Forvia Scales Security Validation Across their Enterprise - Wide Network

Highlight Achievements

- Testing across 44,000 IPs on a monthly basis
- Validate the security controls of the company's 300 sites every 3 months
- Established consistent metrics to track efficiency improvements

Background Information

Forvia is the seventh largest automotive-supply group and the world leader in vehicle interiors and emission-control technologies. With over 160,000 employees across 43 countries, 1 in 2 vehicles worldwide is equipped with FORVIA products. Operating 260+ production sites and 76 R&D centers, the company manages a complex and expansive IT environment.

Frédéric Petrus, the leading IS Control and Vulnerability Manager, and his team oversee threat detection and response, building the local IT team's preparedness, and supporting them to remediate vulnerabilities across hundreds of sites. Petrus and his team provide detailed reports to the local teams on mitigation instructions and evaluations on the effectiveness of remediation efforts.

The Challenge: No Way of Scaling Manual Pentesting Across Remote Networks

At the request of its Group Risk committee, Forvia initiated an internal penetration testing program. However, the process quickly revealed critical time and resource limitations. The manual pentesting approach was limited in frequency and scalability; over a year and a half, they covered only a quarter of the company's sites. Compounding the issue, their vulnerability scanning tool offered no prioritization or context of the vulnerability in the environment, making remediation difficult for local IT teams to act on.

The Need: Fostering a Culture of Cyber Resilience Across a Fragmented Team

The primary objective of Forvia's security team was to ensure uninterrupted production and protect critical assets across its industrial environment, including the integration of IT and industrial VLANs. As a highly decentralized organization, Petrus recognized the importance of fostering a strong cybersecurity culture among Forvia's local IT teams and wanted to empower them to collaborate more effectively and remediate vulnerabilities more precisely.

This vision shaped two core requirements in their search for a security validation solution: the ability to detect vulnerabilities that are actively exploitable, and the capability to map out real attack paths across their environment. Additionally, Forvia aimed to use security validation as a way to support compliance readiness with regulatory standards in the automotive sector, particularly those set by TISAX.

The Solution: Continuous Testing with Localized, Actionable Remediation Deployment

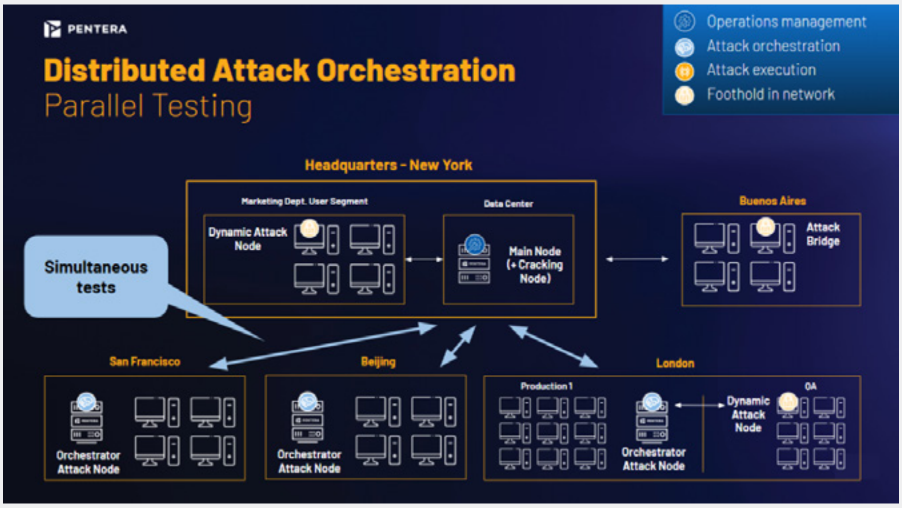
Pentera was selected by Forvia's security leadership to enable their pragmatic approach towards improving security posture. This included frequently testing their security controls across their entire network, while enabling local IT teams to focus their limited resources only on what truly matters. Their goal was to test their entire network every three months, to validate improvements and support frontline remediation efforts more effectively.

To navigate Forvia's sprawling global IT infrastructure, the team began with a targeted pilot program across selected sites in Europe and Asia. These locations were chosen for being representative in size, complexity, and production typology. They provided a realistic demonstration of how long a Pentera test would take to scale across the environment. Close collaboration with Forvia's SOC ensured accurate configuration and alert management, avoiding false escalations during testing. Following the success of the first stage, Pentera was rolled out globally across Asia, Europe, North America, and South America.

Distributed Architecture

To meet its goal of testing all sites every three months, Forvia deployed Pentera's Distributed Attack Orchestration. This architecture setup involves a central node at Forvia's HQ, supported by a network of persistent remote attack nodes embedded across local sites within varying VLANs and data centers. To enhance flexibility, Forvia also utilized dynamic (non-persistent) attack nodes that allowed temporary testing in VLANs as needed. This Distributed Attack Orchestration enables simultaneous, orchestrated penetration testing across multiple sites, improving testing speed and coverage while maintaining network segmentation.

