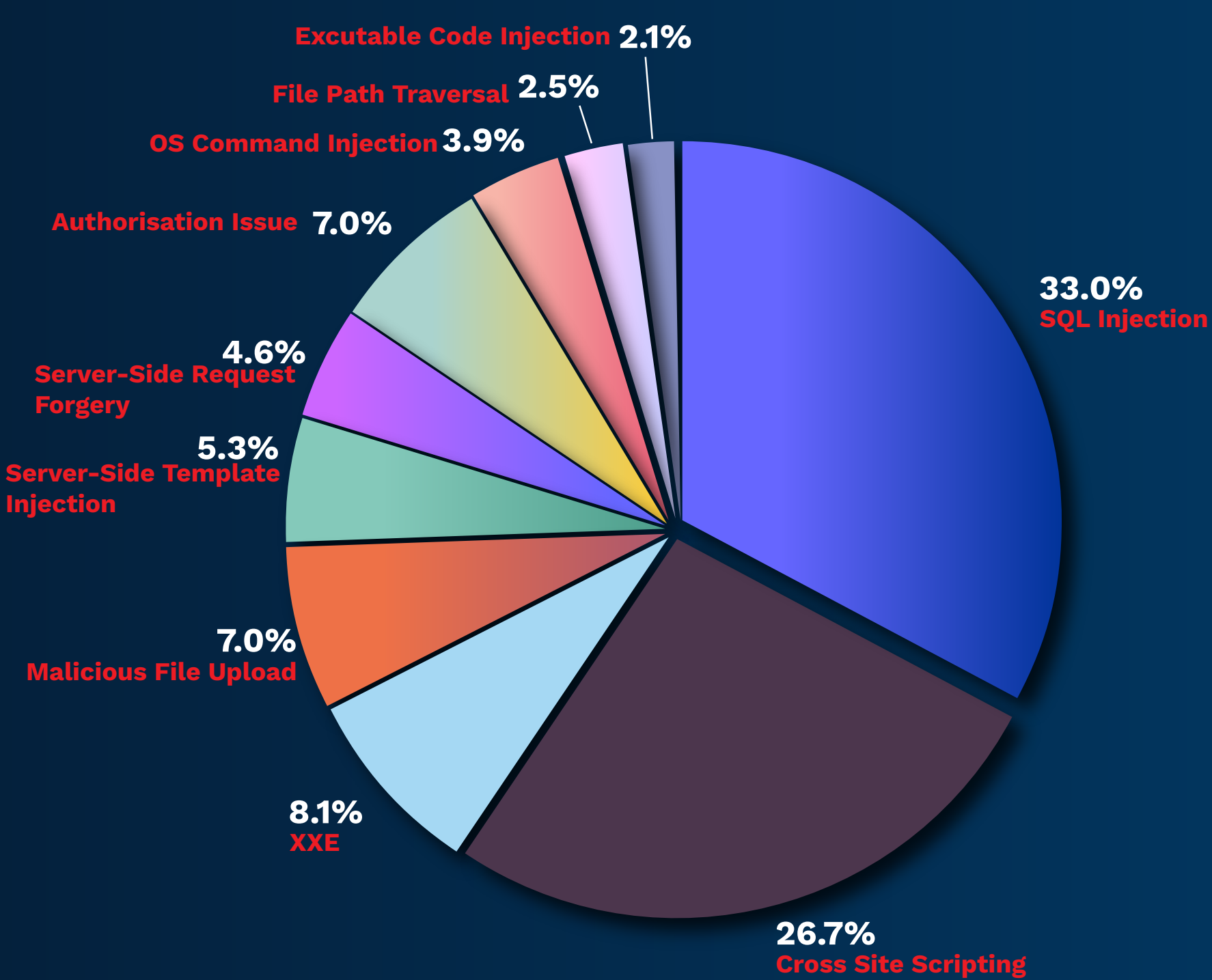
Name	Vulnerability References & Notes	CWE	% of discovered Vulnerabilities
SQL Injection	Data extraction, manipulation and database access via injection attack.	CWE-89	33.0%
Cross Site Scripting	(Reflected & Stored) The XSS risk is based on context of where the vulnerability was discovered.	CWE-79, CWE-725	26.7%
XML external entity injection (XXE)	XML injection which resulted in application compromise or forcing the application to perform functions not intended.	CWE-611, CWE-1030	8.1%
Malicious File Upload	Potential for malware, Trojan, DoS (Large) upload via upload functionality.	CWE-434	7.0%
Server-Side Request Forgery	Induce the backend application to make HTTP requests to an arbitrary domain of the attacker's choosing.	CWE-918	5.3%
Server-side template injection	Injection of malicious input into a template to execute commands on the backend system	CWE-1336	4.6%
Authorisation Issue	Bypassing controls to access data and functions without authorization. Horizontal and vertical privilege escalation is included in this category	CWE-285	7.0%
OS Command Injection	Ability to execute arbitrary system commands on the attacked party's host operating system (OS)	CWE-78	3.9%
File path traversal / Information disclosure	Vulnerability that allows one to read arbitrary files on the server and disclose potentially sensitive information.	CWE-22, CWE-23, CWE-200	2.5%
Executable Code injection	Malicious injection or introduction of code into an application which can be executed in the context of the system being breached.	CWE-94,CWE-96, CWE-78	2.1%

Most Common High Risk Vulnerabilities
Web Applications

SSRF 1.8%
XXE 2.3%
Executable Code Injection 2.8%
Deserialization Attacks 3.2%
Malicious File Upload 3.2%
Direct Object Access 5.1%
Authorisation Issue 6.0%
6.9% File Path Traversal
22.1% Broken Authentication
49.8% Cross-Site Scripting - XSS (Reflected)
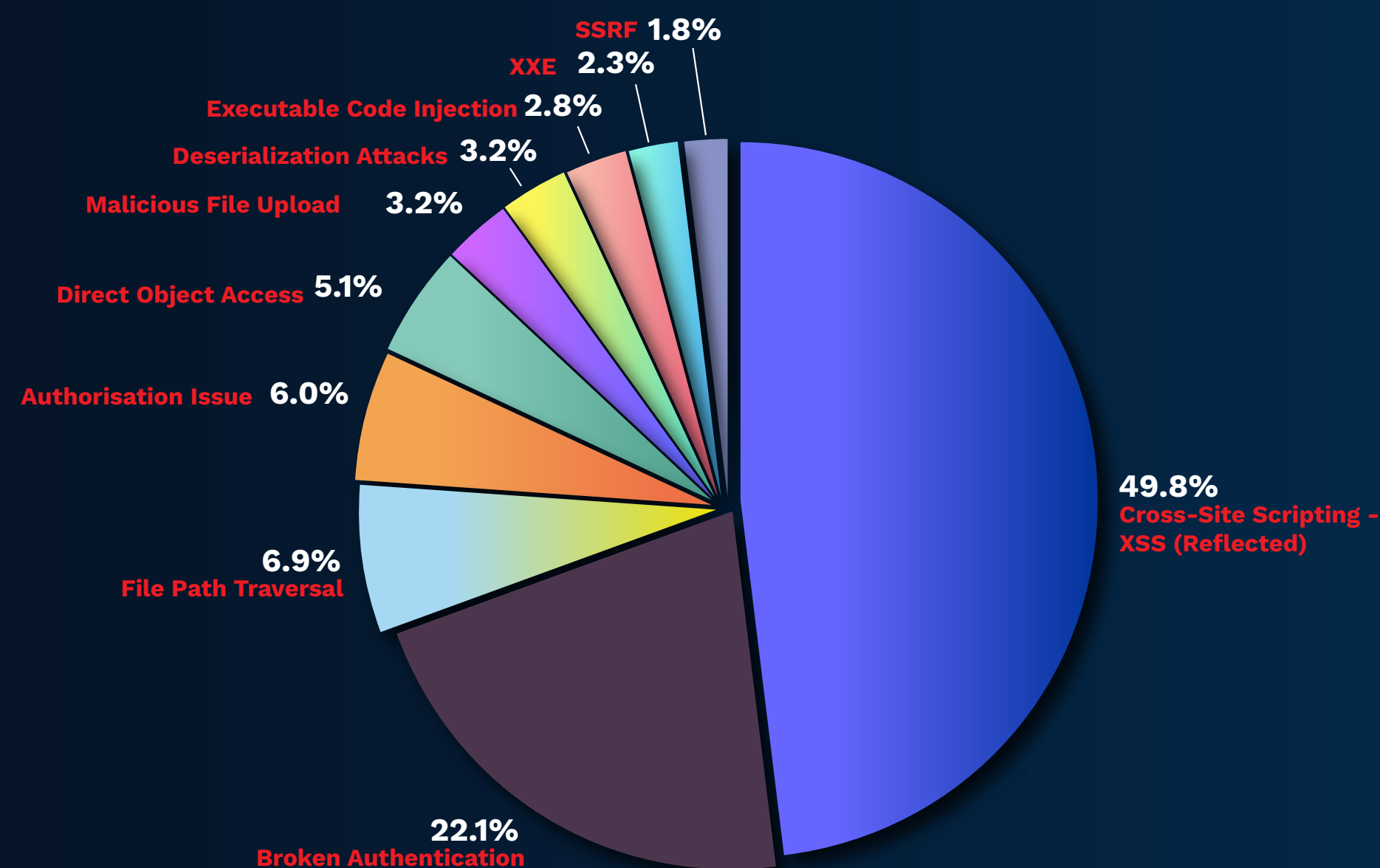
As in previous years, Cross-Site Scripting (XSS) (49.8%) is still king of the hill for High risk issues. This can be used for phishing attacks, redirection to malicious sites, malware proliferation, but to name a few. Think of XSS as a payload delivery vulnerability.

Broken Authentication (22.1%) is high on the list for 2021. This relates to misconfiguration, broken logic, username enumeration or insecure authentication functionality.

XML external entity injection (2.3%) (also known as XXE) is lower than last year (4.7%). It is a vulnerability that allows an attacker to manipulate an applications processing of XML data. By virtue of injecting specific payloads, it can allow an attacker to do things such as gain unauthorized access to files on the application server filesystem or interact with downstream back-end/external systems that the application itself can access. In the case of these high risks, the XXE in question would result in system compromise and data exfiltration.

Name	Vulnerability References & Notes	CWE	% of discovered Vulnerabilities
Cross-Site Scripting - XSS (reflected)	Context of where the XSS was discovered deemed the risk to be high. In many cases XSS is a medium risk due to evolving built-in web browser controls.	CWE-79, CWE-725	49.8%
Broken Authentication/Poor Session Management, Brute Forcing Possible	Broken CAPTCHA, Bypass, Insecure Authentication, Weak Password, Username Enumeration, Unencrypted Authentication. Lack of MFA, No Lockout controls or alerting.	CWE-287	22.1%
File path traversal/Information disclosure/Source Code Disclosure	Vulnerability that allows one to read arbitrary files on the server and disclose potentially sensitive information.	CWE-22, CWE-23, CWE-200, CWE-269, CWE-250	6.9%
Authorisation Issue - Privilege Escalation	Business logic and authorization access escalation.	CWE-285	6.0%
File path traversal/Direct Object Access	Direct access to assets without requirement for authorization or authentication	CWE-22, CWE-23, CWE-200	5.1%
Malicious File Upload	Potential for malware, Trojan, DoS (Large) upload via upload functionality.	CWE-434	3.2%
Deserialization Attacks	Insecure deserialization is when user-controllable data is deserialized by a website. Results in manipulation of serialized objects in order to pass harmful data into the application.	CWE-502	3.2%
Executable Code injection	Malicious injection or introduction of code into an application which can be executed in the context the system being breached	CWE-94,CWE-96, CWE-78	2.8%
XML External Entity Injection (XXE)	XML injection which resulted in application compromise or forcing the application to perform functions not intended.	CWE-611, CWE-1030	2.3%
Server-Side Request Forgery (SSRF)	Induce the backend application to make HTTP requests to an arbitrary domain of the attackers choosing.	CWE-918	1.8%

CVE & CWE
The Evolving Landscape

"Weak Crypto is king of the hill."

Eoin Keary

Most Common CVE discovered in 2021

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program.

The CVE age-landscape is always an interesting one each year. This list represents the most common known vulnerabilities found in 2021 and include one high risk and 3 medium risk issues. The most concerning trend here, is the actual age of these issues – most were first reported six or seven years ago and one right back to 2003! Also, it is no surprise that the majority of these issues are related to some kind of crypto weakness.

CVE-2015-4000: TLS man-in-the-middle. An Attacker can conduct a cipher-downgrade, aka the "Logjam".

CVE-2015-2808: The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks, aka the "Bar Mitzvah" issue.

CVE-2013-2566: The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

CVE-2016-2183: The DES and Triple DES ciphers, as used in the TLS, SSH, and IPsec protocols and other protocols and products, have a weakness which makes it easier for remote attackers to obtain cleartext data via a birthday attack, aka a "Sweet32" attack.

