



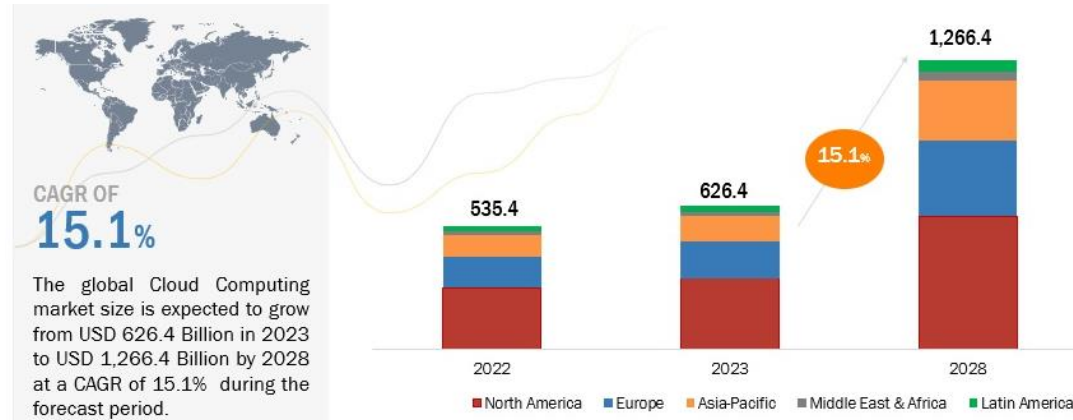
# **Trust Evaluation Based on a Risk Assessment and Game Theory for Virtual Machines in a Cloud Environment**

Victor Morales

[victormoralesavalos@my.unt.edu](mailto:victormoralesavalos@my.unt.edu)

# Problem Definition

- Organizations migrating and adopting cloud computing have changed how the IT infrastructure is managed. According to Markets And Markets this market is expected to growth by 15.1% globally, from \$626.4 Billion in 2023 to \$1,266.4 Billion by 2028. (Markets And Markets, 2023).



Source: <https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html#:~:text=The%20global%20cloud%20computing%20market,17.9%25%20from%202022%20to%202027>

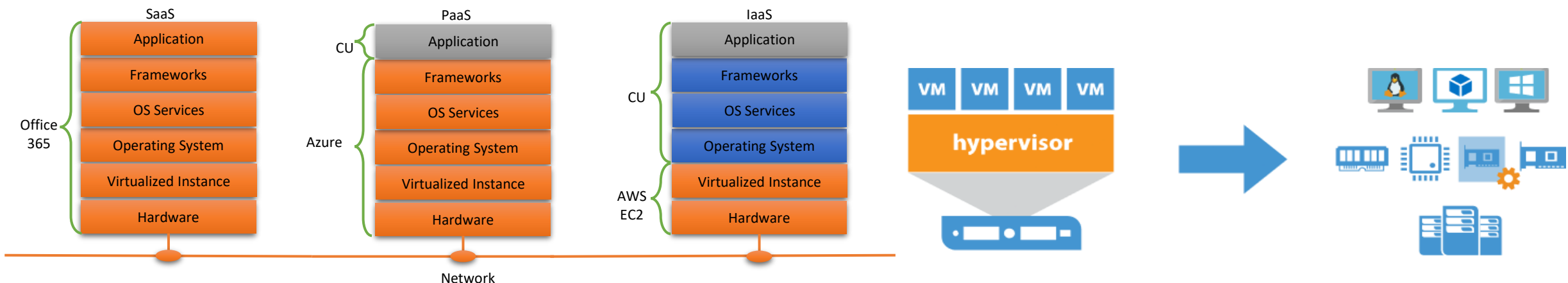
- This introduces security concerns that will need to be addressed, including issues like establishing and preserving Trust of VMs hosted in cloud environments.
- The dynamic environment (migrations, and decommissioning of VMs), will bring a challenges to maintain certain level of trust.
- Cyber threats combine with the dynamic of cloud computing exposed a critical breach to ensure trustworthiness and security.

