David Mortman

The Defense RESTs: Automation and APIs for Better Security

October 3, 2012

Introduction

enSTRATUS

Want to get better at security?

enSTRATUS

Improve your operations

enSTRATUS

Improve your developement

enSTRATUS

The Problem

enSTRATUS

Huge % of incidents revolve around operational or coding issues

enSTRATUS

Why?

enSTRATUS

People Are Bad At Repeatable Tasks!

enSTRATUS

Centralization, automation & testing can address this

enSTRATUS

Use APIs and existing ops/dev tools!

Chef, Puppet, etc

enSTRATUS

Compliance

&

Change Control

enSTRATUS

Configuration Drift

AKA

Variation is Evil

enSTRATUS

Key Management

enSTRATUS

Auto-Scaling

enSTRATUS

Auto-scanning on VM launch

enSTRATUS

```
INSTANCE=`ec2-run-instances $AMI -t $TYPE -k $KEY | grep i- | cut -f 2`; until [ $IP ]; do sleep 15; IP=`ec2-describe-instances $INSTANCE | grep i- | cut -f 17`; done ; curl -H "X-Requested-With: DM Automation"   -u $USER:$PASS "https://qualysapi.qualys.com/msp/asset_ip.php?action=add&host_ips=$IP"; curl -H "X-Requested-With: DM Automation" -u $USER:$PASS "https://qualysapi.qualys.com/msp/scan.php?ip=$IP&save_report=yes"
```

Jenkins

enSTRATUS

Findbugs et al.

http://findbugs.sourceforge.net/

Functional and Unit Testing

Positive and Negative Testing

enSTRATUS

Gauntlt

https://github.com/thegauntlet/gauntlt

Auto-code/site scanning on commit

PUT https://sentinel.whitehatsec.com/api/vuln/retest/<id>

A Little DevOps

Woodward:

Code Changes & Complexity

enSTRATUS

APIs

enSTRATUS

APIs: REST vs SOAP

enSTRATUS

Future Directions

& Resources

enSTRATUS

iControl

&

Space

enSTRATUS

IF-MAP

enSTRATUS

Security Automation List

SecurityAutomata.Com

enSTRATUS

IAM

SCIM/XACML

enSTRATUS

Conclusion

enSTRATUS

Any questions?

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

enSTRATUS