REFERENCE GUIDE

BLUELAVA

Blue Lava Methodology for determining risk scores across CMM requirements

Overview

To help security teams understand the relationship between risk and maturity, Blue Lava mapped the requirements from our capability maturity model (CMM) to various risk scenarios based on their relevance and importance to calculate a weighted average coverage score specific to the identified risk scenario. This was done using the VERIS (Vocabulary for Event Recording and Incident Sharing) risk model, which drives the widely used Verizon Data Breach Investigations Report, to map our security requirements to the risk scenarios via security objectives and the potential risk impact of the requirement.

The Blue Lava Risk Catalog includes four risk categories that define the Blue Lava risk taxonomy. The format of the Blue Lava-defined categories is consistent with the VERIS framework used by Verizon DBIR.

- Each category includes a fixed number of categorization elements (also referred to as attributes). Each attribute is assigned a unique rating (0 to 4).
- The degree of importance of each attribute is determined according to the rating scale. Weighted average calculation considers the varying degrees of importance of each attribute in a given category.
- A formula is used to compute the risk score for each CMM requirement across all risk events in the Catalog.
- Final risk score is the average of scores computed for each risk category.

Note: The rating values for different attributes are periodically updated to refine scores and to ensure that they represent the latest cybersecurity trends.

Establishing relevance between risk events defined in the Catalog and CMM requirements

Requirement risk score is a decimal value (between 0 and 1) that signifies the applicability of the control outlined in the requirement declaration to a given risk event. The Blue Lava CMM uses the weighted average algorithm to compute the average risk scores per each requirement presented in the CMM framework. Having pre-computed risk scores applied to the assessment results enables effective identification and prioritization of top controls (or countermeasures) that the organization should consider in order to manage applicable cyber risks.

Currently there are four categories included in the risk catalog that defines the Blue Lava Risk Taxonomy:

1. Security objective (Attributes: confidentiality, integrity, security)
2. Asset (Attributes: server, mobile, workstation, database, media, network, user)
3. Actor (Attributes: internal, external, partner)
4. Action (Attributes: malware, hacking, social, misuse, physical, error, environmental)

The format of the Blue Lava-defined categories is consistent with the VERIS framework. VERIS framework provides a set of metrics designed to ensure a common language for describing security incidents in a structured and repeatable manner.

Each category includes a fixed number of categorization elements (also referred to as attributes). Each attribute is assigned a unique rating (0 to 4). Weighted average calculation considers the varying degrees of importance of each attribute in a given category. The degree of importance of each attribute is determined according to the rating scale to the right.

1	Not Applicable
2	Somewhat Applicable
3	Applicable
4	Very Applicable
5	Critically Applicable

To establish the ratings for risk events we worked with a group of security experts who provided attribute ratings for each event in the Catalog (independently). The candidate ratings from the array of multiple values were selected according to the following rules:

1. Objective Category (C/ A/ I):
    - when only 1 of 3 properties is rated, then choose the smallest value
    - when 2 of 3 properties are rated then each of them should be rated 3 (for example: 3/0/3)
    - when 3 properties are affected then each one should be ranked as 2 (2/2/2)

2. Asset & Action Categories: choose the smallest value in the range

3. Actor Category: apply 2/4/1 ratio (per DBIR data: the split is roughly 20% / 75% / 5%)

Next, the candidate values were refined by Blue Lava according to various metrics from DBIR 2020/21 reports (VERIS datasets), and other sources.[1]

Once the rating values are established, the following formula is used to compute the risk score for each CMM requirement across all risk events in the Catalog:

$$W_c = \frac{\sum_{i=1}^{n} R_i * E_i}{\sum_{i=1}^{n} E_i}$$

where:

n	is the number of attributes in a given category to be averaged
E	is the attribute ratings defined for each risk event in the Risk Catalog
R	is the attribute ratings defined for each CMM requirement
C	denotes a Category (Objective, Asset, Actor, Action)
Σ	denotes the sum

Final risk score is the average of scores computed for each risk category:

$$W_R = \text{average}(W_{objective} , W_{asset} , W_{actor} , W_{action}) / 4$$

The rating values for different attributes are regularly updated to refine the risk scores and to ensure that they represent the latest cybersecurity trends.

Example

How computing risk score algorithm is calculated:

E.001 Account Takeover Fraud	risk ratings	attribute	req ratings	6017358d-8249-4b3a-ae1b-765790afdf2a Applications are re-scanned after patching to ensure successful patch implementation
If the %risk.event% occurs, it may have an impact on the %attribute.CIA%	2	Confidentiality	3	The control outlined in the %requirement% can help to avoid having %attribute.CIA% compromised
	3	Integrity	3	
	3	Availability	3	
A cyberattack could be performed by the %actor%	2	Internal	3	The control outlined in the %requirement% can help to protect %asset% from being compromised by the %actor%
	4	External	3	
	1	Partner	3	
The %risk.event% may emerge through the attack on the %asset%	2	server	2	The control outlined in the %requirement% can help to improve the security of the %asset% during cyberattack
	2	mobile	0	
	2	workstation	0	
	3	application	4	
	0	network	0	
	0	media	0	
	0	database	3	
	4	user	0	
In order to perform this cyberattack, the %actor% could leverage the %action%	4	malware	4	The control outlined in the %requirement% can help to prevent or detect the %action% or reduce losses caused by the %risk.event%
	4	hacking	4	
	4	social	0	
	0	misuse	2	
	0	physical	0	
	0	error	1	
	0	environmental	0	

weighted.score.objective	3.00000
weighted.score.actor	3.00000
weighted.score.asset	1.23077
weighted.score.action	2.66667
Requirement score for risk event E.001	**0.61859**

Example of computing risk score

[1]Sources

2018. Trustwave. Global security report
2019. Forescout. The Role of Cybersecurity in M&A Diligence
2019. Herjavec Group. Official-Annual-Cybercrime-Report
2019. ZeroFox. Financial Services Digital Threat Report
2020. Akamai. State of Internet Security
2020. Checkpoint. Cyber Security Report
2020. Corero-Juniper. DDoS threat intelligence report
2020. Debate Security. Cybersecurity Technology Efficacy Research Report
2020. F5 Labs. Phishing & Fraud Report
2020. IC3. Internet Crime Report
2020. Kaspersky. Security Bulletin
2020. McAfee. The Hidden Costs of Cybercrime
2020. Netwrix. Data Risk Security Report
2020. NIST. Cybersecurity and Privacy Annual Report
2020. PWC. Cyber Threats. A Year in Retrospect
2020. SIFT. Account Takeover Fraud
2020. VMWare. Modern Bank Heists 4.0
2021. Accenture. Cyber-Threat-Intelligence-Report
2021. Arkise Labs. State of Fraud Report
2021. Checkpoint. Cyber Security Report
2021. EUROPOL. Internet Organised Crime Threat Assessment
2021. ITRC. Data Breach Report
2021. Kaspersky. Incident Response - Analyst Report
2021. McAfee. Advanced Threat Research Report
2021. Microsoft. Digital Defense Report
2021. NexusGuard. DDoS Threat Report
2021. Osterman research

BLUELAVA

Blue Lava empowers you to effectively communicate priorities, needs, recommendations and results to your larger community of business and finance stakeholders, pivoting from reactive to proactive decision making. Communicate security program results and needs to business stakeholders with consistency and ease.