

San Francisco | May 6 – 9 | Moscone Center

CloudSec Hero to Zero: Self-Obsolescing Through Prolific Efficiency

Rich Mogull

SESSION ID: CLS-T01

Cloud Security Curmudgeon Firemon/Securosis @rmogull@defcon.social

Chris Farris

Cloud Security Evangelist PrimeHarbor Technologies @jcfarris [@infosec.exchange]

THE ART OF

POSSIBLE

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2024 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

All of this is based on public sources and doesn't reflect incidents that may or may not have occurred at any employer, past, present, or future.





Mass Casualty Incident (MCI)

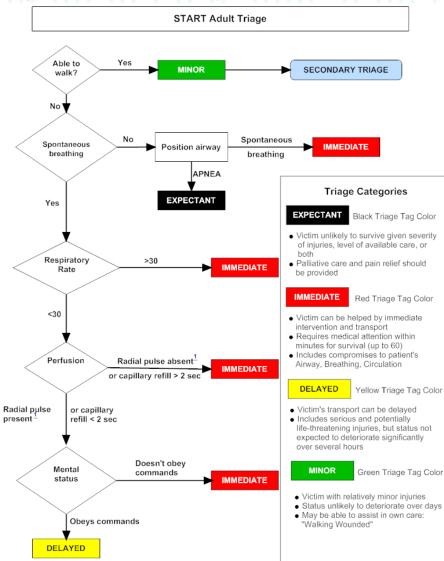
Any incident that exceeds available resources







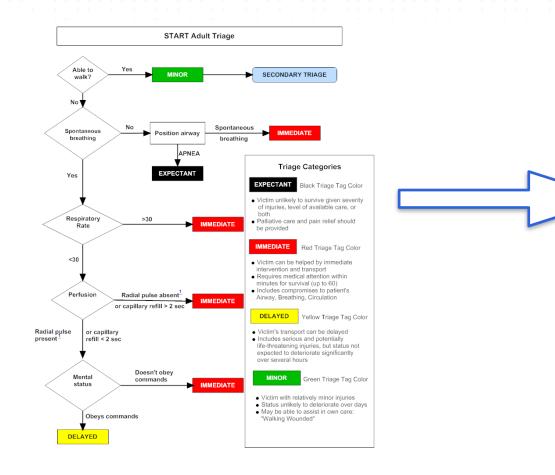
START: Simple Triage and Rapid Treatment





#RSAC

START: Simple Triage and Rapid Treatment





FIREMON PrimeHarbor Technologies

RS∧Conference[®]2024

You wake up one day and....



Welcome to your new cloud environment





Day One - what do you do?

- You're the first cloud security hire
- Company has been in business for 15 years
- Been in the cloud for the last 10 years
- Finished their cloud migration 6 months ago
- Internal Audit said they needed a Cloud Security Program
- CISO hired you to make it all better

FIREMO







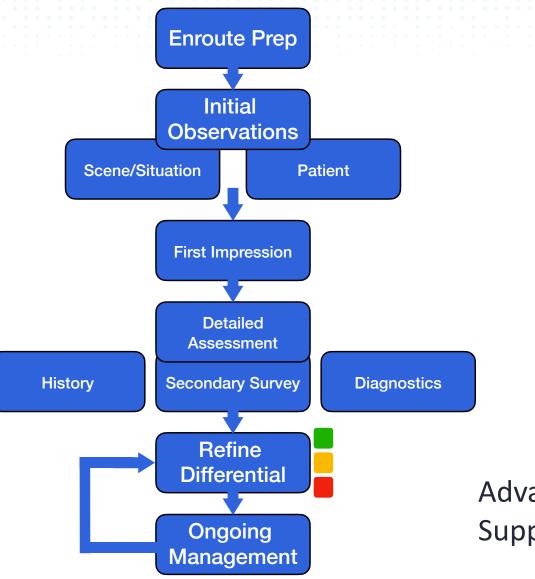
Now What?

