INSIDER RISK IN SOFTWARE SUPPLY CHAINS

OUR SOFTWARE MAY BE TRUSTED, BUT IS IT SECURE?

A software supply chain attack occurs when malicious code is deliberately added to a component, with intent to distribute the malicious code to a target further down the supply chain. These attacks aim to compromise systems and data, and may also cause collateral damage.

INSIDERS:

Create source code, design applications, and contribute to software development

Review, test, and license applications for usage

Update, maintain, and repair existing software

Share, distribute, and utilize applications

VULNERABILITIES TO SOFTWARE INTEGRITY:

Insiders wittingly or unwittingly introduce malware to applications

Insiders utilize un-vetted dependencies during development

Insiders fail to patch software or delay deployment of more secure applications

ENHANCE SOFTWARE INTEGRITY WITH:

Code signing: code with a trusted, cryptographically secure indicator that software has been approved by its developer and not subsequently modified.

Hashing: unique strings of information generated by hashing algorithms, distributed by developers to verify software has not been modified.

User Activity Monitoring: detect anomalous or concerning network behaviors that may put the organization at risk.

Remember: Trusted insiders have access to assets at all stages in the supply chain. Damage to the supply chain caused by insiders may lead to reduced military strength and mission readiness; loss of reputation, innovation, and industry advantage; and financial instability.

CDSE
Center for Development
of Security Excellence

www.cdse.edu

LEARN. PERFORM. PROTECT.