Request for Change

Date: 01 February 2021

Requestor: NATO Communications and Information Agency

POC: Dr. Gernot FRIEDRICH

Email: gernot.friedrich@ncia.nato.int

Target Version: SFIA v8

Rational:

With the adoption of cloud computing services the traditional functions and roles of Software Engineers, Cyber Security Experts and Operations/Information Technology (Ops/IT) Specialists are blurring, and a new discipline known as Development Security Operations (DevSecOps) Engineering has emerged.

DevSecOps engineers ensure continuous delivery of value to end users by optimizing and automating continuous integration and delivery pipelines taking a security by design approach.

DevSecOps engineers work on optimizing processes, tools and methodologies to overcome traditional barriers between software development, security, testing and operations. DevSecOps engineers foster efficiency at every stage of the entire Software Development and Operations Life Cycle.

DevSecOps is now well established in industry and new integrated skill profiles have emerged, which include knowledge about accessing the technological automation tools, managing the cloud deployment, leading software development teams, maintaining compliance and security controls, monitoring operations, and working and improving development process.

As DevSecOps engineers are required to have some skills and prior experience in at least one of the traditional roles before stepping into a broader DevSecOps engineering role it is suggested to add a new skill "DevSecOps Engineering" at levels 4, 5 and 6 to the "Change and Transformation" (category) under a new "Software Life-Cycle Optimization" (sub-category).

DevSecOps Engineering (DSOP)

Overall description:

The cross-functional, agile specification, design, integration, testing, deployment and operations of software applications and services at high velocity to meet business requirements by applying suitable design standards and principles whilst conducting continuous risk assessments and applying security best practices to counter ever-changing cyber security threats. Maximizing the automation of all activities across the development, verification, integration, deployment and service operations phases including the identification of vulnerabilities in order to deliver agreed value to stakeholders by using adaptive (iterative/agile) approaches. Situation-appropriateness is a distinguishing characteristic that requires the adaptation of working practices according to the needs of individual products. DevSecOps Engineering combines the technical proficiencies in DevOps culture, automation and ways of working with knowledge of cybersecurity threats and trends.

Level 4 description:

Elicits requirements and prepares design options for software components or micro services dynamically, using appropriate agile techniques, following DevSecOps patterns and methodologies and using automation tools. Communicates multiple design views to identify and balance the concerns of all stakeholders of the software design and to allow for further

elaboration of functional and non-functional requirements. Explores designs, which take into account target environment, performance and security requirements. Reviews, verifies and improves existing solution designs against requirement to meet stakeholders' requirements, and effective and secure construction of the software. Selects software development approach for software components and micro services and ensures their automatic verification, integration and deployment to achieve well-engineered and secure outcomes. Participates in reviews of own work and leads reviews of colleagues' work.

Level 5 description:

Selects, adopts and adapts appropriate software design methods, tools and techniques; using appropriate agile techniques, following DevSecOps patterns and methodologies and using automation tools. Designs the orchestrations of multiple software components or micro-services required to achieve stakeholder requirements. Undertakes impact analysis on major design options, makes recommendations and assesses and manages associated implementation, life-cycle support and security risks. Evaluates the quality of alternate solution designs and communicates with stakeholders to identify corrective action, as soon as possible. Ensures that the software design balances functional, quality, security and service management requirements. Plans and drives development, verification, integration, deployment and service operations activities. Measures and monitors applications of project/team standards for software construction including software security. Contributes to the implementation of software architecture best practices such as an organisational micro service ecosystem and to the development of overall software and security architecture policies and guidelines.

Level 6 description:

Leads the cultural change within an organisation towards a DevSecOps culture and communicates the benefits to all stakeholders. Improves the DevSecOps methods, tools, techniques and develops organisational policies, standards, and guidelines for designing, developing, integrating and operating software services in an agile and secure way, whilst adhering to technical strategies, and systems architectures (including cyber security). Develops organisational policies, standards, and guidelines for DevSecOps within the organisation. Plans and leads strategic, large and complex DevSecOps projects. Develops new methods and organisational capabilities and drives adoption of, and adherence to policies and standards.