Systemically Taming Chaos

PrimeHarbor

echnologies

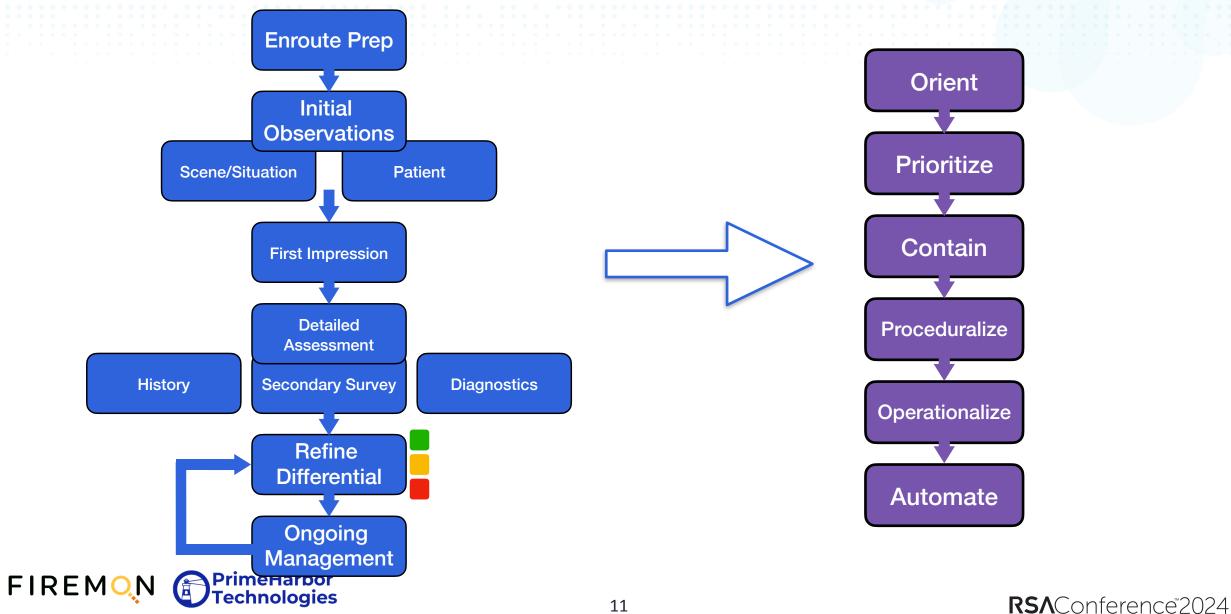
FIREMON



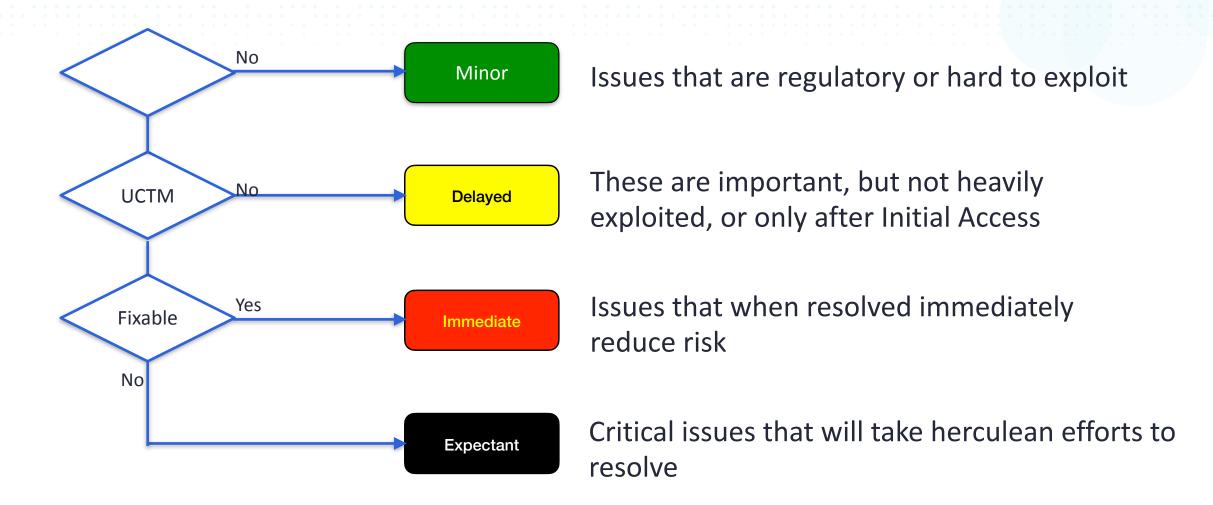
Advanced Medical Life Support (AMLS) Algorithm

RSAConference[®]2024

Systemically Taming Chaos



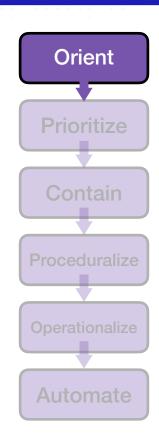
Simple Triage And Rapid Treatment Remediation





RS∧Conference[™]2024

Week 1



Step 1: Orient

- 1. Find your Accounts
- 2. Find your Owners¹
- 3. Deploy a CSPM
- 4. Identify your Telemetry



¹ May take more than a week



Accounts & Owners

- Find your accounts
 - CIS Critical Control 1 & 2
 - 1.5 is know your cloud accounts
- Owners

FIREMON

- Who can make a decision about the account?
- Who can answer technical questions?
- Both are critical



RSAConference[®]2024



- Cloud Audit Logs are the #1 priority
 - Credentials are a common threat vector
 - This logs them
- Any CSP threat services that are already running
- IdP logs if they are available





CSPM

- These are your patients
 - Cloud Resources with some form of misconfiguration
 - Resources that shouldn't exist if you're doing cloud right (IAM Users)
- You don't need fancy attack path methodologies here.
- Look at classes of issues, not each finding!
- Start with the Big Gaping Security Holes
 - these are your Immediate concerns
 - We'll discuss later

STARTing Focus

- Move fast
- Focus on information gathering
- Feed into the rest of the cycle AS you get data
 - You don't have to collect everything before making decisions
- Always be prepared to Stop the Bleed
- Use Free and Open Source if procurement can't keep up
 - Consider CSP tools (more later) if needed but be prepared for the bill
 - Vendor trials are a GREAT cheat code

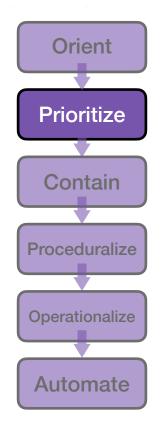






RS∧Conference[™]2024

Prioritize with the Universal Cloud Threat Model



What is the UCTM?

- We're all in the same public clouds
- We all face the same universal threats
- Many of us can afford to threat model
- Many of us cannot
- Crowd Sourcing!





Why the UCTM

- Address the main gaps in non-cloud threat models:
 - In cloud, infrastructure and applications are often deeply entangled
 - In public cloud the Internet-facing attack surface now includes the administrative management plane
 - In public IaaS, nearly all organizations run on the shared infrastructure of three primary cloud service providers followed by a slightly-large set of secondary providers





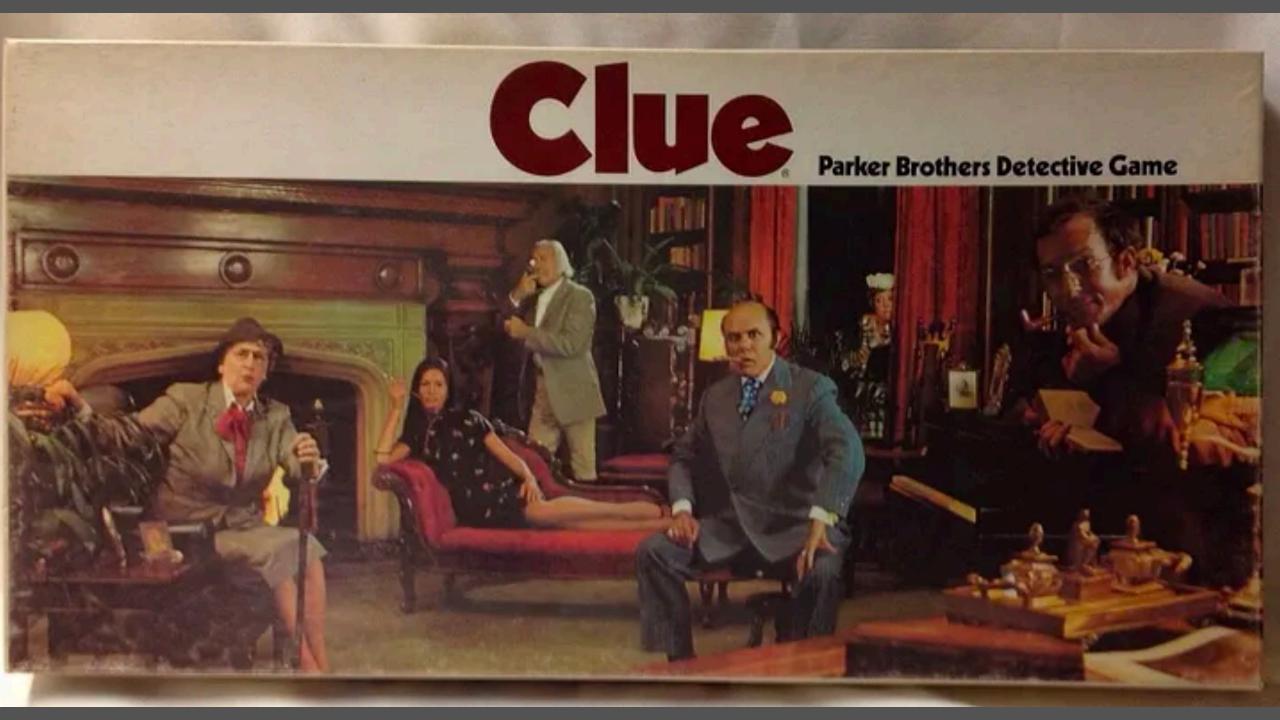


The *Universal* Cloud Threat Model identifies the commonalities faced by all organizations equally based on their cloud usage, regardless of size, vertical, or nationality.