## • Trust

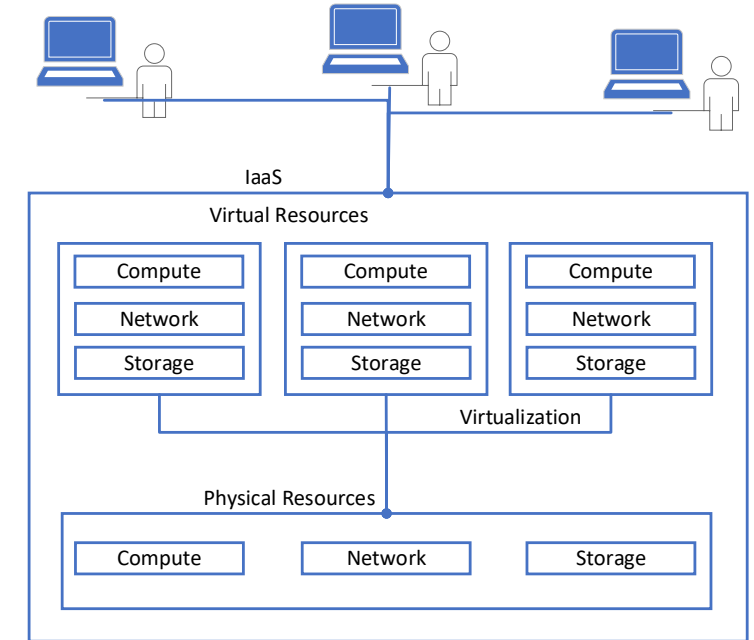
- According the TCG (Trusted Computing Group) trust can be defined as the confidence that an IT device or IT infrastructure will perform according their purpose and specifications.
- Trust quantification.
  - Users feedback, reviews, surveys, SLAs, Frameworks

## • IaaS

- The infrastructure is virtualized and provided as a service
- Consists primarily of network, storage, servers and virtualization layers
- Physical resources are virtualized using a hypervisor before users can access them.

