SANS | CLOUD SECURITY

Can You Really Be More Secure in the Cloud?

Kenneth G. Hartman

SANS Rocky Mountain Fall 2022

About Me

"I help my clients earn and maintain the trust of their customers"

Kenneth G. Hartman

- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- SANS Instructor – SEC488: Cloud Security Essentials
  & SEC510: Public Cloud Security: AWS, Azure, and GCP

www.kennethghartman.com
@kennethghartman

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current client or previous employer.

© 2022 Kenneth G. Hartman – All Rights Reserved

Head In The Clouds

with Kenneth G. Hartman | SANS | GIAC CERTIFICATIONS

Show Notes for the Head in the Clouds YouTube Video Series

Episodes

- Episode 1 - Using jq to Get the Results You Need From Any Command Line Interface
- Episode 2 - Non-Public Buckets Can Still Leak Information
- Episode 3 – Things to Remember When using SSH in the Cloud
- Episode 4 - Use Terraform to Provision a Google Compute instance
- Episode 5 - Tips for success with Command Line Interfaces using BASH
- Episode 6 - Slice and Dice Data using grep, head, tail, cut, sort, tr, uniq and wc
- Episode 7 - Passively Evaluate a SaaS Provider's AppSec using ZAP

Background Story

A leader faces the decision regarding whether to move certain sensitive workloads into the cloud.

There are well-documented breaches and very public outages that raise the stakes

Can I trust the cloud?

© Kenneth G. Hartman – All Rights Reserved

The Problem

Company management clearly believes that they can save money and improve operations by transitioning to the cloud.

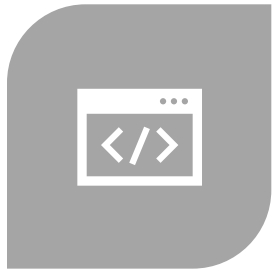
Management has assigned this “digital transformation initiative” to this technical leader and made it very clear everything that is at stake.

Fear, Uncertainty & Doubt

- Can I trust the cloud?
- What if everything goes wrong?
- I don’t feel prepared to lead this change
- I know that I don’t know what I don’t know
- What if they find out that I am faking it?

The Public Cloud Challenge

THE MAJOR CLOUD PROVIDERS HAVE NUMEROUS SERVICES



EACH SERVICE CAN BE CONFIGURED IN VARIOUS WAYS.

THE DEFAULT CONFIGURATIONS ARE TYPICALLY INSECURE

INDUSTRY MARKETING EFFORTS LEAVE ONE'S HEAD SPINNING.

Can the cloud be properly secured so that it is safe enough for my company's sensitive data?

We owe it to our customers and stakeholders to protect their sensitive data!

SANS CLOUD SECURITY CURRICULUM

sans.org/cloud-security @SANSCloudSec
linkedin.com/showcase/sanscloudsec sansurl.com/cloud-discord

SEC 388 — Introduction to Cloud Computing and Security
Ground school for cloud security

SEC 488 — Cloud Security Essentials (GCLD)
License to learn cloud security.

SEC 510 — Public Cloud Security: AWS, Azure & GCP (GPCS)
Multiple clouds require multiple solutions.

SEC 522 — Application Security: Securing Web Apps, APIs, and Microservices (GWEB)
Not a matter of "if" but "when."
Be prepared for a web attack. We'll teach you how.

SEC 541 — Cloud Security Attacker Techniques, Monitoring, and Threat Detection
Attackers can run but not hide. Our radar sees all threats.

SEC 540 — Cloud Security & DevSecOps Automation (GCSA)
The cloud moves fast. Automate to keep up.

SEC 549 — Enterprise Cloud Security Architecture
Design it right from the start.

SEC 557 — Cloud Security Continuous Compliance
Measure what matters, not what's easy.

SEC 588 — Cloud Penetration Testing (GCPN)
Aim your arrows to the sky and penetrate the cloud.

FOR 509 — Enterprise Cloud Forensics & Incident Response (GCFR)
Find the storm in the cloud.

MGT 516 — Managing Security Vulnerabilities: Enterprise and Cloud
Stop treating the symptoms. Cure the disease.

MGT 520 — Leading Cloud Security Design and Implementation
Chart your course to cloud security.

SANS

CLOUD SECURITY

Flight Plan – Career Progression

CURRICULUM

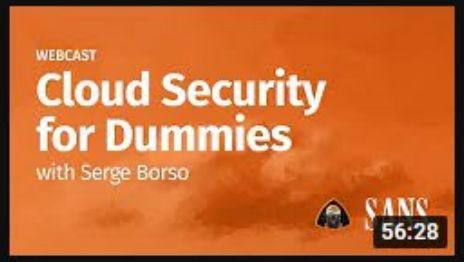
	DevOps Professionals	Cloud Security Analyst	Cloud Security Engineer	Cloud Security Architect	Cloud Security Manager
	Develop, deploy, and manage secure applications and systems	Use cloud security solutions to respond to incidents and enable defenses	Build security solutions for cloud workflows	Design how security functions will adopt cloud services, define knowledge, tooling, and approach for cloud solutions	Develop cloud security roadmap, plan, procurement models, ensure policy and procedure is defined
BASELINE					
SEC 388 — Introduction to Cloud Computing and Security *Ground school for cloud security*		●			●
FOUNDATIONAL					
SEC 488 — Cloud Security Essentials (GCLD) *License to learn cloud security.*		●	●	●	●
CORE					
SEC 510 — Public Cloud Security: AWS, Azure, and GCP (GPCS) *Multiple clouds require multiple solutions.*	●	●	●	●	
SEC 540 — Cloud Security and DevSecOps Automation (GCSA) *The cloud moves fast. Automate to keep up.*	●		●	●	
SEC 541 — Cloud Security Attacker Techniques, Monitoring, and Threat Detection *Attackers can run but not hide. Our radar sees all threats.*		●	●		
SEC 549 — Enterprise Cloud Security Architecture *Design it right from the start.*			●	●	●
SPECIALIZATION					
SEC 522 — Application Security: Securing Web Apps, APIs, and Microservices (GWEB) *Not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.*	●				
SEC 557 — Cloud Security Continuous Compliance *Measure what matters, not what's easy.*		●			●
SEC 588 — Cloud Penetration Testing (GCPN) *Aim your arrows to the sky and penetrate the cloud.*		●	●		
FOR 509 — Enterprise Cloud Forensics and Incident Response (GCFR) *Find the storm in the cloud.*		●			
MANAGEMENT					
MGT 516 — Managing Security Vulnerabilities: Enterprise and Cloud *Stop treating the symptoms. Cure the disease.*				●	●
MGT 520 — Leading Cloud Security Design and Implementation *Chart your course to cloud security.*				●	●

SANS Cloud Security

6.9K subscribers

SUBSCRIBED

HOME | VIDEOS | PLAYLISTS | COMMUNITY | CHANNELS | ABOUT



Cloud Security for Dummies

SANS Cloud Security • 3K views • 8 months ago

Let's take a moment to break down a few things at a basic level: - What is the cloud? - How does it work? - How do you begin to secure it? This webcast is for you if: - You are in need of...

Uploads

PLAY ALL

Quick Wins in Cloud Compliance: Azure

Multicloud Security is Inevitable: Fact or Fiction

Quick Wins in Cloud Compliance: AWS

Free, Virtual, Half-Day, Multi-Lingual SANS 2022 Cloud...

SANS Secure Code Training for Developers

Kubernetes Attack and Defense: Break Out and...

CLOUD ACE

TAKING OFF INTO CYBERSECURITY

CLOUD ACE PODCAST - SEASON 1

Hosted by Brandon Evans

SANS

Discord

JOIN THE COMMUNITY

SANS CLOUD SECURITY

sansurl.com/cloud-discord

CloudSecNext

Summit 2022

FREE Virtual Summit: May 3–4
Courses: May 5–10

Live Online

SANS

Can You Really Be More Secure in the Cloud?