CVE-2003-0661: The NetBT Name Service (NBNS) for NetBIOS in Windows NT 4.0, 2000, XP, and Server 2003 may include random memory in a response to a NBNS query, which could allow remote attackers to obtain sensitive information.

CVE-2014-3566: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, has a weakness that makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
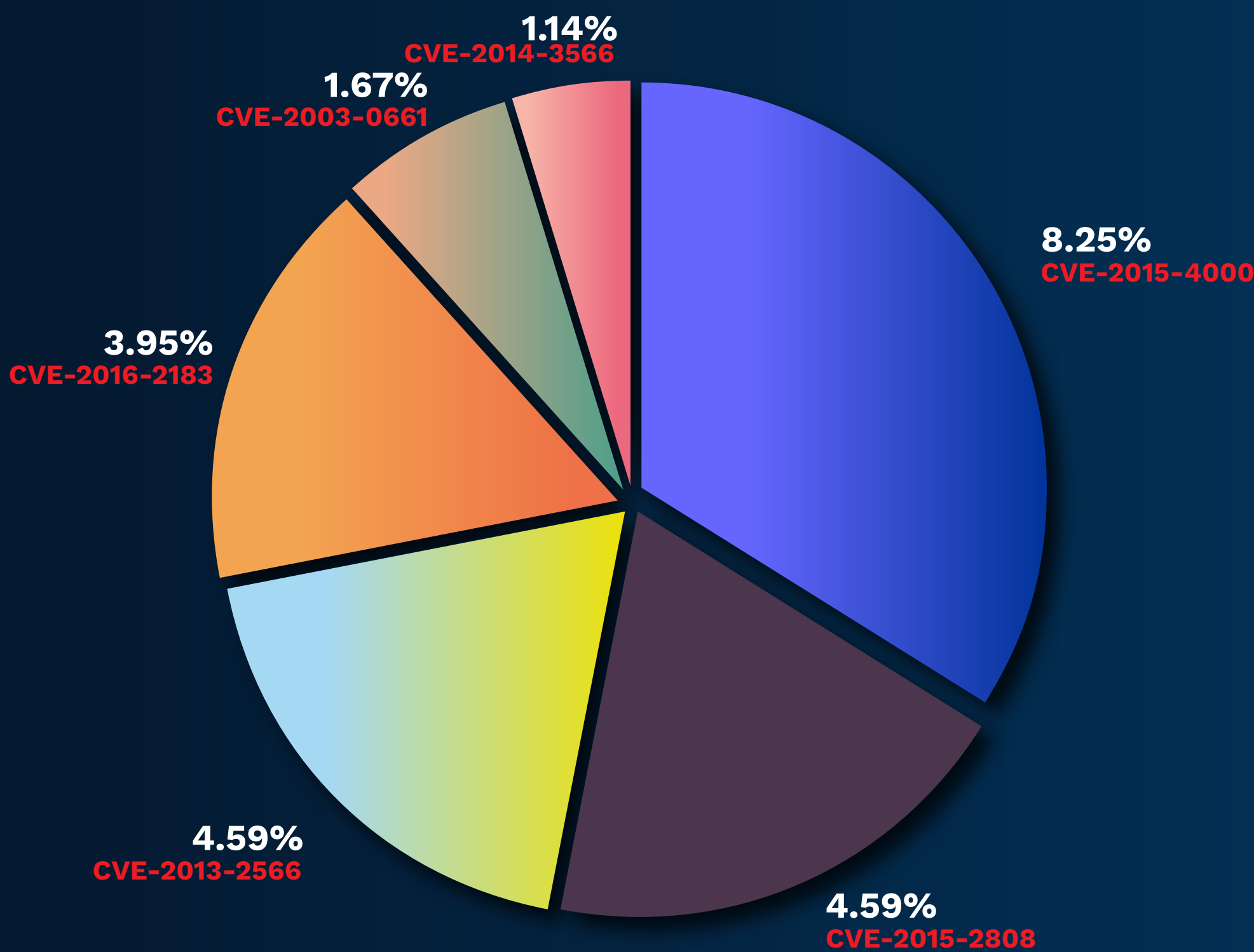
CVE Name	Percentage of Occurence	Risk (CVSS Score)
CVE-2015-4000	8.25%	Low
CVE-2015-2808	4.59%	Medium
CVE-2013-2566	4.59%	Medium
CVE-2016-2183	3.95%	High
CVE-2003-0661	1.67%	Medium
CEV-2014-3566	1.14%	Low

Most Common CWE discovered in 2021

Common Weakness Enumeration (CWE™) is a community-developed list of common software and hardware weakness types that have security ramifications. "Weaknesses" are flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture, that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack. The CWE List and associated classification taxonomy serve as a language that can be used to identify and describe these weaknesses in terms of CWEs.

"Cryptographic issues top the board. Probably due to the prevalence of crypto across the full stack"
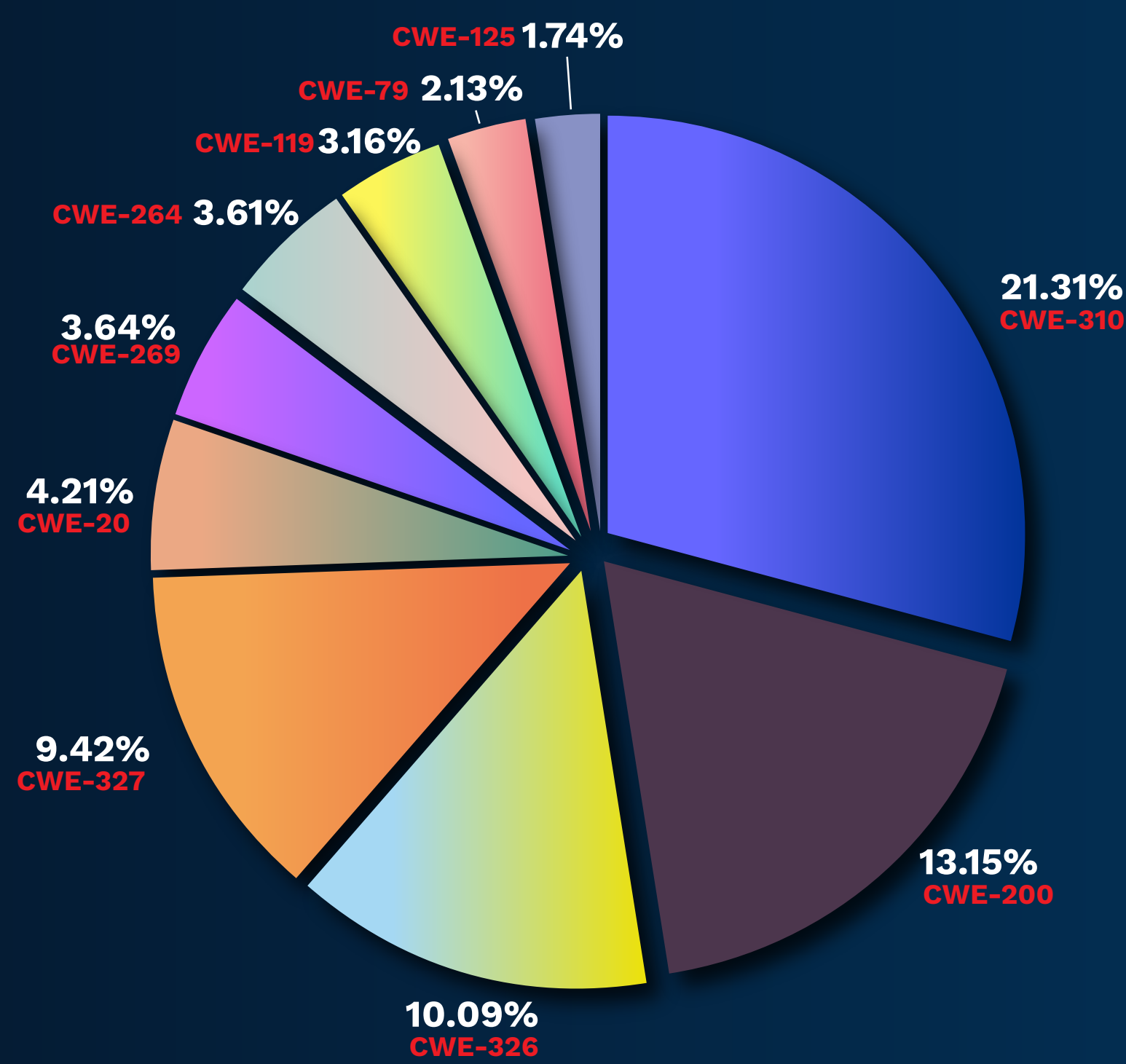
CWE Code	Percentage of Occurrence	Description
CWE-310	21.31%	Cryptographic Issues
CWE-200	13.15%	Exposure of Sensitive Information to an Unauthorized Actor
CWE-326	10.09%	Inadequate Encryption Strength
CWE-327	9.42%	Use of a Broken or Risky Cryptographic Algorithm
CWE-20	4.21%	Improper Input Validation
CWE-269	3.64%	Improper Privilege Management
CWE-264	3.61%	Permissions, Privileges, and Access Controls
CWE-119	3.16%	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-79	2.13%	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-125	1.74%	Out-of-bounds Read

Most Common Device/Framework/Network Layer Vulnerabilities

Critical Risk

When we refer to Device/Network/Framework vulnerabilities as opposed to API/Web Application vulnerabilities, they are generally components or products and not systems written by development teams. The normally have an associated CVE and require a patch or upgrade. The Top 20 Critical risks discovered in 2021 account for 80% of all critical risks discovered. PHP (as per 2020) still is most prevalent. Many of the issues discovered are used by Ransomware and Crypto-miner malware. The associated CVE's (where applicable) range from 2011 to 2021.

Oracle MySQL: Multiple Multiple Vulnerabilities: Security Bypass, Unpatched: 2.1%

CVE-2016-5584, CVE-2016-6662, CVE-2016-7440, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2018-3133, CVE-2018-3174, CVE-2018-3282, CVE-2021-22922, CVE-2021-22923, CVE-2021-22924, CVE-2021-22925, CVE-2021-22926, CVE-2021-22945, CVE-2021-22946, CVE-2021-22947, CVE-2021-35604, CVE-2021-35624, CVE-2021-3711, CVE-2021-3712

CWE-189, CWE-200, CWE-264, CWE-310, CWE-120, CWE-125, CWE-295, CWE-319, CWE-345, CWE-354, CWE-415, CWE-522, CWE-706, CWE-908

Adobe Flash Player : EOL Detection, Patching: 1.6%

CVE-2020-9633

CWE-416

Microsoft Windows RDP 'CVE-2019-0708' RCE Vulnerability (BlueKeep): 2.1%

CVE-2019-0708

CWE-416

Samba: Information Disclosure Vulnerability, Zerologon: 2.0%

CVE-2020-14318, CVE-2020-1472

CWE-269

SAP NetWeaver AS: Java Multiple Vulnerabilities: Bypass, Execution 1.5%

CVE-2020-6286, CVE-2020-6287

CWE-22, CWE-287

Oracle Weblogic Server - Multiple Vulnerabilities: RCE, Unpatched, bypass: 2.1%

CVE-2015-4852, CVE-2016-0572, CVE-2016-0573, CVE-2016-0574, CVE-2016-0577, CVE-2016-0638, CVE-2016-0675, CVE-2016-0688, CVE-2016-0696, CVE-2016-0700, CVE-2016-3416, CVE-2016-3445, CVE-2016-3505, CVE-2016-3510, CVE-2016-3586, CVE-2016-5488, CVE-2016-5531, CVE-2016-5535, CVE-2016-7103, CVE-2017-10063, CVE-2017-10137, CVE-2017-10147, CVE-2017-10148, CVE-2017-10152, CVE-2017-10178, CVE-2017-10271, CVE-2017-10334, CVE-2017-10336, CVE-2017-10352, CVE-2017-3248, CVE-2017-3506, CVE-2018-1257, CVE-2018-2628, CVE-2018-2893, CVE-2018-2894, CVE-2018-2902, CVE-2018-2933, CVE-2018-2935, CVE-2018-2987, CVE-2018-2998, CVE-2018-3191, CVE-2018-3213, CVE-2018-3245, CVE-2018-3248, CVE-2018-3249, CVE-2018-3250, CVE-2018-3252, CVE-2019-11358, CVE-2019-17571, CVE-2019-2568, CVE-2019-2615, CVE-2019-2618, CVE-2019-2645, CVE-2019-2646, CVE-2019-2647, CVE-2019-2648, CVE-2019-2649, CVE-2019-2650, CVE-2019-2658, CVE-2019-2725, CVE-2019-2729, CVE-2019-2824, CVE-2019-2827, CVE-2019-2887, CVE-2019-2888, CVE-2019-2890, CVE-2019-2891, CVE-2020-11022, CVE-2020-14572, CVE-2020-14588, CVE-2020-14589, CVE-2020-14622, CVE-2020-14645, CVE-2020-14652, CVE-2020-14820, CVE-2020-14841, CVE-2020-14859, CVE-2020-14882, CVE-2020-14883, CVE-2020-2519, CVE-2020-2544, CVE-2020-2546, CVE-2020-2547, CVE-2020-2548, CVE-2020-2549, CVE-2020-2550, CVE-2020-2551, CVE-2020-2552, CVE-2020-2766, CVE-2020-2798, CVE-2020-2801, CVE-2020-2811, CVE-2020-2828, CVE-2020-2829, CVE-2020-2869, CVE-2020-2883, CVE-2020-2884, CVE-2020-2963, CVE-2020-2966, CVE-2020-2967, CVE-2020-9488, CVE-2021-1994, CVE-2021-1995, CVE-2021-1996, CVE-2021-2047, CVE-2021-2075, CVE-2021-2109, CVE-2021-2142, CVE-2021-2157, CVE-2021-2204, CVE-2021-2211, CVE-2021-2214, CVE-2021-2294, CVE-2021-2376, CVE-2021-2378, CVE-2021-2382, CVE-2021-2394, CVE-2021-2397, CVE-2021-2403, CVE-2019-2725

