Converged Security – Protect your Digital Enterprise
Questions and Answers
May 24, 2016

Q: Where do I start assuming a zero trust model?
A: From the start. You need to assume that your environment will be breached, which is – essentially – “guilty until proven innocent”. For example, if you are building an interface to your system, you should assume any connection is unsecure and implement an authentication scheme.

Q: You mentioned the 5 domains of converged security, is there a low hanging fruit?
A: This will depend on your situation and what tooling and capabilities at your disposal, but in our experience most customers begin with either the Secure Application Lifecycle (embedding security in application development) and Automated Compliance and Remediation. It is important to note that even within each use case, there are multiple ways to get going. For example, in Automated Compliance and Remediation you can begin by linking security scans to your CMDB to give IT Security insight into the assets they are scanning, even if you do not initially plan on full automation.

Q: We are in the middle of transforming to DevOps, how do you recommend we build security in?
A: A good place to start would be to Continuous Integration and implementing automated code analysis as part of the code check-in and initial testing steps