Ten Reasons Why

1. API-First Cloud Control Plane

- Well-documented REST Application Programming Interface (API)
- Strong authentication and granular access control
- All API calls are logged
- All changes are made via API Calls
  - Web Console
  - Command Line Interface (CLI)
  - Software Development Kits (SDK)
  - Other Tools
  - Other Cloud Services

} **REST API Calls**

CLI Example

```
aws ec2 describe-instances
```


```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                "AmiLaunchIndex": 0,
                "ImageId": "ami-0abcdef1234567890,
                "InstanceId": "i-1234567890abcdef0,
                "InstanceType": "t2.micro",
                "KeyName": "MyKeyPair",
                "LaunchTime": "2018-05-10T08:05:20.000Z",
                "Monitoring": {
                    "State": "disabled"
                },
                "Placement": {
                    "AvailabilityZone": "us-east-2a",
                    "GroupName": "",
                    "Tenancy": "default"
                },
                "PrivateDnsName": "ip-10-0-0-157.us-east-2.compute.internal",
                "PrivateIpAddress": "10.0.0.157",
                "ProductCodes": [],
                "PublicDnsName": "",
                "State": {
                    "Code": 0,
                    "Na          ding"
```

One-Line CLI Script Example

```
for region in $(aws ec2 describe-regions \
--query 'Regions[].RegionName' --output text); \
do aws ec2 describe-instances --region $region \
--output table --query
'Reservations[].Instances[*].[InstanceId,State.Name,Placement.Availabilityzone,PublicIpAddress,LaunchTime]'; done
```

```
----------------------------------------------------------------------------------------
|                                   DescribeInstances                                  |
+---------------------+----------+-------------+----------------+-----------------------------+
|  i-0206766afa3124133|  running |  us-east-1c |  18.210.12.130 |  2021-07-22T23:38:59+00:00  |
|  i-057026ecacfbfa82d|  running |  us-east-1c |  3.239.21.164  |  2021-07-22T23:38:59+00:00  |
+---------------------+----------+-------------+----------------+-----------------------------+
----------------------------------------------------------------------------------------
|                                   DescribeInstances                                  |
+---------------------+----------+-------------+----------------+-----------------------------+
|  i-0e8bf8668aabfefcd|  running |  us-east-2a |  13.58.143.127 |  2021-07-22T23:39:52+00:00  |
+---------------------+----------+-------------+----------------+-----------------------------+
----------------------------------------------------------------------------------------
|                                   DescribeInstances                                  |
+---------------------+----------+-------------+----------------+-----------------------------+
|  i-04ef44375c4f7a83a|  running |  us-west-2a |  54.218.59.234 |  2021-07-22T23:40:42+00:00  |
+---------------------+----------+-------------+----------------+-----------------------------+
```

https://headintheclouds.site/episodes/episode9

CIS Controls Cloud Companion Guide

Center for Internet Security®

Applicability Overview for Each Service Model

Applicability of Service Model

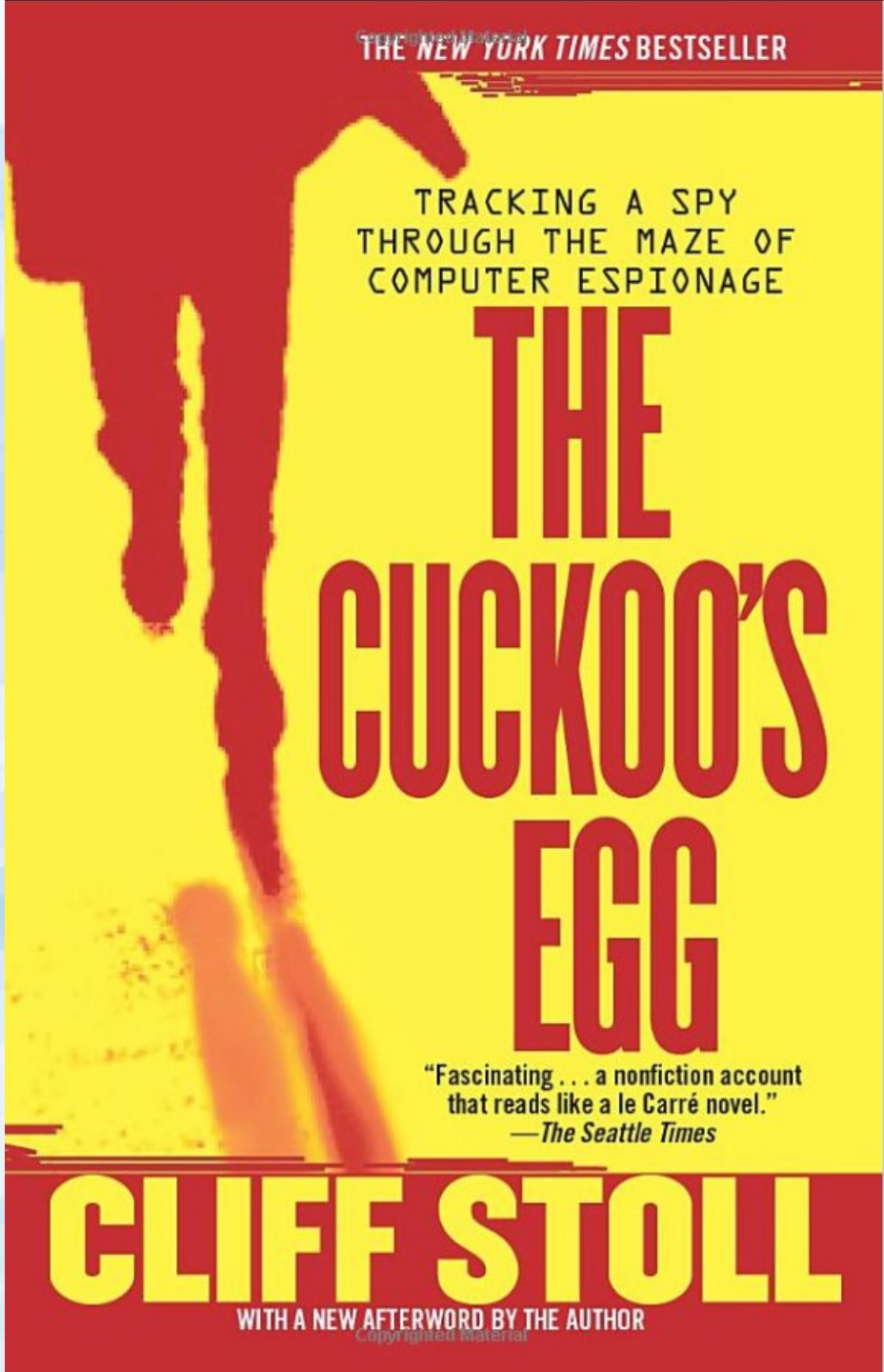
- More than 60% of CIS Safeguards Apply
- Between 60% and 0% of the CIS Safeguards Apply
- 0%

CONTROL	CONTROL TITLE	IaaS	PaaS	SaaS	FaaS
01	Inventory and Control of Enterprise Assets	●	●	○	○
02	Inventory and Control of Software Assets	●	●	●	●
03	Data Protection	●	●	◐	◐
04	Secure Configuration of Enterprise Assets and Software	●	●	◐	◐
05	Account Management	●	●	●	●
06	Access Control Management	●	●	●	●
07	Continuous Vulnerability Management	●	●	◐	◐
08	Audit Log Management	●	●	●	●
09	Email and Web Browser Protections	●	●	●	◐
...	...re Defenses				○

2. Pay-as-you-go Billing

- You pay for every resource that you use
- You pay only when you use the resource
- Precise metering of resource utilization
- Detect fraud and abuse
- Detect abandoned resources

The Cuckoo's Egg is a story about a Unix admin who investigated a $0.75 system charge and discovered "a maze of computer espionage." Published in 1990.



3. Infrastructure as Code (IaC)

- Infrastructure as Code is the managing and provisioning of infrastructure via code rather than using a manual process
- IaC can be stored in a Source Code Control System
- Repeatable. Test environments exactly like Prod

WARNING: Do not deploy half the environment using IaC and the other half manually.

HashiCorp Terraform

```
resource "aws_instance" "web" {
  ami           = data.aws_ami.ubuntu.id
  instance_type = "t2.micro"

  tags = {
    Name = "SANS-System1"
  }
}
```

https://www.terraform.io/language/syntax/configuration

© Kenneth G. Hartman – All Rights Reserved

```
.
├── LICENSE
├── README.md
├── main.tf
├── modules
│   ├── aws
│   │   ├── README.md
│   │   ├── keyPair.tf
│   │   ├── main.tf
│   │   ├── network.tf
│   │   ├── output.tf
│   │   ├── terraform.tfvars.example
│   │   ├── variables.tf
│   │   └── vm.tf
│   ├── azure
│   │   ├── README.md
│   │   ├── main.tf
│   │   ├── network.tf
│   │   ├── output.tf
│   │   ├── resource_group.tf
│   │   ├── terraform.tfvars.example
│   │   ├── variables.tf
│   │   └── vm.tf
│   └── gcp
│       ├── README.md
│       ├── ip_address.tf
│       ├── main.tf
│       ├── network.tf
│       ├── output.tf
│       ├── terraform.tfvars.example
│       ├── variables.tf
│       └── vm.tf
├── output.tf
├── terraform.tfvars.example
└── variables.tf
```

```
~/tf-vm_in3csps$ cat terraform.tfvars.example
# AWS Variables
aws_region = "us-east-1"
aws_creds_file = "~/.aws/credentials"
aws_profile = "default"

# Azure Variables
azure_location = "Central US"

# GCP Variables
gcp_project = "PROJECT_ID"
gcp_region  = "us-central1"
gcp_zone    = "us-central1-a"
gcp_key_file = "~/accesskey/service_account.json"

# Common Variables
ssh_user ="ubuntu"
ssh_pub_key_file = "~/.ssh/id_rsa.pub"
ssh_priv_key_file = "~/.ssh/id_rsa"
```

https://headintheclouds.site/episodes/episode10

What if we could check our Infrastructure-as-Code for security vulnerabilities *before* deployment?