CWE-200, CWE-284, CWE-295, CWE-502, CWE-74, CWE-77, CWE-79

PHP Multiple Vulnerabilities: EOL, DoS, Use-After-Free, RCE, Buffer Overflow: 23.1%

CVE-2011-1148, CVE-2011-1657, CVE-2011-1938, CVE-2011-2202, CVE-2011-2483, CVE-2011-3182, CVE-2011-3267, CVE-2011-3268, CVE-2012-2376, CVE-2014-9425, CVE-2014-9709, CVE-2015-1351, CVE-2015-1352, CVE-2015-8383, CVE-2015-8386, CVE-2015-8387, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8393, CVE-2015-8394, CVE-2015-8865, CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-3141, CVE-2016-3142, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4537, CVE-2016-4539, CVE-2016-4540, CVE-2016-4542, CVE-2016-5385, CVE-2016-5399, CVE-2016-6207, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6293, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297, CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132, CVE-2016-9935, CVE-2017-11142, CVE-2017-11143, CVE-2017-11144, CVE-2017-11145, CVE-2017-11146, CVE-2017-6004, CVE-2017-7890, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-9229, CVE-2016-7411, CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, CVE-2016-7418, CVE-2019-13224, CVE-2019-11043, CVE-2020-7059, CVE-2020-7060

CWE-125, CWE-119,CWE-264,CWE-310,CWE-399, CWE-787, CWE-416, CWE-22

Dell IDrac: Multiple Vulnerabilities: Buffer Overflow, Multiple Vulnerabilities: 1.7%

CVE-2018-1000116, CVE-2018-1207, CVE-2018-1211, CVE- 2020-5344, CVE-2018-15774, CVE-2018-15776, CVE-2019-3705

CWE-22, CWE-787, CWE-94, CWE-863, CWE-200, CWE-79

Microsoft Windows Multiple Vulnerabilities (KB4519998): Bypass, RCE, Information Disclosure: 8.7%

CVE-2019-0608, CVE-2019-1060, CVE-2019-1166, CVE-2019-1192, CVE-2019-1238, CVE-2019-1307, CVE-2019-1308, CVE-2019-1311, CVE-2019-1315, CVE-2019-1316, CVE-2019-1317, CVE-2019-1318, CVE-2019-1319, CVE-2019-1325, CVE-2019-1326, CVE-2019-1333, CVE-2019-1334, CVE-2019-1335, CVE-2019-1339, CVE-2019-1341, CVE-2019-1342, CVE-2019-1343, CVE-2019-1344, CVE-2019-1345, CVE-2019-1346, CVE-2019-1347, CVE-2019-1356, CVE-2019-1357, CVE-2019-1358, CVE-2019-1359, CVE-2019-1365, CVE-2019-1366, CVE-2019-1367, CVE-2019-1371

CWE-125, CWE-200, CWE-290, CWE-354, CWE-59, CWE-611, CWE-755, CWE-787, CWE-863

jQuery End of Life (EOL) Detection: 5.0%

SAP Gateway ACL Misconfiguration Vulnerability: Unauthorized Access risk: 5.0%

Microsoft Windows Server 2008 End Of Life Detection: Unsupported OS, Ransomware Exposure: 4.0%

OS End Of Life Detection: Unsupported OS, Ransomware Exposure: 3.7%

Apache HTTP Server Multiple Vulnerabilities - Linux: 3.7%

CVE-2020-13938, CVE-2020-35452, CVE-2021-26690, CVE-2021-26691

CWE-476, CWE-787, CWE-862

QNAP NAS / QTS Devices:Command Injection Vulnerability, Zerologon, Arbitrary Command Execution: 2.5%

CVE-2018-0719, CVE-2018-0721, CVE-2018-14746, CVE-2018-14747, CVE-2018-14748, CVE-2018-14749

CWE-119, CWE-476, CWE-77, CWE-863, CWE-200, CWE-78

Microsoft Exchange Server 2013 / 2016 / 2019 Multiple RCE Vulnerabilities: Unpatched: 2.4%

CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, CVE- 2021-28483, CVE-2021-33766, CVE-2021-34473, CVE-2021-34523, CVE-2021-26855, CVE-2020-17117, CVE-2020-17132, CVE-2020-17141, CVE-2020-17142, CVE-2020-17143

CWE-269, CWE-287,

VMware vCenter Server Multiple Vulnerabilities (VMSA-2021-0020):Unpatched, file upload, privilege escalation, bypass, information disclosure, path traversal, reflected XSS, RCE, DoS, SSRF: 2.4%

CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22005, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22011, CVE-2021-22012, CVE-2021-22013, CVE-2021-22014, CVE-2021-22015, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018, CVE-2021-22019, CVE-2021-22020

CWE-269, CWE-400, CWE-434, CWE-668, CWE-79, CWE-918, CWE-434, CWE-863, CWE-20, CWE-415

Microsoft Windows MS-NRPC Zerologon Vulnerability: 3.2%

CVE-2020-1472

CWE-269

Aerohive Networks HiveOS:LFI Vulnerability, PHP Code Execution: 1.5%

CVE-2020-16152

CWE-829

Intel Active Management Technology: Multiple Vulnerabilities: 1.4%

CVE-2020-12356, CVE-2020-8746, CVE-2020-8747, CVE-2020-8749, CVE-2020-8752, CVE-2020-8753, CVE-2020-8754, CVE-2020-8757, CVE-2020-8760, CVE-2017-5689, CVE-2020-8758

CWE-125, CWE-190, CWE-787, CWE-119

Pie chart values: 23.1%, 8.7%, 5.0%, 5.0%, 5.0%, 4.0%, 3.70%, 3.7%, 3.2%, 2.50%, 2.40%, 2.40%, 2.10%, 2.10%, 2.10%, 2.0%, 1.70%, 1.60%, 1.50%, 1.50%, 1.40%

Most Common Device/Framework/Network Layer Vulnerabilities

High Risk

The Top 20 High risks discovered in 2021 account for 88% of all Critical risks discovered. Cryptographic vulnerability CVE-2016-2183 is most prevalent. Since 2018 Cryptographic issues are in the top 3 due to the proliferation of cryptographic technology (It's everywhere!). PHP vulnerabilities are also prevalent in the Top 10 High Risk at #2. Many of the vulnerabilities listed are actively used by ransomware, malware and cyber criminal based attacks.

Oracle MySQL: Multiple Multiple Vulnerabilities: Security Bypass, Unpatched: 4.4%

CVE-2021-2478, CVE-2021-2479, CVE-2021-2481, CVE-2021-35546, CVE-2021-35575, CVE-2021-35577, CVE-2021-35591, CVE-2021-35596, CVE-2021-35602, CVE-2021-35607, CVE-2021-35608, CVE-2021-35617, CVE-2021-35612, CVE-2021-35622,CVE-2021-35623, CVE-2021-35625, CVE-2021-35626, CVE-2021-35627, CVE-2021-35628, CVE-2021-35630, CVE-2021-35631, CVE-2021-35632, CVE-2021-35633, CVE-2021-35634, CVE-2021-35635, CVE-2021-35636, CVE-2021-35637, CVE-2021-35638, CVE-2021-35639, CVE-2021-35640, CVE-2021-35641, CVE-2021-35642, CVE-2021-35643, CVE-2021-35644, CVE-2021-35645, CVE-2021-35646, CVE-2021-35647, CVE-2021-35648, CVE-2021-36222, CVE-2020-14773, CVE-2020-14777, CVE-2020-14785, CVE-2020-14786, CVE-2020-14791, CVE-2020-14794, CVE-2020-14804, CVE-2020-14809, CVE-2020-14814, CVE-2020-14821, CVE-2020-14828, CVE-2020-14829, CVE-2020-14830, CVE-2020-14836, CVE-2020-14837, CVE-2020-14838, CVE-2020-14839, CVE-2020-14844, CVE-2020-14845, CVE-2020-14846, CVE-2020-14848, CVE-2020-14852, CVE-2020-14860, CVE-2020-14861, CVE-2020-14866, CVE-2020-14868, CVE-2020-14870, CVE-2020-14873, CVE-2020-14878, CVE-2020-14888, CVE-2020-14891, CVE-2020-14893, CVE-2020-14539, CVE-2020-14540, CVE-2020-14547, CVE-2020-14553, CVE-2020-14559, CVE-2020-14568, CVE-2020-14575, CVE-2020-14576, CVE-2020-14586, CVE-2020-14591, CVE-2020-14597, CVE-2020-14614, CVE-2020-14619, CVE-2020-14620, CVE-2020-14623, CVE-2020-14624, CVE-2020-14631, CVE-2020-14632, CVE-2020-14633, CVE-2020-14634, CVE-2020-14641, CVE-2020-14643, CVE-2020-14651, CVE-2020-14654, CVE-2020-14656, CVE-2020-14663, CVE-2020-14678, CVE-2020-14680, CVE-2020-14697, CVE-2020-14702, CVE-2020-14725, CVE-2020-1967

CWE-327, CWE-476, CWE-189, CWE-125, CWE-200, CWE-674, CWE-787, CWE-416, CWE-190, CWE-125, CWE-787, CWE-399, CWE-125, CWE-674, CWE-327, CWE-20, CWE-416, CWE-668, CWE-787, CWE-909, CWE-399

Apache HTTP Server Multiple Vulnerabilities: 2.2%

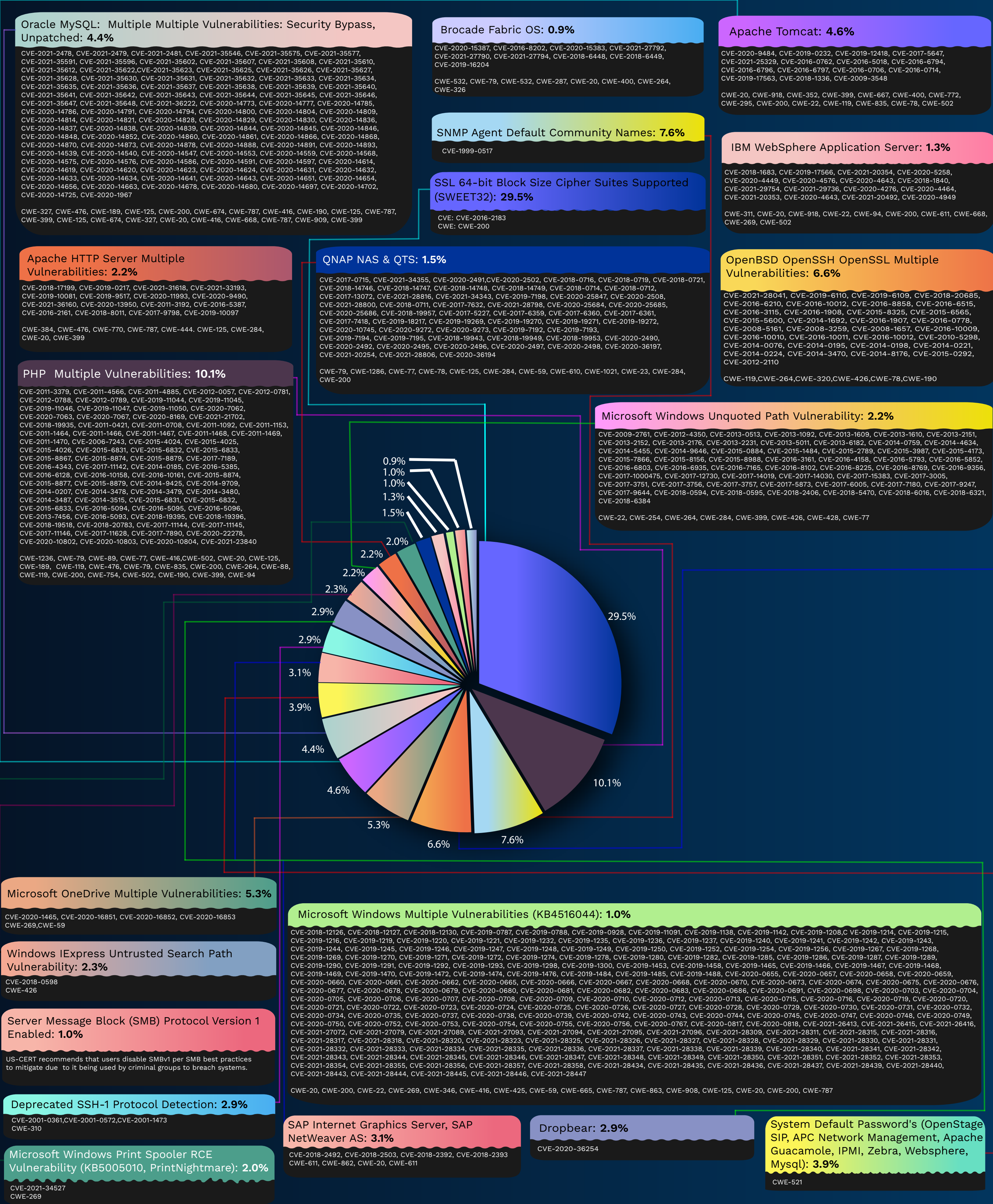CVE-2018-17199, CVE-2019-0217, CVE-2021-31618, CVE-2021-33193, CVE-2019-10081, CVE-2019-9517, CVE-2020-11993, CVE-2020-9490, CVE-2021-36160, CVE-2020-13950, CVE-2011-3192, CVE-2016-5387, CVE-2016-2161, CVE-2018-8011, CVE-2017-9798, CVE-2019-10097

