DAMOVO
SECURITY SERVICES
POWERED BY
LARES

APPLICATION SECURITY

HELP YOUR EMPLOYEES, PARTNERS, AND CUSTOMERS TRUST YOUR BUSINESS.

Every organisation utilizes software on a daily basis to conduct business with their customers. As a result, customers view software applications as an extension of the company they are dealing with. The last thing that any organisation wants to do is to break that trust by exposing their customers to a breach as a result of poor, or nonexistent, application security.

Let Damovo Be Your Guide…

Damovo, together with our cybersecurity division Lares, can help your organisation validate its security posture through offensive security focused services such as complex adversarial simulations, penetration tests, insider threat assessments, vulnerability research, continuous security testing, and coaching.

APPLICATION SECURITY OFFERINGS

Web
Whether it's white-box or black-box testing, our engineers prioritise manual testing over automated scanning to produce actionable and validated results. Using a combination of open source and commercial tools, Damovo can identify authentication, authorisation, and logic flaws by leveraging our Dynamic Application Security Testing (DAST) methodology.

Mobile
Our team has extensive experience testing applications on mobile platforms such as Apple iOS and Android. With our detailed knowledge of mobile security practices, we can identify weaknesses with the application, how the data is stored, bundled or third-party APIs, and the mobile platform itself.

Thick-Client
Thick-clients are the applications and associated services installed on a desktop or server operating system. These applications introduce an additional attack surface to your systems that often require creative testing methods to identify vulnerabilities, coding errors, and other exposures.

Code Review
Sometimes the best way to identify security vulnerabilities is to review the application's source code. Damovo engineers can conduct detailed code reviews of applications created in today's most popular programming languages to identify weaknesses in the code, its logic and implementation, or its use of vulnerable third-party libraries.

Damovo leverages a team of senior consultants to partner with businesses and prepare internal teams to measure the organisation's defensive maturity, and advance its security program.

Architecture and Configuration Review
A house is only as sturdy as the foundation upon which it is built. In addition to reviewing the design, architecture, and configuration of applications prior to deployment, our engineers can also review the underlying platforms, APIs, and integrations through advanced threat modeling exercises and discussions with asset owners.

Cloud
Applications deployed in Amazon Web Services (AWS), Microsoft Azure, or Google Cloud may require additional security scrutiny as they are no longer protected by your on-premise security controls. Damovo can review proposed and current cloud application implementations against security best practices from the Cloud Security Alliance (CSA) and the providers themselves.

Embedded
Often overlooked as a potential security threat, embedded devices generally receive less focus than typical computing platforms like laptops, workstations, and servers. Damovo has provided application security testing solutions for embedded systems such as Automated Teller Machines (ATMs), automotive infotainment systems, and other non-standard computing platforms.

IOT
Unlike most security firms, Damovo can provide a mix of application, network, and hardware security expertise to identify vulnerabilities. Whether you're concerned about commercial "smart devices", appliances, or industrial IOT (IIOT) hardware, Damovo has a proven track record of delivering detailed analysis, recommendations, and fixes to help prevent an IOT-related breach from happening.

Product Security Review
Looking for a comprehensive and vendor-agnostic review of a particular internally developed or COTS application? We can review the entire system as a whole and recommend incremental security mitigations for any discovered vulnerabilities or flaws.

DevSecOps and Secure SDLC
Your organisation's Software Development Lifecycle (SDLC) likely employs a combination of manual code commits and automated development and build tools that may overlook critical security concerns. Let Damovo help identify weaknesses and infuse security into the Continuous Integration and Continuous Delivery (CI/CD) pipeline to prevent vulnerabilities from ever reaching production.

ICS / SCADA
Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems require a specialised level of domain expertise to test thoroughly. Damovo's engineers are deeply experienced in how to effectively test these systems without jeopardizing the operational state of production environments.

Reverse Engineering & Full Decompile/Recompile Capabilities
We can reverse engineer target applications, such as malware or suspicious applications, to better identify purpose and capabilities. We can also perform decompilation and recompilation as part of our testing engagements to defeat or validate enforced restrictions and safeguards.

About Damovo & Lares
Lares is Damovo's cybersecurity division. All of the Lares engineers are required to meet a minimum baseline standard of eight years information security fieldwork before joining the team. Together we help companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching.