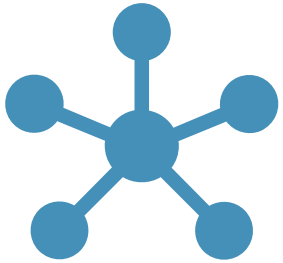
F5- VULNERABILITY PREDICTABILITY COST MODEL

BUSINESS DECISIONS ANALYTICS

NICOLE BERNARD



Network

Data

Bot, DDoS Protection

Multi-Cloud

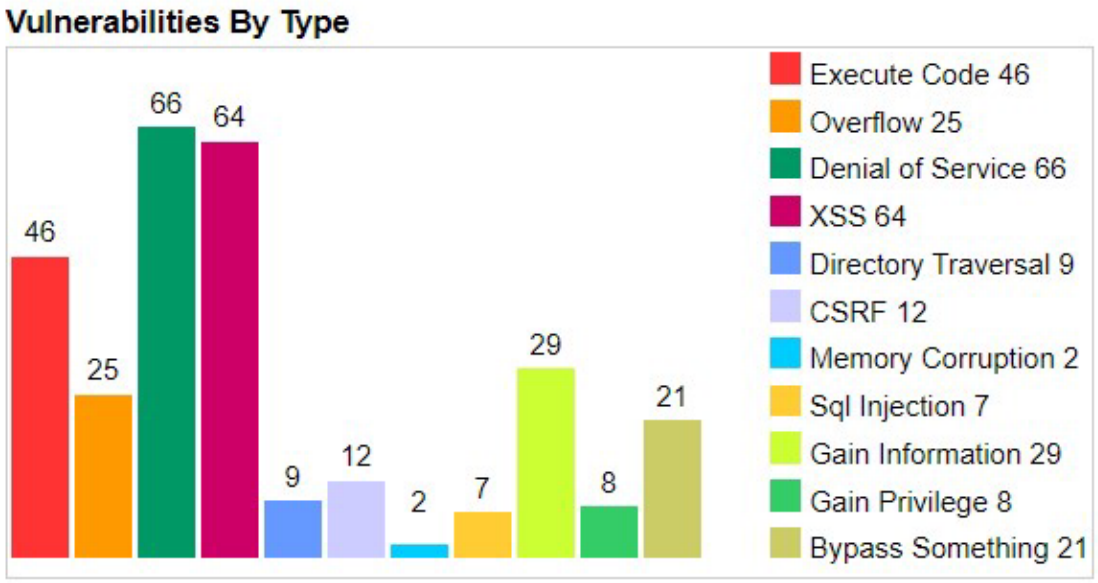
F5- SPECIALIZES IN DELIVERING CYBERSECURITY AND NETWORKING SOLUTIONS THROUGH PARTNERING WITH ENTERPRISES.

VULNERABILITY PREDICTABILITY COST MODEL- METRICS

- CVSS- Common Vulnerabilities and Exposures Scoring System
- EPSS- Exploit Predication Scoring System
- Bug Bounty Cost Assessment

CVE- COMMON VULNERABILITIES AND EXPOSURES

- A CVE stands for common vulnerability and exposure.
- A vulnerability is a weakness to the logic or code in software or hardware components. When exploited it results in negative impact. Mitigation of vulnerabilities includes creating a patch.



CVSS- COMMON VULNERABILITY SCORING SYSTEM

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1		0.00
1-2		0.00
2-3	3	2.90
3-4	5	4.80
4-5	27	25.70
5-6	34	32.40
6-7	17	16.20
7-8	12	11.40
8-9		0.00
9-10	7	6.70
Total	105	

Weighted Average CVSS Score: **6.2**

- CVSS- is a rating for each CVE. There is a rating from 1 (lowest) 10 (Most severe.)
- In 2019 the department of Homeland Security (DHS) mandated that government agencies must report:
  - Vulnerabilities that have a score of **10** must have a patch in 15 days of detection,
  - High severity vulnerabilities those with a CVSS score over 7 there must be a patch within **30** days of detection.

