Cloud Security To Go

SANS Cloud Security Summit 2020

Steal these Ideas!

- **Ideas aren't worth jack unless other people can put them to use.**
- **Ideas won't change the world unless others can improve on them.**
- **Ideas grow by participation, not isolation.**
- **Ideas change as they grow. Their core remains the same, but their scope enlarges with successful use.**
- **Ideas have unexpected results. No one person can begin to imagine all the results of a good idea. That's another reason to welcome participation.**
- **Authority derives from originality and respect. You can't get respect for your original ideas unless those ideas prove useful to others.**

--Doc Searles, Linux Journal, 2006 “Ten ideas about Ideas”

Securing Cloud Deployments: A Red Team Perspective --Matt Burrough

Red Team Goals:

- Make the Blue Team Better
- Find Flaws Before the Attackers Do
- Prove Threats have Real World Impact

"Learn from the mistakes of others. You can't live long enough to make them all yourself." — **Eleanor Roosevelt**

1. **Lift & Shift Gone Wrong**
2. **Improperly Configured Storage**
3. **Secrets in Source Code**
4. **Insecure Network Settings**
5. **Social Engineering**
6. **Confusing Authentication for Authorization**
7. **Gray Clouds**

Threat Hunting in the Microsoft Cloud: The Times They Are a-Changin'

--John Stoner

"Over time, Clouds Change Shape"

Windows Event Logs + Azure AD logs + OneDrive Logs

- What accounts are being modified?
- What properties are being changed?

What can we operationalize?

Mapping to the ATT&CK Matrix

Play with the Splunk Datasets in Github

Static Analysis of Infrastructure as Code

--Barak Schoster Goihman

Configuration errors found in the wild ►

checkov
by bridgecrew

TerraGoat
by bridgecrew

Don't Just Lift and Shift! Why Traditional Controls Don't Always Apply to the Cloud and What You Can Do About It --Steve Turner

- **“You may not even know what you are logging”**
- **“Unwinding Technical Debt”**
- **“Don’t backhaul all the traffic”**

→Core Recommendations across Cloud Services

Cloud Native Controls + Add-on Controls (CASB, SWG, etc.)

AWS / Azure / Microsoft 365 / Salesforce / Workday

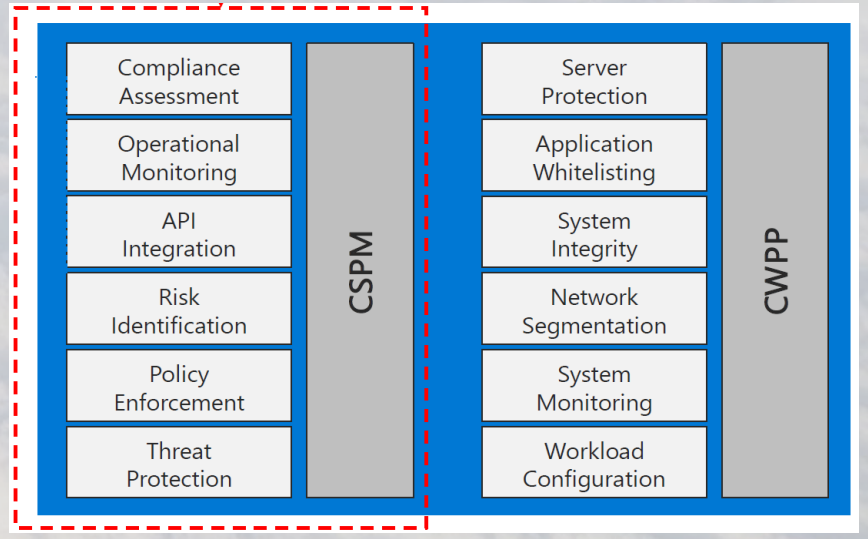
Cloud Security Posture Management from Security Hygiene to Incident Response

--Yuri Diogenes & Jess Huber

"37% of orgs have suffered a Cyberattack on Cloud Env due to Lack of Basic Cloud Security Hygiene"

- **Security Score**
- **Policy as Code / Policy Enforcement**
- **Targeted vs Commodity**

"Incident Response is the ability to go from one dumpster fire to another with no loss of enthusiasm." –Jess Huber



Cloud Security Posture Management (CSPM)
Cloud Workload Protection Platform (CWPP)

➔ Investigate these Software Categories

Modern Identity Strategies to Securely Manage Your Cloud Infrastructure
--Michael Soule

Goal: Consistent management across accounts of policies & roles

Storage Bucket + Serverless ➔ Deploy & Enforce Config

- Define a federation strategy
- Use specific permissions

Lots of Resources listed in the slides

Reimagining Vulnerability Management in the Cloud --Eric Zielinski

“Not all Apps need a full CI/CD pipeline”

Pets & Cattle & Ghosts (oh my!)