Threat Actors have Objectives against Targets using Attack Vectors that are observed by defenders as Attack Sequences





Threat Actors

- State-nexus threat actors
- Cybercriminals & financially motivated threat actors
- Hacktivists & cause-motivated threat actors
- Insider threats

FIREMON

- Script-kiddies, reputation builders, 80s-style hackers
- Rich's Cat. He's a legitimate turdhole.











₿ M



Objectives

- Financial Gain from:
 - CryptoMining
 - Spam

FIREMO

- Ransomware (encryption or deletion)
- threat of sensitive information disclosure (blackmail)
- selling Sensitive Data on black market

- Leveraging Cloud Infrastructure for:
 - Financial attacks against others
 - Geo-Political attacks against others
- Denial of Service Attacks
- Industrial espionage
- Nation-state espionage

Targets

- Data
- Compute
- Network
- Pipelines
- Supply Chain



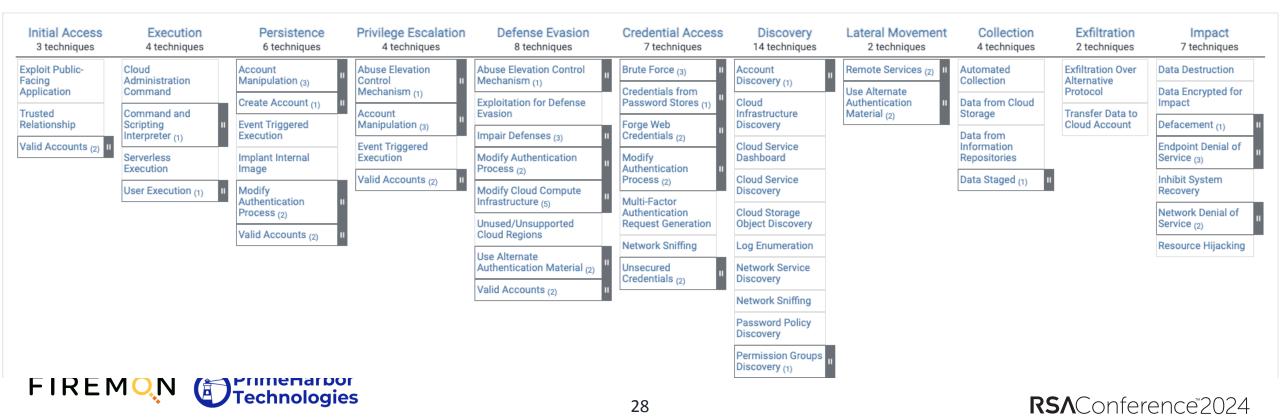




Attack Vectors

• These are the things to defend against

Involve credentials, network exposure, misconfigurations



For the Cloud is Dark

And Full of Terrors

VECTOR: Lost, stolen, or exposed credentials







VECTOR: Publicly Exposed Resources



ACHIEVEMENT UNLOCKED!

S3 Bucket Negligence Award

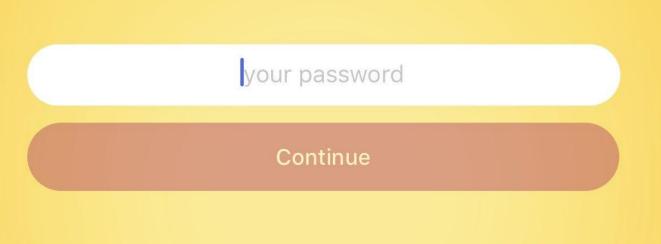
You have failed to adequately safeguard the data with which you were entrusted. You have failed those who relied upon you.



VECTOR: Credentials exposed via application security flaws

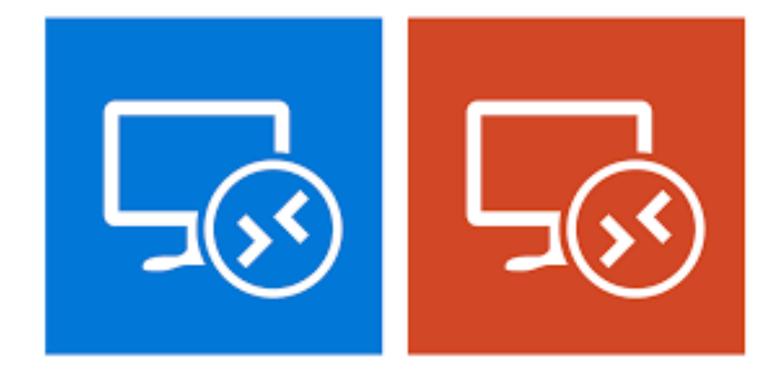
Pick a password

Don't reuse your bank password, we didn't spend a lot on security for this app. At least 6 characters



