

NETFLIX

The Psychology of Security Automation

Jason Chan

QCon San Francisco 2016

@chanjbs





Clan
Tynker

THE DE
THR

**MOVE
FAST AND
BREAK
THINGS**



A blue wall with yellow hand-painted text and a triangular warning symbol. The text reads "SAFETY IS WHEN NOTHING HAPPENS". The symbol is a triangle with a vertical line on the left side, indicating a hazard.

SAFETY IS WHEN
NOTHING HAPPENS



**MOVE
FAST AND
BREAK
THINGS**





**Opportunities for Developers
are also
Opportunities for Security Teams**

Opportunities + History = Powerful Tools

Design Principles for Security Automation

Design Principles

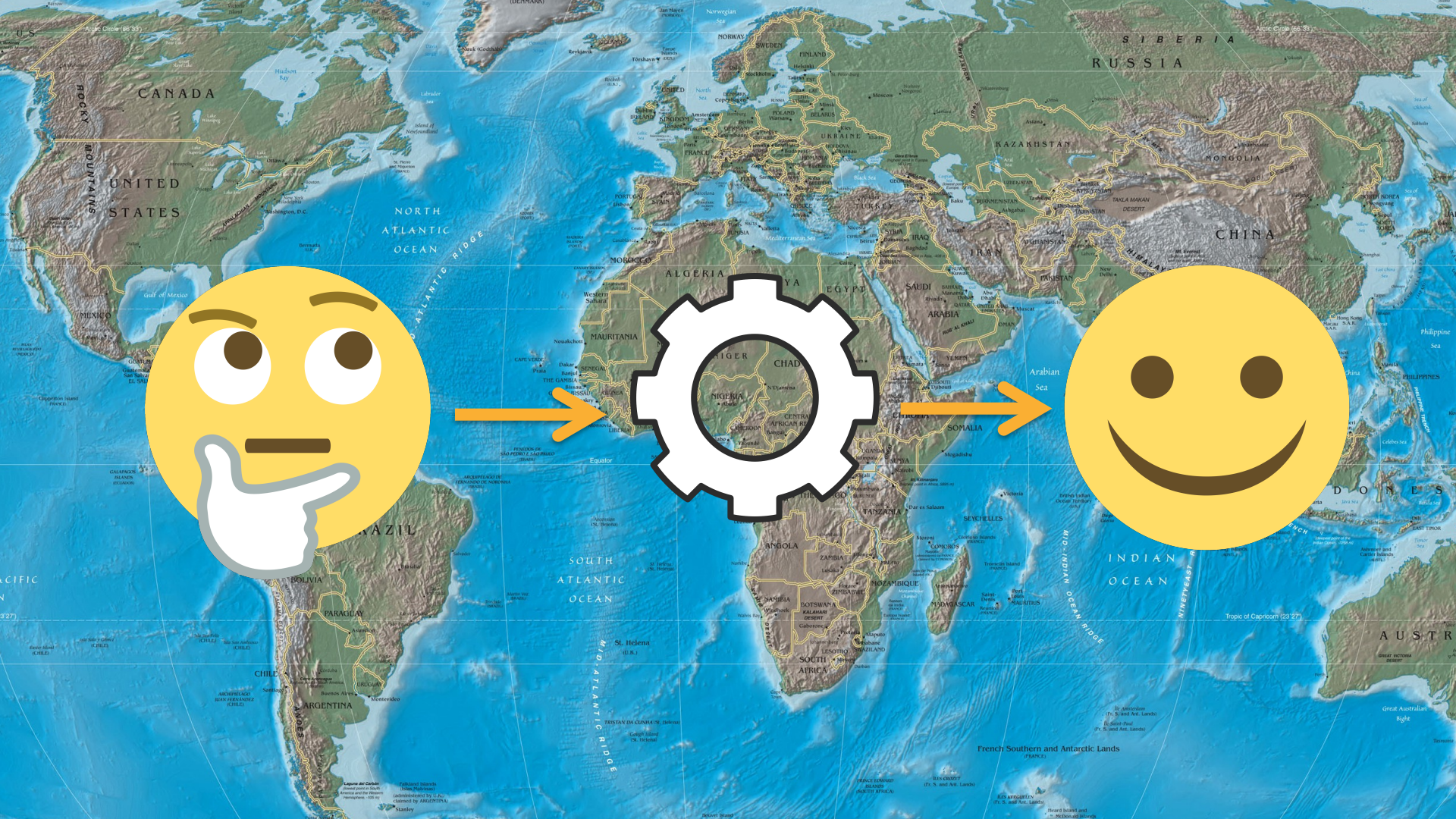
Integrate

Security++

Transparency

Low Touch and Decoupled

Reduce Cognitive Load



SSL

Google SSL certificate update error affects millions of Gmail users

SSL certificate expiry shuts users out of mail

Expired SSL certificate causes Microsoft Azure outages

Brian Sin - Feb 23, 2013

Oops: Instagram forgot to renew its SSL certificate