CWE-384, CWE-476, CWE-770, CWE-787, CWE-444, CWE-125, CWE-284, CWE-20, CWE-399

PHP Multiple Vulnerabilities: 10.1%

CVE-2011-3379, CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788, CVE-2012-0789, CVE-2019-11044, CVE-2019-11045, CVE-2019-11046, CVE-2019-11047, CVE-2019-11050, CVE-2020-7062, CVE-2020-7063, CVE-2020-7067, CVE-2020-8169, CVE-2021-21702, CVE-2018-19935, CVE-2011-0421, CVE-2011-0708, CVE-2011-1092, CVE-2011-1153, CVE-2011-1464, CVE-2011-1466, CVE-2011-1467, CVE-2011-1468, CVE-2011-1469, CVE-2011-1470, CVE-2006-7243, CVE-2015-6024, CVE-2015-4025, CVE-2015-4026, CVE-2015-6831, CVE-2015-6832, CVE-2015-6833, CVE-2015-8867, CVE-2015-8874, CVE-2015-8879, CVE-2017-7189, CVE-2016-4343, CVE-2017-11142, CVE-2014-0185, CVE-2016-5385, CVE-2016-6128, CVE-2016-10158, CVE-2016-10161, CVE-2015-8874, CVE-2015-8877, CVE-2015-8879, CVE-2014-9425, CVE-2014-9709, CVE-2014-0207, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3515, CVE-2015-6831, CVE-2015-6832, CVE-2015-6833, CVE-2016-5094, CVE-2016-5095, CVE-2016-5096, CVE-2013-7456, CVE-2016-5093, CVE-2018-19395, CVE-2018-19396, CVE-2018-19518, CVE-2018-20783, CVE-2017-1144, CVE-2017-11145, CVE-2017-11146, CVE-2017-11628, CVE-2017-7890, CVE-2020-22278, CVE-2020-10802, CVE-2020-10803, CVE-2020-10804, CVE-2021-23840

CWE-1236, CWE-79, CWE-89, CWE-77, CWE-416,CWE-502, CWE-20, CWE-125, CWE-189, CWE-119, CWE-476, CWE-79, CWE-835, CWE-200, CWE-264, CWE-88, CWE-119, CWE-200, CWE-754, CWE-502, CWE-190, CWE-399, CWE-94

Brocade Fabric OS: 0.9%

CVE-2020-15387, CVE-2016-8202, CVE-2020-15383, CVE-2021-27792, CVE-2021-27790, CVE-2021-27794, CVE-2018-6448, CVE-2018-6449, CVE-2019-16204

CWE-532, CWE-79, CWE-532, CWE-287, CWE-20, CWE-400, CWE-264, CWE-326

SNMP Agent Default Community Names: 7.6%

CVE-1999-0517

SSL 64-bit Block Size Cipher Suites Supported (SWEET32): 29.5%

CVE: CVE-2016-2183
CWE: CWE-200

QNAP NAS & QTS: 1.5%

CVE-2017-0715, CVE-2021-34355, CVE-2020-2491,CVE-2020-2502, CVE-2018-0716, CVE-2018-0719, CVE-2018-0721, CVE-2018-14746, CVE-2018-14747, CVE-2018-14748, CVE-2018-14749, CVE-2018-0714, CVE-2018-0712, CVE-2017-13072, CVE-2021-28816, CVE-2021-34343, CVE-2019-7198, CVE-2020-25847, CVE-2020-2508, CVE-2021-28800, CVE-2018-0711, CVE-2017-7632, CVE-2021-28798, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2018-19957, CVE-2017-5227, CVE-2017-6359, CVE-2017-6360, CVE-2017-6361, CVE-2017-7418, CVE-2019-18217, CVE-2019-19269, CVE-2019-19270, CVE-2019-19271, CVE-2019-19272, CVE-2020-10745, CVE-2020-9272, CVE-2020-9273, CVE-2019-7192, CVE-2019-7193, CVE-2019-7194, CVE-2019-7195, CVE-2018-19943, CVE-2018-19949, CVE-2018-19953, CVE-2020-2490, CVE-2020-2492, CVE-2020-2495, CVE-2020-2496, CVE-2020-2497, CVE-2020-2498, CVE-2020-36197, CVE-2021-20254, CVE-2021-28806, CVE-2020-36194

CWE-79, CWE-1286, CWE-77, CWE-78, CWE-125, CWE-284, CWE-59, CWE-610, CWE-1021, CWE-23, CWE-284, CWE-200

Apache Tomcat: 4.6%

CVE-2020-9484, CVE-2019-0232, CVE-2019-12418, CVE-2017-5647, CVE-2021-25329, CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-0706, CVE-2016-0714, CVE-2019-17563, CVE-2018-1336, CVE-2009-3548

CWE-20, CWE-918, CWE-352, CWE-399, CWE-667, CWE-400, CWE-772, CWE-295, CWE-200, CWE-22, CWE-119, CWE-835, CWE-78, CWE-502

IBM WebSphere Application Server: 1.3%

CVE-2018-1683, CVE-2019-17566, CVE-2021-20354, CVE-2020-5258, CVE-2020-4449, CVE-2020-4576, CVE-2020-4643, CVE-2018-1840, CVE-2021-29754, CVE-2021-29736, CVE-2020-4276, CVE-2020-4464, CVE-2021-20353, CVE-2020-4643, CVE-2021-20492, CVE-2020-4949

CWE-311, CWE-20, CWE-918, CWE-22, CWE-94, CWE-200, CWE-611, CWE-668, CWE-269, CWE-502

OpenBSD OpenSSH OpenSSL Multiple Vulnerabilities: 6.6%

CVE-2021-28041, CVE-2019-6110, CVE-2019-6109, CVE-2018-20685, CVE-2016-6210, CVE-2016-10012, CVE-2016-8858, CVE-2016-6515, CVE-2016-3115, CVE-2016-1908, CVE-2015-8325, CVE-2015-6565, CVE-2015-5600, CVE-2014-1692, CVE-2016-1907, CVE-2016-0778, CVE-2008-5161, CVE-2008-3259, CVE-2008-1657, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2010-5298, CVE-2014-0076, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470, CVE-2014-8176, CVE-2015-0292, CVE-2012-2110

CWE-119,CWE-264,CWE-320,CWE-426,CWE-78,CWE-190

Microsoft Windows Unquoted Path Vulnerability: 2.2%

CVE-2009-2761, CVE-2012-4350, CVE-2013-0513, CVE-2013-1092, CVE-2013-1609, CVE-2013-1610, CVE-2013-2151, CVE-2013-2152, CVE-2013-2176, CVE-2013-2231, CVE-2013-5011, CVE-2013-6182, CVE-2014-0759, CVE-2014-4634, CVE-2014-5455, CVE-2014-9646, CVE-2015-0884, CVE-2015-1484, CVE-2015-2789, CVE-2015-3987, CVE-2015-4173, CVE-2015-7866, CVE-2015-8156, CVE-2015-8988, CVE-2016-3161, CVE-2016-4158, CVE-2016-5793, CVE-2016-5852, CVE-2016-6803, CVE-2016-6935, CVE-2016-7165, CVE-2016-8102, CVE-2016-8225, CVE-2016-8769, CVE-2016-9356, CVE-2017-1000475, CVE-2017-12730, CVE-2017-14019, CVE-2017-14030, CVE-2017-15383, CVE-2017-3005, CVE-2017-3751, CVE-2017-3756, CVE-2017-3757, CVE-2017-5873, CVE-2017-6005, CVE-2017-7180, CVE-2017-9247, CVE-2017-9644, CVE-2018-0594, CVE-2018-0595, CVE-2018-2406, CVE-2018-5470, CVE-2018-6016, CVE-2018-6321, CVE-2018-6384

CWE-22, CWE-254, CWE-264, CWE-284, CWE-399, CWE-426, CWE-428, CWE-77

Microsoft OneDrive Multiple Vulnerabilities: 5.3%

CVE-2020-1465, CVE-2020-16851, CVE-2020-16852, CVE-2020-16853
CWE-269,CWE-59

Windows IExpress Untrusted Search Path Vulnerability: 2.3%

CVE-2018-0598
CWE-426

Server Message Block (SMB) Protocol Version 1 Enabled: 1.0%

US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate due to it being used by criminal groups to breach systems.

Deprecated SSH-1 Protocol Detection: 2.9%

CVE-2001-0361,CVE-2001-0572,CVE-2001-1473
CWE-310

Microsoft Windows Print Spooler RCE Vulnerability (KB5005010, PrintNightmare): 2.0%

CVE-2021-34527
CWE-269

Microsoft Windows Multiple Vulnerabilities (KB4516044): 1.0%

CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-0787, CVE-2019-0788, CVE-2019-0928, CVE-2019-11091, CVE-2019-1138, CVE-2019-1142, CVE-2019-1208,CVE-2019-1214, CVE-2019-1215, CVE-2019-1216, CVE-2019-1219, CVE-2019-1220, CVE-2019-1221, CVE-2019-1232, CVE-2019-1235, CVE-2019-1236, CVE-2019-1237, CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1244, CVE-2019-1245, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1254, CVE-2019-1256, CVE-2019-1267, CVE-2019-1268, CVE-2019-1269, CVE-2019-1270, CVE-2019-1271, CVE-2019-1272, CVE-2019-1274, CVE-2019-1278, CVE-2019-1280, CVE-2019-1282, CVE-2019-1285, CVE-2019-1286, CVE-2019-1287, CVE-2019-1289, CVE-2019-1290, CVE-2019-1291, CVE-2019-1292, CVE-2019-1293, CVE-2019-1298, CVE-2019-1300, CVE-2019-1453, CVE-2019-1458, CVE-2019-1466, CVE-2019-1467, CVE-2019-1468, CVE-2019-1469, CVE-2019-1470, CVE-2019-1472, CVE-2019-1474, CVE-2019-1476, CVE-2019-1484, CVE-2019-1485, CVE-2019-1488, CVE-2020-0655, CVE-2020-0657, CVE-2020-0658, CVE-2020-0659, CVE-2020-0660, CVE-2020-0661, CVE-2020-0662, CVE-2020-0665, CVE-2020-0666, CVE-2020-0667, CVE-2020-0668, CVE-2020-0670, CVE-2020-0673, CVE-2020-0674, CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0678, CVE-2020-0679, CVE-2020-0680, CVE-2020-0681, CVE-2020-0682, CVE-2020-0683, CVE-2020-0686, CVE-2020-0691, CVE-2020-0698, CVE-2020-0703, CVE-2020-0704, CVE-2020-0705, CVE-2020-0706, CVE-2020-0707, CVE-2020-0708, CVE-2020-0709, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0715, CVE-2020-0716, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0727, CVE-2020-0728, CVE-2020-0729, CVE-2020-0730, CVE-2020-0731, CVE-2020-0732, CVE-2020-0734, CVE-2020-0735, CVE-2020-0737, CVE-2020-0738, CVE-2020-0739, CVE-2020-0742, CVE-2020-0743, CVE-2020-0744, CVE-2020-0745, CVE-2020-0747, CVE-2020-0748, CVE-2020-0749, CVE-2020-0750, CVE-2020-0752, CVE-2020-0753, CVE-2020-0754, CVE-2020-0755, CVE-2020-0756, CVE-2020-0767, CVE-2020-0818, CVE-2021-26413, CVE-2021-26415, CVE-2021-26416, CVE-2021-27072, CVE-2021-27079, CVE-2021-27089, CVE-2021-27093, CVE-2021-27094, CVE-2021-27095, CVE-2021-27096, CVE-2021-28309, CVE-2021-28311, CVE-2021-28315, CVE-2021-28316, CVE-2021-28317, CVE-2021-28318, CVE-2021-28320, CVE-2021-28323, CVE-2021-28325, CVE-2021-28326, CVE-2021-28327, CVE-2021-28328, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28347, CVE-2021-28348, CVE-2021-28349, CVE-2021-28350, CVE-2021-28351, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434, CVE-2021-28435, CVE-2021-28436, CVE-2021-28437, CVE-2021-28439, CVE-2021-28440, CVE-2021-28443, CVE-2021-28444, CVE-2021-28445, CVE-2021-28446, CVE-2021-28447