To drive the most efficiency out of their local IT teams, Forvia runs 11 parallel pentests every Tuesday and Thursday, totaling 22 pentests each week. This aggressive cadence allows them to test a range of 11,000 IPs per weekly run, amounting to over 132,000 IPs tested in a 3-month cycle - a scale and frequency that was previously unattainable with manual or automated processes. What's more, achieving all of this without disrupting operations.



PENTERA

Distributed Attack Orchestration

Parallel Testing

- Operations management
- Attack orchestration
- Attack execution
- Foothold in network

Prioritizing Vulnerabilities

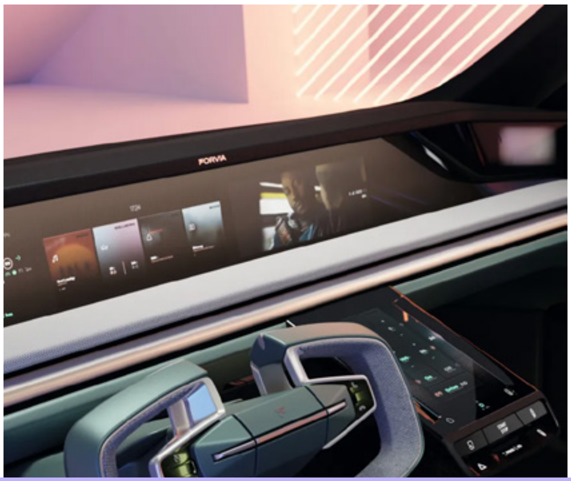
To help build the efficiency of their local IT teams, Forvia implemented a pragmatic remediation strategy that focused only on the vulnerabilities they wanted each local team to address. Before sharing action items, vulnerabilities with low or medium severity were excluded, as were those requiring resolution by the central Competence Center. Only the five most exploitable vulnerabilities at the site were prioritized, so remediation remained focused and actionable. This filtering strategy allowed Forvia to streamline communication and reduce noise enabling them to navigate the high volume of security data.

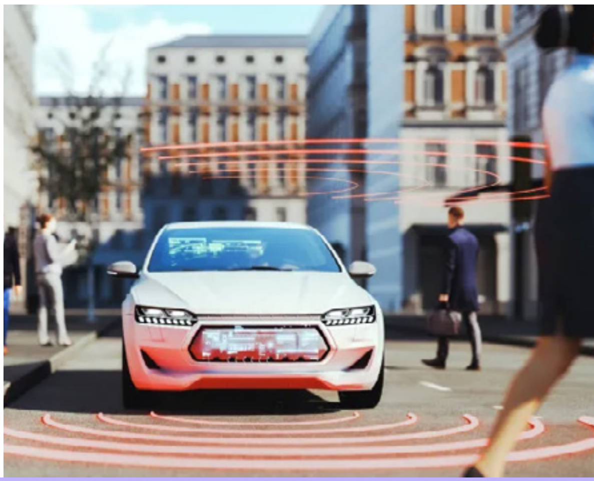
Automated Workflow

Forvia integrated Pentera with ServiceNow via API, enabling automation of the remediation lifecycle. Once a tailored remediation plan is issued to a local team, action items are automatically logged in ServiceNow at 10-day and 20-day intervals post-assessment. This ensures consistent follow-up and provides local teams with a structured, trackable workflow, driving faster response and accountability.

> **Working with Pentera’ support team was great, they helped us overcome deployment issues as they arose, always being flexible and responsive. The strong partnership meant there was constant communication to begin with and even now we have regular project reviews**

Frédéric Petrus
IS Control and Vulnerability
Manager at Forvia





Results: Security Gaps Closed and Remediation Tracked at Scale

Critical Discoveries

Pentera revealed that some servers were running exposed, partially outside the protection of the EDR. This critical oversight triggered Forvia's security team to assess for this exposure across their other sites as well. In an Active Directory password audit, another Pentera testing scenario, the team detected a password stored using reversible encryption. This meant the clear-text password could be obtained, as opposed to having to brute force it. This discovery highlighted the risks that traditional vulnerability management tools had missed.

Greater Team Efficiency

Forvia's IT team significantly improved operational efficiency by automating every step of the pentesting process - from preparation to execution and result application. While a degree of manual input is retained to tailor remediation plans for local teams, all automatable tasks have been streamlined, allowing the local teams to focus their efforts where they matter most.

Tracked Efficiency Improvements

With a quarterly testing cadence in place, key performance indicators (KPIs) were established to track remediation timelines and ensure local teams have sufficient time to act. In addition to speed, Forvia is now tracking remediation quality, validating that closed tickets truly reflect resolved issues with no recurrence, ensuring long-term effectiveness at each site.

Closing

While every business may be different, the need for continuous testing is evident. Attackers are not slowing down and the list of organizations compromised grows. Large enterprises such as Forvia have multiple challenges facilitating complex testing in their sprawling environments; however, with Pentera, security validation is not one of them. A distributed, scalable architecture is a must-have in order to truly understand and measure risk across the environment.

About Pentera

Pentera is the category leader for Automated Security Validation™, allowing any organization to test all cybersecurity layers, over all the attack surfaces, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.