PUTTING THE SEC IN DEVSECOPS

DTCC

"Traditional cyber protection and detection mechanisms are struggling to keep up with the increase in ransomware attacks. Attackers have flipped the script. We have to respond in kind and apply a 'hacker-mindset' by automating SEC into DEVOPS." – Marc Masri, DTCC Enterprise DevSecOps

ANATOMY OF AN ATTACK

- Hackers leverage automation to run attacks 24/7 designed to identify "leads" or weak points in a defense.
- Once a weakness is identified, the program "phones home" and the hacker architects an attack.
- The hacker needs only find a single weak point to launch an attack and the reward can be substantial.

THINK LIKE A HACKER

- Integrate security automation into the software development and delivery pipeline.
- Provide feedback about security to developers throughout the development process.
- Automate the decision making to govern and block releases that do not comply.

EXAMPLES IN ACTION

The following capabilities have been continuously integrated into our development process:

- Automated security scans that review source code for potential security vulnerabilities during the development processes.
- Automated scans of open-source libraries which are integrated into our software to identify and prevent the spread of known security exploits.
- Integrated security penetration tests into the QA process. These tests attempt to exploit the software by simulating malicious attacks in the same way a hacker would.