by OWEN WILLIAMS — 1 year ago in APPS





How to create an SSL cert

Google Search

I'm Feeling Lucky



Thanks @cdorros!

Lemur

<https://github.com/Netflix/lemur>



Lemur

One-stop shop for SSL certificate management

Request, provision, deploy, monitor, escrow

Identify SSL configuration issues

Plugin architecture to extend as necessary

Create Certificate encrypt all the things



Owner	<input type="text" value="security@netflix.com"/>
Custom Name ⓘ	<input type="text" value="the.example.net-SymantecCorporation-20150828-20160830"/>
Description	<input type="text" value="Jason's awesome site."/>
Certificate Authority	<input type="text" value="VERISIGN"/>
Certificate Template	<input type="text"/>
Common Name	<input type="text" value="jason.netflix.com"/>

**Certificate
Signing Request
(CSR)**

PEM encoded string...

Roles

Role Name

0

Replaces

Certificate123...

0

Notifications

Email

0

Destinations

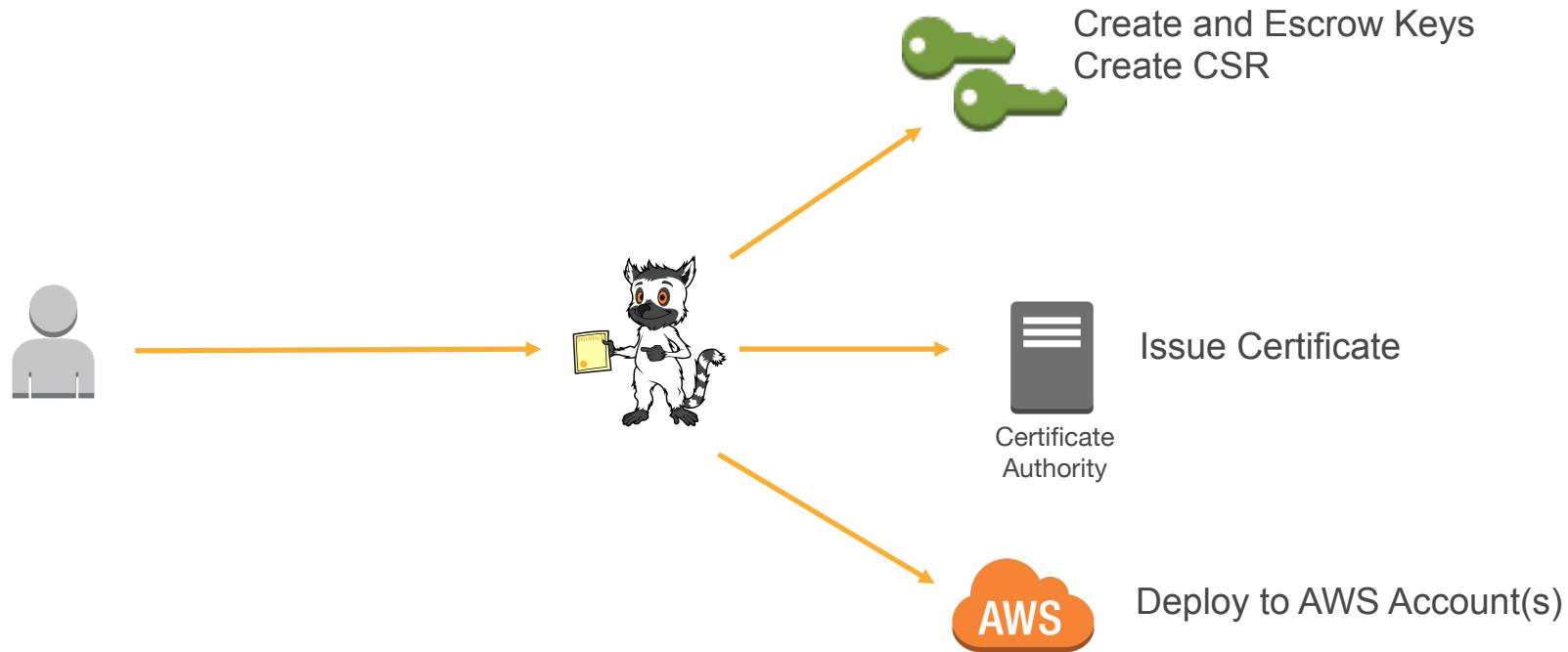
AWS...

