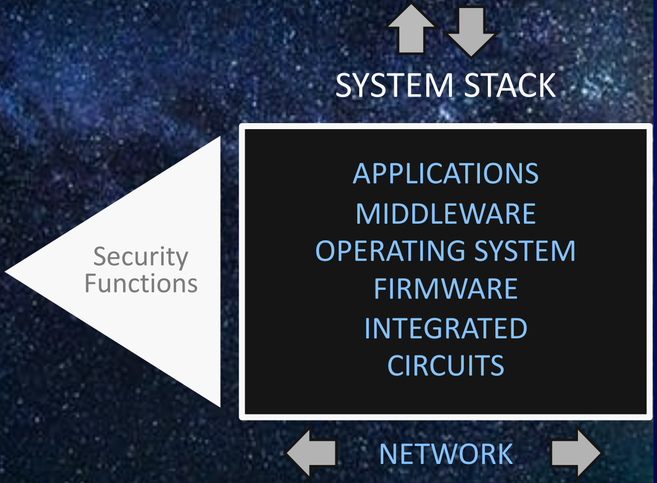
The Game Changing Benefits of DevSecOps

Moving the Needle on Security Assurance

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The Current Landscape…

Little or no understanding of what’s in the ”black box.”



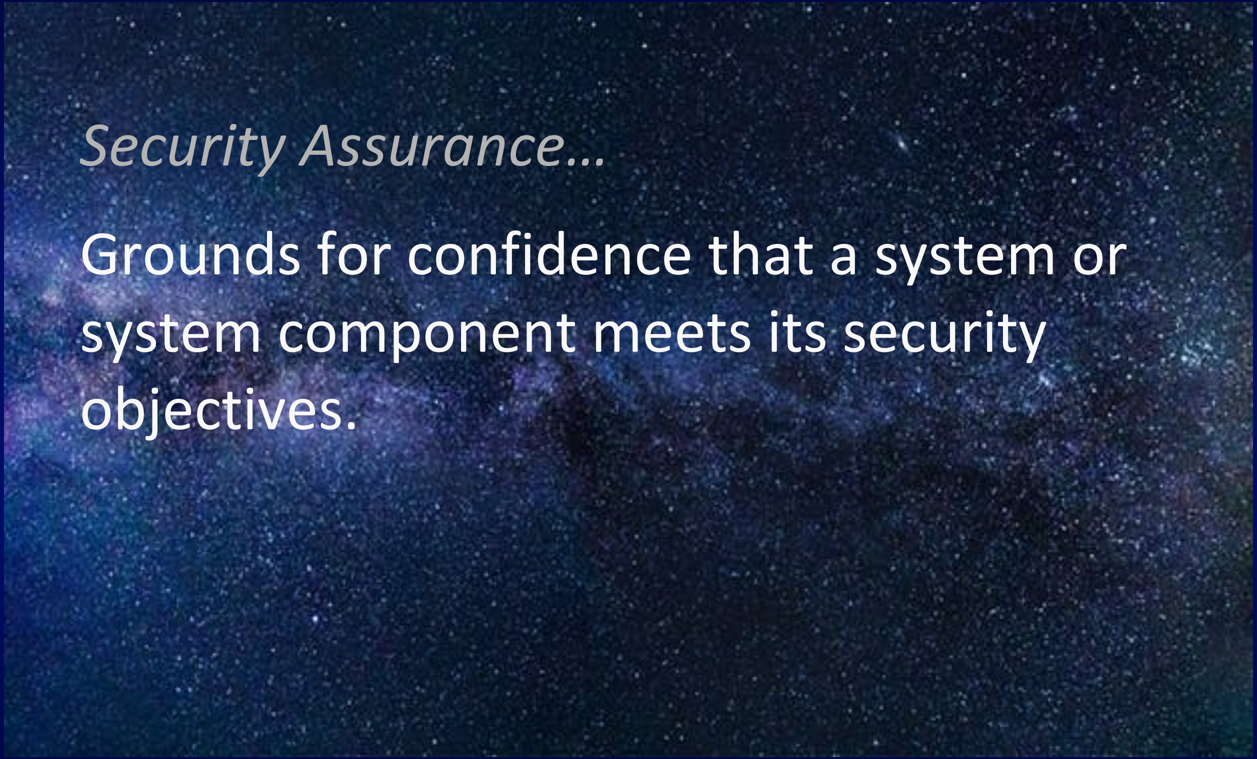
SYSTEM STACK

Security Functions

APPLICATIONS
MIDDLEWARE
OPERATING SYSTEM
FIRMWARE
INTEGRATED CIRCUITS

NETWORK

Transparency
Traceability
Visibility
Assurance



Security Assurance…

Grounds for confidence that a system or system component meets its security objectives.

Security Vulnerability…

Weakness in a system, security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Source: CNSSI 4009

Vulnerabilities can occur through failures in…

Requirements—

- System or component possesses all the functions and features required and still contains vulnerabilities that make it unsuitable or ineffective with respect to security.

Development—

- System or component does not meet its specifications and/or vulnerabilities exist as a result of poor development standards or incorrect design choices.

Operation—

- System or component has been constructed correctly to a correct specification, but vulnerabilities exist as a result of inadequate controls during operation.

Source: ISO/IEC 15408

Vulnerabilities should be…

Eliminated—

- Active steps are taken to expose, and remove or neutralize, all exploitable system or component weaknesses (i.e., vulnerabilities).

Minimized—

- Active steps are taken to reduce, to an acceptable residual level, the potential adverse impact resulting from the exploitation of a vulnerability.

Monitored—

- Active steps are taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.

Source: ISO/IEC 15408

Security Functionality and Assurance in the Traditional System Life Cycle

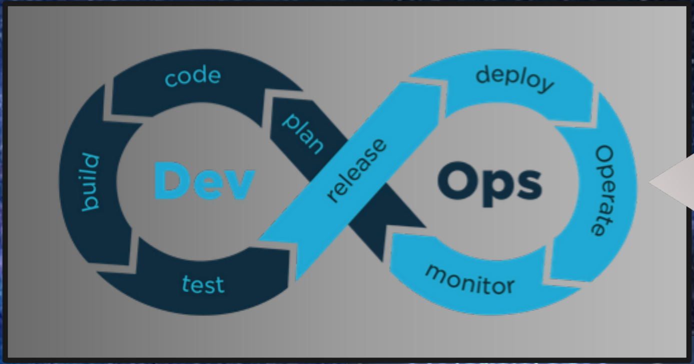
ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

NIST SP 800-160 Volume 1

- Business or mission analysis
- Stakeholder needs and requirements definition
- System requirements definition
- Architecture definition
- Design definition
- System analysis
- Implementation
- Integration
- Verification
- Transition
- Validation
- Operation
- Maintenance
- Disposal

Next Generation Development Processes



Credit: Network Intelligence

Security Integration

DevSecOps

AGILE DEVELOPMENT
SECURE ARCHITECTURE
APPLICATION SECURITY
CODE REVIEW/TESTING
SECURE CONFIGURATION
SECURE OPERATIONS

Transparency
Traceability
Visibility
Assurance

100 Bureau Drive Mailstop 7770
Gaithersburg, MD USA 20899-7770

Email
ron.ross@nist.gov

Mobile
301.651.5083

LinkedIn
www.linkedin.com/in/ronrossecure

Twitter
@ronrossecure

Web
csrc.nist.gov

Comments
sec-cert@nist.gov