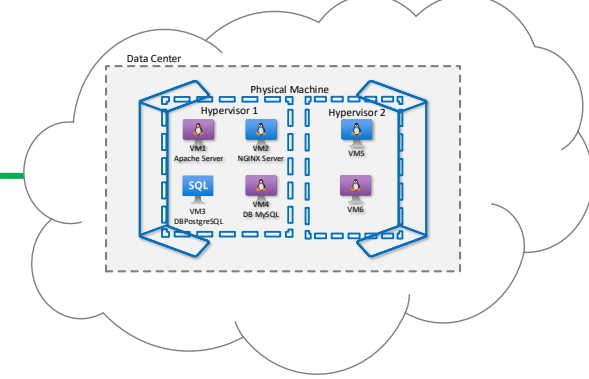
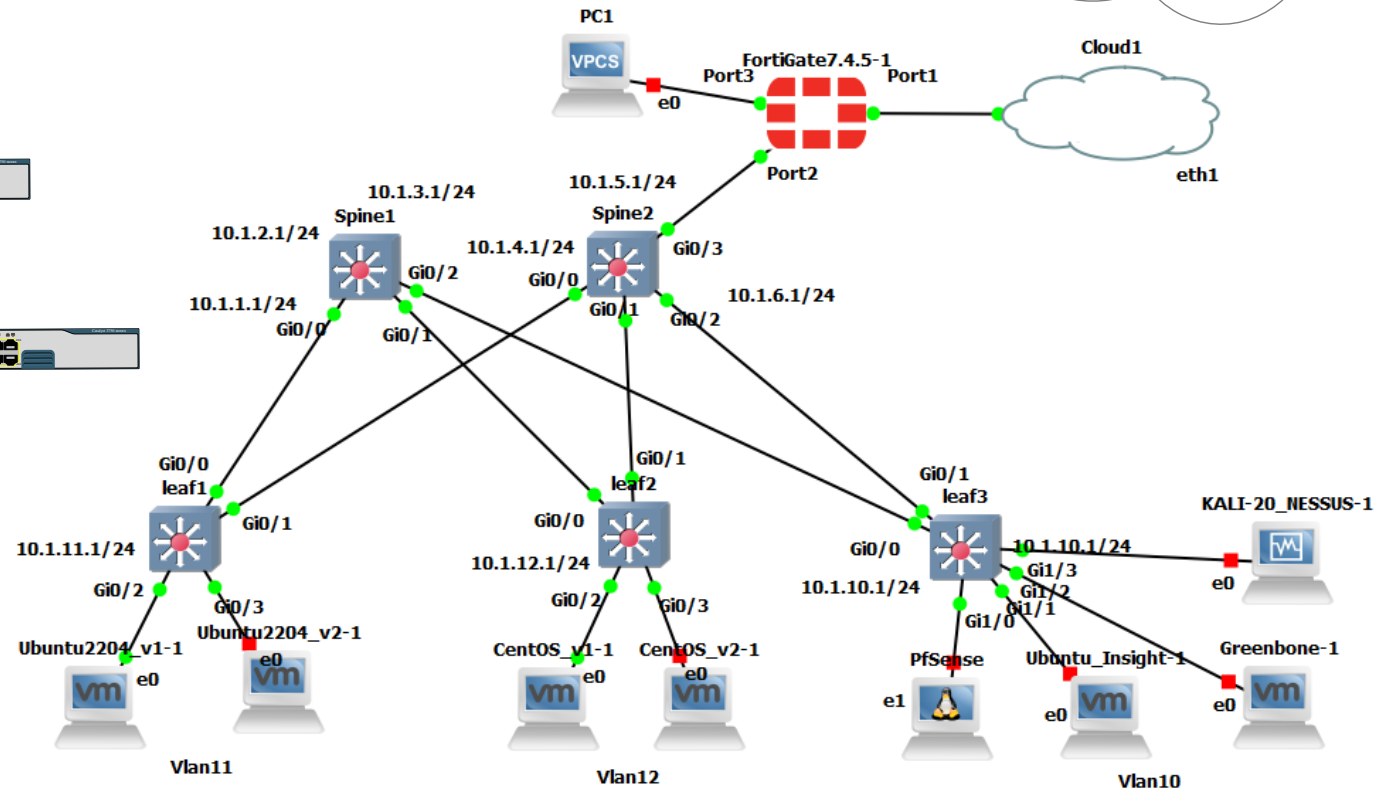
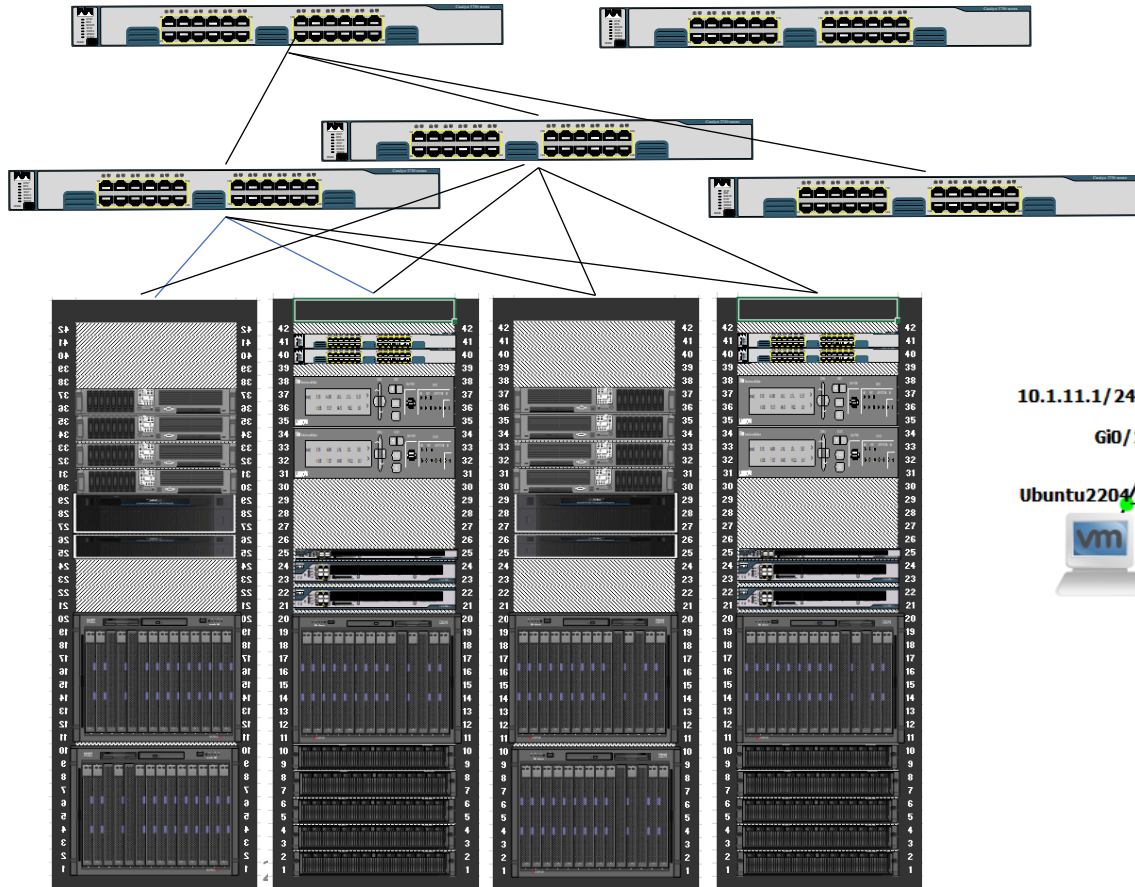


- Virtualization -> ability to emulate hardware via software.
- Hypervisor -> Virtual Machine Monitor/Manager (VMM), the component responsible for emulating specific hardware configurations to guest OS.
  - VM Hardware is emulated hardware via the Hypervisor.
  - Physical Server (Host)
- A hypervisor can contain multiple virtual machines that isolate IT resources from the physical hardware. Still, it has limited storage, memory, processing capacity, and network resources that should be shared between trusted virtual machines.