0

CREATE

NEXT

Lemur Certificate Creation



Endpoints 443 or bust


FILTER

Name ▾

Port ▾

Type ▾

lem

 **lemur--frontend**
internal-lemur--frontend-1629233400.us-east-1.elb.amazonaws.com

443

ELB

MORE

 **lemur-test-redacted**
internal-lemur-test-redacted-1056045653.us-east-1.elb.amazonaws.com

443

ELB

MORE

CERTIFICATE**ISSUES****Deprecated cipher**

Protocol-TLSv1 has been deprecated consider removing it.

CIPHERS/PROTOCOLS**Protocol-TLSv1****Protocol-TLSv1.1****Protocol-TLSv1.2****Server-Defined-Cipher-Order****ECDHE-ECDSA-AES128-GCM-SHA256**

Lemur Takeaways

APIs = Opportunities

Focus automation investments on persistent, difficult, common problems

Security++

Permissions Management and Access Control

Goal = Least Privilege

But . . .

“It is often easier to ask for forgiveness than to ask for permission”

– Grace Hopper



AWS Permissions Management

- Innovation is enabled by composition of multiple services, but
- Sophisticated policy language
- 2500+ individual API calls
- New services and features released weekly

Repoman: Right-Sizing AWS Permissions





Last 30 Days

← < > → Only show my roles

Search



25

Search

GROUPS

ROLES

Name	Members	Unused Permissions	API	API Errors	API Access Denied
RolliePollie	59	348 unused of 553	286698	1298	2
SecurityMonkey	59	2 unused of 91	62672534	601825	119
Awwwdit	59	163 unused of 253	78541320	9820913	9
FlowbeetCollectorLambdaProfile	56	37 unused of 67	2253272	223	0



Usage

Name: SecurityMonkey

Member Count: 59

Removable Permissions 2

Total Inline Permissions 91

CLOUDTRAIL

ACCESS ADVISOR

Usage

API Call	Count
iam:getrolepolicy	23339491
iam:listentitiesforpolicy	9754574
elasticloadbalancing:describeloadbalancerpolicies	4956733
iam:listrolepolicies	3773506
iam:listinstanceprofilesforrole	3773438
iam:getservercertificate	2988869
iam:listattachedrolepolicies	976542
iam:getrole	864290
iam:getpolicyversion	476697