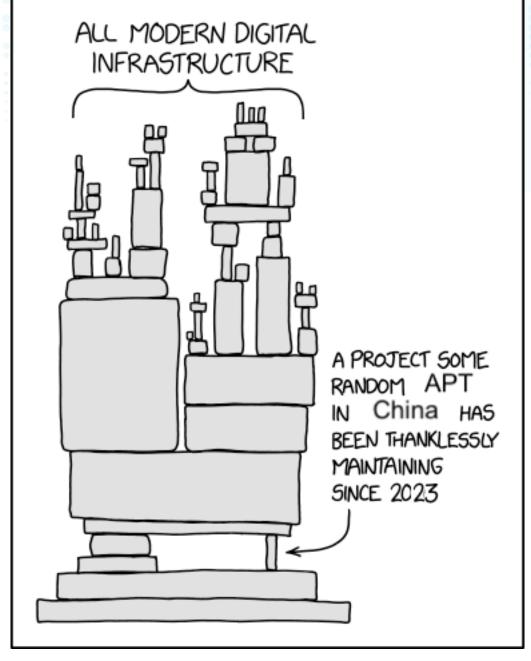


VECTOR: Unpatched vulnerabilities and zero-days in overly exposed systems





VECTOR: Supply Chain





VECTOR: Domain Takeover

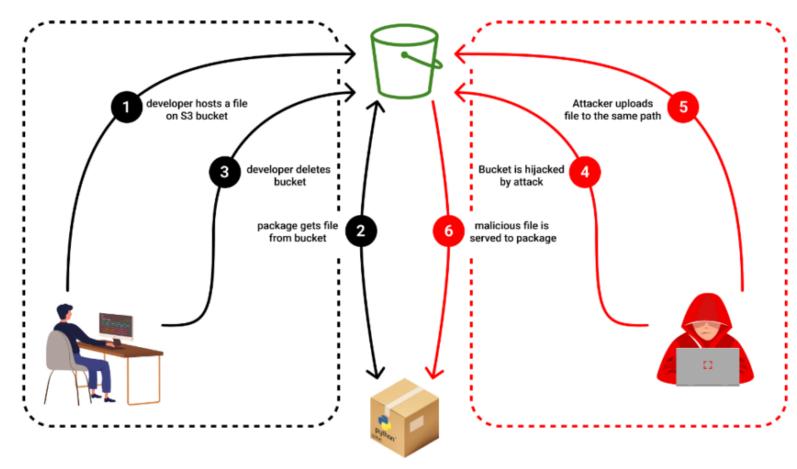


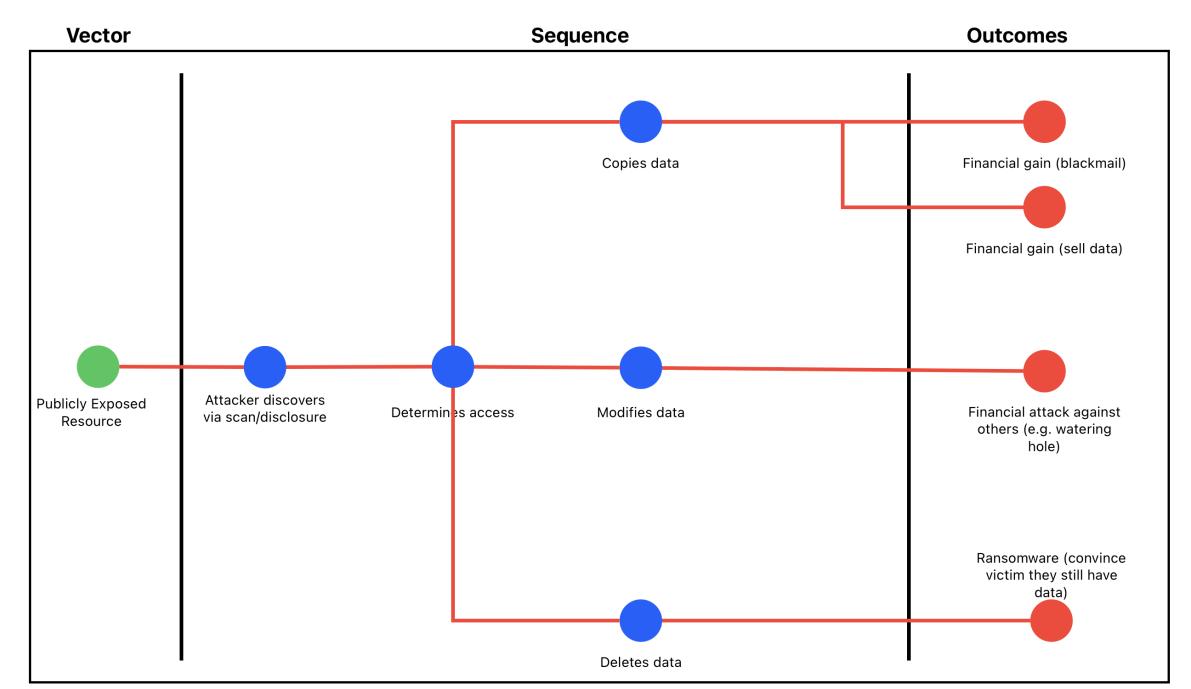
Image courtesy of Checkmarx -Hijacking S3 Buckets: New Attack Technique Exploited in the Wild by Supply Chain Attackers



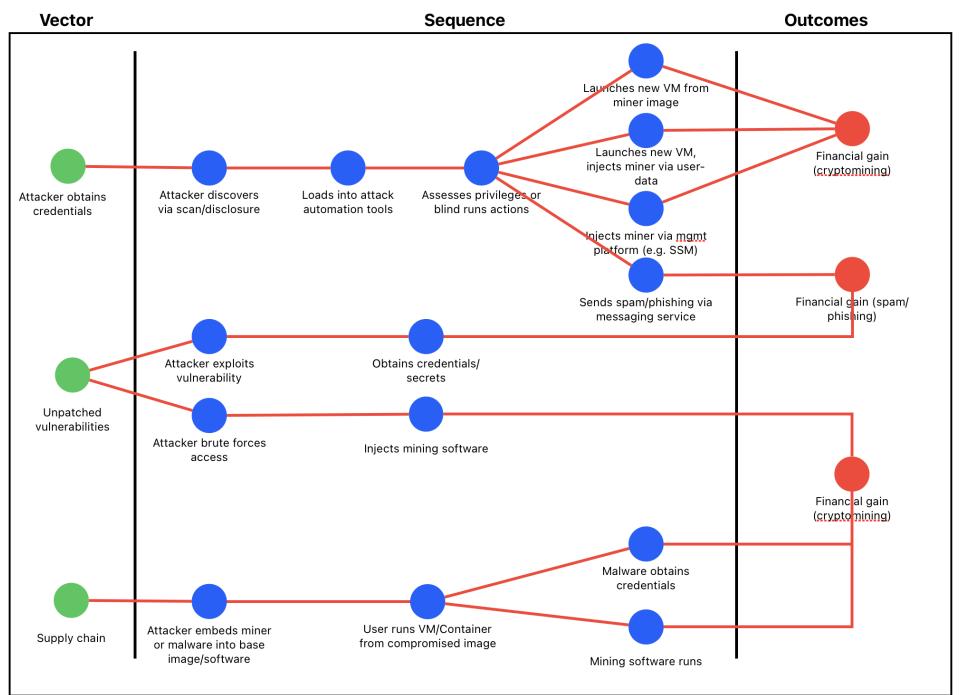




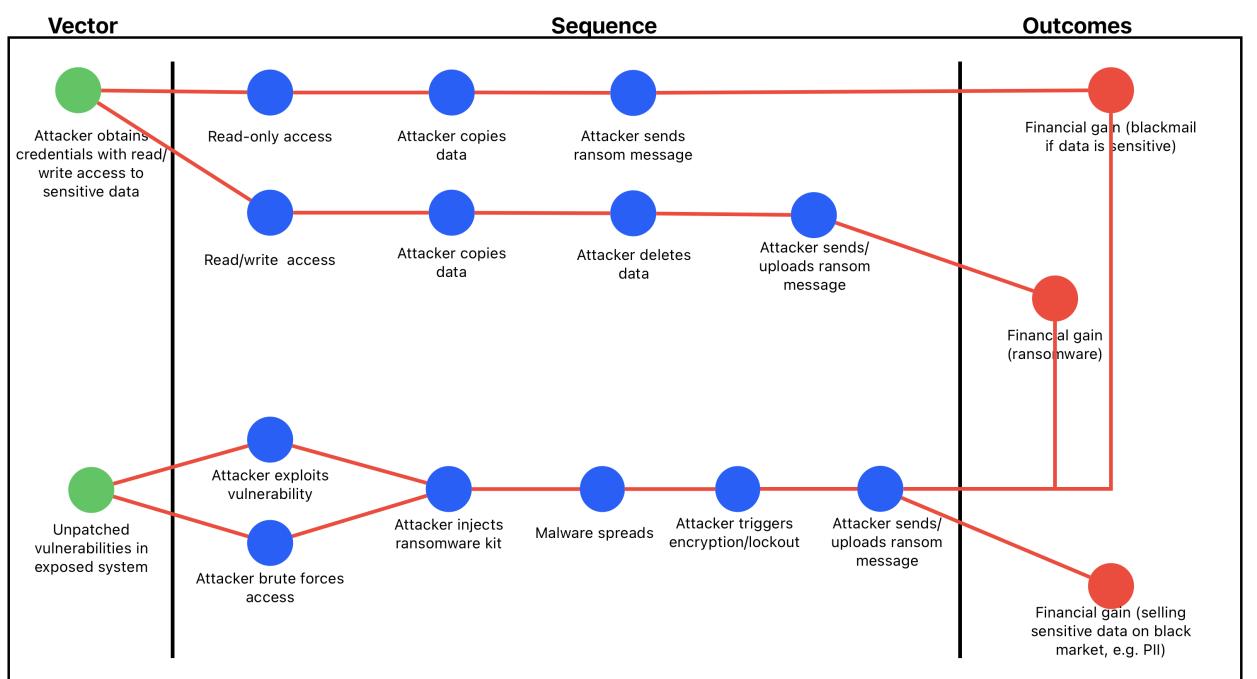
Threat Actor Copies/Alters a Public Data Resource