CWE-20, CWE-200, CWE-22, CWE-269, CWE-346, CWE-416, CWE-425, CWE-59, CWE-665, CWE-787, CWE-863, CWE-908, CWE-125, CWE-20, CWE-200, CWE-787

SAP Internet Graphics Server, SAP NetWeaver AS: 3.1%

CVE-2018-2492, CVE-2018-2503, CVE-2018-2392, CVE-2018-2393
CWE-611, CWE-862, CWE-20, CWE-611

Dropbear: 2.9%

CVE-2020-36254

System Default Password's (OpenStage SIP, APC Network Management, Apache Guacamole, IPMI, Zebra, Websphere, Mysql): 3.9%

CWE-521

Pie chart values: 0.9%, 1.0%, 1.0%, 1.3%, 1.5%, 2.0%, 2.2%, 2.2%, 2.3%, 2.9%, 2.9%, 3.1%, 3.9%, 4.4%, 4.6%, 5.3%, 6.6%, 7.6%, 10.1%, 29.5%
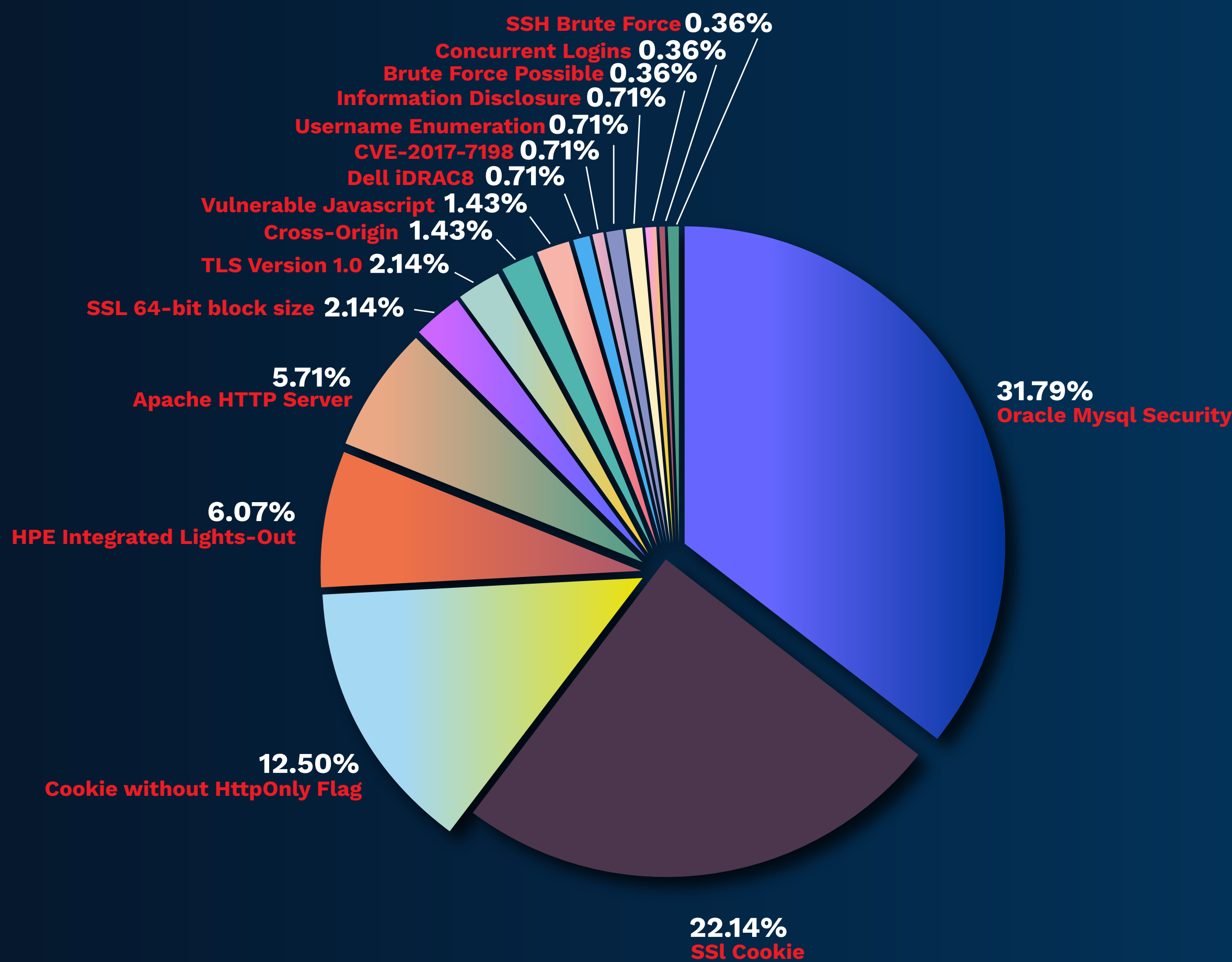
Most Common Risk-Accepted Vulnerability
What Organizations sometimes accept

Most organizations maintain the concept of accepting known risks. There are lots of reasons why this is done and some common ones include; the presence of some other compensating control, acknowledgement that the risk is impractically low or the fact that an upcoming change might remove the risk completely.

Edgescan clients with appropriate privileges can risk-accept vulnerabilities in the platform. A Risk-accepted issue puts a discovered vulnerability in a "non-closed" state so it can be tracked but it is not deemed a risk by the organization. The below table shows a list of the most common vulnerability types that our clients tend to accept the risk posed by them.

SSH Brute Force 0.36%
Concurrent Logins 0.36%
Brute Force Possible 0.36%
Information Disclosure 0.71%
Username Enumeration 0.71%
CVE-2017-7198 0.71%
Dell iDRAC8 0.71%
Vulnerable Javascript 1.43%
Cross-Origin 1.43%
TLS Version 1.0 2.14%
SSL 64-bit block size 2.14%
5.71% Apache HTTP Server
6.07% HPE Integrated Lights-Out
12.50% Cookie without HttpOnly Flag
22.14% SSl Cookie
31.79% Oracle Mysql Security

Vulnerability Name	Percentage of Total	Average Risk
Oracle Mysql Security Multiple Vulnerabilities	31.79%	Medium
SSL cookie without secure flag set	22.14%	Low
Cookie without HttpOnly flag set	12.50%	Low
HPE Integrated Lights-Out (iLO) 4 and 5 Information Disclosure Vulnerability	6.07%	Medium
Apache HTTP Server < 2.4.6 Multiple Vulnerabilities	5.71%	High
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	2.14%	High
TLS Version 1.0 Protocol Detection	2.14%	Medium
HTML5 cross-origin resource sharing	1.43%	Medium
Vulnerable Javascript library	1.43%	Low
Dell iDRAC8 Multiple Vulnerabilities	0.71%	Medium
PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows)	0.71%	High
Username Enumeration	0.71%	Medium
Web Server robots.txt Information Disclosure	0.71%	Informational
Brute Forcing Possible	0.36%	High
Concurrent Logins Permitted	0.36%	Low
SSH Brute Force Logins With Default Credentials	0.36%	High

CVE Dispersion and Clustering

This provides a snapshot view of the health of assets in general, both public internet facing and internal hosts combined. The % of Assets with more than ten CVE's has increased significantly from the 2021 report (up from 4%). There is a marked increase of systems with at least one CVE (43% in 2021 report).

System with at least one CVE
51%

System with at least two CVEs
30%

System with at least Ten CVEs
5%
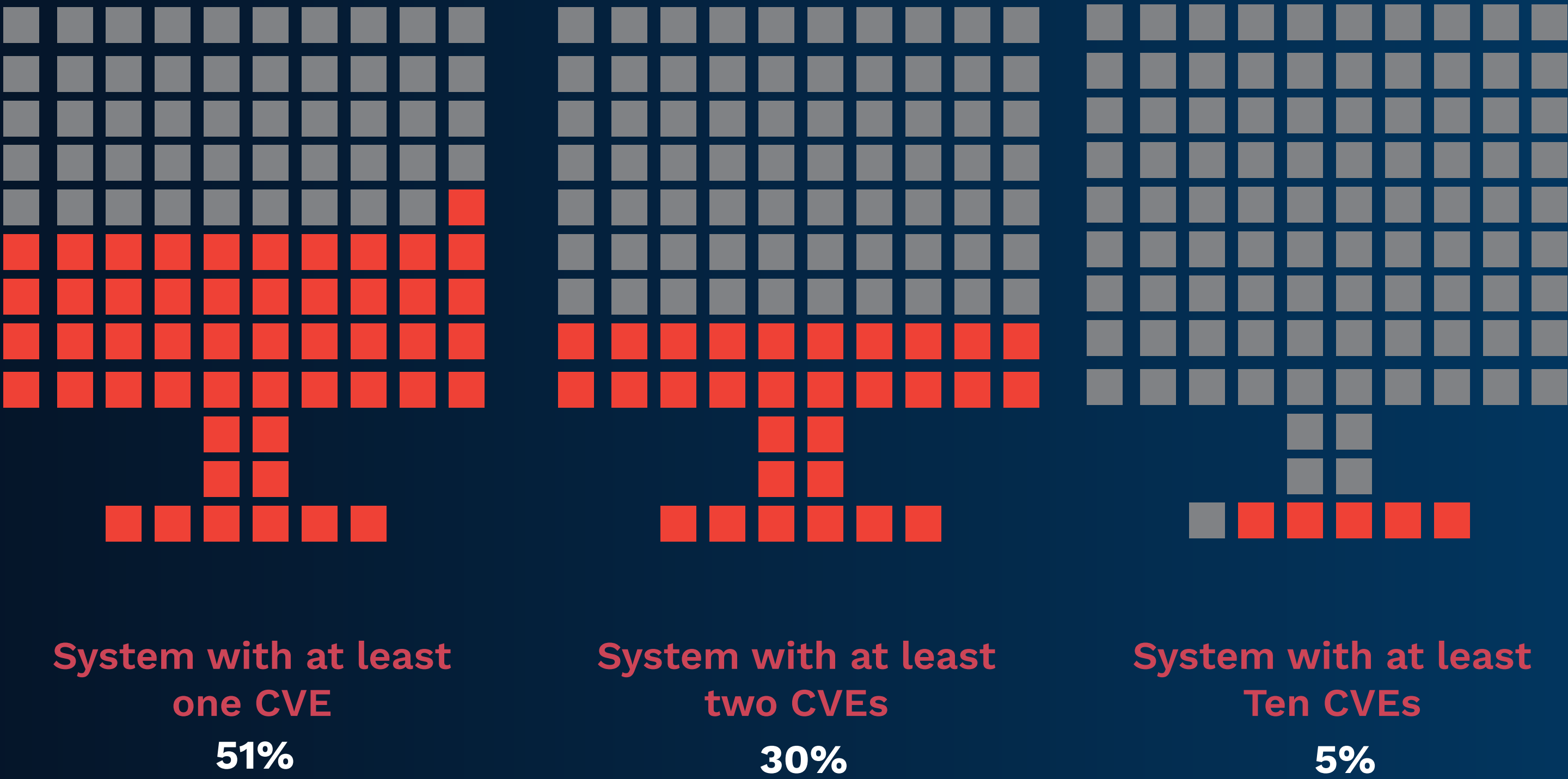
The density of known vulnerabilities within a single system, can really say something about an organisation. For the 5% of systems with more than ten CVE's, the presence of such can often be a sign to an attacker that an organisation does not have adequate security resources or perhaps they are running a large number of legacy systems. Legacy systems, those which cannot be patched due to various reasons, should be further protected. Organisations that hold a large number of systems which are in this 5% are susceptible to malware proliferation, should a malware attack take hold.