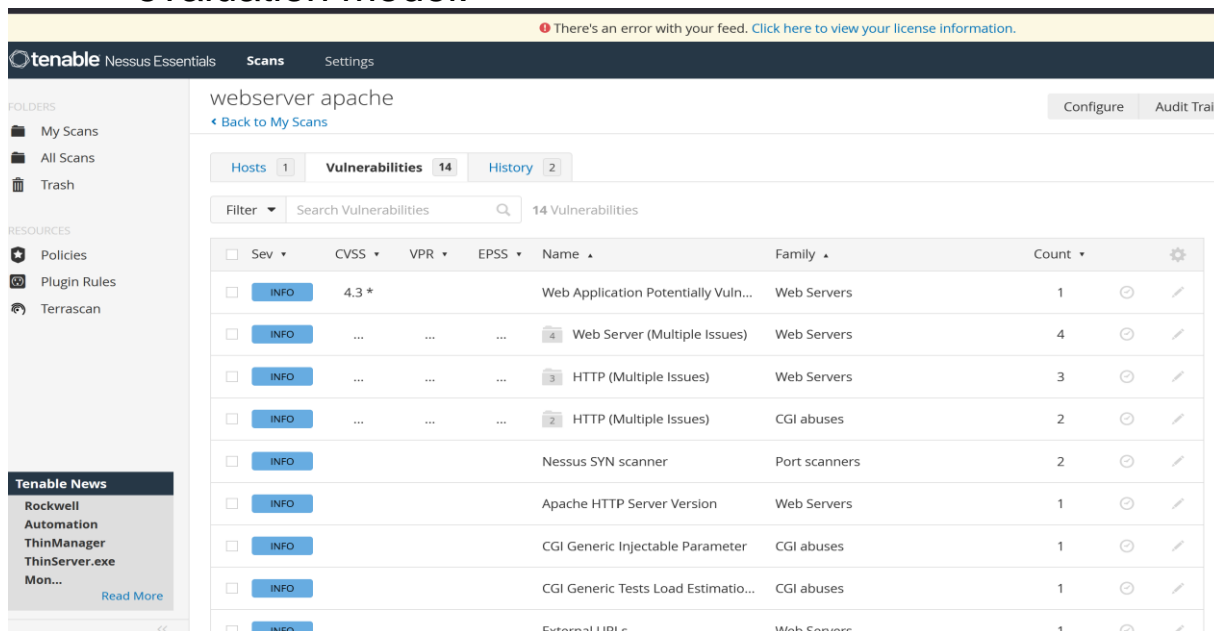
# Approach / Methodology

[video1862752002.mp4](#)



# Collecting the Data - Testbed

- Tools and OS to collect the data:
  - Rapid7, Greenbone, Nessus, Nikto
  - VMs (VMware Workstation (Webserver Ubuntu, Centos, DB server, Ubuntu, Centos))
  - Performed the vulnerability assessment and risk analysis,
  - Incorporated the risk analysis into the Trust evaluation model.



There's an error with your feed. [Click here to view your license information.](#)

**tenable** Nessus Essentials Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

**Tenable News**

- Rockwell Automation ThinManager ThinServer.exe Mon...

Read More

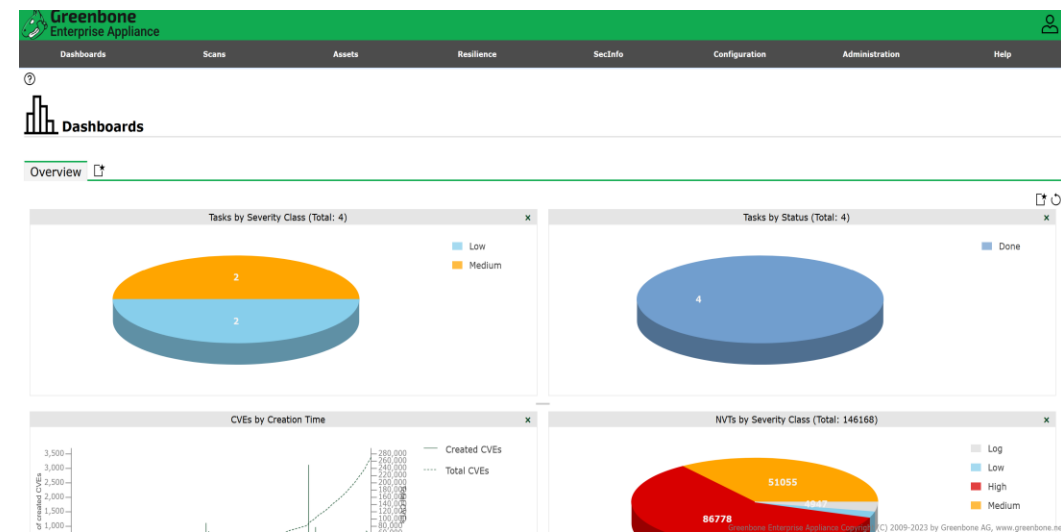
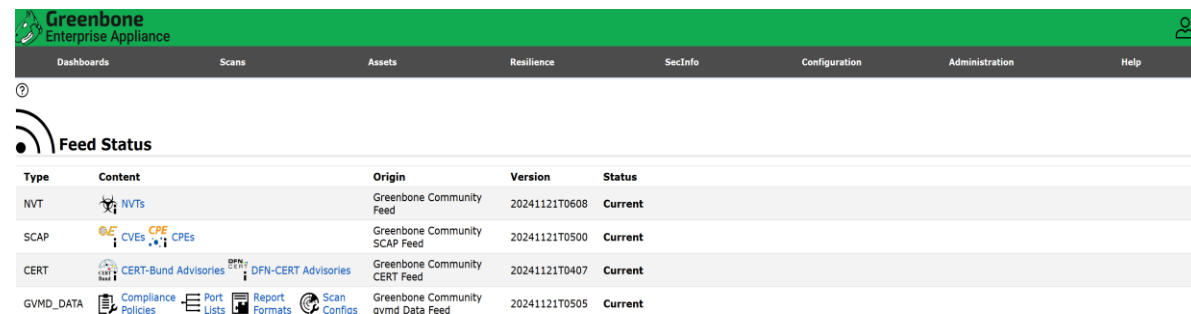
webserver apache

