
Taming the Noise:
Efficient Kubernetes Security Strategies
ARMO
Creators of Kubescape
PROACT

/whoami

Jonathan Kaftzan

VP Marketing and Biz-Dev at ARMO

Developer Advocate

Crossfit addicted

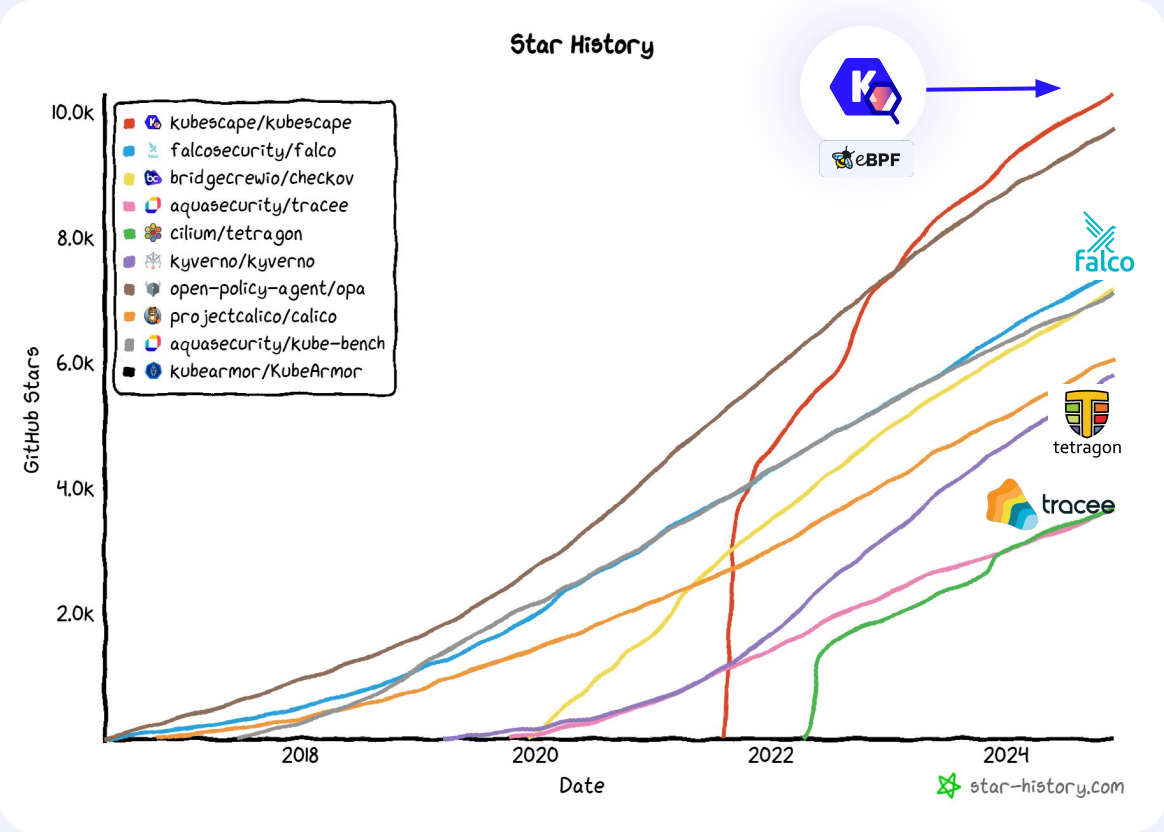
Jonathan Kaftzan

Jonathan Kaftzan

@JKaftzan

github.com/xxx

/Kubescape: The fastest growing CNCF Cloud Security project



/Kubescape: The fastest growing CNCF Cloud Security project

BLOG / STAFF POST

Kubescape becomes a CNCF incubating project

Posted on February 26, 2025

The CNCF Technical Oversight Committee (TOC) has voted to accept **Kubescape** as a CNCF incubating project.

