SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Dell EMC Incorporates SAFECode into its Product Security Practices

Eric Baize
Dell EMC Vice President of Product Security

When computer technology behemoth Dell and storage leader EMC merged in September 2016, the $58 billion deal set a record for a tech merger. It also marked a major step forward in Dell Technologies' strategy to offer customers end-to-end solutions spanning everything from servers to storage to networking to virtualization.

At the time of the merger, EMC was already an industry leader as the world's largest provider of data storage systems by market share. Over the years, the company expanded its business to include information security (RSA Security, acquired in 2006), virtualization (VMware, acquired in 2004), analytics, cloud computing, and other products and services that enable businesses to store, manage, protect, and analyze data.

Eric Baize, Dell EMC Vice President of Product Security, has played a key role in guiding the company's product security efforts since joining EMC in 2002. He leads Dell EMC practices for secure product development, vulnerability response and for driving a consistent security architecture across the product portfolio. Mr. Baize is also the Chairman of the Board of Directors of SAFECode, the industry non-profit he helped found in 2007.

What are the most effective mechanisms you've employed to improve product security in your organization?

ERIC BAIZE: One of the core components of our strategy is threat modeling. Threat modeling is the concept of taking a system or product and finding ways to break in and exploit potential security weaknesses that may exist in the design. The reason we believe it's one of the most effective mechanisms, is that, first of all, product engineers are always challenged by new problems – they love doing it. It enables them to look at their products in a new way.

Engineers enjoy this challenge and it's a good way to understand where a product may have weaknesses, and potentially prioritize additional activities such as code review or testing. Developing secure software is a process, not just one activity. Threat modeling is an activity that allows you to find issues and plan your future moves.

How does Dell EMC leverage the work of SAFECode?

ERIC BAIZE: SAFECode is a formidable platform to learn and gain from the experience of other organizations and to contribute your own know-how. Take threat modeling is an example. Our threat modeling experts get together with experts from other SAFECode companies, learn from each other and contribute to a final report that will publish for the broader community. We also leverage SAFECode training extensively. Not only do we contribute to creating new training modules at SAFECode, we also incorporate the training into our own curriculum. I talked earlier about security being a process. At SAFECode, we have documented this process in the report "Fundamental Practices for Secure Software Development". We have contributed to those processes and we're also using them to validate that we have no gaps. It allows us to sit with practitioners like ourselves who share our goals and to get different ideas on how to solve the same problems. So SAFECode has aligned very well with how we approach software security at Dell EMC.

As the cyber security landscape has changed in tactics and intensity, how has your organization shifted to address the latest threats?

ERIC BAIZE: We have shifted left. If you look at the product lifecycle from left to right, from early to late as a timeline, many organizations start security practices with testing, which is pretty late in the lifecycle. We prefer focusing on earlier stages in the lifecycle, starting with requirements and the design with threat modeling This forces engineers to think about threats early.

Also, as security has become a priority for our customers, we are getting more security questions from customers about our practices. So we have seen a need, for instance, to improve our capabilities around customer communication and customer documentation, so that customers have access to more information about vulnerabilities, about security, and about our practices.

Can you tell us about emerging threats or new opportunities that Dell EMC is focusing on addressing in the near future?

ERIC BAIZE: A few things. First of all, now you have software everywhere. It used to be that software was run on computers, but now everything is a computer – the fridge is a computer, the car is a computer. Our software and our secure development practices have to follow our company strategy. When the company started building products for the cloud, we had to look at the cloud as a new threat vector. Now the company is building products for the Internet of Things, we have to look at our security practices and make sure they are optimized for the IoT threat landscape.

We also have to stay aligned with the different development methodologies. When we started our product security initiatives back in 2004, most products were developed using the waterfall development methodology. Most teams have now shifted to an agile methodology, which is much more iterative and fast and

lightweight. It doesn't remove the need to develop secure code, but how you do it has to adapt to the methodology. In some cases now, we have teams doing DevOps. So every time we have to adapt and make sure that our security practices are aligned and compatible with these development methodologies.

What recommendations do you have for organizations formalizing and/or advancing their product security organization?

ERIC BAIZE: First of all, I would really recommend that they look at what exists today. SAFECode is a great source of information.

Second, think about product security, first and foremost, as an engineering discipline, and not a security discipline. Similar to quality assurance, you don't add quality just by creating a quality organization. You add quality by improving your processes and making your engineers accountable for quality. For security, it's the same thing.

We have this cliché about 'built-in 'security versus 'bolted-on' security – it's really about building security into the processes. Doing testing is important for quality, but you don't improve quality by just doing quality assurance. Doing quality assurance measures how good or bad your quality is, but the thermometer doesn't cure the fever.

So, for companies that are just formalizing their organizations, they really need to pick and choose what works for them, what fits their maturity level, what fits the type of product that they're building, and I assume that SAFECode has resources to help those companies navigate that process.

ERIC BAIZE: Yes, that's exactly the case. SAFECode has a variety of documents outlining all of the steps and activities needed. Then we have started to develop more in-depth documents to support these resources. Equally important is the training discipline, because whatever you do, if you want your engineering organization, your developers, to take ownership of security, they must be trained. Typically engineers try to do the right thing when they know what the right thing is, and training gets you there.

Why should companies get involved with SAFECode?

ERIC BAIZE: There are plenty of reasons. First, it's worth it to get access to the free training and the guidance. I would also recommend that companies join SAFECode, to collaborate with their industry peers. At SAFECode members interact with people who do the same job you do, and who are trying to solve the same problems you are trying to solve. And you can contribute to the community and influence how the industry builds secure products.

About SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe Systems Incorporated, CA Technologies, EMC Corporation, Intel Corporation, Microsoft Corp., SAP AG, Siemens AG and Symantec Corp. For more information, please visit www.safecode.org.