©2019 Kenneth G. Hartman – All Rights Reserved

4. Policy as Code

An approach to policy management in which policies are defined, updated, shared, and enforced using code.

- The idea of writing code in a high-level language to manage and automate policies.
- Move more quickly and reduce the potential for mistakes due to human error.
- By representing policies as code in text files, proven software development best practices can be adopted such as version control, automated testing, and automated deployment.

Examples of Policy as Code Tools

- **Chef InSpec** - an open-source testing framework for infrastructure with a human- and machine-readable language for specifying compliance, security and policy requirements.
- **Open Policy Agent (OPA)** - an open source, general-purpose policy engine that enables unified, context-aware policy enforcement across the entire stack.
- **Hashicorp Sentinel** - a language and framework for policy built to be embedded in existing software to enable fine-grained, logic-based policy decisions. A policy describes under what circumstances certain behaviors are allowed.
- **Pulumi CrossGuard** - empowers you to set guardrails to enforce compliance for resources so developers within an organization can provision their own infrastructure while sticking to best practices and security compliance.
- **PacBot** - a platform for continuous compliance monitoring, compliance reporting and security automation for the cloud. In PacBot, security and compliance policies are implemented as code.

©2019 Kenneth G. Hartman – All Rights Reserved

Checkov is a static code analysis tool for scanning infrastructure as code (IaC) files for misconfigurations that may lead to security or compliance problems.

Checkov includes more than 750 predefined policies to check for common misconfiguration issues.

Checkov also supports the creation and contribution of custom policies.

https://www.checkov.io/

©2019 Kenneth G. Hartman – All Rights Reserved

5. Continuous Integration/Continuous Delivery (CI/CD) Pipelines

- A CI/CD pipeline **automates your software delivery process.** The pipeline builds code, runs tests, and safely deploys a new version of the application.
- Automated pipelines **remove manual errors**, provide **standardized feedback loops** to developers, and **enable fast product iterations**.
- Any systems not deployed using IaC and CI/CD should be considered technical debt.

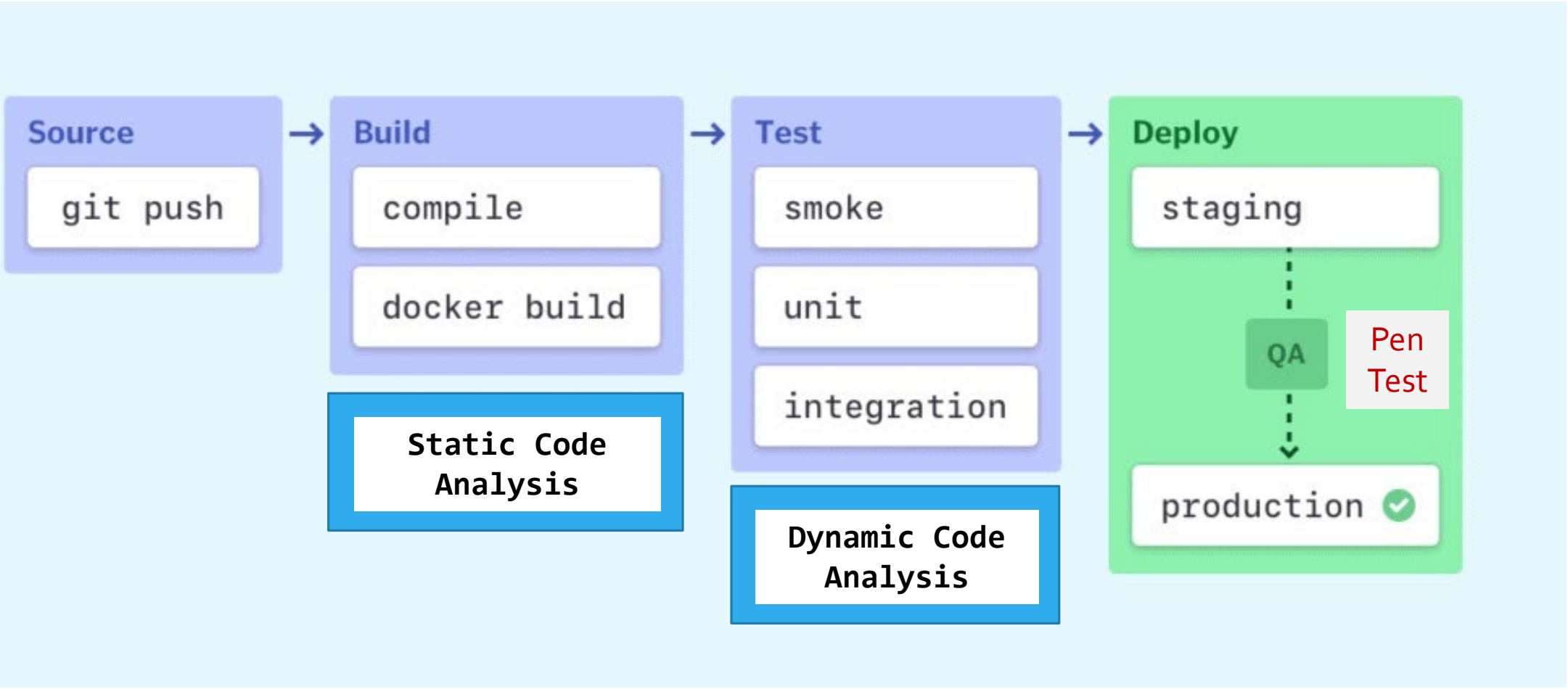
Electrify the Fence – Anything new that is not deployed by CI/CD and any Administrative Access to a Production System should be treated as an "Incident" and require a root cause analysis.

CI/CD Benefits & Advantages

- Developers can stay focused on writing code and monitoring the behavior of the system in production.
- QA and product stakeholders have easy access to the latest, or any, version of the system.
- Product updates are not stressful.
- Logs of all code changes, tests and deployments are available for inspection at any time.
- Rolling back to a previous version in the event of a problem is a routine push-button action.
- A fast feedback loop helps build an organizational culture of learning and responsibility.

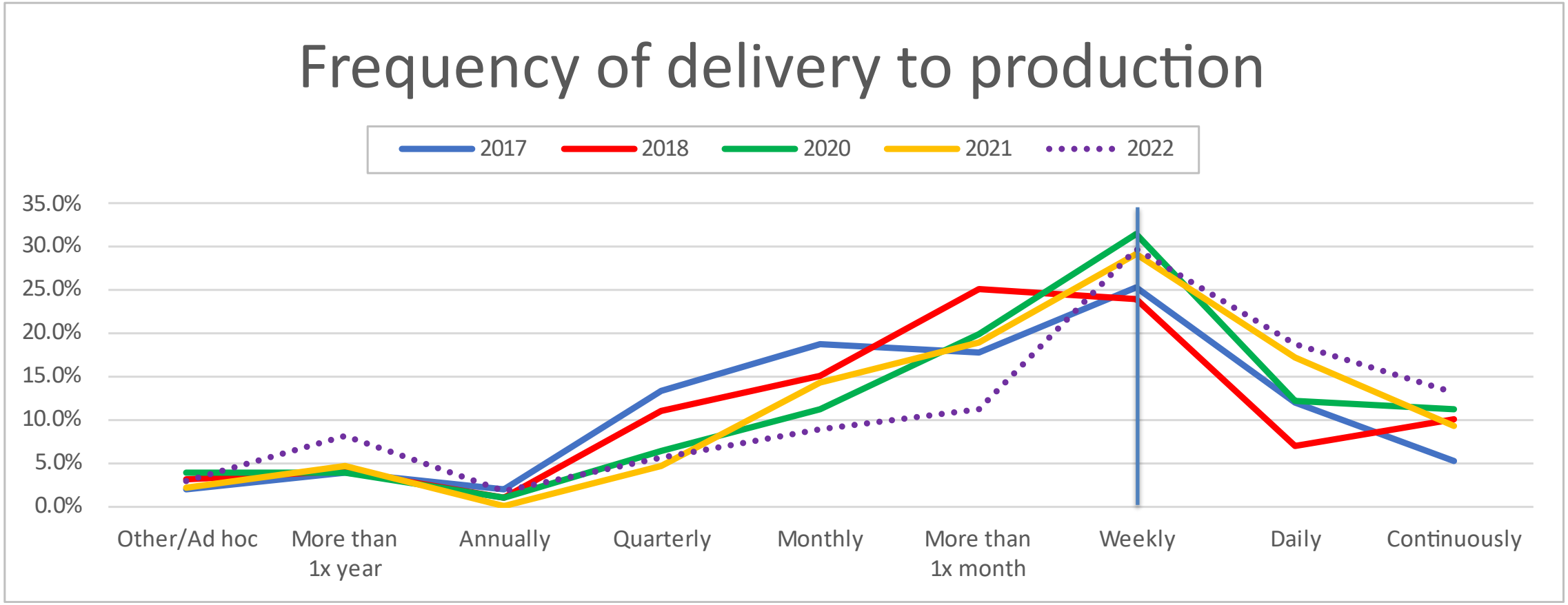
© Kenneth G. Hartman – All Rights Reserved

