

Continuous Risk & Vulnerability Assessment (CORVA)

Uncovering Your Vulnerabilities Always



Cybersecurity Landscape

In today's digital world, change is the new constant. The conventional way of performing vulnerability assessment and penetration testing (VAPT) yearly or even monthly is no longer sufficient to outwit cyber attackers. These adversaries now daunt cyber defenders to secure their organisations, from the Information Technology (IT) to the Operational Technology (OT) environment.

Continuous and automated testing is the key to combat evolving threats.

Survey with Security Professionals

70% 

recognised the need to validate security controls frequently against evolving threat tactics.

61% 

said continuous validation is needed to identify new gaps from constant changes in IT architecture.

59% 

acknowledged with constant change to security implementations, continuous testing is a priority to identify risk exposure from human error.

Source: ST Engineering, Breach & Attack Simulation, 2021

Conventional VAPTs No Longer Sufficient

Usually, cybersecurity professionals would manually conduct VAPT regularly to identify and mitigate cybersecurity risks across an organisation’s IT environment. Reports generated are applicable at the point of time the tests are conducted and vulnerability scanning tools can only identify single points of failure.

With the dynamic nature of cyber-attacks, these conventional VAPTs are no longer sufficient in addressing evolving threats swiftly. It is essential to have 24/7 visibility of your organisation’s security posture and the ability to prioritise remediation steps to protect key assets across environments, such as the Cloud, IT and OT infrastructures.

Challenges of Conventional Security Assessment



Complex Processes

- Assess complex systems and networks effectively



Human Intensive

- Need for skilled experts
- Possibility of human errors



Regulatory Compliance & Audit Requirements

- Fulfill the requirement to regulatory compliance and audit requirements





Outdated Assessment Outcomes

- Impossible to conduct manual risk assessment and VAPT continuously
- Adapt to changes in infrastructure

INTRODUCING CORVA

Continuous Risk & Vulnerability Assessment (CORVA) is one of the advanced cybersecurity solutions offered in our managed security services (MSS).

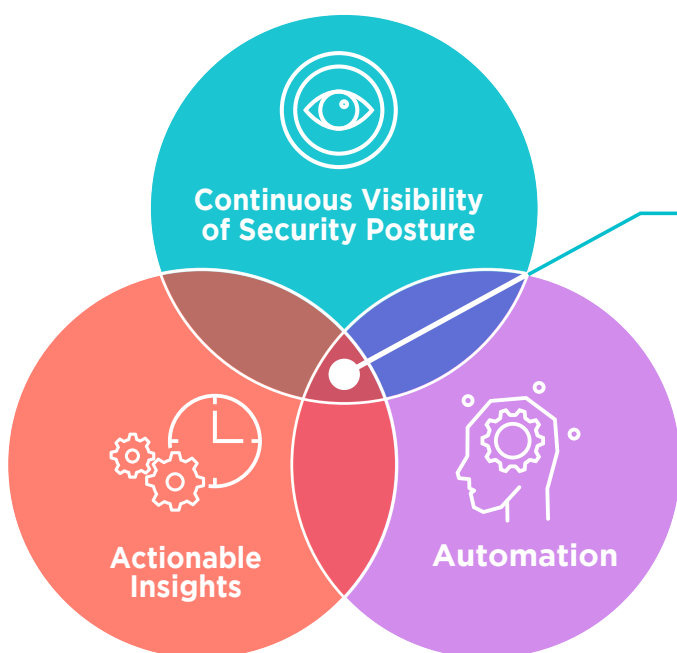
Unlike the usual security assessment,

-  Tedious processes of conventional security assessments are automated.
-  Real-time risk assessments are continuously conducted 24/7 across environments such as the cloud, IT and OT networks.

CONTINUOUS ATTACK SIMULATIONS



By simulating realistic techniques of attack vectors, the platform-as-a-service helps identify the latest vulnerabilities in enterprises' environments and increases the visibility to their security posture. Prioritised remediation steps are also provided, enabling enterprises to protect their key digital assets and maintain cyber resilience proactively.



What CORVA can help your organisation achieve:

- Plug the resource gap
- Leverage automation to optimise expertise and resources

How it Works




Protection of Key Digital Assets

Intelligence output from CORVA is used to trigger threat hunting activities. A hunt team can use the information about active threat groups and latest relevant breaches to identify active or past compromise. This is essential to help identify critical areas of compromise and protect key digital assets in the organisation.



Identification of Vulnerabilities Across Environments

CORVA also helps identify and prioritise threats based on likelihood and impact of the compromise. Environmental context around vulnerabilities and loopholes are also provided. With these information, Incident Response (IR) can rapidly contain breaches and repeated compromises.