All Errors

API Call	Count
s3:getbuckettagging	180983
s3:getbucketlifecycle	155103
s3:getbucketpolicy	110360
iam:getloginprofile	25352
ec2:describenatgateways	14487
ec2:describeroutetables	102
ec2:describevpcs	67
ec2:describesecuritygroups	56
ec2:describedhcpoptions	42

Access Denied

API Call	Count
ec2:describevpcpeeringconnections	7288
cloudtrail:describetrails	7286
ec2:describesnapshots	7254
rds:describedbsnapshots	7248
ec2:describenetworkacls	7185
rds:describedbclusters	7180
rds:describedbclustersnapshots	7161
rds:describedbinstances	7138
ec2:describenatgateways	6717

Manage Permissions

Name: Awwwdit

Member Count: 59

Removable Permissions 163

Total Inline Permissions 253

[PROPOSAL](#)

[TEMPLATES](#)

Review the permissions that would be removed below. Select a decision (keep, remove, maybe) for a detailed explanation.

```
{
  "Statement": [
    {
      "Action": [
        "autoscaling:describeaccountlimits",
        "autoscaling:describeadjustmenttypes",
        "autoscaling:describeautoscalinggroups",
        "autoscaling:describeautoscalinginstances",
        "autoscaling:describeautoscalingnotificationtypes",
        "autoscaling:describeautohealingconfigurations",
        "autoscaling:describelifecyclehooks",
        "autoscaling:describelifecyclehooktypes",
        "autoscaling:describemetriecollectiontypes",
        "autoscaling:describenotificationconfigurations",
        "autoscaling:describepolicies",
        "autoscaling:describescalingactivities",
        "autoscaling:describescalingprocesstypes",
        "autoscaling:describescheduledactions",
        "autoscaling:describetags",
        "autoscaling:describeterminationpolicytypes",
        "cloudtrail:describe_trails",
        "cloudtrail:gettrailstatus",
        "cloudtrail:listtags",
        "dynamodb:describereservedcapacity",
```

"autoscaling:describeaccountlimits",	remove
"autoscaling:describeadjustmenttypes",	maybe
"autoscaling:describeautoscalinggroups",	keep
"autoscaling:describeautoscalinginstances",	remove
"autoscaling:describeautoscalingnotificationtypes",	maybe
"autoscaling:describeautohealingconfigurations",	remove
"autoscaling:describelifecyclehooks",	remove
"autoscaling:describelifecyclehooktypes",	maybe
"autoscaling:describemetriecollectiontypes",	maybe
"autoscaling:describenotificationconfigurations",	remove
"autoscaling:describepolicies",	remove
"autoscaling:describescalingactivities",	remove
"autoscaling:describescalingprocesstypes",	maybe
"autoscaling:describescheduledactions",	remove
"autoscaling:describetags",	remove
"autoscaling:describeterminationpolicytypes",	remove
"cloudtrail:describe_trails",	keep
"cloudtrail:gettrailstatus",	remove
"cloudtrail:listtags",	remove
"dynamodb:describereservedcapacity",	remove

autoscaling:describescalingprocesstypes

Below are the factors Repoman used to determine whether to keep or remove this permission:

CloudTrail Documentation Claims Support:	Yes
Has Repoman <i>*ever*</i> seen this API call recorded from any user/role in any account?	No
Has Repoman observed <i>*this*</i> role making the API call?	No
Does IAM Access Advisor think the service is being used by this role:	No
Based solely on CloudTrail data, we would:	maybe
With CloudTrail and Access Advisor, we would:	maybe

