



Harmony Purple

An Automated Continuous Threat Exposure
Management (CTEM) Platform

Updated by August 2023

Copyright

Copyright ©2023 by Orchestra Group Ltd. All Rights Reserved.

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

No part of this document may be reproduced in any form for any purpose without the prior written permission of Orchestra Group Ltd.

The Orchestra Group Ltd logo and all Orchestra Group Ltd product and service names listed herein are either registered trademarks or trademarks of Orchestra Group Ltd or its subsidiaries. All other marks are the property of their respective owners.

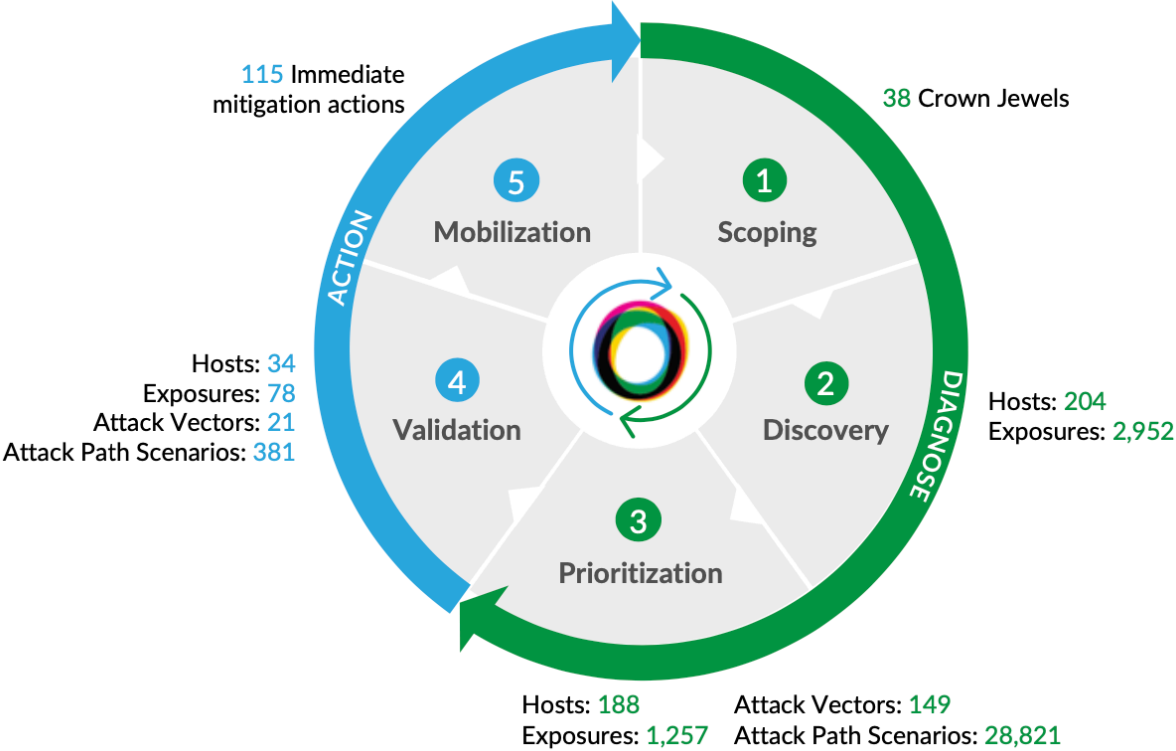
Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Harmony Purple Unique Values

Harmony Purple offers a comprehensive solution for Continuous Threat Exposure Management (CTEM), delivering unique value to organizations. According to Gartner, by 2026, organizations that manage their security investments based on a continuous exposure management program, like that supported by Harmony Purple, will experience three times fewer breaches.

How Harmony Purple Automates Continuous Threat Exposure Management?

Harmony Purple solution orchestrates and provides insights into all 5 essential steps of a CTEM program: scoping, discovery, prioritization, validation, and mobilization.



- Scoping:** Our network map presents a comprehensive overview of crown jewel assets within your organization's network, considering the associated threats. Harmony automates the scoping of crown jewels and empowers you to customize it according to critical business assets.

- **Discovery:** Harmony offers agentless discovery capabilities to identify issues such as misconfigurations, vulnerabilities, and weaknesses across all assets, including network equipment. By creating a cyber twin of your organization (a digital representation of the cyber related aspects of your assets and connectivity) Harmony Purple provides invaluable insights into your production environment from an attacker's perspective.
- **Prioritization:** Harmony Purple relies on risk analysis utilizing the cyber twin and our proprietary MITRE ATT&CK knowledge base to craft attack path scenarios. These scenarios prioritize threats by considering the probability of an attack and its impact on your organizational assets.
- **Validation:** Leveraging the cyber twin, Harmony Purple conducts comprehensive analyses of cyber threats and evaluates the effectiveness of organizational controls across networks, hosts, and users. Our solution provides remediation suggestions based on the performance of current controls in your production environment, in line with recommendations from MITRE, NIST 800-53, CIS, and industry best practices.
- **Mobilization:** Benefit from host-by-risk and weakness reports that offer an actionable overview of actual threats and recommended remediation strategies. These reports facilitate estimation, planning, and inspection of specific IT actions, granting you the required visibility and control for successful execution of the change.

What are the main Harmony Purple's Breakthrough Technologies?

Smartscan™ Network Discovery

- Agentless
- Lightweight
- Discovers:
 - Hosts
 - Network Gear
 - Applications
 - Configs
 - Policies
 - Vulnerabilities

Digital Cyber Twin™

- Virtual twin of the IT environment
- Zero impact platform for unlimited attack simulation

AI Attack Path Scenarios

- Attackers eye view of the network
- First reasoning - based AI attack simulation
- Automatically adapts to new threats
- Measures likelihood and impact