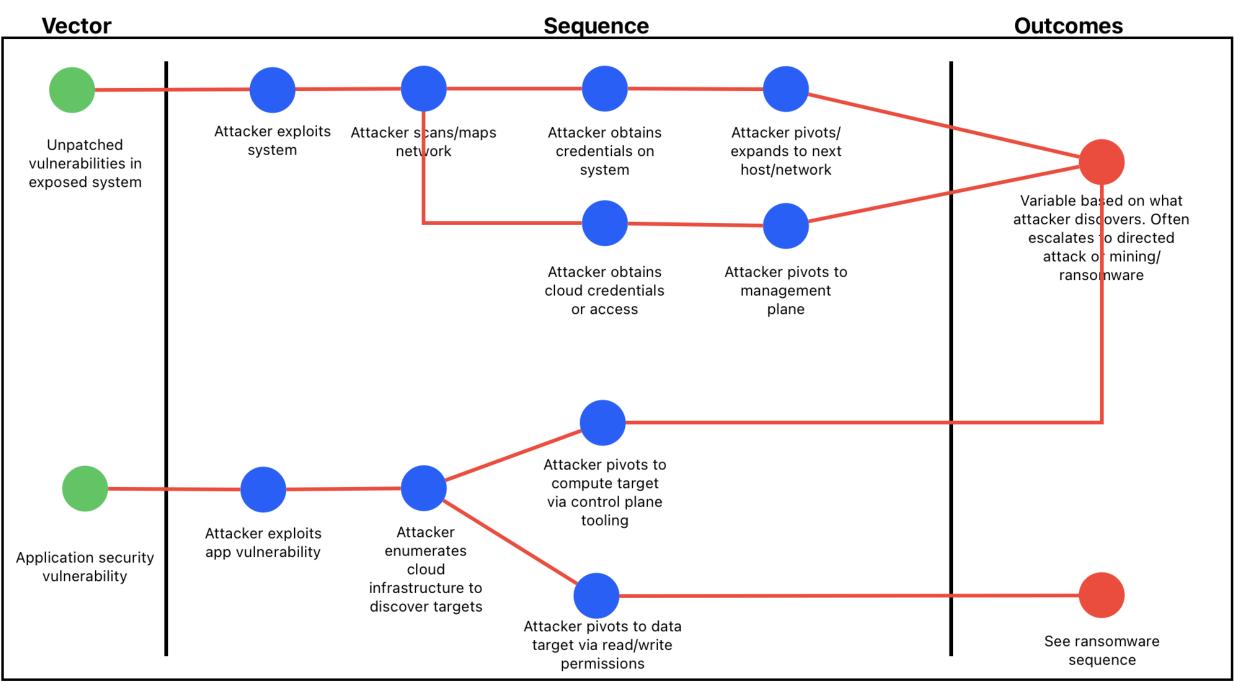
Threat Actor Hijacks Resources for Cryptomining, Spam, or Phishing



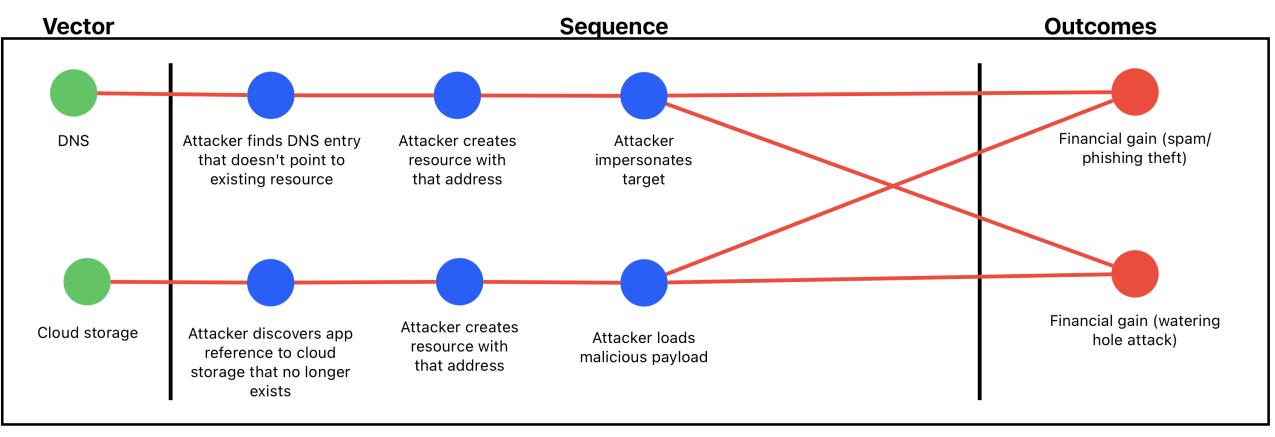
Threat Actor Engages in Ransomware



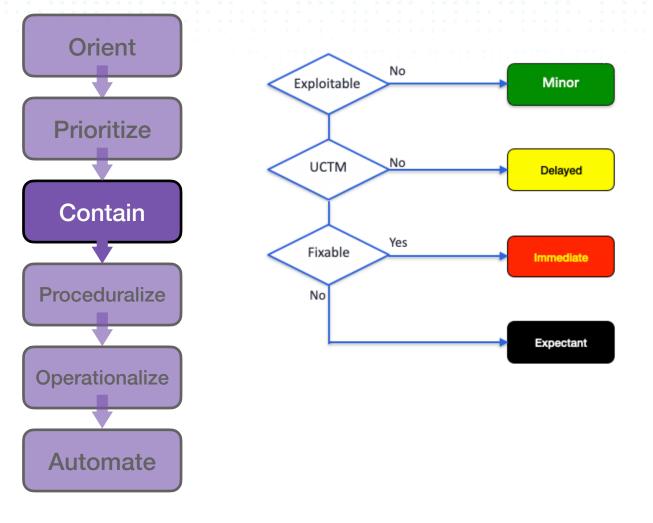
Threat Actor Engages in Lateral Movement



Threat Actor Engages in Subdomain Takeover



What's a Big Gaping Security Hole™?