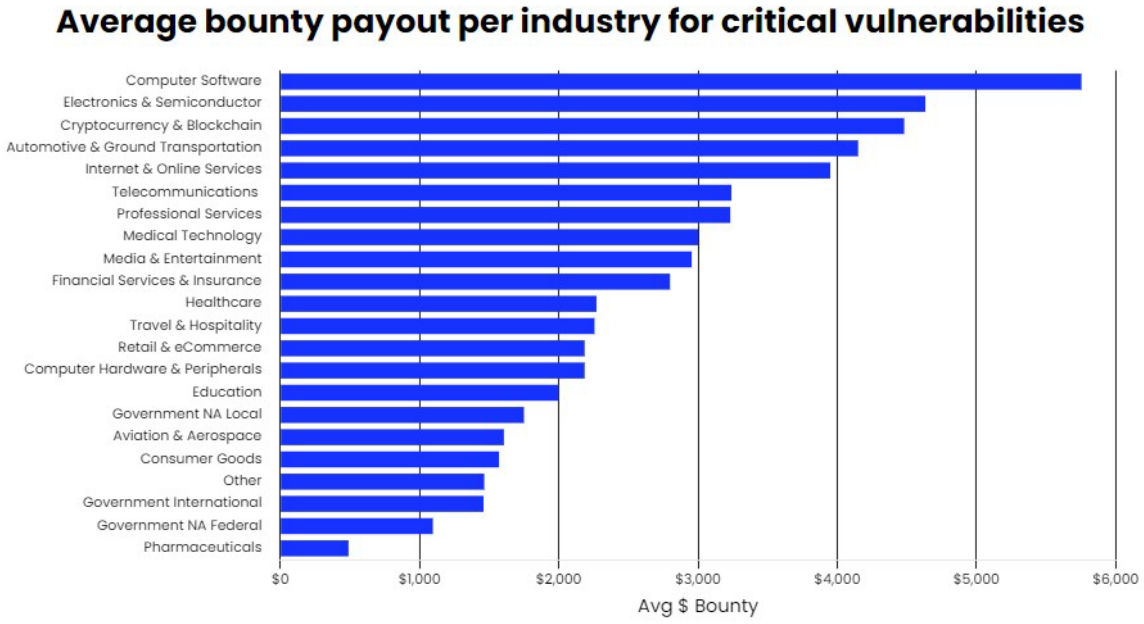
EPSS- EXPLOIT PREDICTION SCORING SYSTEM

- Mike Roytman and Jay Jacobs of Cyentia Institute released a “Exploit Prediction Scoring System (EPSS) model in 2019.
- Based on the machine learning analysis there were 16 significant factors usable to determine predictability.
- By running a log calculation, they could predict the probability percentage of the exploitation in the next 12 months. The higher the probability the higher priority the patch.

Factor	Weight
Is this a vulnerability in a Microsoft product?	2.44
Is this a vulnerability in an IBM product?	2.07
Has vulnerability been weaponized as an attack tool exploit?	2.00
Is this a vulnerability in an Adobe product?	1.91
Is this a vulnerability in an HP product?	1.62
Is there a proof-of-concept exploit for this vulnerability?	1.50
Is this a vulnerability in an Apache project?	1.10
Count of vendor references in the vulnerability	Log(count +1) * 1.01
Does this vulnerability allow arbitrary code execution?	0.57
Can this vulnerability be exploited remotely?	0.23
Does this exploit cause denial of service?	0.22
Does this vulnerability impact web service?	0.06
Does this exploit cause memory corruption?	-0.20
Can this vulnerability only be exploited locally?	-0.63
Is this a vulnerability in a Google product?	-0.89
Is this a vulnerability in an Apple product?	-1.92

BUG BOUNTY COST ASSESSMENT

- A bug bounty is a program put on by a company to pay ethical hackers for finding weaknesses in their networks.
- There are different award amounts for the size of the company and the specific vulnerability.
- To find the cost of each vulnerability type bug bounties gave an estimate of the cost it would take to fix each vulnerability.



MONTE CARLO SIMULATION- F5 VULNERABILITY PREDICTABILITY AND COST

- Vulnerability Probability with EPSS
- Likelihood of event occurrence
- Bug Bounty Cost Assessment

MONTE CARLO SIMULATION

- Includes the CVE ID, Vulnerability Type, critical score, EPSS Score, and Vulnerability Exploration Probability.
- Created the event occurrence to predict the probability that each specific vulnerability would be exploited.