Attack Surface
Unseen Threat Within

"You cannot protect what you cannot see"

Eoin Keary

Attack Surface
Exposed Ports

Based on a sample of 2 million IP's the table below depicts the most common ports and ports of note. The highlighted rows with the exception of the common web ports, would be considered by most cyber security professionals as ones which may pose a risk and generally should not be open to the public Internet.

In particular Remote Access, Database and Network Management protocols should not be exposed and are also commonly used by ransomware gangs to breach an organization.

Remote Desktop Protocol (RDP) credentials can be found on the dark web, with some selling as cheaply as $20 each.

Protocol	Port	% of all devices	Description
tcp	443	14.34%	HTTPS
tcp	80	11.54%	HTTP
tcp	22	3.33%	Secure Shell (SSH)
tcp	8443	2.17%	HTTPS
tcp	25	1.22%	Simple Mail Transfer Protocol (SMTP)
udp	123	1.19%	Network Time Protocol
tcp	3389	1.11%	RDP (Windows)
tcp	8080	0.99%	HTTP
udp	161	0.84%	Simple Network Management Protocol (SNMP)
tcp	1720	0.77%	H.323 (Microsoft NetMeeting) call setup protocol
tcp	53	0.75%	DNS
tcp	111	0.61%	Portmapper/RPC
tcp	445	0.57%	Windows AD/SMB
tcp	135	0.56%	RPC/Database
tcp	179	0.51%	BGP
tcp	444	0.50%	SNPP
tcp	222	0.50%	Berkeley rshd
tcp	21	0.50%	FTP
udp	500	0.46%	IPSEC
udp	53	0.43%	DNS
tcp	139	0.37%	NetBios
tcp	110	0.31%	PoP (Mail)
tcp	3306	0.28%	MySQL
tcp	5060	0.23%	SIP (IoT)
tcp	5432	0.12%	PostGreSQL
tcp	1723	0.09%	Microsoft PPTP VPN
tcp	1433	0.09%	MS SQL
tcp	23	0.08%	Telnet
tcp	514	0.04%	Syslog
tcp	513	0.03%	rlogin, rsh, rexec
tcp	1434	0.02%	MS SQL
tcp	512	0.02%	rlogin, rsh, rexec
tcp	3351	0.01%	Pervasive SQL
tcp	1583	0.01%	Pervasive SQL
tcp	3050	0.01%	Interbase DB

Exposed Ports Continued

"Remote access exposures across the attack surface are a worrying trend and accounted for 5% of total attack surface exposures in 2021. "

Description	Notes
Secure Shell (SSH)	With SSH providing long term privileged access, this is not only a top targeted service for entry, but a larger priority of REENTRY, SSH versions may be secure but the credential attacks are always a top priority, if this fails and secure keys are in place it does not remove the risk of being a long term re-entry to the system, as well as pivoting to additional systems with static SSH keys been a common issue.
Simple Mail Transfer Protocol (SMTP)	SMTP being internet facing exposed leads to a serious issue - there may be no mechanisms implemented to stop unauthorized access, or protection such as a SPF in place to prevent Open Relay attacks leading to both spam and phishing, or malware. This can also be used as a form of DoS attacks by flooding servers.
RDP (Windows)	RDP is greatly misunderstood as not being a significant risk if exposed to the internet. This could not be more incorrect - RDP servers can suffer from poorly implemented security, such as not having rate-limiting or failed login limits. This exposes the server to become an entry point into private networks. RDP should be protected further by implanting an additional layer of security, such as a VPN.
Simple Network Management Protocol (SNMP)	SNMP should be also have a firewall rule to block UDP:161, UDP:162 - SNMP can be misunderstood as secure as no vulnerability may exist - but this is overlooking the fact that SNMP is inherently an insecure protocol that was designed predating what we know as security today. It is unencrypted and provides very useful management advantages, however these can also be abused by a malicious user.
H.323 (Microsoft NetMeeting) call setup protocol	This is common when VOIP is being used. Misconfigured H.323 can result in VOIP system breach and access to internal numbers resulting in potential evesdropping.
Windows AD/SMB	There is no practical reason for SMB to be exposed to the internet, and inbound traffic should be blocked. Unlike other less complicated/limited sandboxed protocols, SMB is deeply integrated to the OS and will continue to be a top 5 attack which we have experienced with EternalBlue, WannaCry, NotPetya
Berkeley rshd	Remote Access
FTP	FTP is one of the big 5, with it being an unencrypted protocol. It is one of the top 5 ports checked for by BOTs along with SFTP. An exposed FTP service often tells hackers "They cant even set up SFTP and so must have little security experience"
MySQL	Exposed Database: These may and usually contain data, which is a big priority to organisations, their clients and therefore to attackers. Databases are invaluable assets to attack and will always be a high priority target if found. Exposed databases are often misunderstood to be secure due to password protection or being fully patched. However, this is often not the case and databases are highly susceptible to credential brute-force attacks and other authentication based attacks.
SIP (IoT)	VOIP
PostGreSQL	Exposed Database
Microsoft PPTP VPN	Remote Access
MS SQL	Exposed Database
Telnet	With telnet being one of the earliest remote login protocols it is also important to note that in the early days these protocols were built with the purpose to perform high privilege tasks. Cleartext packet sniffing and credential attacks are still widely used against this protocol.
rlogin, rsh, rexec	Remote Access
MS SQL	Exposed Database
rlogin, rsh, rexec	Remote Access
Pervasive SQL	Exposed Database
Pervasive SQL	Exposed Database
Interbase DB	Exposed Database

Attack Surface
Exposed Services and Systems

Struggling With Visibility:

In general we see that organizations struggle with visibility of their own IT estates, knowing what is running and where, at any given time. This can and likely has lead to many security breaches, some of which were hot topics during the year.

Attack Surface Management (ASM) is a trending solution, something Edgescan has delivered since 2016 and can provide continuous visibility across an enterprise estate, helping to detect exposures and vulnerabilities as they occur. ASM scanning can occur from multiple geographic locations in order to circumvent geo-locked source IP scans.

2,000,000
Based on sample IP's during 2021

Exposed Remote Access

66,506
SSH

22,109
RDP

10,932
rLogin & rshrexec

1,679
Telnet

1,815
Microsoft PPTP VPN

Exposed Administration Consoles

3,469
Administrative Access Portals

Exposed IoT/Communication Systems

15,436
H.323 - Call setup protocol

4,627
SIP

Exposed Data Systems

4,78
Pervasive SQL

2,129
MS SQL Databases

5,609
MySQL Databases

983
Oracle Databases

Exposed Data

135
Exposed Backup Directories/Files

Edgescan
What makes us tick

"I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times"

Bruce Lee

What is **Edgescan?**

Application Security
- Continuous Application/API vulnerability assessment
- Pentesting as a Service (PTaaS)
- API Security assessment and Pentesting
- Alerting and integration

Host Security
- Continuous External /Internal Vulnerability Assessment
- Pentesting as a Service (PTaaS)
- Alerting and integration

Continuous Monitoring
- Live system and service 24/7 discovery
- Alerting and integration
- Exposed service alerting

API Discovery
- Continuous API discovery and enumeration
- Eliminate blind spots
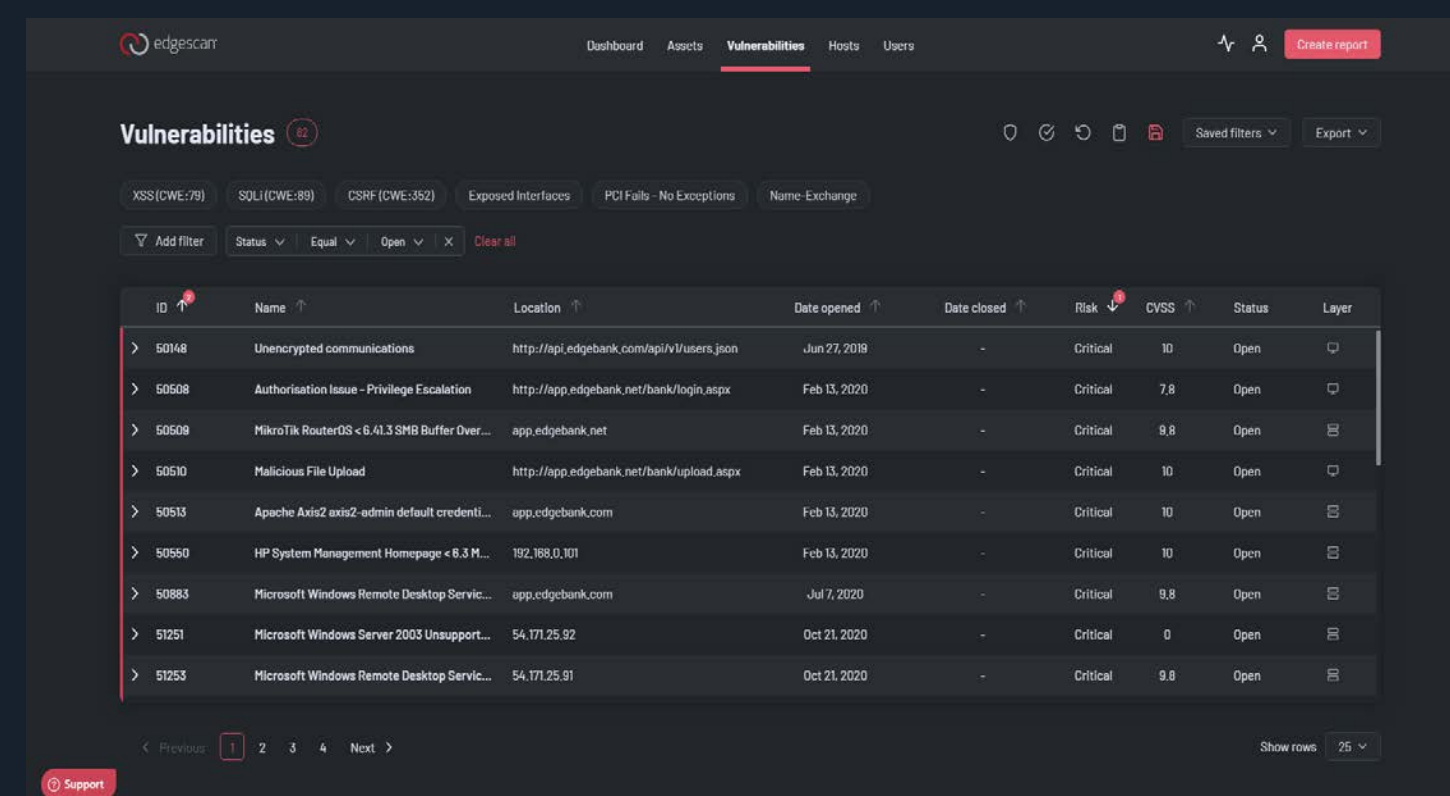
- **Fullstack coverage**
- **Validated by experts**
- **Mitigation Support**
- **On-demand**

What does Edgescan do?
Simply, we detect & validate cyber vulnerabilities in your IT systems; Web, Network, API, CI/CD, IoT, Internal, External – fullstack! We provide continuous visibility to help you maintain security. We provide on-demand Pen Testing as a Service (PTaaS)

Why should I use Edgescan?
We deliver a dedicated vulnerability detection solution (SaaS). We're extremely accurate and provide support to guide you through your journey. We deliver a comprehensive and cost effective solution. We're PCI Approved Scanning Vendors.

40%
Reduce Mean Time To Remediation (MTTR) by 40%

2.1+
Save on average the equivalent of 2.1 full time staff members per month using Edgescan

What is Edgescan?

What's different?
- All vulnerabilities are validated for accuracy and risk.
- We're a fullstack cyber SaaS (Web applications and Network security).
- We support our clients to help them understand and fix issues with our certified penetration testing team.
- We can scale to thousands of assessments.
- Unlimited assessments.

What are the main features?
- Continuous fullstack security testing
- Automatic assessments of new endpoints as they are discovered
- Validation and support for all issues discovered
- Continuous asset and API monitoring and detection
- Internal and External Assessments
- On-demand assessments and penetration testing.
- Alerting and Integration customizable for you.

Does this help me?
The Edgescan Team are experts at vulnerability detection. We save you time and money by helping you focus on items that matter.

How?
We deliver a cyber assessment service from our cloud which provides continuous and on-demand detection.

Why?
Finding weaknesses in IT Systems helps prevent a data breach or cyber attack.
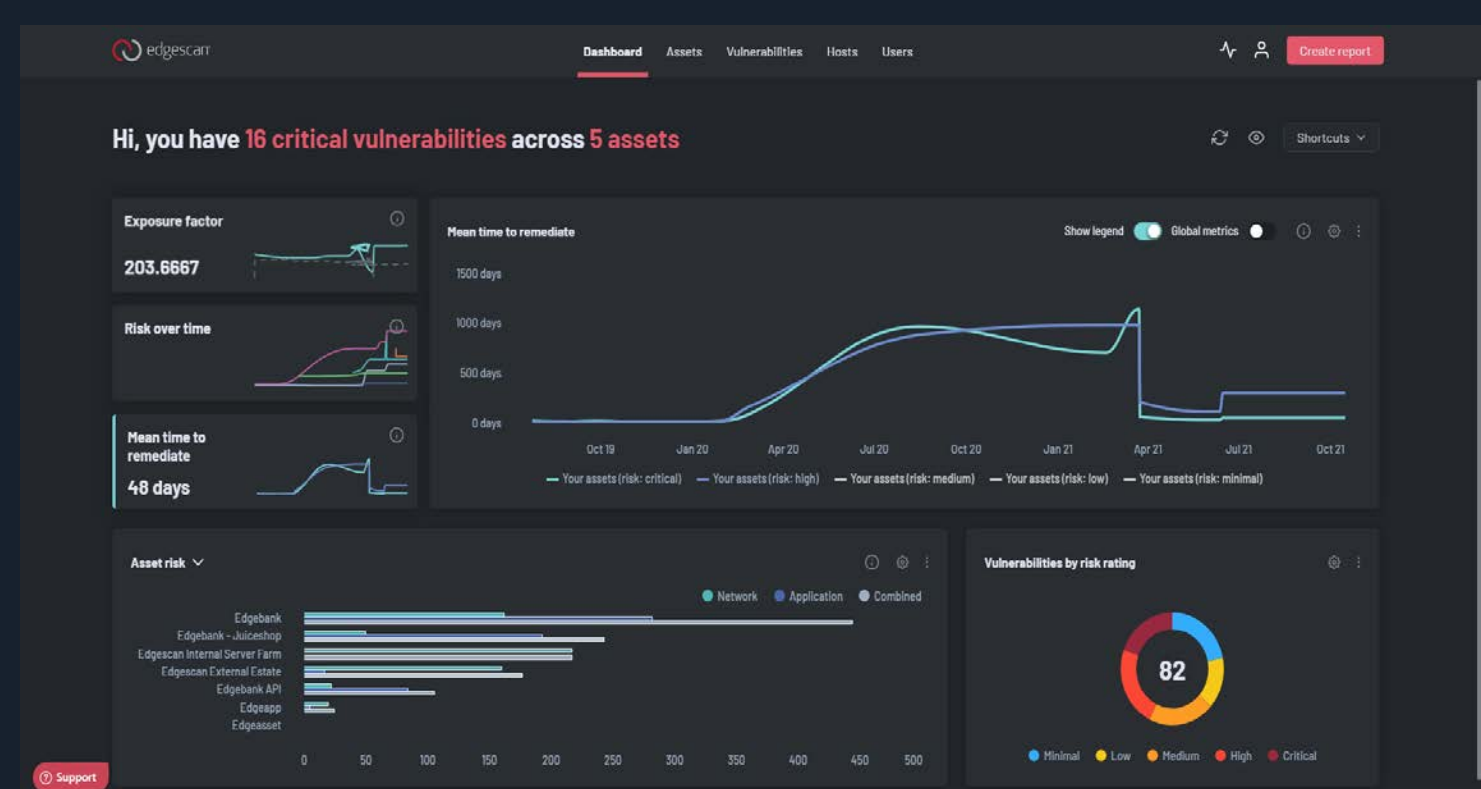
If you think Edgescan can help your organisation increase its security posture, get in touch with our sales team for a trial at sales@edgescan.com

100%
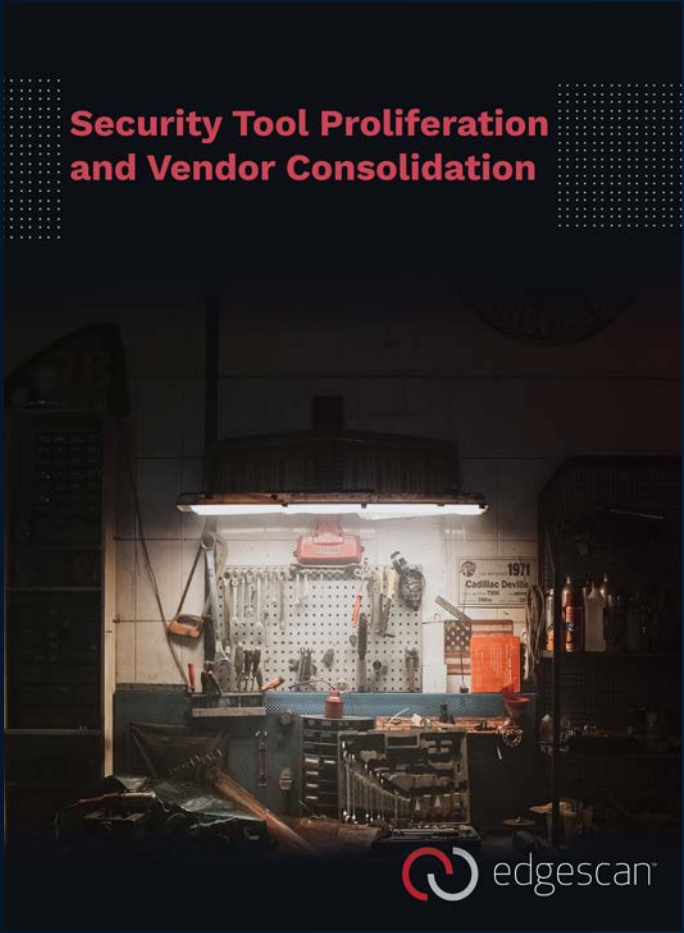**Full OWASP Application Security Coverage**

24/7/365
Continuous asset profiling and discovery

Edgescan Whitepaper
Links to Whitepapers hosted on Edgescan

Want to find out more? Click on any of the links below to get indepth look at popular subjects such as the Evolving Attack Surface, Security Tool and Vendor Consolidation and more. Learn more about how you can protect your organization.

Security Tool Proliferation and Vendor Consolidation

Does a Hybrid Model for Vulnerability Management Make Sense?

Can You have a Single Touchstone of Truth for Your Vulnerability Management Program? (And Is it Worth It?)

What is Smart Vulnerability Management and Why Does it Matter?

Why Does a Single Full Stack Vulnerability Management Solution Matter?

The Evolving Attack Surface

Resilance to Ransomware

A Journey into the Smart Vulnerability Management War Room

January 2022 Vulnerability Snapshot

AWARD WINING PLATFORM

2020 Computing Security Awards
WINNER
Cloud-Delivered Security Solution of Year

2020 Computing Security Awards
WINNER
Penetration Testing Solution of the Year

SC 2020 awards EUROPE
WINNER
Best Vulnerability Management Solution

2021 Computing Security Awards
WINNER
Enterprise Security Solution of the Year

2021 Computing Security Awards
WINNER
Penetration Testing Solution of the Year

2021 Computing Security Awards
WINNER
Penetration Testing Solution of the Year

Gartner peer insights™

Check out our Gartner Reviews

Edgescan Platform

Centralized Dashboard
Get all your information in one location with an interactive & exportable risk metrics dashboard

Assets
Keep track of all assets and perform assessments on-demand for a holistic management of assets across your organization
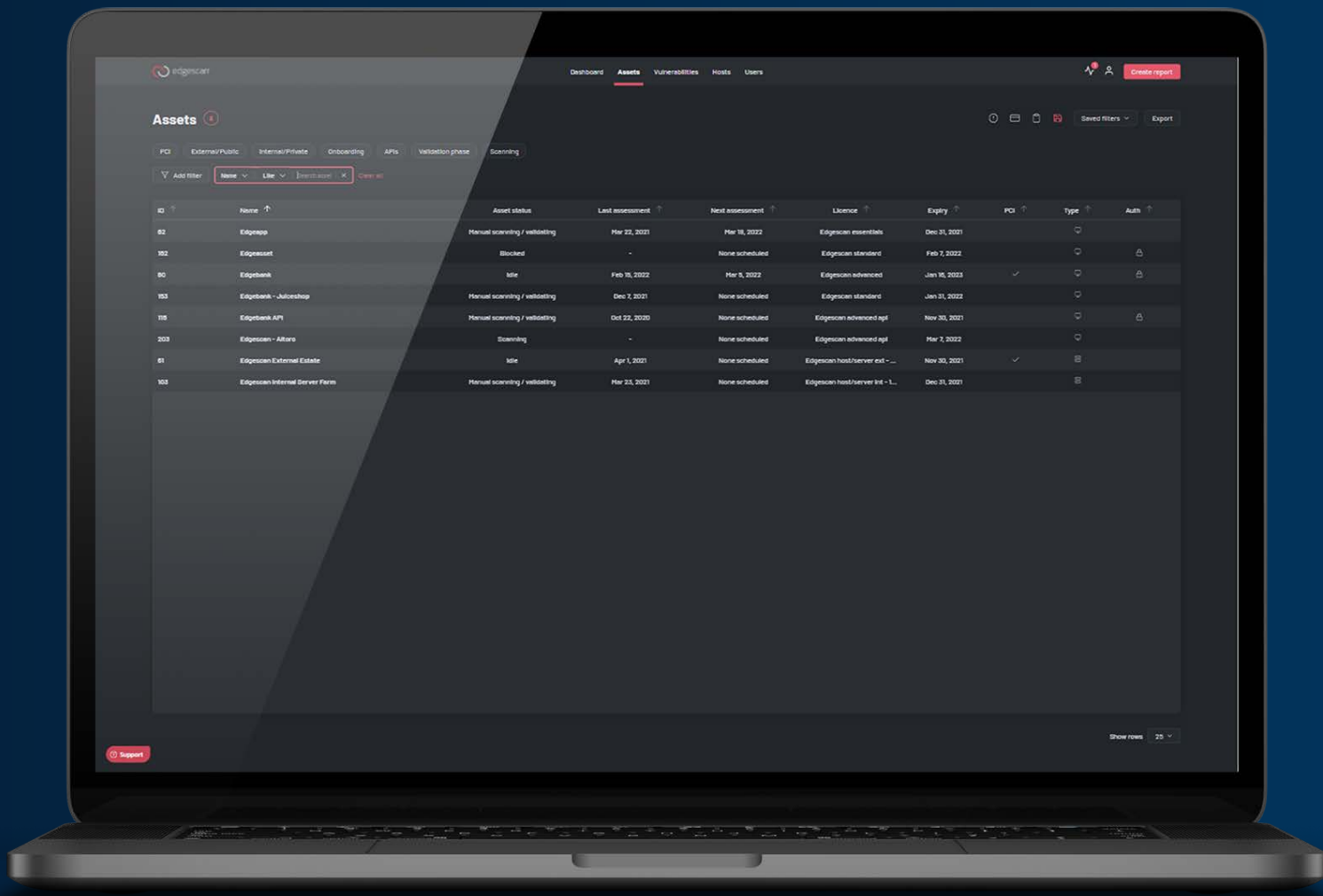
Vulnerabilities
Receive actionable risk intelligence with the ability to rescan on-demand to ensure that your hosts and asset vulnerabilities are fixed
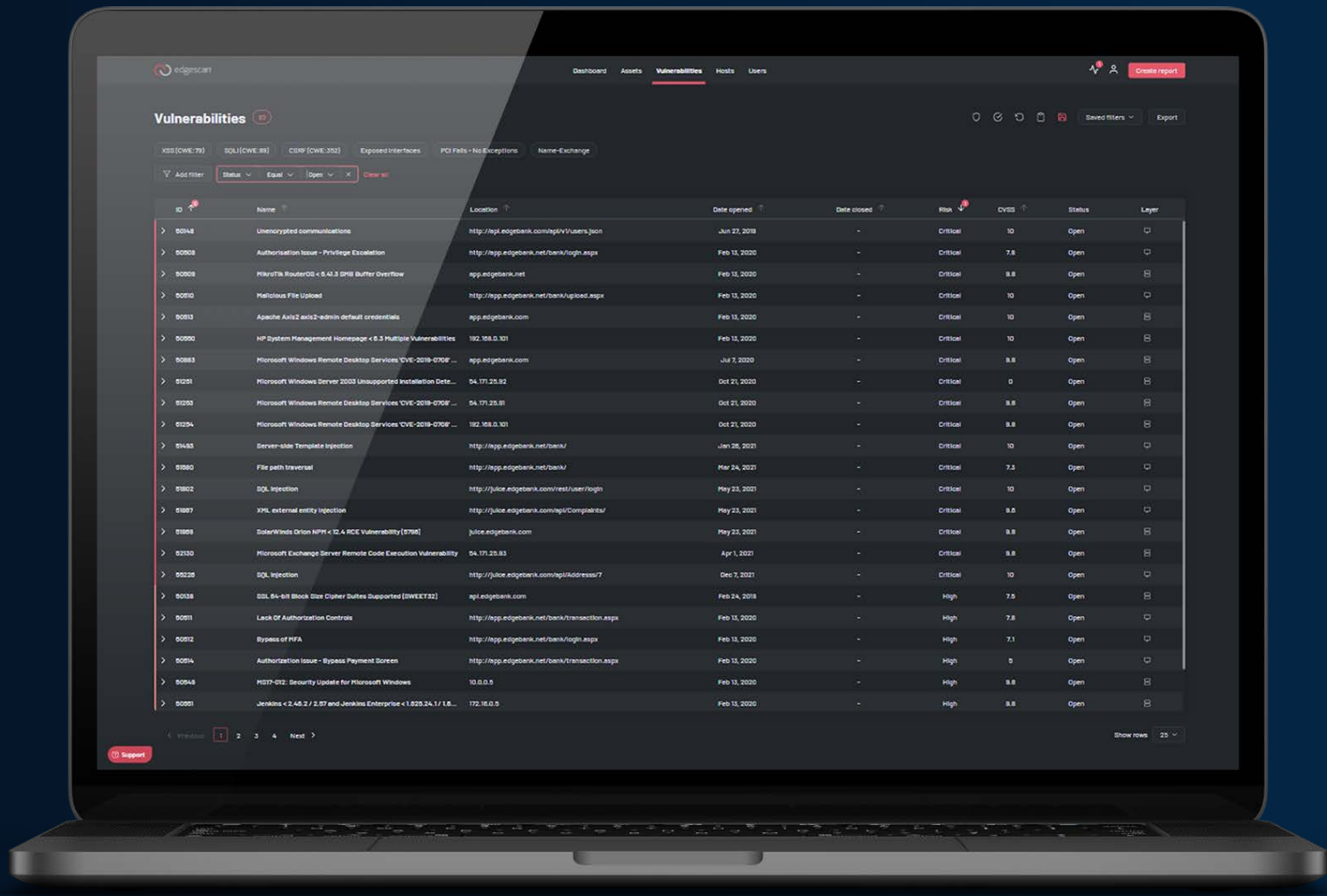
Edgescan Platform
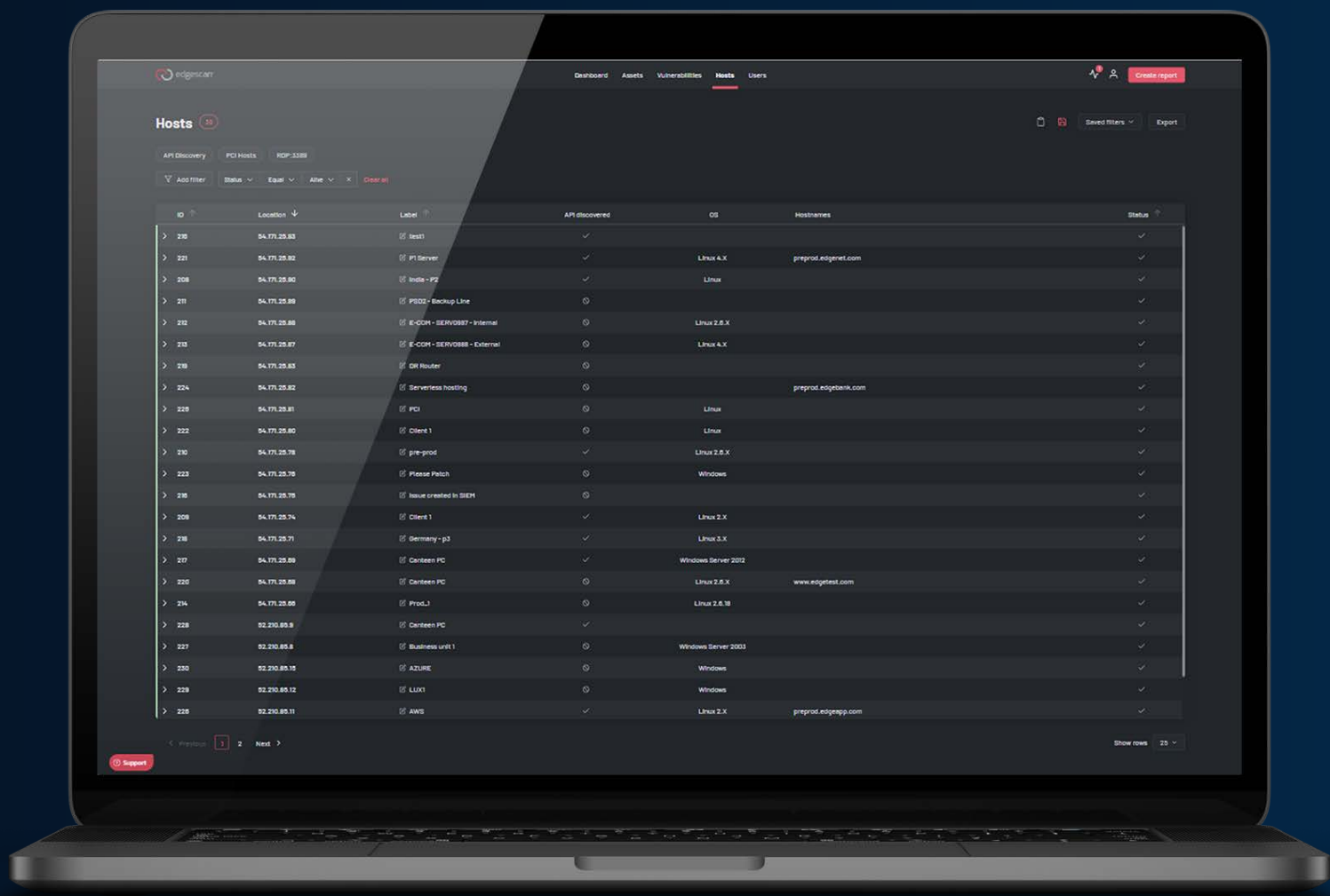
Hosts
Always know what's going on with our 24/7/365 visibility of your external exposures that have been added to the platform, allowing you to know exactly what is going on at any given time