[Back to My Scans](#)

Hosts 1 Vulnerabilities 14 History 2

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO	4.3 *			Web Application Potentially Vuln...	Web Servers	1
INFO	...	...	...	4 Web Server (Multiple Issues)	Web Servers	4
INFO	...	...	...	3 HTTP (Multiple Issues)	Web Servers	3
INFO	...	...	...	2 HTTP (Multiple Issues)	CGI abuses	2
INFO				Nessus SYN scanner	Port scanners	2
INFO				Apache HTTP Server Version	Web Servers	1
INFO				CGI Generic Injectible Parameter	CGI abuses	1
INFO				CGI Generic Tests Load Estimatio...	CGI abuses	1
INFO				External URLs	Web Servers	1

**Greenbone Enterprise Appliance**

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

**Feed Status**

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20241121T0608	Current
SCAP	CVES CPEs	Greenbone Community SCAP Feed	20241121T0500	Current
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20241121T0407	Current
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gymd Data Feed	20241121T0505	Current

# Risk Analysis

- Continue assessment of Risks based on CVSS
- Results comparison.

CVE-ID	Vulnerability type	Vulnerability	Nessus	GreenBone OpenVas	Rapid7	parta/Nikto
CVE-1999-0524	Ubuntu Web Server	ICMP TimestampReply Information Disclosure	X	X	X	
		Web Server Transmits Cleartext Credentials	X			
		Web Application Potentially Vulnerable to Clickjacking	X			X
		Weak MAC Algorithm(s) Supported (SSH)	X	X	X	
		TCP Timestamps Information Disclosure	X	X	X	
		mDNS Detection (Local Network)	X			
		HyperText Transfer Protocol (HTTP) Information	X			
		HTTP server type and version	X			
		Web Application Cookies Not Marked Secure	X			
		Web Server Harvested Email Addresses	X			
CVE-2022-23943		Apache HTTPD: mod_sed: Read/write beyond bounds			X	
CVE-2022-31813		Apache HTTPD: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism			X	
CVE-2022-22720		Apache HTTPD: HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier			X	X
CVE-2022-28615		Apache HTTPD: Read beyond bounds in ap_strcmp_match			X	
CVE-2022-22721		Apache HTTPD: core: Possible buffer overflow with very large or unlimited LimitXMLRequestBody			X	
CVE-2022-28614		Apache HTTPD: read beyond bounds via ap_rwrite			X	
CVE-2022-28330		Apache HTTPD: read beyond bounds in mod_isapi			X	
CVE-2022-26377		Apache HTTPD: mod_proxy_ajp: Possible request smuggling			X	
CVE-2022-29404		Apache HTTPD: Denial of service in mod_lua r:parsebody			X	
CVE-2022-30556		Apache HTTPD: Information Disclosure in mod_lua with websockets			X	
CVE-2022-22719		Apache HTTPD: mod_lua Use of uninitialized value of in r:parsebody			X	
CVE-2022-37436		Apache HTTP Server: mod_proxy prior to 2.4.55 allows a backend to trigger HTTP response splitting			X	
CVE-2023-45802		Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST			X	
CVE-2023-27522		Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting			X	
CVE-2023-31122		Apache mod_macro buffer over-read			X	
CVE-2006-20001		Apache mod_dav out of bounds read, or write of zero byte			X	
CVE-2022-36760		Apache HTTP Server: mod_proxy_ajp Possible request smuggling			X	
CVE-2023-25690		Apache HTTP request splitting with mod_rewrite and mod_proxy			X	
		HTTP OPTIONS Method Enabled	X		X	X
		The X-Content-Type-Options header is not set				X
		No CGI Directories found (use '-C all' to force check all possible dirs)				
		index.php: Uncommon header 'x-redirect-by' found, with contents: WordPress.				X
CVE-2003-1418		Server may leak inodes via ETags, header found with file				X
		index.php/123: Drupal Link header found				X
		wp-content/plugins/akismet/readme.txt				X
		wp-links-opml.php				X
		license.txt				X
		phpmyadmin /: Uncommon header 'x-ob_mode' found, with contents: 1				X
		phpmyadmin/: phpMyAdmin directory found	X			X
		wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag				X
		wp-login.php: Wordpress login found				X



# Risk Analysis – Probability, CIA

- Following ISO27001, and ISO 27005 best practices. I set criteria for how risks are identified, how risks impact confidentiality, integrity, and availability, and how risk impact and likelihood are calculated.