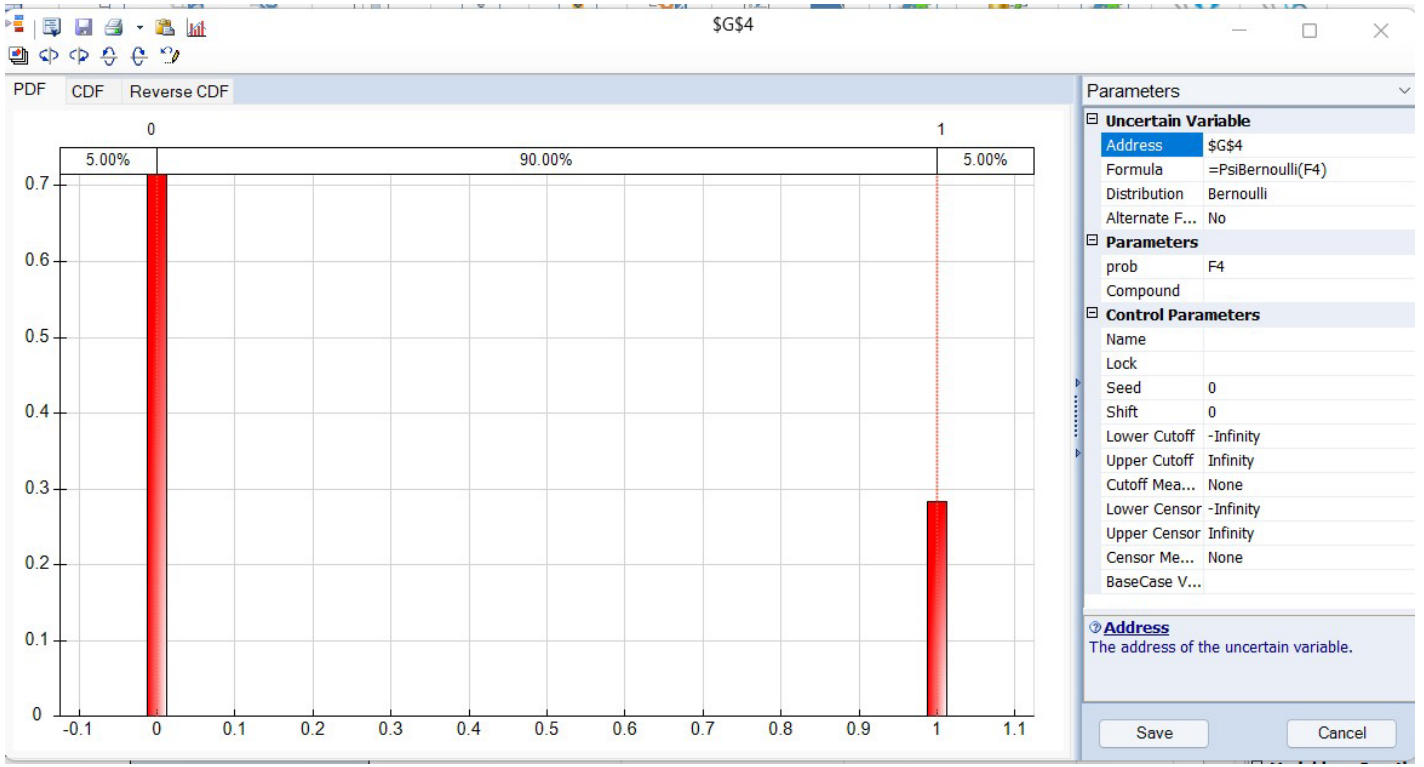
Top 20 Vulnerability Probability

#	CVE ID	Vulnerability Type(s)	Critical Score	EPSS Score	Vulnerability Exploitation Probability	Event Occurrence 1 =Y 0=N
1	CVE-2021-40438	CSRF	6.8	0.36558	99.14%	1
2	CVE-2021-23054	XSS	4.3	0.00442	28.42%	0
3	CVE-2021-2306	SQL Injection	5	0.00416	26.18%	0
4	CVE-2021-2308	SQL Injection	4.3	0.00624	45.88%	1
5	CVE-2021-23123	XSS	7.8	0.0184	76.13%	1
6	CVE-2021-23124	XSS	5.8	0.00416	26.18%	0
7	CVE-2021-23125	XSS	3.5	0.00416	26.18%	0
8	CVE-2021-23126	Overflow	6.5	0.00416	26.18%	1
9	CVE-2021-23127	Execute Code	5.8	0.00416	26.18%	1
10	CVE-2021-23128	CSRF	6.9	0.00416	26.18%	0
11	CVE-2021-23129	XSS	4.3	0.00416	26.18%	0
12	CVE-2021-23130	XSS	5.1	0.00416	26.18%	0
13	CVE-2021-23131	XSS	5	0.00416	26.18%	0
14	CVE-2021-23132	CSRF	5	0.0184	76.13%	1
15	CVE-2021-23133	Execute Code	4.3	0.02678	79.77%	1