Stages of a CI/CD Pipeline

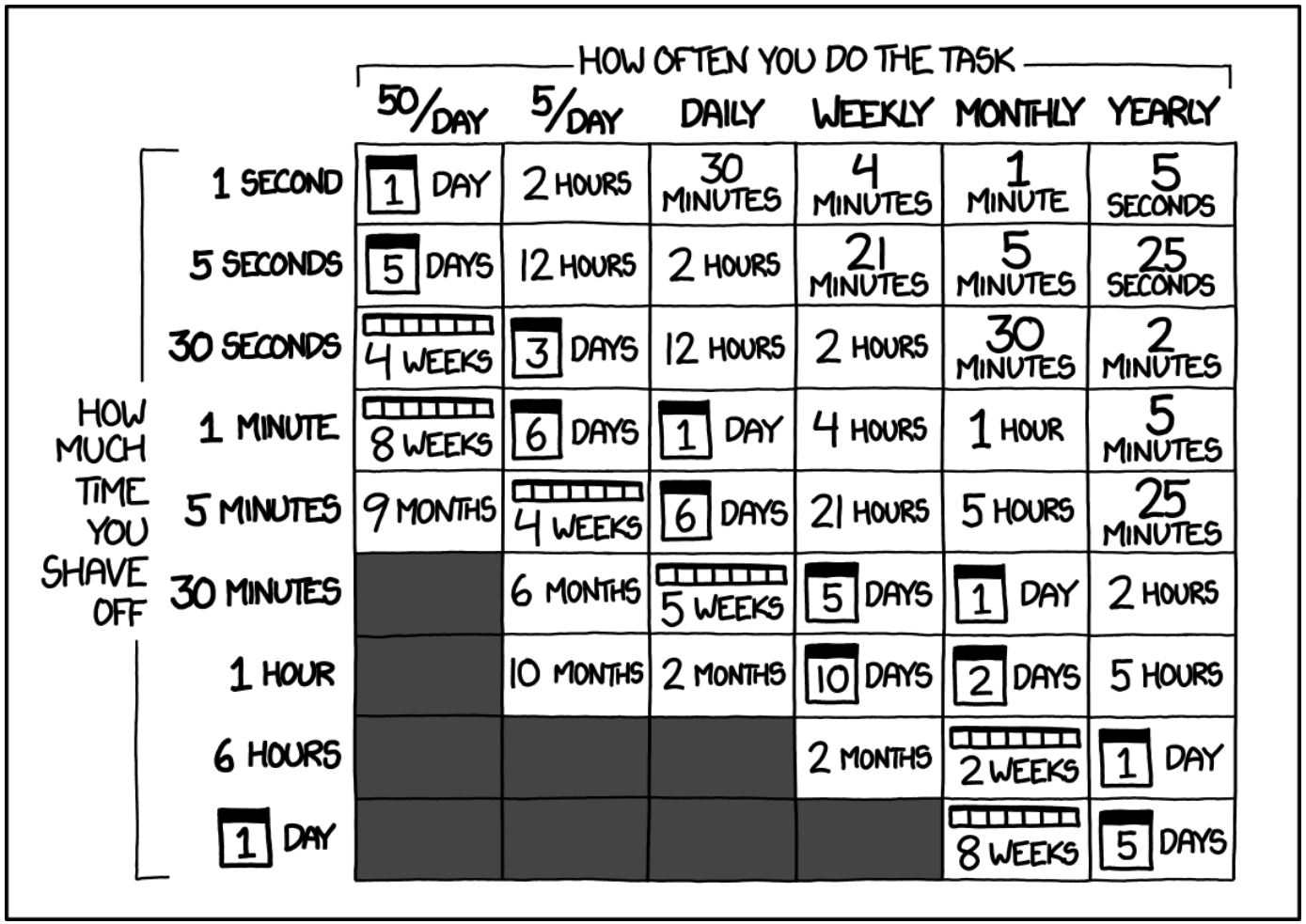


©2019 Kenneth G. Hartman – All Rights Reserved

Security at Velocity



©2022 SANS™ Institute | www.sans.org



https://xkcd.com/1205/

6. Immutable Infrastructure

What if our services were already patched, hardened, configured, and tested ***before*** they were provisioned into production?

➔*Wait, that should be the goal of CI/CD!*

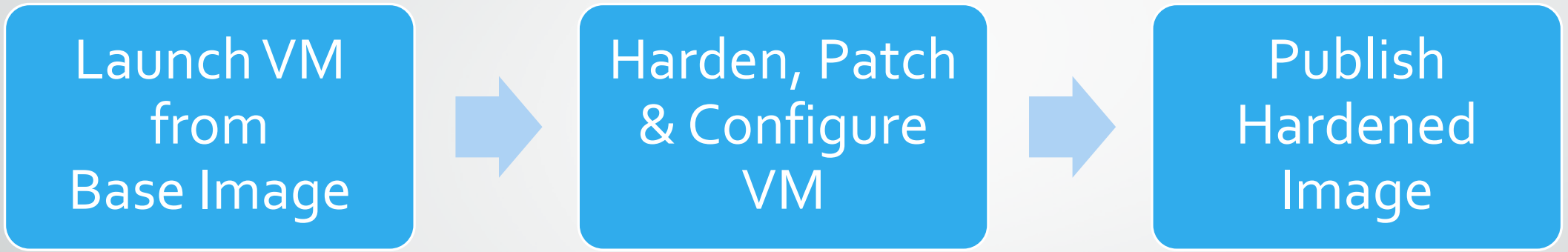
How can we be secure if we do not patch our Virtual machines in place?

➔*Rotate VMs frequently using a fresh image*

What if we need to SSH in and make a configuration change?

➔ *Do a root cause analysis and determine how to avoid changes outside of the CI/CD pipeline*

Image Hardening

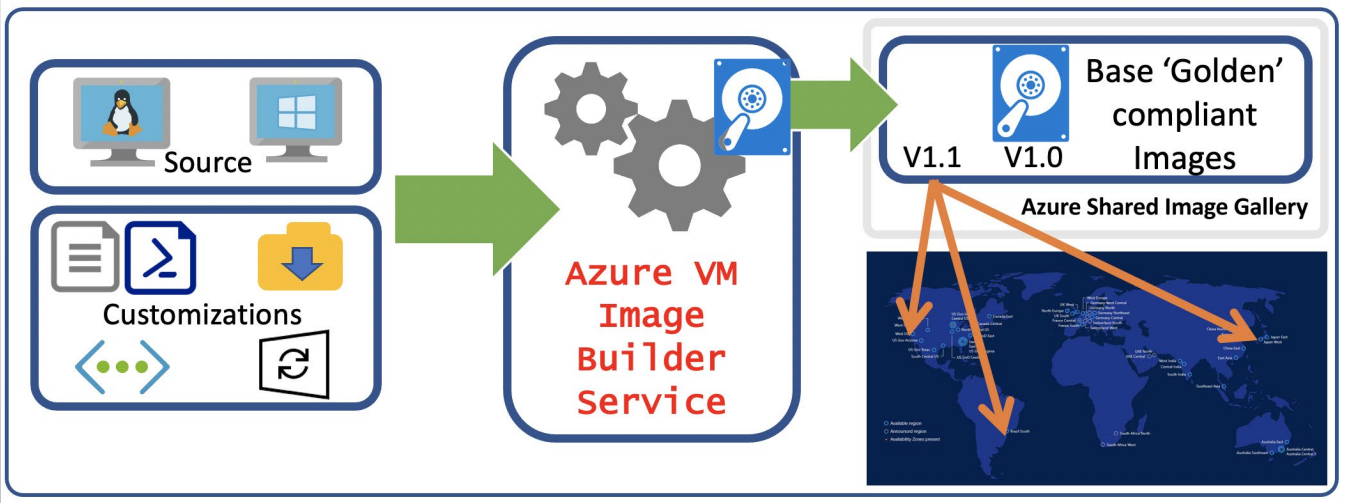


- *Perform this as a service for other teams to consume!*
- *"Hardened Images-as-a-Service"*