OK

```
    "sns:getendpointattributes", maybe
    "sns:getplatformapplicationattributes", maybe
    "sns:getsubscriptionattributes", remove
    "sns:gettopicattributes", remove
    "sns:listendpointsbyplatformapplication", maybe
    "sns:listplatformapplications", remove
    "sns:listsubscriptions", remove
    "sns:listsubscriptionsbytopic", remove
    "sns:listtopics", remove
    "sqs:getqueueattributes", maybe
    "sqs:listqueues", maybe
    "workspaces:describeworkspacebundles", remove
    "workspaces:describeworkspacedirectories", remove
    "workspaces:describeworkspaces" remove
  ],
  "Effect": "Allow",
  "Resource": [
    "*"
  ],
  "Version": "2012-10-17"
}
]
```

PROMOTE TO TEMPLATE

REGENERATE PROPOSAL

Repoman Benefits

Low-risk access reduction

Transparent and versioned operations

Enables innovation and high-velocity development

Security++

Rollie Pollie – AWS Permissions Management via ChatOps

ChatOps Basics



Otter T. Bot BOT 10:42 AM

New JIRAs Have Been Found in the CldSec Project

- [CLDSEC-4638](#) - Otters really like fish (Mike Grima/Auto-assigned to @jheffner)



██████████ 6:54 PM

@bhagen: I've a connectivity issue between jenkins slave (west, VPC) and E███ service (east, classic). This used to work before but is broken now, can someone help me?



Otter T. Bot BOT 6:54 PM

Hi! Security people take breaks too! Our normal operating hours are between 9AM and 5PM, Monday through Friday. We'll be sure to follow up, but if you have a critical issue please page "Cloud Security" via PagerDuty. For non-critical issues, please file a "CLDSEC" JIRA with as much detail as you can provide. Thanks!



Ben Hagen 6:59 PM

███, : is this urgent?



██████████ 7:00 PM

😊 no, will follow up with you tomorrow. Otter reminded me



Ben Hagen 7:00 PM

cool 😊 thanks!



Otter T. Bot BOT 10:02 AM

AWS Instance: i-0168 (r3.2xlarge - running)

- Identity: atlas_tier1-testapp-v010
- Account: 179 @netflix.com)
- Location: us-east-1c
- Security Groups:
- Network: 19

Rollie Pollie



Otter T. Bot BOT 8:53 AM

RolliePollie Template Changes

The following changes have been synced to the RolliePollie S3 bucket (inventory.json has been updated; RolliePollie will automatically scan for changes and create tickets where appropriate):

[~] roles/swordfish.json

A new job is awaiting approval

- **RP-10133** - IAM state differs from the 'roles/swordfish.json' template; will run RolliePollie in commit mode.



Otter T. Bot BOT 8:53 AM

RolliePollie Template Changes

The following changes have been synced to the RolliePollie S3 bucket (inventory.json has been updated; RolliePollie will automatically scan for changes and create tickets where appropriate):

[~] roles/swordfish.json

A new job is awaiting approval

- **RP-10133** - IAM state differs from the 'roles/swordfish.json' template; will run RolliePollie in commit mode.



Ben Hagen 8:58 AM

!describe RP-10133



Otter T. Bot BOT 8:58 AM

added a Plain Text snippet: [RolliePollie Role Sync 'roles/swordfish.json'](#)

```
1  [+] IAM Role Policy 'swordfish' does not match in [REDACTED]; would  
2  sync  
3  Curent state in IAM:  
4  {  
    "Statement": [  
      {  
        "Action": "iam:CreateRolePolicy",  
        "Effect": "Allow",  
        "Resource": "arn:aws:iam::[REDACTED]:role/[REDACTED]"  
      }  
    ]  
  }
```



Ben Hagen 8:58 AM

!describe RP-10133



Otter T. Bot BOT 8:58 AM

added a Plain Text snippet: [RolliePollie Role Sync 'roles/swordfish.json'](#)

```
1 [+] IAM Role Policy 'swordfish' does not match in [REDACTED]; would
  sync
2 Curent state in IAM:
3 {
4   "Statement": [
```



Ben Hagen 9:00 AM

!approve RP-10133



Otter T. Bot BOT 9:00 AM

💡 Sending Duo verification to approve **RP-10133** to [@bhagen](#) ...

