



DAMOVO

Identify vulnerabilities and
address them effectively

Vulnerability Management by Damovo



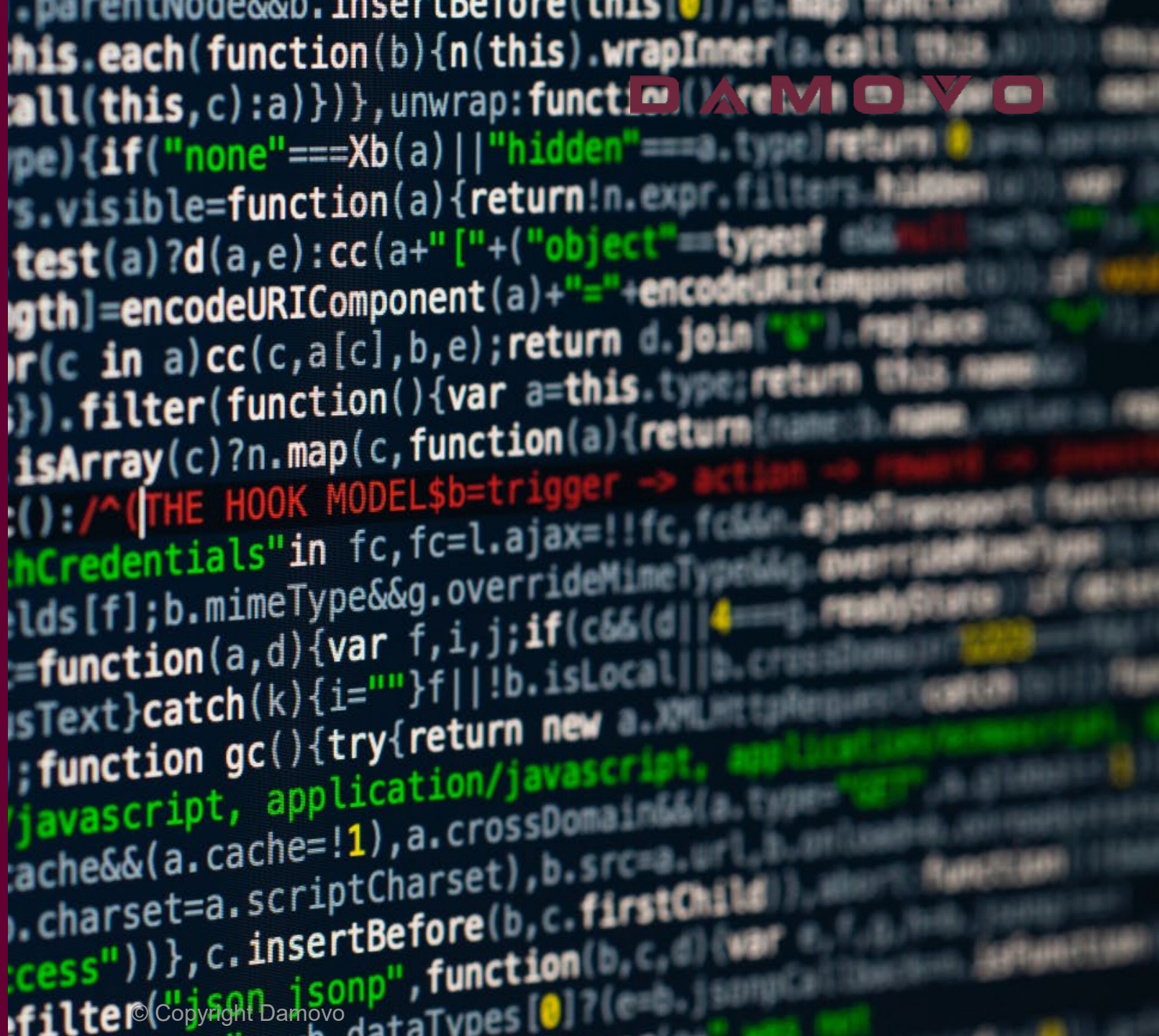
Change Driver

The security officer of a retail and logistics company deals conceptually with the topic of security based on the existing Information Security Management System (ISMS).

On the one hand, compliance guidelines require continuous monitoring, risk assessment and, if necessary, updating of systems and applications.

On the other hand, a glance at current vulnerability databases show an increase in vulnerabilities in systems and applications. Known vulnerabilities can be exploited in a targeted manner, e.g. with extensive exploits (prefabricated attack programs) and thus also by script kiddies, i.e. by users with insufficient basic knowledge.

The security officer is therefore focused on risk mitigation and must adequately consider vulnerability and patch management in the context of cyber hygiene. He requires the support of an external service provider to do this effectively.





Damovo Approach

As part of a consulting engagement, Damovo designed a vulnerability management programme that goes far beyond simple patch management.

Damovo's Vulnerability Management (VM), is a solution component of Damovo's Security Operation Center (SOC).

It is based on a conceptual approach, with a mix of continuous processes and automation. This is the only way to win the race against attackers.

In addition, vulnerabilities and risk management are linked in a way so that the weakest link in the security chain can be prioritized, preventing attacks from the outset.



Customer Value

DAMOVO

How the safety officer benefits

With the introduction of Damovo's Vulnerability Management solution, IT resources have now been freed up for other higher-value and more interesting tasks

The tension with the IT manager, who demands a timely elimination of existing vulnerabilities, is also mitigated.

How the company benefits

With the Vulnerability Management solution the company's resistance against attacks is strengthened and thus the threat of cyber risk is reduced.

In addition, the use of the solution fully meets the requirements of ISO/IEC 27001 and PCI DSS in this area.