Reporting
The Edgescan platform has an extensive reporting system that allows you to generate a report on any page that you are on
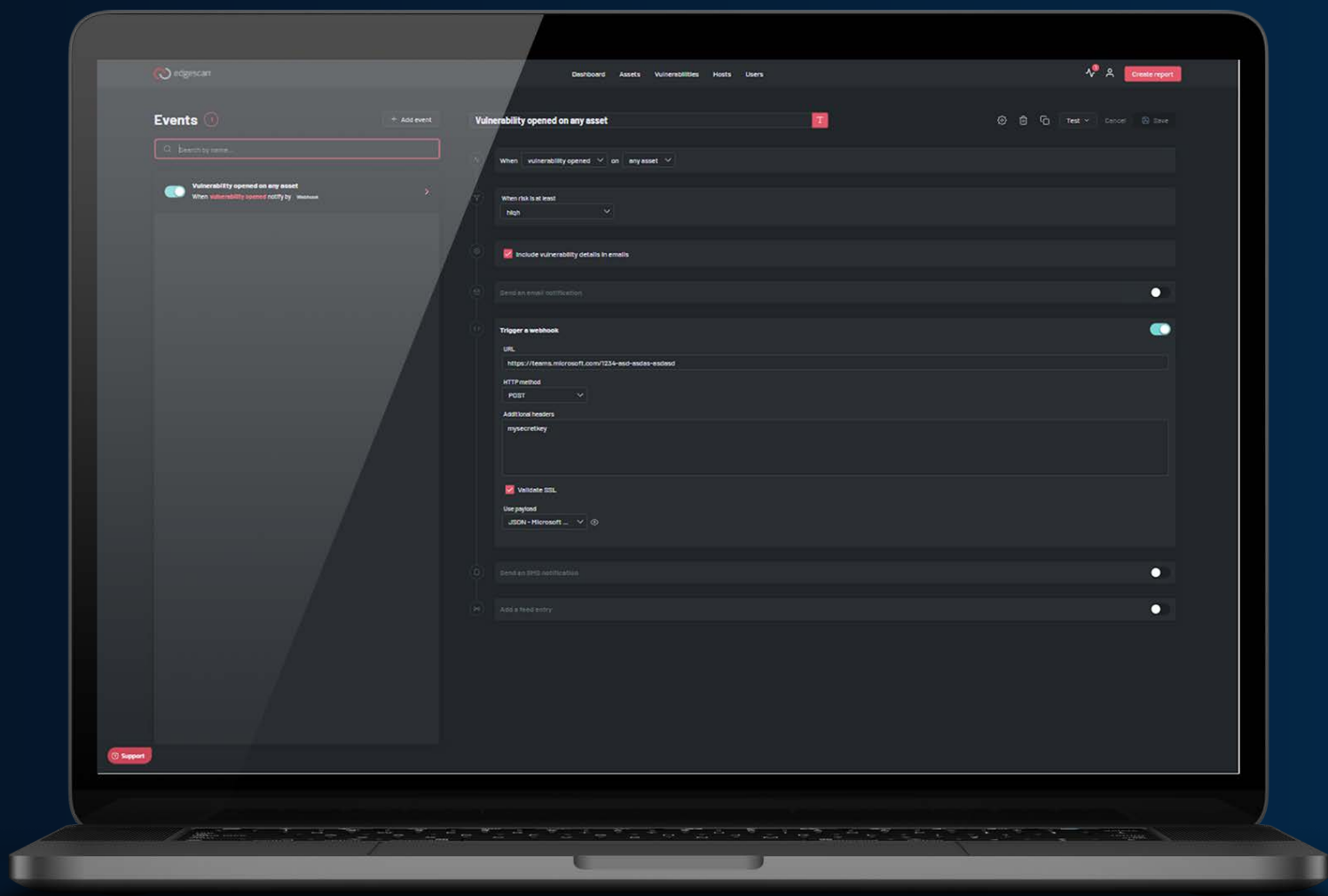
Events & Integrations
Edgescan has introduced a new vital service which is called Events. Using integrations with events allows users and organizations to create live alerts for any changes and to connect the platform into many other services, allowing you to extend the capabilities of your security team

Customer Anecodotes

Skills for Care

The main return on investment that Skills for Care noticed following the commencement of the Edgescan SaaS, was the **time resource saved.**

"Any time the security team had to onboard a new penetration testing provider, it would typically take two members of staff an entire week to collate all the necessary information. With Edgescan, this can be done in seconds. Being a charity with a small security team, this is a huge advantage for the business as whole! The scalability of Edgescan's solution is another advantage – should the Department of Health assign more systems to Skills for Care to use, Edgescan can integrate them immediately and seamlessly into their platform. "

Immedis

After following a robust procurement process, the Edgescan bid came out on top for its **simplicity of use and broad coverage** as well as the willingness to provide a proof of value. The exercise confirmed that Edgescan's claims on having a solution that is virtually free of false positives were not just a sales pitch. The human validation component of the Edgescan SaaS guaranteed Immedis that every single alert was an issue worth investigation.

"It wouldn't be a hyperbole to call them unsung heroes. What they do is excellent, and their product deserves all the praise it receives." - David Quirke, CISO, Immedis.

Customer Anecodotes

CX Index

Continuous vulnerability assessments have made it a lot easier for us to identify gaps or concerns in the security posture of our product offering. The **amount of detail provided** when a vulnerability is detected makes it easy for us to address them quickly. Plus, we can sleep more easily in the knowledge that we are doing our utmost to ensure the data of our customers and their customers is protected!

"Seamless deployment and unparalleled customer service: how Edgescan helped CX Index up their vulnerability management game" David Heneghan, CEO and Co-founder of CX Index

Archroma

Edgescan gives us the peace of mind that comes with knowing that our vulnerability management solution is **virtually false-positive** free. The accuracy that comes with human validation, paired with the efficiency of automatic continuous scanning, means that my team now knows that whenever a vulnerability is flagged, the vulnerability is there, and they can continue working until they find it and fix it.

Glossary

Asset - a web application, an IP network range, mobile application, API, microservice or a CI/CD pipeline

API - Application Programming Interface

CI/CD - Continuous Integration / Continuous Deployment

CVE - Common Vulnerabilities and Exposures

CVSS - Common Vulnerability Scoring System

CWE - Common Weakness Enumeration

DNS - Domain Name System

DOM - Document Object Model

External - Public Internet Facing

FTP - File Transfer Protocol

Internal - Non-Public Internet Facing

MTTR - Mean Time To Respond/Remediate

PCI - Payment Card Industry

PTaaS - Penetration Testing as a Service

RCE - Remote Code Execution

RDP - Remote Desktop Protocol

SNMP - Simple Network Management Protocol

SMTP - Simple Mail Transfer Protocol

SME - Small and Medium Enterprises

SSH - Secure Shell

SSO - Single Sign-On

XML - eXtensible Markup Language

XSS - Cross-Site Scripting

edgescan™

SMART VULNERABILITY MANAGEMENT™

IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

🐦 @edgescan
in @edgescan

Edgescan HQ   **Edgescan New York**
Dublin,   New York,
D15 CH26,   NY 10023,
Ireland   USA