PrimeHarbor Technologies

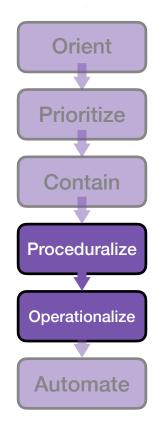
FIREMON

Examples:

- Root Access Keys
- Public Write/List Buckets
- 3389 open to the world
- Missing MFA
- Access Keys from the Obama Administration

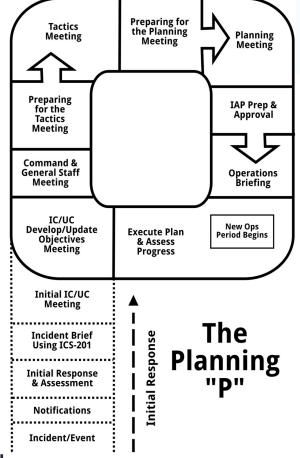
RS∧Conference[™]2024

Setting up incident command (and beyond)



After your initial response

- You should have:
 - Identified and analyzed initial telemetry
 - Closed the BGSHs
 - Prioritized using the UCTM
 - Begun playing politics (ICS 400 FTW)
- Now you
 - Start the planning cycle
 - Implement procedures and guardrails based on prioritization
 - Begin transitioning into daily operations vs. crisis mode



What other tools do you need?

- CSPM (permanent)
- Inventory
- Cloud API Logging
 - And event (e.g. GuardDuty/Defender) handling
- Identity Federation
- Secrets Scanning!
- SBOM



Cloud Providers are not your friend!

- In all providers, Security is an up-charge
- They're typically not as good as what you'll see on the show floor
- But...

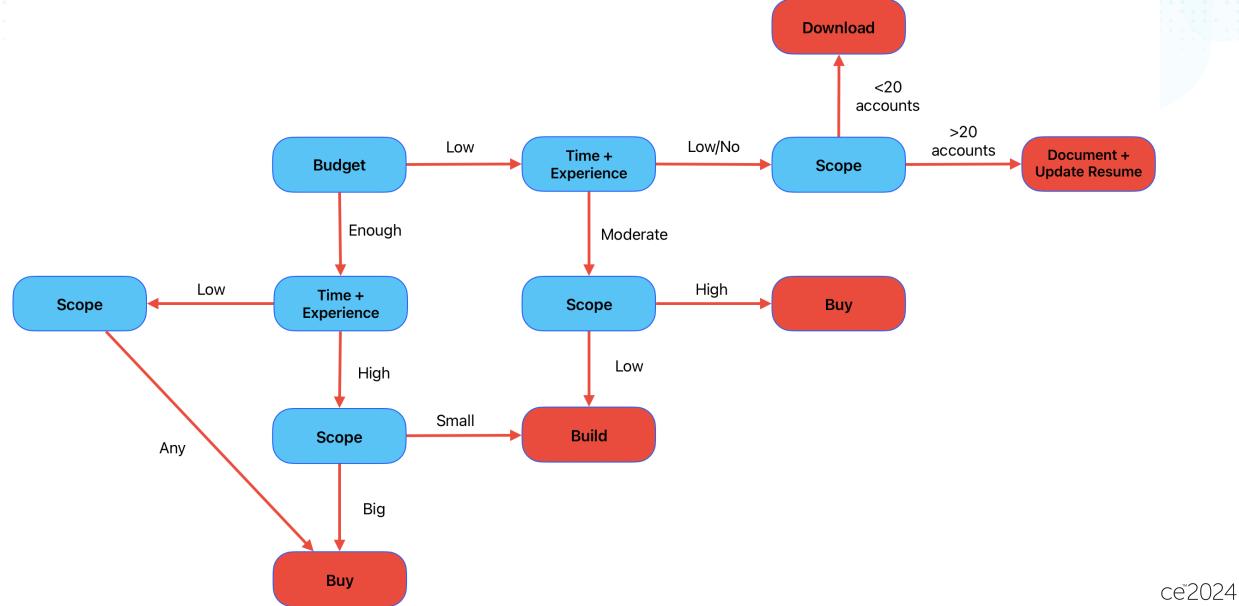
FIREMON

- No procurement process
- Less setup
- (Usually) Better than nothing
- Often you have no choice



#RSAC

Build vs Buv vs Download



Transition Period

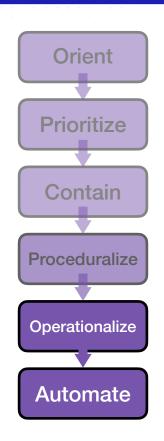
- Slowly move from reactive to engaging with teams
- Begin putting in initial guardrails for the BGSHs
 - Detective with alerting
 - Preventative with policies (SCPs/Azure Policy/etc.)
- Now the politics get fun



#RSAC

RS∧Conference[™]2024

Moving from Pandemic to Endemic



Find your systemic issues

- Wide open security groups?
 - Lack of VPN, no RFC1918 connections
- Lots of IAM Users?
 - No centralized identity system
- Public Buckets?
 - User education
 - Lack of understanding of IAM and cloud APIs



#RSAC

You're not lke

FIREMON

- Don't start with paved-roads
- Clear the path first remove obstacles
 - Get an centralized identity system
 - Get VPN/RFC1918 routing working
 - Write a Baseline (<u>https://pht.us/baseline</u>)
- Then focus on guard-rails







Extend the Cloud Threat Model

- What threat actors want to target you?
- What are their objectives and motivations?
- What do you have that they want? (Targets)
- Now go brainstorm how they'd do it!