Prioritised Remediation Guidance

CORVA provides prioritised remediation guidance and actionable insights, informing IT teams of the types of blocks or monitoring that need to be in place to stop threats. IT teams no longer need to fear the endless patch cycles and can use this information to inform patch and upgrade priorities.

With CORVA, organisations are empowered to take a proactive stance to maintain cyber resilience.

Optimum Expertise & Efficiency with Automation

Identifying possible attack paths can be challenging. With CORVA, your analysts will be able to simulate any attack scenario with ease. The platform shows what will happen in the event of a successful breach, the type and amount of information at risk. CORVA automates these attack scenarios, empowering your organisation to be more efficient in identifying and preventing possible malicious activities.

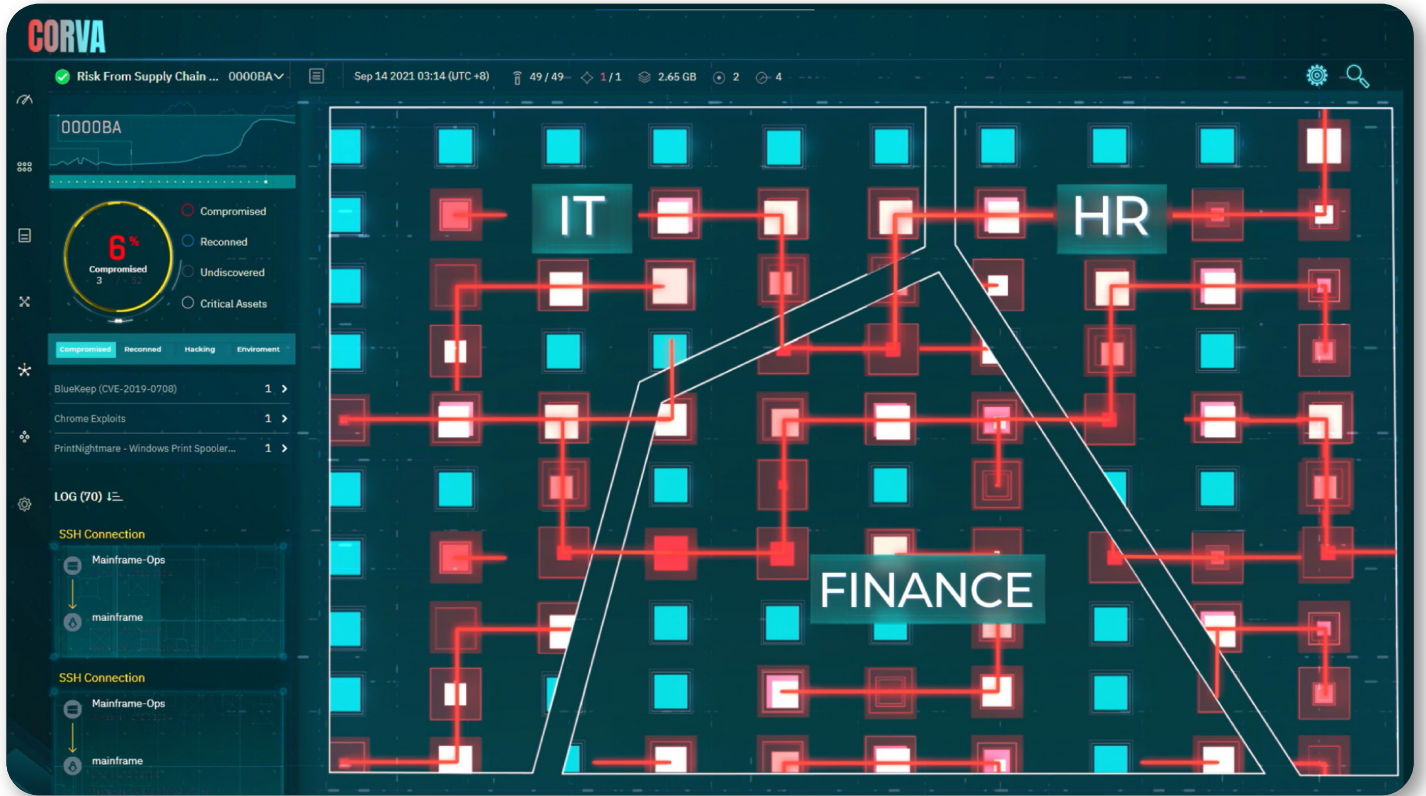
Full Visibility to Organisation's Security Posture

Acting as a virtual hacker, the platform shows all possible attack paths from a machine that is compromised, including hybrid attacks moving from on-premise devices to cloud-based assets.