PROBABILITY EVALUATION CRITERIA			
Value	Classification	Percentage	Description
0.9	Certain	81% - 100%	Event is known to occur with some degree of certainty and the recurrence is high.
0.7	Likely	61% - 80%	Event will occur within a period of time that implies action to deal with it, but the recurrence is not high.
0.5	Possible	41% - 60%	The event may occur at a low recurrence
0.3	Unlikely	21% - 40%	Event can occur, the period between one event and another can be
0.1	Very unlikely	1% - 20%	Event never or almost never occurs

INFORMATION EVALUATION CRITERIA					
Value	Classification	Confidentiality	Integrity	Availability	Color Value
0.8	Critical	Unauthorized disclosure of information irreversibly impacts legal compliance, image or operations (very serious damage to the organization)	Unauthorized destruction or modification of information irreversibly impacts operations, competitiveness, legal compliance, profitability or institutional image (very serious damage)	Non-availability of information at the required time considerably irreversible impacts operations, competitiveness, legal compliance, profitability or institutional image (very serious damage).	
0.4	High	Unauthorized disclosure of information seriously impacts legal compliance, institutional image or operations (serious damage)	Unauthorized destruction or modification of information seriously impacts operations, competitiveness, legal compliance, profitability or institutional image (serious damage)	Non-availability of information at the required time seriously impacts operations, competitiveness, legal compliance, profitability or institutional image (serious damage).	
0.2	Medium	Unauthorized disclosure of information considerable impacts legal compliance, institutional image or operations (important damage)	Unauthorized destruction or modification of information considerably impacts operations, competitiveness, legal compliance, profitability or institutional image (important damage)	Non-availability of information at the required time considerably impacts operations, competitiveness, legal compliance, profitability or institutional image (significant damage).	
0.1	Low	Unauthorized disclosure of information partially impacts legal compliance, institutional image or operations (minor damage)	Unauthorized destruction or modification of information partially impacts operations, competitiveness, legal compliance, profitability or institutional image (minor damage)	Non-availability of information at the required time partially impacts operations, competitiveness, legal compliance, profitability or institutional image (minor damage).	
0.05	None	Unauthorized disclosure of information does not impact legal compliance, institutional image or operations (irrelevant)	Unauthorized destruction or modification of information does not impact operations, competitiveness, legal compliance, profitability or	Non-availability of information at the required time does not impact operations, competitiveness, legal compliance, profitability or	