Unique Adversaries & Threats

Auditors

FIREMON

- Mergers & Acquisitions
- Those other Nation-State Actors



PrimeHarbor

echnologies







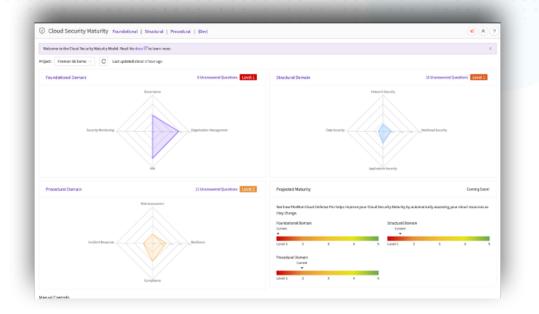
#RSAC





Measure Twice, breach never

	aturity Mo 2.0 (Updated Nov. 2023)		LEVEL 2	LEVEL 3	LEVEL 4 Capable	LEVEL 5 Efficient Al major activities centrally managed, covering all of the CSNM
		LEVEL 1 Initial Manualy managing policinal procedures, manaly dirough console. Architectures send to reasenble marking and investment of the sen on network security control (s). MM mostly ad-bac with loties to no federation.	Repeatable Polycycheckist based and rely more on marau de relyeite toning. High variability between projects: net coordinate deroek delogivmens. Initial use of inferoructure are node (Theraferm/Outomusion). but security not constatently engaged in designitrative. Polieration on some accounts. but immed use of High are a difficulte supporting teams (sepecially on the command line).	Policies and central coordination in plices. Some initial security automation still executed menually. Some third parry solving (orderestration with other tools), Pederation on meat accounts with underpared MPA, but still paps en constraining: Security namiting to review and promote use of CloudPermation/Terreform. CloudPermation/Terreform. Use.	oring environments becamp endogenerations becamp enformers. Automation and guardials across multiple deployments. Espanding flows, Big shift frem manual management and execution to running security operations with centralized platforms with centralized management and reporting toolchains.	domain, integrated into findestructure as code enforment. Build in to the each with ponitioning automation. Redention guatomation. Redentional build and MEA uncluing command line support).
Core, critical categories to ensure availability of a secure baseline.	Governance	No formal cloud goverance. Either cloud is not allowed not officially	Main cloud providers are approved. Some collicies in development that	Cloud team, CCoE, or equivalent in place to quide usage. Initial policies	Central cloud team has SMEs for current providers and responsibility	Governance is managed using automated tooling (e.g. database,
	Overall governance of sloud providers, deployments, applications, and general usage.	supported or teams completely self manage cloud usage.	denn minis no-cicca (p-spenn) often minis no-cicca (p-spenn) standards. No cloud-specific org structure.	protein spectra seager a read potential in suns. Tassic use of standardst and banchmarks (e.g. OS) for control objectives established for at least 1 provider. Cloud registry in place.	coming promotion in the responsion of and survival to set rules/baselines. Cloud security control objectives in use. Control specifications for primary cloud provider are defined/enforced.	automatic recently flip, constants LaC). Defined process to update control objectives/specifications as cloud providers add/modify services.
	Organization Management Core cloud deployment security and multi-deployment/provider architectures to control blast radius and ensure baseline security.	Single or unconnected deployments with inconsistent core security.	Checklat for core deployment security on primary cloud platform. Most ecounts associated with organization, but manually managed.	Deployments centrally managed with consistent manual provisioning of orce security. Security checklots for each current cloud provider. Initial use of CSPM or similar for security visibility.	Deployments provisioned via IaC including most core security controls. Multiple deployments in a provider used to control blast radius and organized hierarchically. CSP preventative policies (guardralia) in use.	Deployments used estensively to control blast radius. Deployment sourity provisioned through submation aligned with landing zona/account factory. Automated deprovisioning also in use.
	IAM Managing users, authentication, and authorization to the cloud provider and resources within the cloud. Also indires to managing IAM within the provider.	Identities managed within indusidual cloud accounts. No federation. MPA inconsistent.	Initial Preferation, likely using a Pederated identity broker or similar. Extensive use of cloud-aide enbites. MPA mostly consident for console. but not for command line or API.	Federation consistent through booker or similar, initial secrets management use for static coredentials for command line and code. MFA mostly consistent across console, command line and APs. Manual configuration of IAM policies within accounts.	Complete federation for all cloud accounts. MFA consistent: Initial use of automated provisioning of IAM. Secrets management consistent. Initial use of advanced conditional authorization where needed and supported to enforce IAM perimeter.	Fully automated provisioning of IAM. Extensive use of advanced conditional authorizations for robust IAM perimeter. Console, command line tools and API access integrated into privileged user and secrets management.
	Security Monitoring Merisoning and logging of both cloud administrative activity (the "management plane") and assets within the cloud (networks, workloads, applications, data).	No monitoring/alerting on telemetry gathered by the cloud provider.	Multi-account monitoring/alerting with logs aggregated across some accounts.	Management plane logs and some ad-hoc service/vorkload logs collected across all relevant deployments. Initial alers. Initial desectors for security deviations, but inconsistently in place.	Robust security telemetry collected for the management plane, services, and workloads. Cloud native fineat detertors in place, but not necessarily consistent across providers.	Consistent telemetry collected across all in-use cloud providers. Robust cloud-eative threat detectors with enrichment. Alerts noused to the team that owns/manages the deployment.
Categories to protect the building blocks of your cloud environment.	Network Security Security of the virtual networks in the cloud, and the connections to from the cloud.	Cloud network arthitectures replicating ex-greenise patterns. Network security ad-hoc using overly open controls. Uklizes virtual applanoses from estating network security verdor instead of equivalent cloud-native capabilities.	Networks manually built to defined cloud standards. Applications forced to fit supported networking models. Initial use of cloud-native security controls but often overlapping with legacy controls.	Initial use of cloud-native architectures to isolata/segment cloud resources and break network attack parks. Initial use of network templanes and transit networks. Uses a combination of cloud-native and hybrid networking approaches depending on the application.	Estensive use of cloud native network architectures and PaaS. Initial adoption of the Minimum Wable Network concept: Network security policies enforced with extenses guarduals.	Nerworks designed to fit the application and enhance app security (Minimum Yable Nerwork), Leverage cloud-native anchitecures and design patterns. Centralized and automated controls.
	Workload Security Securing the environment where code runs, including virtual modules/instances, containers and function as a service (FaaS - serveless).	Most workloads are long-running visual muchines levenaging existing dasacement-centric security controls parted directly to cloud.	Generally relient on trachtonal dissounter management tools. Use of automated configuration management to standardize building of infrastructure. No FaaS or container-specific security.	Mostly cloud-eative tools in use. Initial use of Immutable infrastructure, birdl integration of security configurations and tools into image creation/spiplines. Initial security controls implemented on containers.	Internatable infrastructure is the recommended pattern, where possible. Security testing integrated into image pipelines. Only cloud-rative cools is use. Baseline container security in place. Faa5 security ad-hoc, but evailable.	Interactable infrastructure in the standard (where possible) with multiple dely deployments. Orde assessment and real-time defenses integrated using FacS.
	Application Security Full mark application escuty. This includes starting and protection of pipelines, workloads, architectures, etc.	Traditional application security testing (*AST) and defenses (e.g. legacy WAF)	Mostly traditional testing. Ad-hoe assessment of pipeline security. Initial use of cloud provider's appace tools (WMF/DDuS). Serverless app security is a gap.	Some cloud-specific testing. Pipelines manually secured. Consistent WAF/DDvS for Internet facing apps. Serverless Internet facing apps. Serverless Initial security testing in CI/CD.	Stack testing partially externated. Consistent pipeline security utilized. Extensive security testing in CUOD pipelines. Appsec guardrails implemented.	Stack testing automated across all workload models and consistently implemented in CUCD pipelines. Cloud-centric red team to test cloud-based applications.
	Data Security Encryption and access control of cloud data.	Basic access controls, usually improperly configured.	"Checkbox" data security. Encryption turned on using default keys. Manual encryption and key management. Manually configured access controls.	Initial use of customer managed keys. Simple automation for most. Policy-based access controls and encryption. Data access logs consistently collected in production deployments.	Extensive use of oustomer managed keys. All oritical data encrypted. Some automation using data guardnals, but mostly manual. httial content-based access controls and encryption.	Minimal use of default keys. Data lifecycles/backups automated for realiency Encryption specifications built into deployment pipelines. Deployment on situately assessed for unapproved data.
Categories to high light the processes needed to protect your cloud (and keep it protected).	Risk Assessment & Provider Management There are three subjects of rike assessment: 1) pender selection (Choosing providers) 2) ongoing providers-assessment and management 3) risk assessment of specific projects and programs.	Use existing risk assessment module and provider selection process.	Provider selection driven by business unit, but security assesses the provider and can styger an escalariso. Beautry incontiseethy engaged in early project risk assessments (e.g. architecture risk).	Basic security standards for cloud providers of different service models (bask, Pask, Sask) in use. Initial provider registry in use, showing approvals by data classification/visk/compliance.	Security engaged with process for evaluating providers and deployments. Existing provider and deployment integration and the eployment integration and the ensurement of the security of the approvals at the service level.	Security-driven risk assessment for new projects and cloud migrations, with formal templating and nemediation plans. Existing providers and projects are evaluated continuously for updated risk profiles.
	Resilience Ensuring realiset use of cloud that meets an organization's business requirements for availability and recovery.	No formal resiliency for cloud deployments.	Seme basic data backup/Hecycles. Seme use of autoealing/ sutomation for workloads. Largely alogie provider/region deployments.	Moderate use of subscaling/automation for workload estillency, where possible, Initial use of multi-region realisency. Some deployments use IaC for additional realisency.	Most deployments provisioned with late. Some use of multi-region and multi-account resiliency. Deployment: use anseaable realilency control specifications. Data-plane realilent to larger CSP feitures.	All production deployments provisioned with IAC, IAC repositories implement resiliency. Automated failowers and redeployments in use. Chaos engineering in place.
	Compliance & Audit Meeting regulatory compliance requirements and mandates.	No reporting or compilance actions taken for cloud-specific resources.	No cloud-specific standards, Ad-hoc assessment and remediation of deficiencies on cloud-based resources.	Cloud provider and service (SaaS or PeatS) approved list. Scheduled assessments of cloud providers. Manual reporting of cloud controls versus standards.	Continuous assessment of in-scope resources using automated guardnals, manual remediation of deficiencies. Reporting is partially automated.	Continuous assessment and automatic remediation of deficiencies using cloud automatics. Reporting fully automated across all applicable standards with deebboarding.
	Incident Response Dicus specific incident response processes, including compromise of the cloud console/management plane.	No cloud-specific response, uses existing IR playbooks (if they exist).	Manual IR response to cloud events. Inconsistent data collection and escalation.	Consistent manual response with rudimentary tooling.	Trained responders using cloud-specific tooling and refined processes. Some platform-based automation (quarantine asset, take	Fully automated and orchestrated IR workflow backed by a cloud IR team and response platform. Testing using a cloud-focused Red Team and