16	CVE-2021-23134	Execute Code	6	0.00888	60.12%	1
17	CVE-2021-23135	Execute Code	5	0.00442	28.42%	1
18	CVE-2021-23136	Dir. Trav.	7.5	0.00416	26.18%	1
19	CVE-2021-23139	Gain Information	4	0.06701	91.34%	1
20	CVE-2021-23140	XSS	4.3	0.00416	26.18%	0
					Total	11

BERNOULI DISTRIBUTION FOR EVENT OCCURRENCE

- Calculated the Event Occurrence by using a 1=Yes and 0=No
- Bernoulli distribution was used with a binomial distribution to calculate the predictability of the vulnerability exploitation in 12 months.

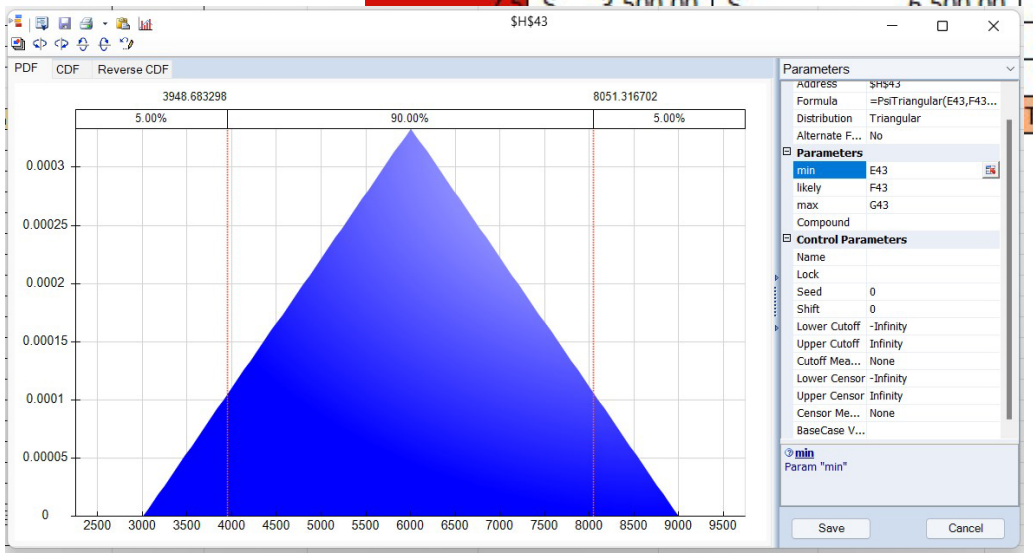
Event Occurrence 1 =Y 0=N
1
0
0
1
1
0
0
1
1
0
0
0
0
1
1
1
1
1
1
1
0
11



TOTAL ESTIMATED COST

- Estimated best, case, and high costs for each CVE by using industry data from bug bounty programs.
- Simulated the information in a triangular distribution to identify the total estimated cost of each vulnerability.