©2019 Kenneth G. Hartman – All Rights Reserved

Automate the VM Image Baking Process

- HashiCorp Packer – https://www.packer.io/
- Azure Image Builder – https://docs.microsoft.com/en-us/azure/virtual-machines/image-builder-overview
- AWS EC2 Image Builder – https://aws.amazon.com/image-builder/



©2019 Kenneth G. Hartman – All Rights Reserved

© Kenneth G. Hartman – All Rights Reserved | www.kennethghartman.com

7. Cloud Security Posture Management (CPSM)

- A class of security tools that are designed to identify misconfiguration issues and compliance risks in the cloud.
- Continuously monitors cloud infrastructure for gaps in security policy enforcement.
- These tools compare a cloud environment against a defined set of best practices and known security risks.
- Some CSPM tools will alert the cloud customer when there is a need to remediate a security risk, while other more sophisticated CSPM tools will use robotic process automation (RPA) to remediate issues automatically.

Key capabilities of CSPM

- Detect and perhaps automatically remediate cloud misconfigurations;
- Maintain an inventory of best practices for different cloud configurations and services;
- Map current configuration statuses to a security control framework or regulatory standard;
- Work with IaaS, SaaS and PaaS platforms in containerized, hybrid cloud and multi-cloud environments; and
- Monitor storage buckets, encryption and account permissions for misconfigurations and compliance risks.

©2019 Kenneth G. Hartman – All Rights Reserved

CLOUD CUSTODIAN

- Cost Saving
- Tagging
- Security
- Compliance
- Operations
- Inventory

©2019 Kenneth G. Hartman – All Rights Reserved

CSP Security Management Services

AWS Security Hub

Azure Defender for Cloud

Google Cloud Security Command Center

© Kenneth G. Hartman – All Rights Reserved

CLOUD SECURITY SERVICE MATRIX

SANS CLOUD SECURITY

	Used for...	Amazon Web Services (AWS)	Azure	Google Cloud Platform (GCP)
IDENTITY & ACCESS MANAGEMENT	Manage user access and encryption keys	AWS Identity & Access Management (IAM)	Azure Active Directory (Azure AD)	GCP Identity & Access Management (IAM)
	Cloud single-sign-on (SSO) service	AWS Single Sign-On	Azure Active Directory (Azure AD)	Cloud Identity
	Identity management for your apps	Amazon Cognito	Azure Active Directory (Azure AD)	Firebase Authentication
	Managed Microsoft Active Directory	AWS Directory Service	Azure Active Directory Domain Services	Managed Service for Microsoft Active Directory
	Secure service to share resources	AWS Resource Access Manager	Azure Resource Manager	Resource Manager
	Centrally governing and management across accounts	AWS Organizations	Azure Governance	
N	Security and compliance center	AWS Security Hub	Microsoft Defender for Cloud	Security Command Center
	Threat detection	Amazon GuardDuty	Microsoft Defender for Cloud	Security Command Center

Auditing Cloud Security Posture

Multi-Cloud

- CloudSploit by Aqua - https://github.com/aquasecurity/cloudsploit
- Scout Suite by NCC Group - https://github.com/nccgroup/ScoutSuite

AWS

- Prowler - https://github.com/prowler-cloud/prowler

Azure

- Azucar - https://github.com/nccgroup/azucar

GCP

- Forseti Security - https://forsetisecurity.org/

© Kenneth G. Hartman – All Rights Reserved

8. Cloud Workload Protection Platforms (CWPP)

- Hardening, configuration, and vulnerability management
- Network firewalling, visibility, and microsegmentation
- System integrity assurance
- Application control and allow listing
- Exploit prevention and memory protection
- Server workload endpoint detection and response (EDR), behavioral monitoring, and threat detection and response
- Host-based intrusion prevention with vulnerability shielding
- Anti-malware scanning

Microsoft Defender for Cloud | Overview

Showing 54 subscriptions

Search
Subscriptions
What's new

General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems

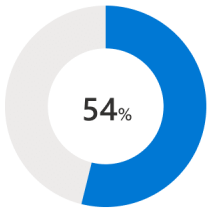
Cloud security
Secure score
Regulatory compliance
Workload protection

54 Azure subscriptions
4 AWS accounts
18 GCP projects
8928 Assessed resources
215 Active recommendations
7768 Security alerts

Secure score

Unhealthy resources
7566 To harden these resources and improve your score, follow the security recommendations

Current secure score



COMPLETED
Controls 0/15

COMPLETED
Recommendations 24/99

Improve your secure score >

Regulatory compliance

Azure security benchmark
2 of 44 passed controls

Lowest compliance regulatory standards
by passed controls

CMMC Level 3	0/55
ISO 27001	1/20
AWS CIS 1.2.0	3/43

Improve your compliance >

Firewall manager

5 Firewalls
3 Firewall policies
4 Regions with firewalls

Network protection status
by resource

Virtual hubs	0/0
Virtual networks	8/126

Improve your network security>

Inventory

Unmonitored VMs
54 To better protect your organization, we recommend Install agents

Total resources
8928

Unhealthy (7566) Healthy (1156) Not applicable (206)

Explore your resources >

Information protection Preview

Integrated with Purview

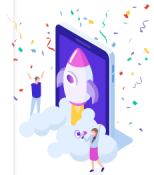
Resource scan coverage
2% For full coverage scan additional resources

Recommendations & Alerts
by classified resouces

View classified resources in inventory >

Insights

Upgrade to New Containers plan



Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

Click here to upgrade >

Most prevalent recommendations

Audit diagnostic setting	619 Resources
Storage account public access should...	161 Resources
A vulnerability assessment solution...	107 Resources

Most attacked resources

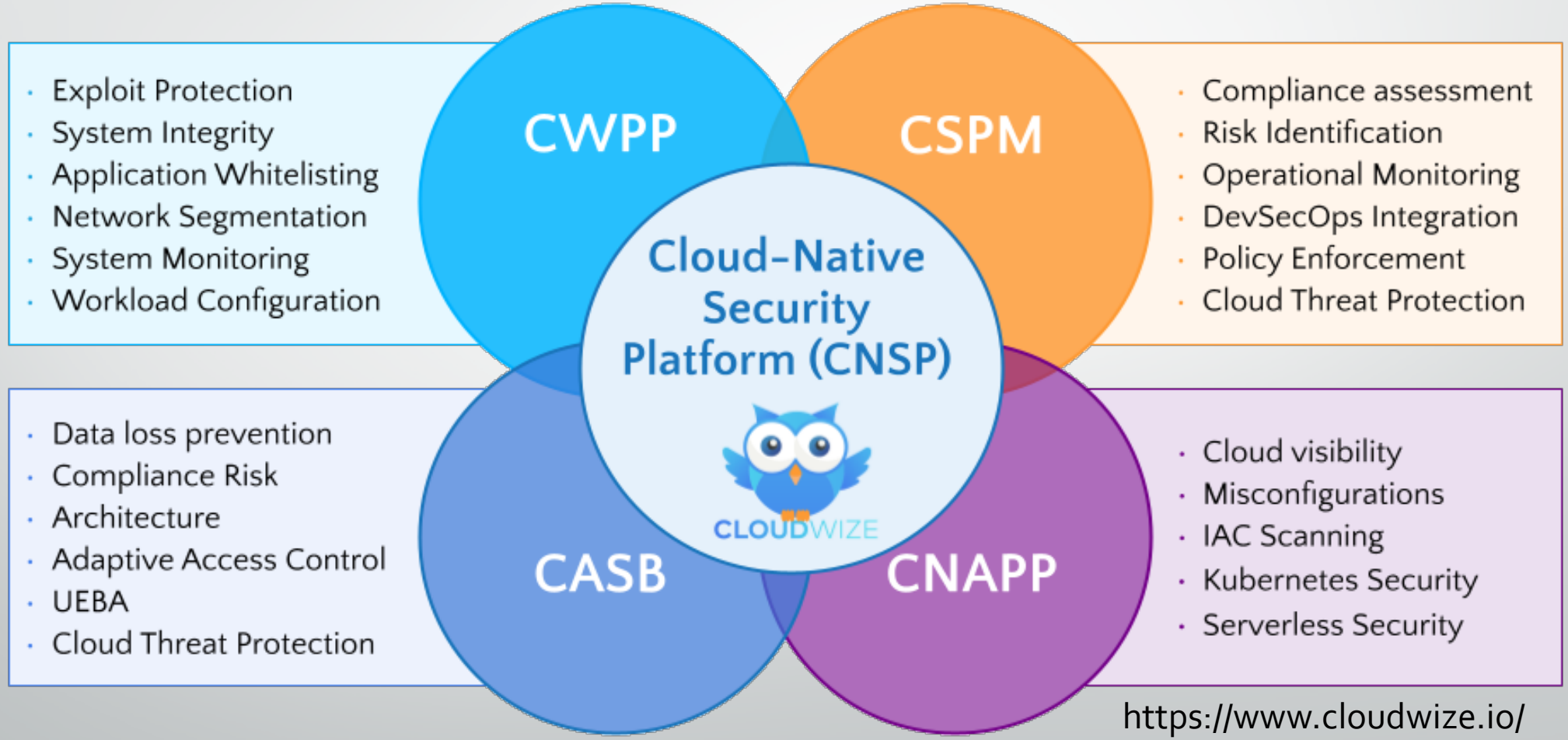
contoso5.cloudapp.net	63 Alerts
Virtual machine 2	41 Alerts
CentOS	28 Alerts