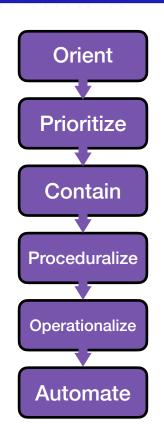


https://www.iansresearch.com/ resources/cloud-security-maturity-model



RS∧Conference[™]2024

Putting it all together





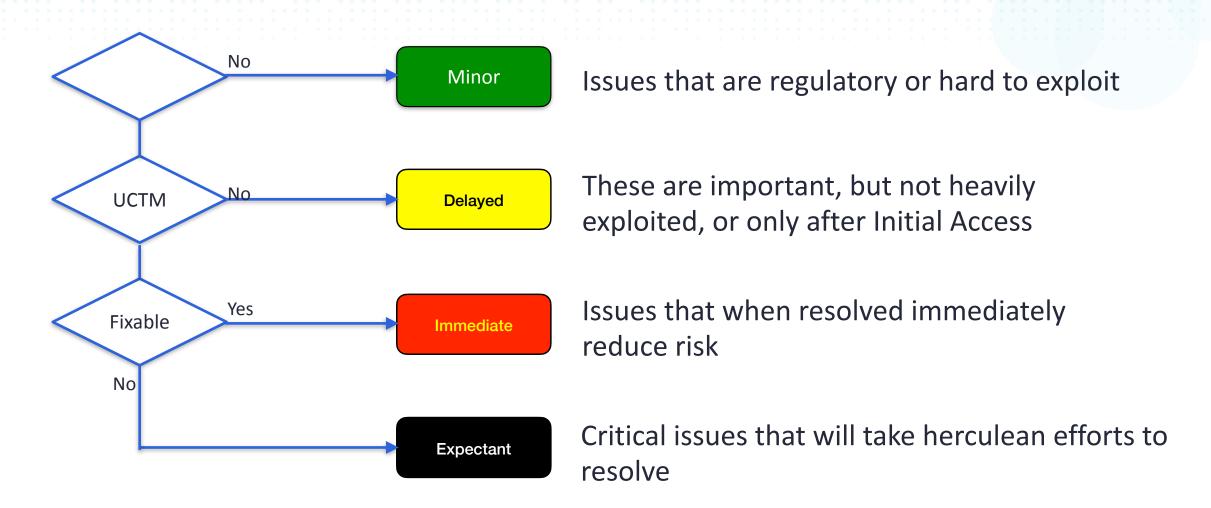
Apply the Universal Cloud Threat Model

Threat Actors have Objectives against Targets using Attack Vectors that are observed by defenders as Attack Sequences

https://pht.us/uctm

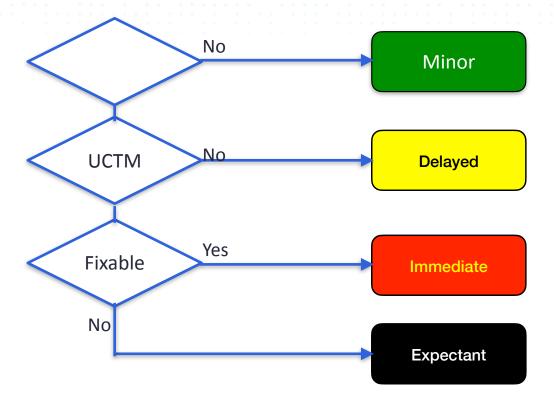


Apply START to prioritize your issues.





Apply START to prioritize your issues.



Issues that are regulatory or hard to exploit

These are important, but not heavily exploited, or only after Initial Access

Issues that when resolved immediately reduce risk

Critical issues that will take herculean efforts to resolve

Then start to Implement GuardRails





Questions?



@rmogull (rarely there anymore)

@rmogull@defcon.social

https://securosis.com

https://slaw.securosis.com

https://defense.firemon.cloud

Chris Farris

💟 @jcfarris



@jcfarris@infosec.exchange

<u>https://www.chrisfarris.com</u>

https://primeharbor.com



https://pht.us/uctm



#RSAC