Critical Score	Low Cost	Best Case Cost	High Cost	Total Estimated Cost
6.8	$ 3,000.00	$ 6,000.00	$ 9,000.00	$ 5,797.56
4.3	$ 500.00	$ 1,000.00	$ 1,500.00	$ 1,320.78
5	$ 600.00	$ 900.00	$ 1,200.00	$ 1,122.14
4.3	$ 500.00	$ 1,000.00	$ 1,500.00	$ 948.02
7.8	$ 4,000.00	$ 7,000.00	$ 13,000.00	$ 8,211.55
5.8	$ 1,000.00	$ 2,000.00	$ 3,000.00	$ 1,855.27
3.5	$ 100.00	$ 230.00	$ 350.00	$ 300.16
6.5	$ 4,000.00	$ 6,000.00	$ 10,000.00	$ 7,775.43
5.8	$ 1,200.00	$ 1,600.00	$ 1,800.00	$ 1,284.96
6.9	$ 1,000.00	$ 2,000.00	$ 3,000.00	$ 1,694.74
4.3	$ 500.00	$ 1,000.00	$ 1,500.00	$ 1,006.09
5.1	$ 700.00	$ 900.00	$ 1,200.00	$ 1,034.61
5	$ 600.00	$ 900.00	$ 1,200.00	$ 856.18
5	$ 1,500.00	$ 2,500.00	$ 3,500.00	$ 2,570.54
4.3	$ 500.00	$ 1,000.00	$ 1,500.00	$ 747.63
6	$ 2,000.00	$ 4,000.00	$ 6,000.00	$ 3,921.94
5	$ 900.00	$ 1,200.00	$ 1,500.00	$ 1,084.09
[illegible]	$ [illegible]	$ [illegible]	$ 11,000.00	$ 10,247.03
			$ 1,500.00	$ 620.75
			$ 1,800.00	$ 863.33
Total				$ 53,262.81