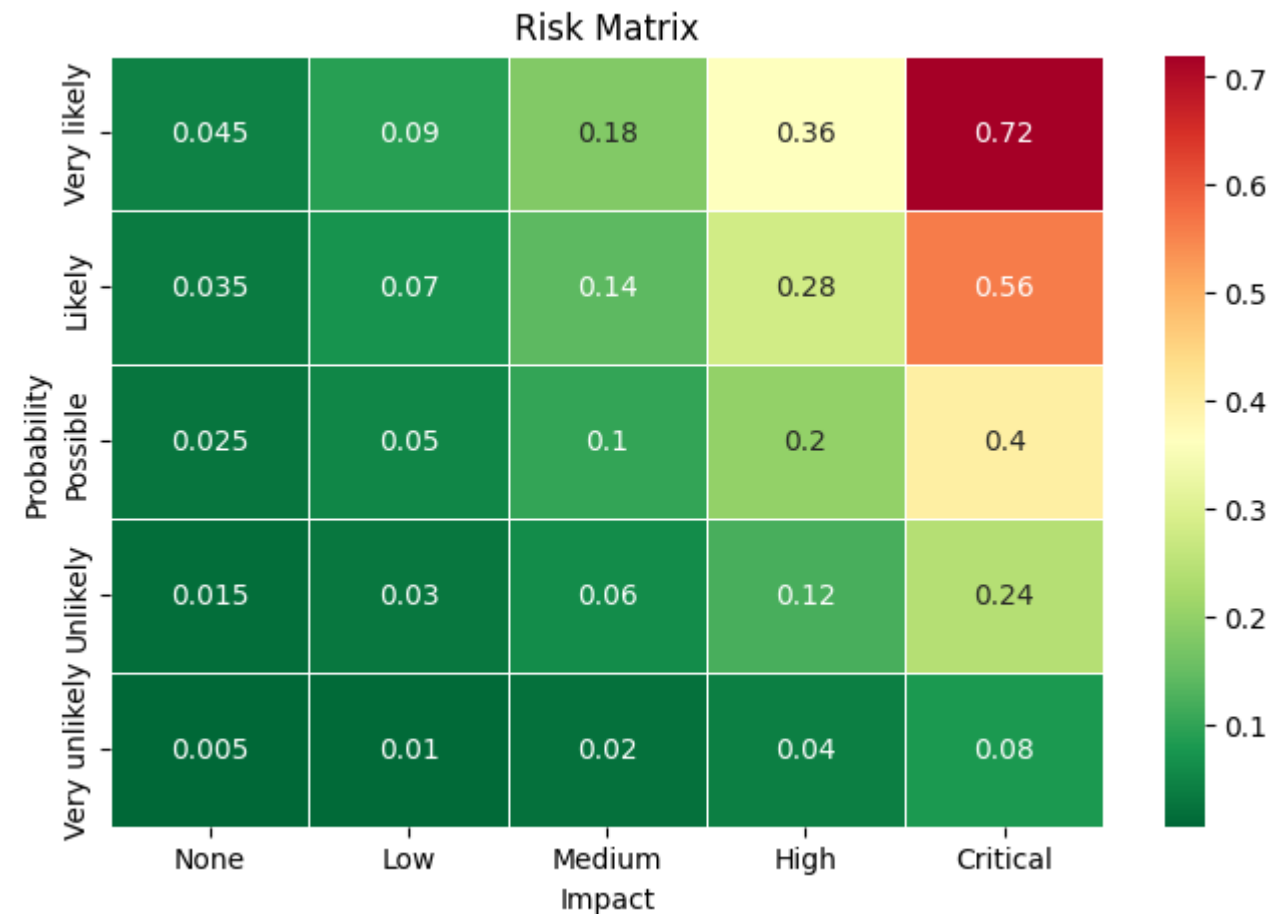


# Risk Analysis

	CVE ID	Base Score	Impact Score	Exploitability Score \
0	CVE-2022-23943	0.75	0.64	0.100
1	CVE-2022-31813	0.75	0.64	0.100
2	CVE-2022-22720	0.75	0.64	0.100
3	CVE-2022-28615	0.64	0.49	0.100
4	CVE-2022-22721	0.58	0.49	0.086
5	CVE-2022-28614	0.50	0.29	0.100
6	CVE-2022-28330	0.50	0.29	0.100
7	CVE-2022-26377	0.50	0.29	0.100
8	CVE-2022-29404	0.50	0.29	0.100
9	CVE-2022-30556	0.50	0.29	0.100
10	CVE-2022-22719	0.50	0.29	0.100
11	CVE-2022-37436	0.53	0.14	0.039
12	CVE-2023-45802	0.59	0.36	0.022
13	CVE-2023-27522	0.75	0.36	0.039
14	CVE-2023-31122	0.91	0.52	0.039
15	CVE-2006-20001	0.75	0.36	0.039
16	CVE-2022-36760	0.90	0.60	0.022
17	CVE-2023-25690	0.98	0.59	0.039