👤 Verification succeeded! executing **RP-10133** (RolliePollie) with supplied parameters.

Rollie Pollie Benefits

Engineering-native workflows

Transparent decisions

Automated, secure, consistent

ChatOps allows quicker changes and reduced context switching

Security in the Development Lifecycle

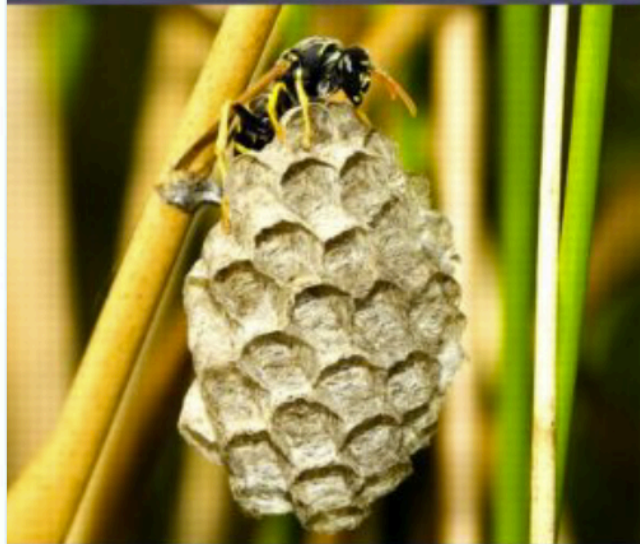
Building Secure Software

How to Avoid Security Problems the Right Way



John Viega
Gary McGraw
Foreword by Bruce Schneier

Secure and Resilient Software Development



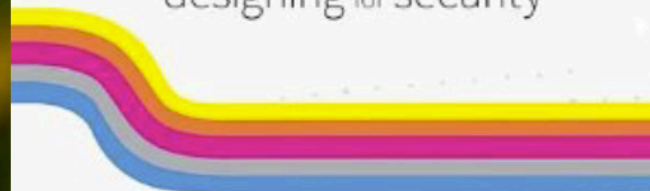
Mark S. Merkow ♦ Lakshminanth Raghavan

 CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Copyrighted Material
Adam Shostack
Microsoft's Threat Modeling Expert

threat modeling

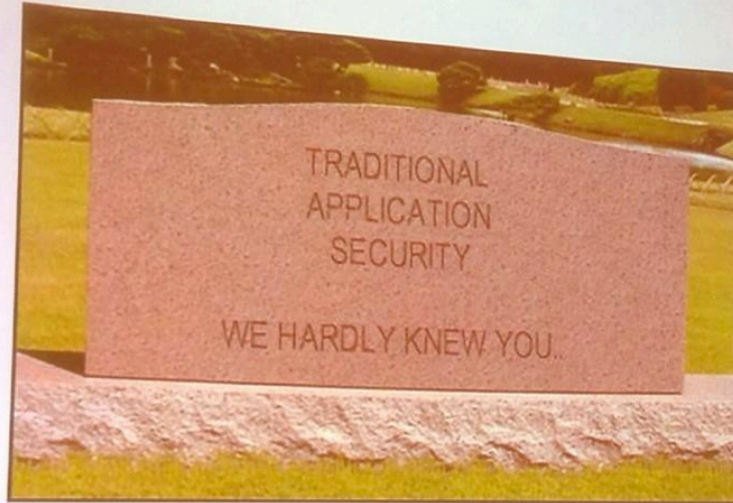
designing for security



Copyrighted Material

WI

A time to mourn...