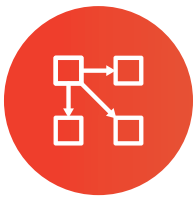
Unlike simplistic cyber-attacks of the past, lateral movement attacks are difficult to detect and stop. By constantly examining your organisation's environments for weaknesses, it helps your team identify vulnerabilities in service and domain accounts that are open to exploitation, and local or key configurations that would allow attackers to move with ease.

Key Features

DASHBOARD



The CORVA dashboard gives full visibility of the cybersecurity posture of organisations in real-time.



Attack Path Visualisation

- Automated generation of the network map of assets with possible attack paths in a chronological manner.
- Allows security teams to drill down on critical asset discovery or identify exact attack techniques and paths used by virtual hackers.

Comprehensive Up-To-Date Attack Scenarios

- 24/7 continuous running of multiple and simultaneous attack scenarios, to improve security posture.
- Latest hackers' techniques and methods used, such as the MITRE ATT&CK framework.

Flexible Architecture

- Quick and easy deployment to existing or new organisation's architecture for on-premise or in the cloud.



Vulnerabilities are identified across different environments and users can easily access prioritised remediation guidance to achieve greater cyber resilience.

DASHBOARD — Overall Security Posture

Utilising the concept of a choke point, the platform also identifies assets that will affect other assets. By eliminating the choke point or the vulnerability of that one asset, the risk to the entire network will be greatly reduced.

CORVA identifies the exposure of your organisation, from misconfigurations, open credentials, poor user behaviour, to other vulnerabilities caused by poor IT hygiene.



Critical Assets Identification

- Identification and prioritisation of critical assets, according to potential impact.
- Prioritisation improves investigative process, allowing customers to fully understand how adversary might move laterally and compromise critical assets.



Choke Points Identification

- Identification and prioritisation of top choke points that can cause greater risk for remediation.



Security Score

- Provides insight on organisation's overall security posture.

The screenshot displays the 'Aggregated System Report' for 'Domain Credentials'. It features a sidebar with navigation options like 'Attack Techniques', 'Entities at Risk', and 'Entities Impact'. The main content area is divided into three sections:

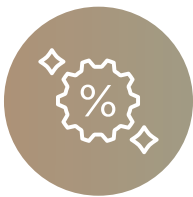
- Summary:** Shows 31 Affected Entities, 0 Choke Points, and 25% Critical Assets at Risk. It also includes 'Complexity' (Low) and 'Severity' (High) indicators.
- Technical Details:** Provides a description of the risk and lists 7 MITRE Technique Alignments (T1021, T1075, T1097, T1175).
- Table of Affected Entities:**

Name	Type	Critical Assets at Risk
Hugh	Windows	0
Fred	Windows	0
Ted	Windows	0
Joe	Windows	0
SWIFTServer	Windows	0
Victoria	Windows	0
- Remediations (12):** Lists 12 actionable steps, such as 'Prevent the credential from being stored in the machine memory' and 'Enable Protected Process Light for LSA', each with a 'Remediation' button.

System reports are generated in CORVA. Remediation steps and actionable insights are provided to execute and mitigate risks in the organisation's systems and networks effectively.

SYSTEM REPORTS — Prioritised Remediation Steps

In the platform, the security team is also able to easily access prioritised remediation steps and actionable insights to mitigate risks and vulnerabilities, empowering them to focus on the most critical assets.



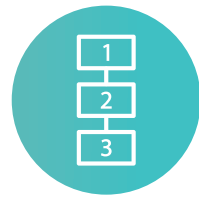
Critical Assets Weighted Scoring

- Weighted scoring for risks of individual assets.
- Machines marked as "high value" by the threat and vulnerability management module will receive more weightage in the score calculation.



Evaluation of Risk of Critical Assets

- Evaluates the severity and risk of critical assets.
- Provides security team with ability to answer with a simple "Yes" or "No" on whether a business-critical asset is susceptible of a breach.

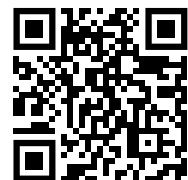


Prioritised and Actionable Insights

- Prioritises actionable insights based on critical ratings.
- Empowers security team to focus on critical issues.
- Expedites entire exposure, assessment and remediation cycle.

ST Engineering Info-Security Pte. Ltd.
cybersecurity@stengg.com

© 2022 ST Engineering Info-Security Pte. Ltd. All rights reserved.



www.stengg.com/cybersecurity