5 Enablers to Engineer a SecDevOps Culture

By Peter Anih, Dynanet Corporation Chief Technology Officer

The buzz around DevOps and the various iterations surrounding the term (DevSecOps, SecDevOps, DevOpsSec, etc.) has been rising at an exponential rate given the increases in Cloud capabilities, Agile adoption, and of course, IT automation. Being part of several different "DevOps-like" initiatives, I have found that they all had one thing in common — creating a culture to embrace the initiative. If the organization isn't dedicated to embracing a DevOps Cultural Mindset, the initiative will fail.

Key factors for engineering a SecDevOps Culture are communication, Agile adoption, security, sense of ownership, and challenging the known. There are literally dozens of other factors besides the five I mentioned that can and have fostered the development of a SecDevOps culture. Through my experiences, conversations, and research, these enablers either coupled together or as a part of a mix with others seem to be foundational to creating a SecDevOps Culture.

Increase Communication and Transparency within your Organization

Whether you are organizing a pot luck lunch or developing a mission critical system, communication is essential for a successful outcome. Continuous communication along with reducing internal organizational fiefdoms must be one of the first steps taken towards building a SecDevOps culture. The essence of a SecDevOps culture is completely reliant upon open and fluid communication throughout an organization.

One might ask, "Ok Peter, how do you do this?". It doesn't happen overnight and it's certainly not easy. I've listed a few techniques below that I've seen be successful:

- Establishing daily touch points either in person or virtual
- Developing Information Radiators such as wiki's, blogs, internal portals, and work boards
- Developing messaging apps either via desktop client or mobile devices
- Hosting information sharing sessions such as brown bags, lunch and learns, or meet-ups

At the end of the day, it's more about developing the expectations of continuous communication, which breeds the enablement and eventual understanding from members of an organization. If people expect to receive communication on a steady basis, it will seem unusual when they aren't engaged and collaborating with fellow members. Members will then make sure constant communication and awareness is not an afterthought but a necessity.

Organizational Adoption of Agile

Some say the SecDevOps movement is the continuation of the Agile movement. This article isn't for discussing or debating where in the Agile continuum SecDevOps fits. More so, how a mature or maturing Agile organization has the foundational elements in place or identified to foster a SecDevOps culture. IT tools and technology are a piece of what is needed to deploy and operate a SecDevOps pipeline. In order to create a cultural mindset that embraces the philosophy, Agile and iterative cadences must be in place. Having a solid organizational understanding of Agile will enable incremental

and continuous development, testing, deployment, and sustainment of a system, which fosters the success of a SecDevOps implementation.

Organizational understanding and adoption of Agile enables the path to a SecDevOps culture by putting in place Agile components for a SecDevOps framework. The following components are vital for a successful SecDevOps culture and all come from basic Agile principals:

- Customer Satisfaction
- Embracing Change
- Incremental Delivery
- Collaboration
- Supportive Environment
- Fostering Conversation
- Functioning Systems and Software
- Sustainable and Constant Pace of Development
- Strive for Technological Excellence

Agile maturity and a sound understanding of incremental execution serves as the foundation for a SecDevOps cultural mindset. Without organizational Agile adoption, a true SecDevOps culture will be very difficult to achieve if at all.

Security First Mindset

In today's digital climate, security has to be at the forefront and a primary focus for every organization. Putting a SecDevOps framework in place implies that an organization is being proactive instead of reactive when it comes to security. Security-minded personnel should be engaged early and often, ensuring that all engineering and non-engineering projects meet security best practices, requirements, and regulations.

Having an organizational mindset of "Security First" fosters the creation of hearty systems and applications that will be reliable and resilient. With the hyper-competitive IT world we live in today, organizations can no longer afford to catch security vulnerabilities in production environments. Attacks that uncover exploits are costly and can often have a crippling effect on a system and organization. Leveraging SecDevOps within an organization enables continuous focus on security at every stage of the pipeline. It creates peace of mind knowing that you are engineering secure systems and applications with features and functionalities that users are requesting. We all know that hackers will never stop trying to find ways to exploit systems, hopefully leveraging a security-minded framework such as SecDevOps will make it harder for them to be successful in their efforts.

Everyone has Skin in the Game

The days of stove-piped systems and applications and who "owns" them between development organizations, testing groups, and sustainment teams are a thing of the past. In a SecDevOps environment everyone has to have skin in the game throughout the lifecycle of a system or application. The reason for this is transition of accountability often causes a lack of focus and quite honestly caring. In order for a SecDevOps organization to have systems seamlessly flow from development to sustainment, with bug fixes and enhancements being incorporated on a continual basis, everyone must

be accountable at all times. Yes, during certain key milestones one group within the organization might carry more of the load. This doesn't mean that the other members are waiting in the wings. Everyone should be in constant communication, so they understand what needs to be done next to continue the success of the effort.

Continued and mutual accountability also fosters an environment of support and togetherness. If one knows a failure from one part of the organization will have a damaging effect on what you do, most people will work to ensure that failure doesn't happen. Building this type of communal environment increases confidence within individuals that they will be successful as well as the organization as a whole. Members will feel that someone always has there back and is looking out for their best interests.

Encourage and Embrace Challenge

Challenging the norm and fostering an environment that breeds challenge is often one of the most overlooked attributes of successful organizations. Within the SecDevOps world how can you do this? Several different aspects of the organizational environment can be challenged such as:

- What tools are we using and why?
- Why are events/stages in the continuous integration/continuous delivery (CI/CD) pipeline ordered the way they are?
- Should we deploy to production without manual intervention?
- How often should code be tested?

Within a given organization there is no right or wrong answer to these questions or several others like them. Yet, people often feel compelled to follow the status quo and comply to what processes and decisions are currently in place.

Instituting a SecDevOps culture is most beneficial when an organization can look at what it's doing and how it's doing it and then decompose processes to their most granular form and figure out how they can be done better. Continual improvement must be a routine event. When activities like this become a part of the fabric of the culture of a security first organization, stovepipes dissolve, communication increases, and there is shared accountability. Creating a successful SecDevOps environment doesn't start with IT tools and technology, it's about engineering a culture that enables SecDevOps to thrive.

About the Author: *Peter Anih (CSM, ICP), Dynanet CTO, is a strategic thinker and IT leader, driven to excel through rapid consumption of new technology capabilities, continuous team motivation, and collaborative work with technical and functional stakeholders. Strong advocate for continual technology and business transformation—passionate in driving innovation, building viable business cases for modernizing IT infrastructures and practices.*

Dynanet Corporation, a minority-owned small business located in Maryland, has provided a range of information technology services to multiple Government agencies. Our focus on customer satisfaction and performance has established long-term relationships with the federal, civilian and state government agencies. Our executive leadership team has built Dynanet's dedicated workforce from 20 employees to over 100 key personnel, while maintaining a 90% retention rate. Our managers are PMP certified and our employees maintain many sought after professional certifications, such as Certified Scrum Masters and ITIL certified. Dynanet has been appraised at CMMI Maturity Level 3 and our quality management processes have been audited and found to be in compliance with the ISO 9001:2015 quality standards. For more information, please visit Dynanet's website at www.dynanetcorp.com.