Joshua Corman @joshcorman · Sep 19

Heh. Time to mourn Traditional AppSec - @matt_tesauro at #AppSecUSA #DevOps talk pic.twitter.com/i7vkT3UDwL

↩ Reply ↻ Retweet ★ Favorite

Flag media

Security in the Agile Lifecycle

1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	17. Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modelling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

17 steps across 7 phases 😞

Application Risk Assessment



Application Risk Assessment

Historic Issues

Spreadsheet and human-driven

One-time

Presupposes managed intake

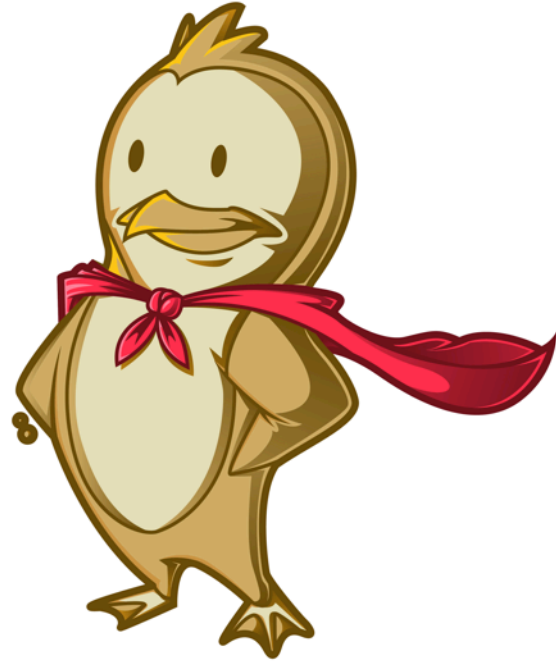
Now

Objective observability

Ongoing analysis

No humans required!

Penguin Shortbread: Automated Risk Analysis for Microservice Architectures



Penguin Shortbread Operation

Passively and continually analyze system dimensions, e.g.:

- Instance count
- Dependencies
- Connectivity to sensitive systems
- Internet-accessibility
- AWS account location

Risk Assessment

Develop risk scoring based on observations

Use risk scoring to prioritize efforts

Application Risk Metric

Metrics

Dependent Applications

Display Name: Dependent Application

Hint: How many application depend on this one?

Method value: Me
application_services.map{|s| s.application_dependencies.count}.sum

Metric type: integer

← Metric summary

Thresholds (5)

Operator	Value (low/primary)	Value (high/secondary)	Points	Result Text	Color
between?	5	9.9	5.0	Low	Yellow
between?	10	49.9	10.0	Medium	Orange
between?	50	99.9	15.0	High	Red
>=	100		25.0	Very High	Dark Red
<	5		0.0	Very Low	Blue

← Scoring →

Application Risk Rollup

CRYPTEX

Metric	prod				test			
	us-east-1	us-west-1	us-west-2	eu-west-1	us-east-1	us-west-1	us-west-2	eu-west-1
Dependent Applications	25 pts. (443)	10 pts. (19)	10 pts. (41)	25 pts. (194)	25 pts. (402)	10 pts. (34)	10 pts. (40)	25 pts. (166)
Edge	0 pts. (0)	0 pts. (0)	0 pts. (0)	0 pts. (0)	0 pts. (0)	0 pts. (0)	0 pts. (0)	0 pts. (0)
Instances	0 pts. (12)	0 pts. (2)	0 pts. (9)	0 pts. (2)	0 pts. (2)	0 pts. (2)	0 pts. (2)	0 pts. (2)
Uses Sensitive Services	10 pts. (1)	10 pts. (1)	10 pts. (1)	10 pts. (1)	10 pts. (1)	10 pts. (1)	10 pts. (1)	10 pts. (1)
Is Sensitive	25 pts. (1)	25 pts. (1)	25 pts. (1)	25 pts. (1)	25 pts. (1)	25 pts. (1)	25 pts. (1)	25 pts. (1)