View full alert list >

Controls with the highest potential increase

Remediate vulnerabilities	+11% (6pt)
Enable encryption at rest	+7% (4pt)

Cloud Security Tool Groups

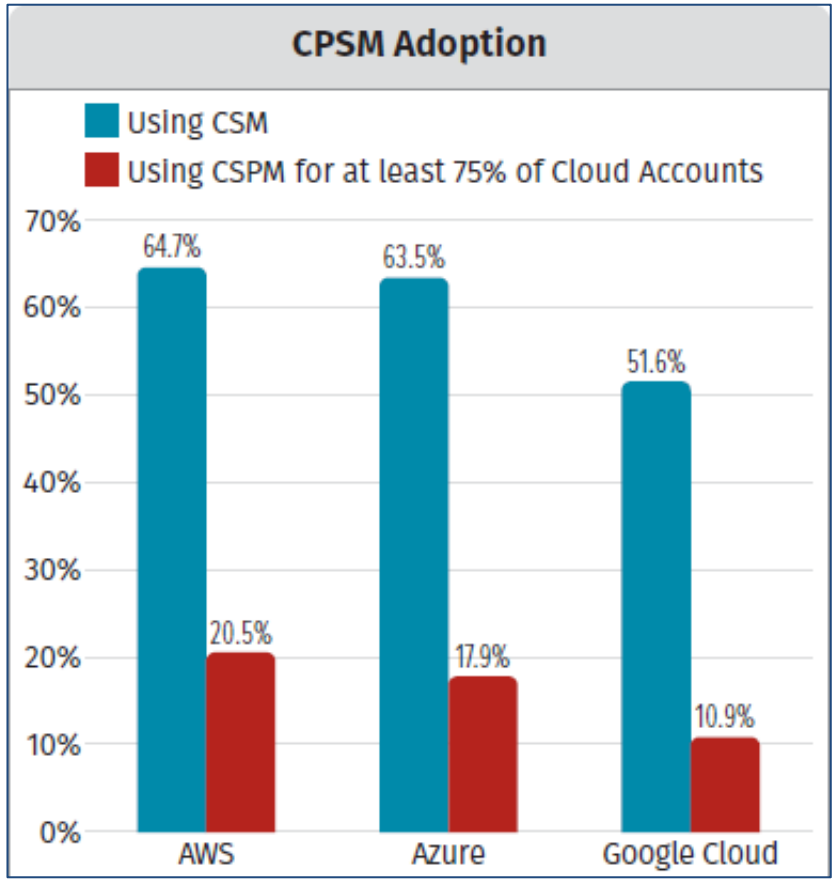


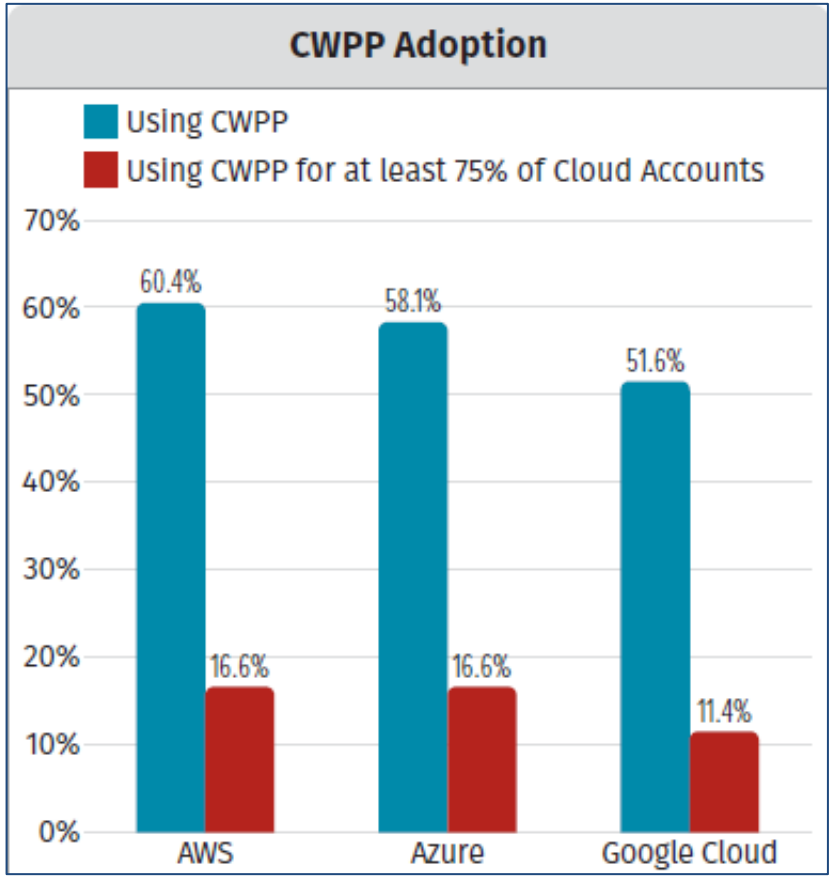
https://www.cloudwize.io/

©2019 Kenneth G. Hartman – All Rights Reserved

Analyst Program

Securing Cloud Environments at Scale





©2022 SANS™ Institute | www.sans.org

9. Zero Trust Architectures

The Zero Trust Model

Based on "Never Trust, Always Verify" Principle

Verify Every User

Validate Every Device

Enforce Least Privilege Access

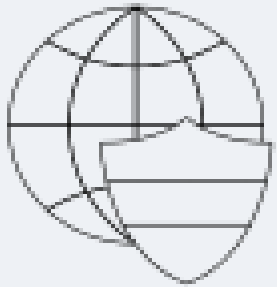
ZT is a data-centric security architecture centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and must verify everything trying to connect to its resources before granting access - based on identity, device and data/resource.

https://www.youtube.com/watch?v=56VRwg7apkY

Is
Zero Trust
a
Buzz Word
Yet?

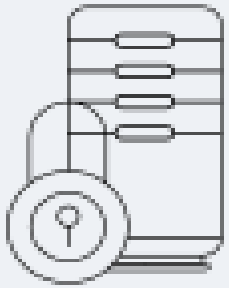
© Kenneth G. Hartman – All Rights Reserved

Google's BeyondCorp Initiative



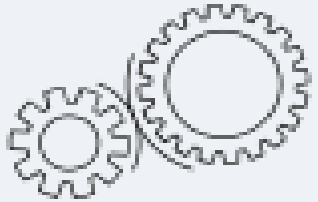
Perimeterless Design

Connecting from a particular network must not determine which services you can access.



Context-Aware

Access to services is granted based on what we know about you and your device.