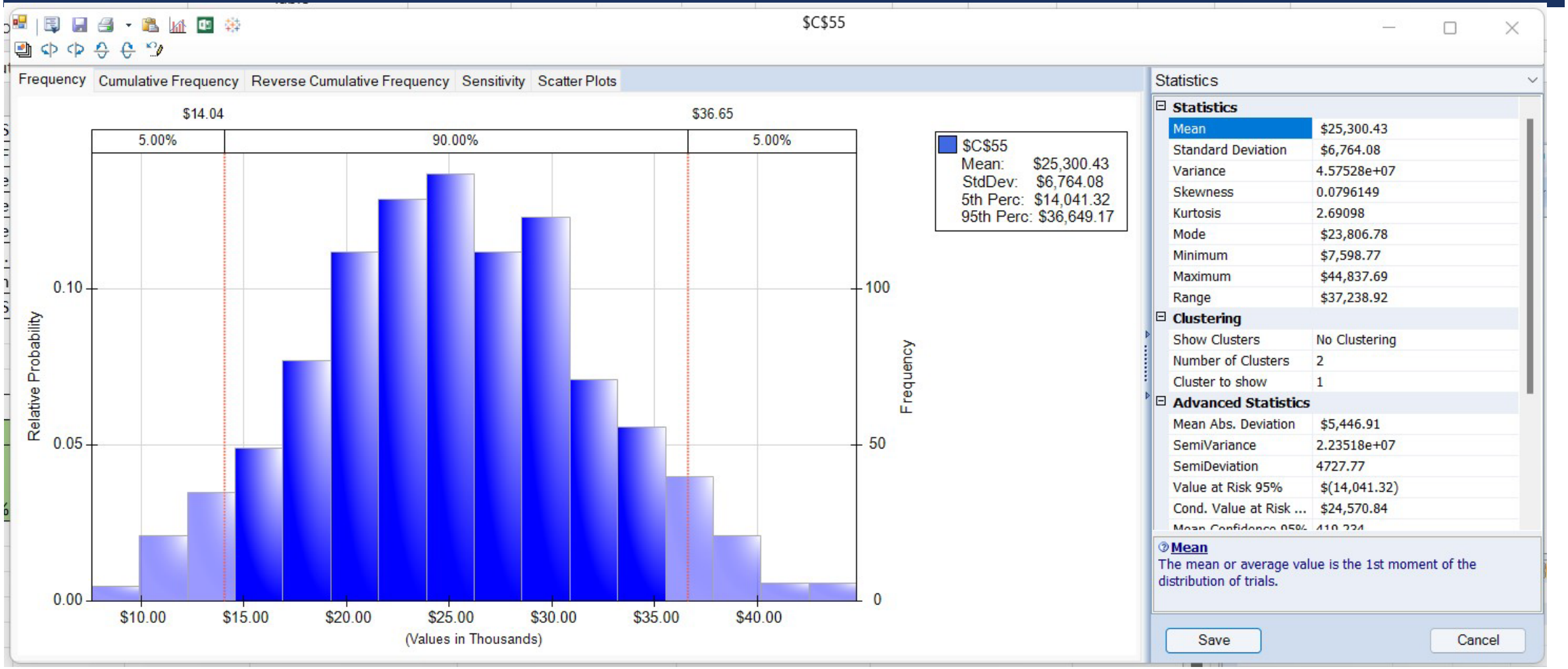


ESTIMATED EVENT COST

- Estimated the event cost by taking the probability of the event occurrence times the total estimated cost.
- Calculated the total Estimated event cost by adding the sum of all the Vulnerabilities in Estimated Event Cost

Event Occurrence 1 =Y 0=N	Total Estimated Cost	Estimated Event Cost
1	$ 4,814.79	$ 4,814.79
0	$ 819.66	$ -
0	$ 887.57	$ -
1	$ 1,028.94	$ 1,028.94
1	$ 9,537.55	$ 9,537.55
0	$ 2,382.48	$ -
0	$ 213.04	$ -
1	$ 5,572.75	$ -
1	$ 1,408.59	$ 1,408.59
0	$ 1,771.21	$ 1,771.21
0	$ 1,170.91	$ -
0	$ 837.73	$ -
0	$ 942.70	$ 942.70
1	$ 2,379.39	$ 2,379.39
1	$ 842.88	$ 842.88
1	$ 5,128.75	$ 5,128.75
1	$ 1,283.85	$ 1,283.85
1	$ 7,084.71	$ -
1	$ 923.81	$ -
0	$ 1,281.62	$ -
11	$ 50,312.93	$ 29,138.64

RESULTS


C55
Frequency
Cumulative Frequency
Reverse Cumulative Frequency
Sensitivity
Scatter Plots
$14.04
$36.65
5.00%
90.00%
5.00%
C55
Mean: $25,300.43
StdDev: $6,764.08
5th Perc: $14,041.32
95th Perc: $36,649.17
Relative Probability
Frequency
0.10
0.05
0.00
100
50
0
$10.00
$15.00
$20.00
$25.00
$30.00
$35.00
$40.00
(Values in Thousands)
Statistics
Statistics
Mean $25,300.43
Standard Deviation $6,764.08
Variance 4.57528e+07
Skewness 0.0796149
Kurtosis 2.69098
Mode $23,806.78
Minimum $7,598.77
Maximum $44,837.69
Range $37,238.92
Clustering
Show Clusters No Clustering
Number of Clusters 2
Cluster to show 1
Advanced Statistics
Mean Abs. Deviation $5,446.91
SemiVariance 2.23518e+07
SemiDeviation 4727.77
Value at Risk 95% $(14,041.32)
Cond. Value at Risk ... $24,570.84
Mean
The mean or average value is the 1st moment of the distribution of trials.
Save
Cancel

RECOMMENDATIONS

- Calculated the Average cost by using the mean of the Estimated Cost.
- Calculated the Average Monthly Cost by dividing the Average Cost Yearly by 12
- Calculated the Vulnerability Probability for each month by taking the Event Occurrence divided by 12
- I recommend that f5 budgets these vulnerability costs into their security budget for the year to increase their security posture.
- The mean is $25,484 of yearly cost for 20 vulnerabilities. The number of vulnerabilities may be up to 100 or more a year.
- The average monthly costs are around $2 -3K

Decisions	
Estimated Cost	$ 23,910.49
Average Cost	=@PsiMean(I48)
Vulnerability Probability for Month	58.33%

Decisions	
Estimated Cost Yearly	$ 18,057.69
Average Cost Yearly	$ 25,484.38
Average Monthly Costs	$ 2,123.70
Vulnerability Probability for Month	50.00%

THANK YOU

NICOLE BERNARD