Metrics



Risk metrics by region/environment



Developer View in Context

SECURITY BRAIN

Application Search

Search

PRESIDENT'S OFFICE (REED HASTINGS) > PRODUCT MANAGEMENT (NEIL HUNT) > CLOUD PLATFORM ENGINEERING (YURY IZRAILEVSKY) > CLOUD PLATFORM ENGINEERING (JASON CHAN)

Organization: Cloud Platform Engineering (Jason Chan)

Application	Organization	Security Risk Rating	Security Grade
scumblr	Cloud Platform Engineering (Bryan Payne)	High (200)	D
paymentsappsecquestion	Cloud Platform Engineering (Bryan Payne)	High (110)	C-

Penguin Shortbread Benefits

Low touch and ongoing

Objective and transparent view to application risk

Simple prioritization helps reduce cognitive load

Security Requirements

**Security
Requirements
via Production
Ready**

**PRODUCTION
READY**

A red stylized pen nib graphic, oriented horizontally. The nib has a small red dot at the tip. Below the nib are two curved, grey lines that resemble motion lines or a signature flourish.

Production Ready

SRE-driven developer outreach program

Evangelize well-established patterns and practices, e.g.:

- Deployment
- Monitoring and Alerting
- Testing

Automated scoring

Uncover risk and reward operational excellence

Security-Specific Production Ready Measures

App-Specific Security Group

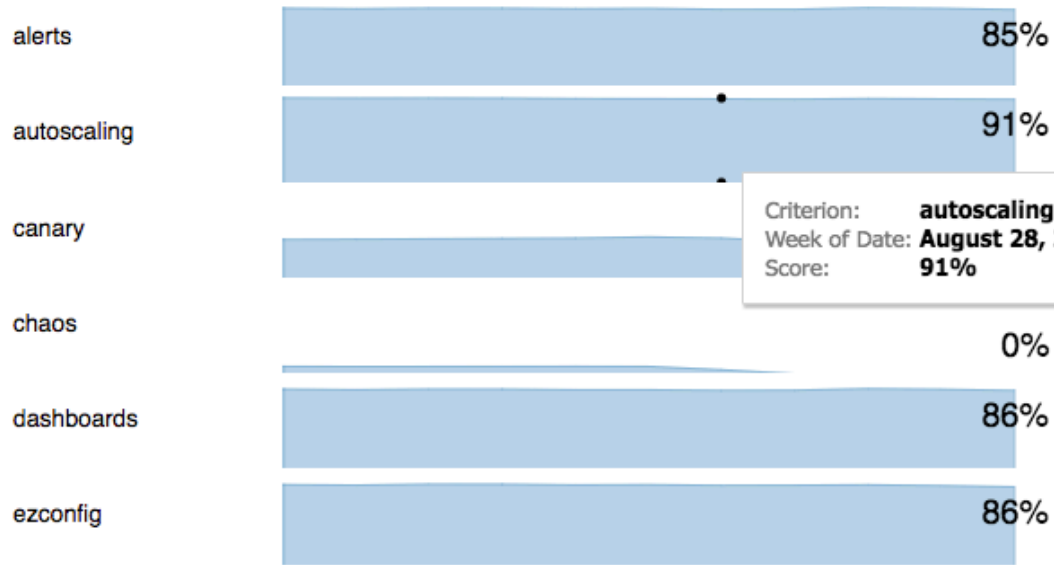
App-Specific IAM Role

No plaintext secrets in code

Production Ready Scorecard

Prod Ready Score

77%



Criterion: **autoscaling**
Week of Date: **August 28, 2016**
Score: **91%**



Tracking over time

Production Ready Benefits

Security integrated with other measures of readiness

Simple to evaluate compliance

Paved road lowers cognitive load

Easy to extend as capabilities expand

Takeaways

- Security teams can and should leverage the high-velocity development ecosystem
- Shared history provides both lessons and input to development
- Aim to make security more integrated and ubiquitous while also improving other system characteristics

NETFLIX

Questions?

Jason Chan

QCon San Francisco 2016

@chanjbs