Dynamic Access Controls

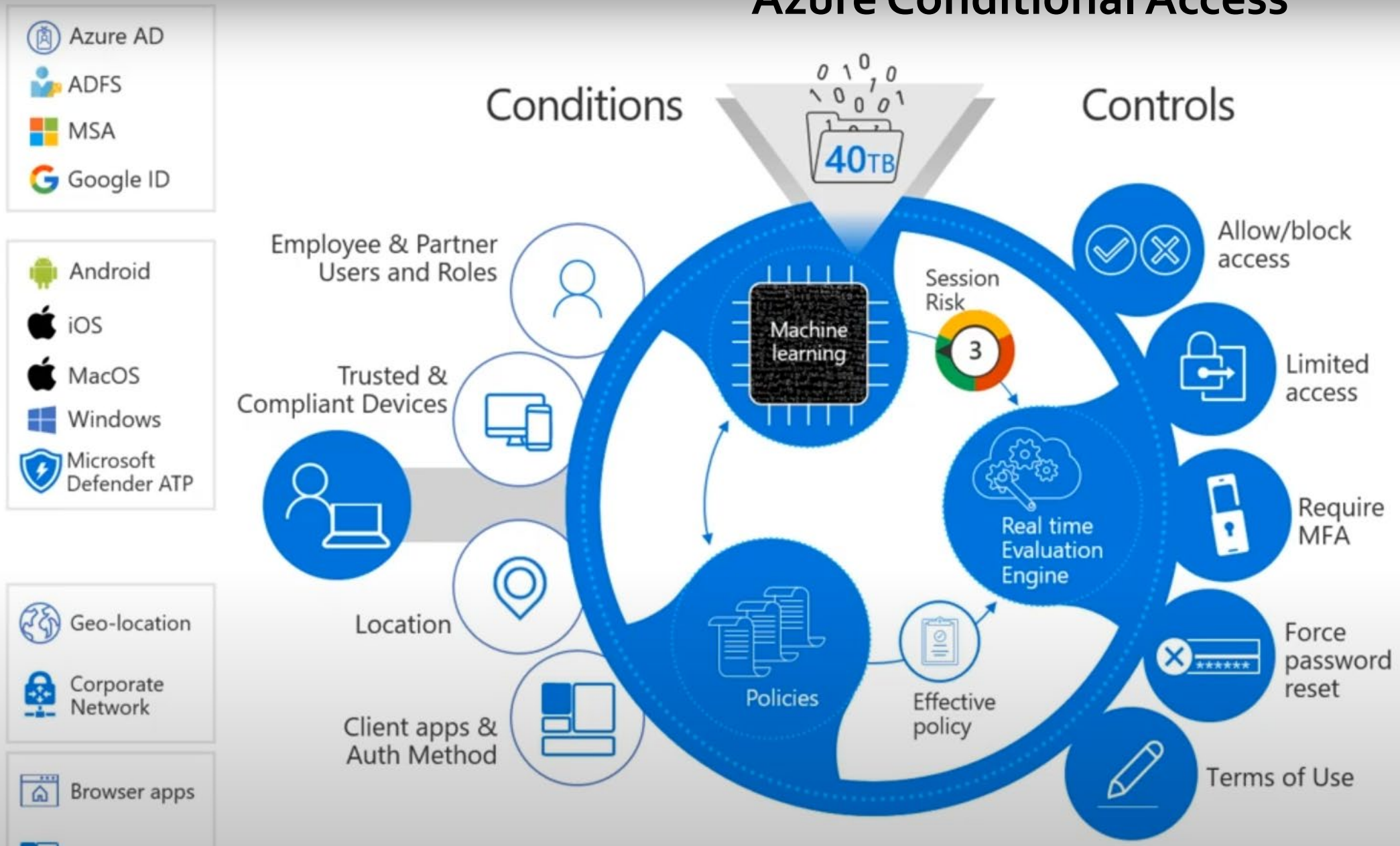
All access to services must be authenticated, authorized and encrypted.

www.beyondcorp.com

© Kenneth G. Hartman – All Rights Reserved

What is conditional access? | Azure Active Directory

Azure Conditional Access



https://youtu.be/ffMAw2IVO7A

Zero Trust:
Over-Simplified

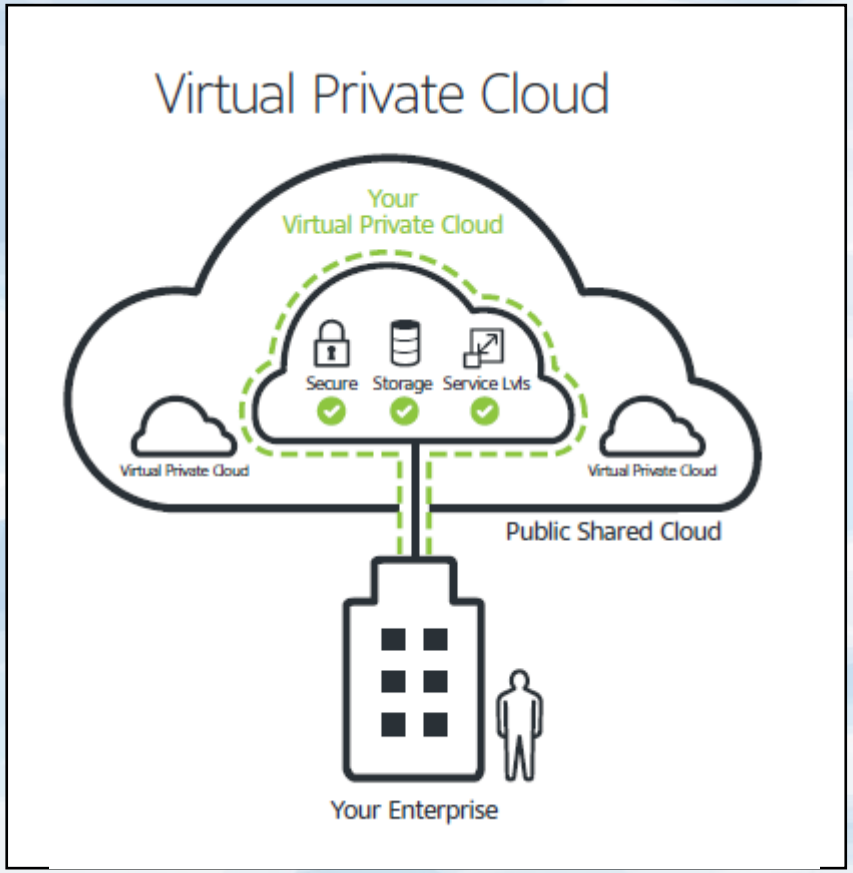
Do not allow network connectivity between two systems that do not need to communicate.

Require strong authentication between any two systems that do need to communicate.

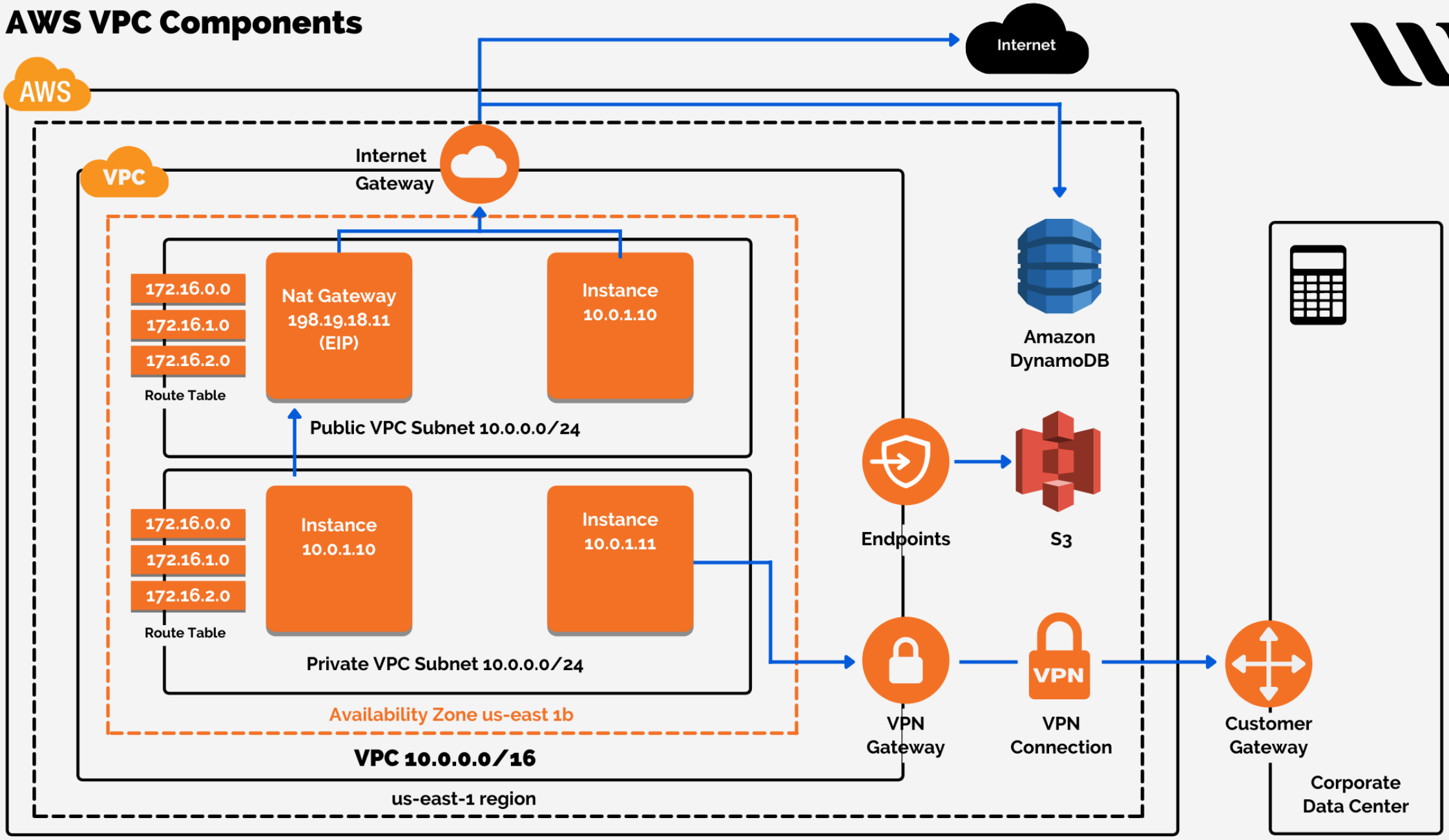
© Kenneth G. Hartman – All Rights Reserved