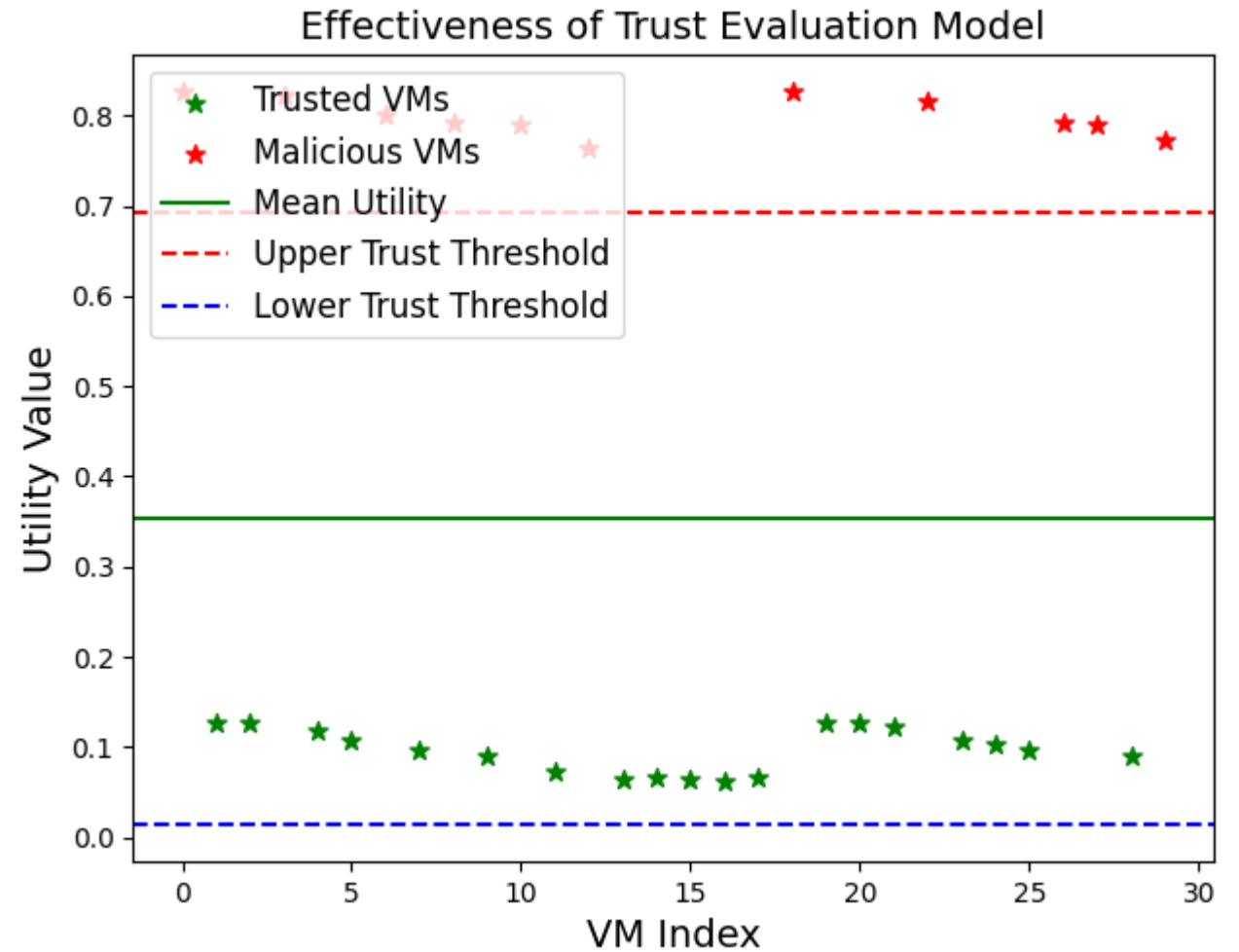
  

	Risk Level	Weight	Category	Smoothed Risk
0	0.252982	0.048000	Critical Risk	0.252982
1	0.252982	0.048000	Critical Risk	0.252982
2	0.252982	0.048000	Critical Risk	0.252982
3	0.221359	0.031360	Higher Risk	0.243495
4	0.205280	0.024441	Higher Risk	0.232031
5	0.170294	0.014500	Higher Risk	0.213510
6	0.170294	0.014500	Higher Risk	0.200545
7	0.170294	0.014500	Higher Risk	0.191470
8	0.170294	0.014500	Higher Risk	0.185117
9	0.170294	0.014500	Higher Risk	0.180670
10	0.170294	0.014500	Higher Risk	0.177557
11	0.073892	0.002894	Tolerable Risk	0.146458
12	0.088994	0.004673	Higher Risk	0.129219
13	0.118491	0.010530	Higher Risk	0.126000
14	0.142408	0.018455	Higher Risk	0.130922
15	0.118491	0.010530	Higher Risk	0.127193
16	0.114891	0.011880	Higher Risk	0.123502
17	0.151690	0.022550	Higher Risk	0.131959



# VM Trust Values and classification

	VM ID	Initial Trust	Initial Risk	Behavior Consistency	Utility	Classification
0	VM_1	0.500000	0.252982	0	0.826491	Malicious
1	VM_2	0.421009	0.252982	1	0.126491	Trusted
2	VM_3	0.313518	0.252982	1	0.126491	Trusted
3	VM_4	0.500000	0.243495	0	0.821748	Malicious
4	VM_5	0.331469	0.232031	1	0.117515	Trusted
5	VM_6	0.393245	0.213510	1	0.106755	Trusted
6	VM_7	0.500000	0.200545	0	0.800272	Malicious
7	VM_8	0.404265	0.191470	1	0.095735	Trusted
8	VM_9	0.500000	0.185117	0	0.792558	Malicious
9	VM_10	0.457165	0.180670	1	0.090335	Trusted
10	VM_11	0.500000	0.177557	0	0.788779	Malicious
11	VM_12	0.474271	0.146458	1	0.073229	Trusted
12	VM_13	0.500000	0.129219	0	0.764609	Malicious
13	VM_14	0.484500	0.126000	1	0.063000	Trusted
14	VM_15	0.434539	0.130922	1	0.065461	Trusted
15	VM_16	0.439307	0.127193	1	0.063596	Trusted
16	VM_17	0.442998	0.123502	1	0.061751	Trusted
17	VM_18	0.434541	0.131959	1	0.065979	Trusted
18	VM_19	0.500000	0.252982	0	0.826491	Malicious
19	VM_20	0.421009	0.252982	1	0.126491	Trusted



Thank you,  
Questions?