The Defense RESTs: Automation and APIs for Better Security

October 3, 2012

David Mortman
Introduction
Want to get better at security?
Improve your operations
Improve your development
The Problem
Huge % of incidents revolve around operational or coding issues
Why?
People Are Bad At Repeatable Tasks!
Centralization, automation & testing can address this
Use APIs and existing ops/dev tools!
Chef, Puppet, etc
Compliance & Change Control
Configuration Drift

AKA

Variation is Evil
Key Management
Auto-Scaling
Auto-scanning on VM launch
Jenkins
Findbugs et al.

http://findbugs.sourceforge.net/
Functional and Unit Testing
Positive and Negative Testing
Gauntlt

https://github.com/thegauntletlet/gauntltt
Auto-code/site scanning on commit
PUT
https://sentinel.whitehatsec.com/api/vuln/retest/<id>
A Little DevOps
Woodward: Code Changes & Complexity
APIs
APIs: REST vs SOAP
Future Directions

& Resources
iControl
&
Space
IF-MAP
Security Automation List
SecurityAutomata.Com
IAM

SCIM/XACML
Conclusion
Any questions?

David Mortman
Chief Security Architect
david.mortman@enstratus.com
@mortman