10. Software Defined Cloud Networking

- Global & Regional Load Balancers
- Web Application Firewalls
- Virtual Private Clouds
- Public & Private Subnets
- Custom Routing
- VPN Termination
- Private Service Endpoints
- API Gateways
- Service Mesh



AWS VPC Components



https://www.whizlabs.com/blog/aws-virtual-private-cloud-guide/

What to Expect at a SANS Cloud Course

- Drink from the firehose
- Immersive learning
- We listen and iterate
- Get ready for certification

The SANS Promise: Return to work with practical skills that you can apply on Day 1


CALL TO ACTION:
Jump in and dive deep, participate and collaborate.
Leverage the SANS Cloud Security Flight Plan.
Embrace the transformational journey with us.
SANS
CLOUD
SECURITY

Make the Most of This Week!

- Explore the SANS free resources:
  - Tools, posters, webcasts, blog posts, etc.
  - www.sans.org/free
- Learn how SANS involvement has helped others (ask them)
- Chat with those that have certifications
- Network with fellow students
- Participate in class, use Slack and join Discord.
- Get to know your Instructor, vTAs, and Facilitators.

Murder in the Amazon Cloud

Code Spaces Status

Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a irreversible position both financially and in terms of on going credibility.

As such at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us.

All that we can say at this point is how sorry we are to both our customers and to the people who make a living at Code Spaces for the chain of events that lead us here.

In order to get any remaining data exported please email us at support[at]codespaces.com with your account url and we will endeavour to process the request as soon as possible.

On behalf of everyone at Code Spaces, please accept our sincere apologies for the inconvenience this has caused to you, and ask for your understanding during this time! We hope that one day we will be able to and reinstate the service and credibility that Code Spaces once had!

https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html

© 10/13/2022 Kenneth G. Hartman

Information on the Capital One Cyber Incident

English | Español

- **100 Million individuals in US and 6 Million n Canada**
- **Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information.**
- **140,000 Social Security numbers**
- **80,000 linked bank account numbers**

Important updates

April 22, 2022 update:

2019 Cyber Incident Settlement Reached. On February 7, 2022, a U.S. federal court preliminarily approved a class action settlement relating to the cyber incident Capital One announced in July 2019. Please visit www.CapitalOneSettlement.com for additional details.

February 22, 2021 update:

On January 27, 2021, as a result of Capital One's ongoing analysis of the files stolen by the unauthorized individual in the 2019 Cybersecurity Incident, we discovered approximately 4,700 U.S. credit card customers or applicants whose Social Security Numbers were among the data accessed, but not previously known. Capital One is directly notifying these affected individuals and will make two years of free credit monitoring and identity protection available at no cost to them.

https://www.capitalone.com/digital/facts2019/

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

CRYPTOCURRENCY JACKING —

Tesla cloud resources are hacked to run cryptocurrency-mining malware

Crooks find poorly secured access credentials, use them to install stealth miner.

DAN GOODIN - 2/20/2018, 12:21 PM

- Hackers accessed one of Tesla's Amazon cloud accounts and used it to run currency-mining software.
- The initial point of entry was an unsecured administrative console for Kubernetes.
- Within one Kubernetes pod, access credentials were exposed to Tesla's AWS environment which contained an Amazon S3 (Amazon Simple Storage Service) bucket that had sensitive data

https://arstechnica.com/information-technology/2018/02/tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware/

SANS Cloud Security Training Alumni

- Know that they are designing secure architectures, based on proven practices from the leading companies in cloud security
- Are equipped with the skills, knowledge, experience, and confidence to face the future
- Have a track record of success

www.sans.org/cloud-security/

SANS CLOUD SECURITY

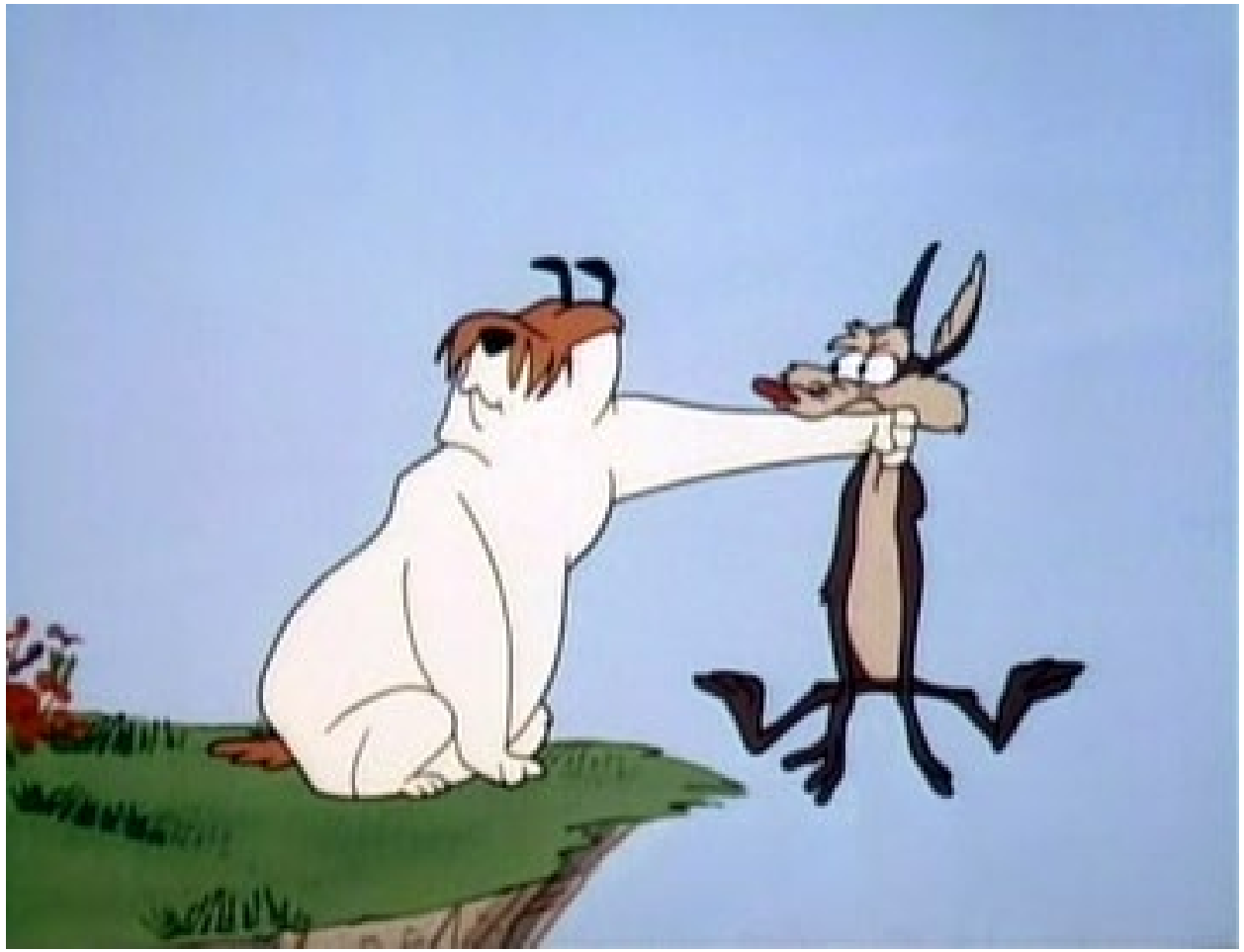
Join Us on Social

Twitter: @sanscloudsec

LinkedIn: SANS Cloud Security

YouTube: youtube/sanscloudsecurity

Discord: sansurl.com/cloud-discord



Questions & Discussion

© 2021 Kenneth G. Hartman – All Rights Reserved