Golden Image Process (and Process Deviations)

10 Things that you should consider for cloud vulnerability management

- Accurate inventory
- Test zero-day response plan
- Process map all VM processes
- Plan for non-compliance

Doing Cloud in China
--Kenneth G. Hartman

- Extremely large market opportunities
- China Cloud Spend is ¼ of Global Spend
- Risks: IP Theft, Quality of Service, Compliance
- Specific Permits for Cloud Providers & Customers
- Alibaba is China's largest CSP
- AWS & Azure Operate in mainland China
- Play with as many cloud service providers as you can!

2020 Global Cloud Market

China Others

As a cloud security professional you may be expected support cloud operations in China at some point (soon) in your career

Lessons Learned from Cloud Security Incidents, Past and Present
--Dave Shackleford

Cloud Incidents are on the Rise!

- **Code Spaces:** I hope they didn't have the only copy of your code!
- **Azure Admin Keys:** What's in your images? API Key Attacks
- **CloudFlare:** Who is your proxy?
- **Tesla**: What's your attack surface?
- **Randsomware:** What's running on your compute?
- **Capital One:** How are you managing Roles?
- **MS Support DB Incident:** How are network changes managed?

'Those who cannot remember the past are condemned to repeat it."
--George Santayana-1905

Put a Lid on Those AWS S3 Buckets
--Lily Lee

- **Common S3 Bucket Errors → Best Practices**
- **How Cryptojacking Occurs**
- **Autoscaling Cryptominers**
- **> What to look for in CloudTrail**
- **> What to look for in S3 Access Logs**
- **> Bootstrapping an EC2 Instance**
- **> Looking in ELB Access Logs**

1. Review S3 bucket Permissions
2. Audit S3 bucket access
3. Securing the S3 Bucket Permissions
4. Reverting the Website Code version

- Core Security Practices
- Continuous Monitoring
- Access Logging
- Shared Responsibility

Cover Your SaaS: practical SaaS security tips --Ben Johnson

"Clouds talk to clouds"

"The absence of disease does not mean health."

Logins, Access / Priv Changes, Admin Activity

➢O365, GSuite, Salesforce, Dropbox, Box

Broadly Shared Files → Detecting over-sharing

"Oauth Attacks make MFA irrelevant"

"Operators don't need production access if the right data is flowing to the right place"

- **Turn review tasks into alerts**
- **Make Access have a half-life**
- **Lockdown what you can**
- **Easy to do the right thing**
- **Integrate it into the Biz**

Slow Attackers Down
&
Speed Defenders Up

Leveling-up Your Workforce for Cloud Enablement -- Aaron Lancaster

- **CISSP / CCSP**
- **CSA CCSK**
- **AWS Security Specialty**
- **Azure Security Engineer**
- **GIAC Cloud Security Automation (GCSA)**
- ***Other GIAC Cloud Certifications Planned!***

At Least 40% of all businesses will die in the next 10 years...if they do not figure out how to change their entire company to accommodate new technologies.

--John Chambers

Multi-Cloud Visibility for Large Organizations --Chris Farris

Cloud Sec Ops Problems at Scale

- "I've got 99 open buckets but this ain't one"
- External IP Address Space
- Multiple AWS Organizations
- Tech Sprawl

→ Don't put Lambda in all your accounts

- **Scorecards!!**

Alternatives:

- **AWS Config**
- **CloudMapper**

Build vs Buy Decision

http://www.chrisfarris.com
https://github.com/turnerlabs/antiope

Cloud Breaches: Case Studies, Best Practices, and Pitfalls

--Dylan Marcoux & Christopher Romano

- Rogue Devices and Shadow IT
- Credential Compromise via Public Exposure
- Cloud Platform Service Attacking
- Hybrid-Cloud Lateral Movement via Cloud App
- Third-Party Library Supply Chain Attack

“Gatekeeper”	**“Guard Rails”**	**“Night Watch”**
Robust IAM Solution	Assess & Enforce Existing Controls	Threat Detection & Response

Building a Pipeline for Secure Virtual Machines in AWS --Shaun McCullough

- **Start with a Solid VM Baseline**
- **Patch & Prepare**
- **Build a Deployable Image**
- **Redeploy Everywhere Daily**
- **Test (via the Pipeline)**
- **Optimize**

- **Know the provenance of your image!**
- **Enforce security policies via code**
- **Test before you deploy**
- **Never patch a live system**
- **Destroy old images**

Special Thanks

- **Matt Burrough**
- **John Stoner**
- **Barak Schoster Goihman**
- **Steve Turner**
- **Yuri Diogenes & Jess Huber**
- **Michael Soule**
- **Eric Zielinski**
- **Lily Lee & Melisa Napoles**
- **Ben Johnson**
- **Aaron Lancaster**
- **Chris Farris**
- **Dylan Marcoux**
- **Christopher Romano**
- **Shaun McCullough**

The SANS Summit Team

- Jennifer Santiago
- Emily Blades
- Brian Glennon
- Brian Corcoran
- Alison Kim
- Korrigan Roman
- Jessica Hill