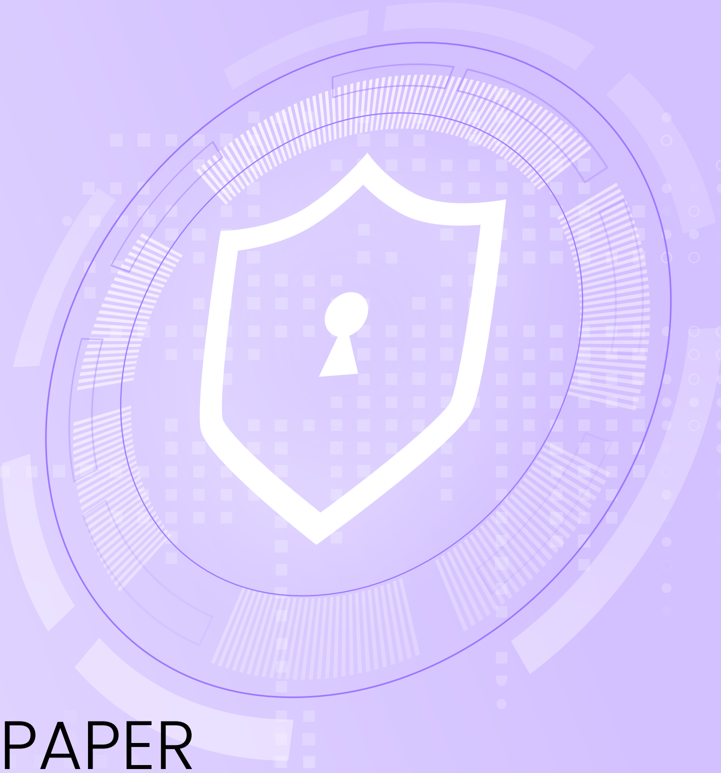
letsbloom



WHITE PAPER

Cyber Security Risk Management

Value at Risk (VaR) Assessment

INTRODUCTION

Value at Risk (VaR) is an essential statistic in risk management that allows an organization to predict the greatest possible losses over a specific time frame. It is a widely used metric across risk types within the organization.

The calculation of VaR requires 3 key input variables, namely period, confidence level and size of possible loss. Amongst these, calculating the size of possible loss is the most difficult. While its use in financial and market risk assessment can rely on historical data to predict the variability of the markets and estimate the size of possible loss over a given period, the same does not always hold true when used in Cyber Security Risk Assessment.

Simplistically, the size of possible loss from a cyber security event depends on the likelihood of the event and the impact it has on the assets at risk. Organizations often use qualitative measures while calculating the likelihood and impact of a cyber security event which reduces the effectiveness of VaR calculated in predicting the risk.

How to track structurally and in an automated manner the security value at risk quantitatively
(Instead of the typical balanced scorecard like approach using a qualitative likelihood/impact assessment)?

An effective framework for likelihood and impact assessment for cyber security events involves:

Asset Identification: Start with identifying the key assets (crown jewels) that are in scope for the risk assessment. The key here is to identify and group all related assets into an easily trackable unit for which you can apply the next steps. This often means having a way to identify all assets for a given workload and using a workload-specific approach for risk assessment.

Threat & Vulnerability Assessment: Perform a targeted attack surface analysis for the workload and identify vulnerabilities, possible attack vectors for exploitation and current threats (using threat intelligence). These factors can then be combined for threat-based risk assessment and prioritization which can inform the likelihood of a cyber security event.

Impact Assessment: Determine the potential impact of a successful cyber security event for the organization including financial losses, operational disruptions, reputational damage, regulatory fines, and legal liabilities.

Calculate VaR & Conduct Sensitivity Analysis: Calculate VaR using the inputs and conduct sensitivity analysis to identify which threat vectors and risk factors have the maximum impact on the overall risk posture.

Continuous Monitoring: Targeted attack surface analysis, vulnerability and threat assessments are ongoing activities and should continuously feed into the calculation for likelihood assessment which in turn allows for ongoing VaR calculation.

Which metrics can we track to assess continuously the security value at risk (e.g. for daily/weekly/ monthly reporting and analysis)?

As mentioned in the framework above, the key metrics to track are:

- **Automated Asset Tracking:** Continuously track asset changes for the cloud workloads including changes in source infrastructure-as-code (IaC), application deployment packages (e.g., container or OS images, app packages) and the deployed cloud resources.
- **Automated Threat and Vulnerability Assessment:** Monitor the cloud workload for vulnerabilities and threats from misconfiguration, CVEs (including zero-days), and exploitable attack paths using workload context-specific analysis.
- **Automated Attack Surface Analysis:** Continuously monitor the identified workloads' attack surface to detect and assess any changes in the exploitable attack vectors.
- **Threat Identification & Likelihood Assessment:** Use threat intelligence feeds to identify active threats and use the results of vulnerability assessment and attack surface analysis to identify the likelihood of a threat being exploited against the specific workload.

How to build structural feedback/improvement loops for security (e.g. genAI-based identification or protection, semi-automated learning from attack attempts)?

Enabling continuous observability for cloud environments and performing automated assessments as mentioned above allows an organization to build automated and self-learning feedback loops that improve likelihood analysis of future cyber security events.

Continuous automated monitoring will allow the system to detect patterns in different types of vulnerabilities and misconfigurations that open exploitable attack paths in cloud workloads. Real-time threat intelligence feeds will allow the system to map attack vectors to active exploits to enable threat-based risk prioritization.

The use of cyber security-specific AI models will accelerate this feedback loop. However, existing general-purpose GenAI models may not be ideal, and this requires purpose-specific model development.

LETSBLOOM ADVANTAGE

Using letsbloom platform's continuous security and compliance observability for cloud cyber security risk assessment allows organizations to:

- ✓ **Identify, categorize, and tag all relevant assets** for a workload using workspaces to allow workload-specific risk assessment.
- ✓ **Use our context-specific actionable intelligence (CSAI)** to perform workload-specific automated attack surface analysis, vulnerability assessment, and threat detection. letsbloom automatically detects and categorizes vulnerabilities in a cloud workload (using MITRE ATT&CK framework) and perform contextual identity and entitlement analysis to identify exploitable attack paths.
- ✓ **Leverage letsbloom risk assessment engine** to integrate threat intelligence with context-specific actionable intelligence and automate the likelihood assessment for cyber security events through a risk score that can be directly used in VaR calculation.