/whoami

Jonas Larson

Head of DevOps at Proact

Loves requirements - “*can you test it?*”

Jonas Larson

Jonas Larson

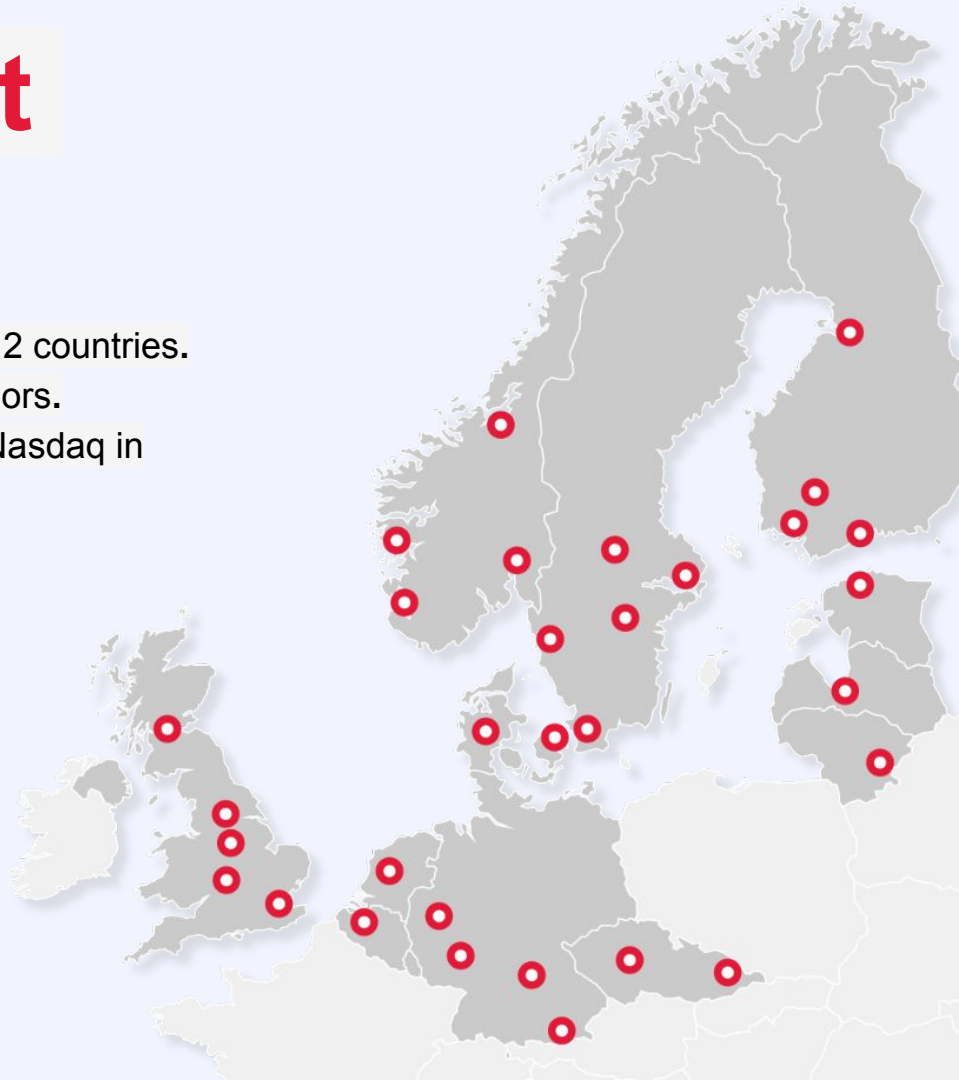
@carljonaslarson

github.com/cjl7

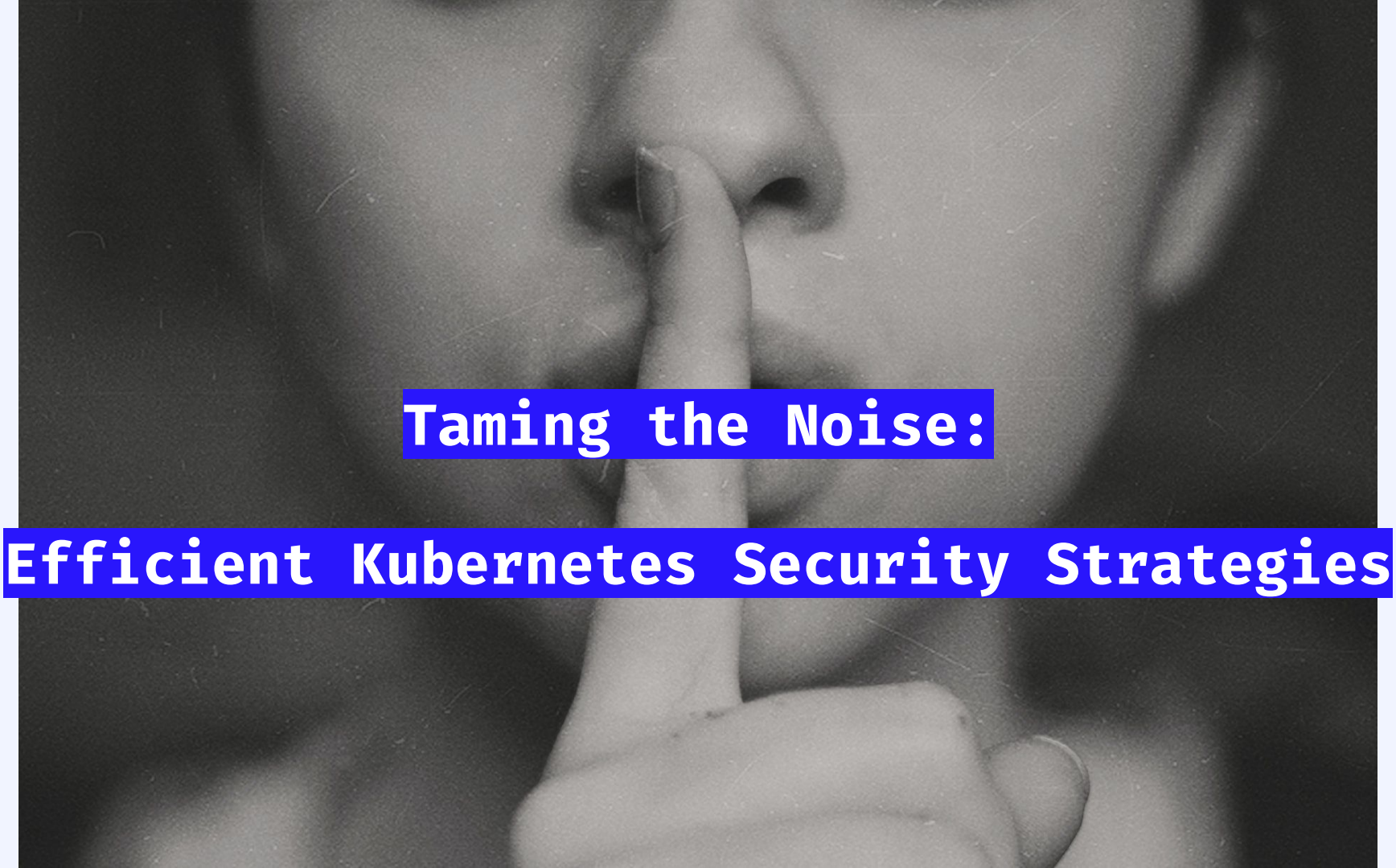
Proact

- ➔ **1200 specialists** across 35 offices in 12 countries.
- ➔ **Innovative** partner to world-class vendors.
- ➔ A **financially stable** partner listed on Nasdaq in Stockholm.
- ➔ Capabilities across the **hybrid cloud**.
- ➔ Trusted by **4000+ customers.**

Big enough to act,
small enough to care.



ARMO



Taming the Noise:

Efficient Kubernetes Security Strategies

ARMO

/CIS Benchmark as an example

CIS Benchmarks™

5 Policies .....
5.1 RBAC and Service Accounts.....
5.1.1 Ensure that the cluster-admin role is only used where required (Automat
5.1.2 Minimize access to secrets (Automated) .....
5.1.3 Minimize wildcard use in Roles and ClusterRoles (Automated) .....
5.1.4 Minimize access to create pods (Automated) .....
5.1.5 Ensure that default service accounts are not actively used. (Automated)

- Is this even fixable???

On average ARMO customers have ~0.9 misconfiguration per cloud object

ARMO

/Scanning !== Security

So you scanned it, now what?

- Privileged container - misconfiguration?
- RunAsRoot - misconfiguration?
- ...

/The **ARMO Cloud Runtime Security** Offering

Cloud Security

{Kubernetes-first} Cloud Posture

+ CSPM (Agentless scanning)
+ KSPM
+ Runtime-reachability Vulnerability management
+ IaC security
+ Identity security (CIEM) & RBAC

Real Time Protection

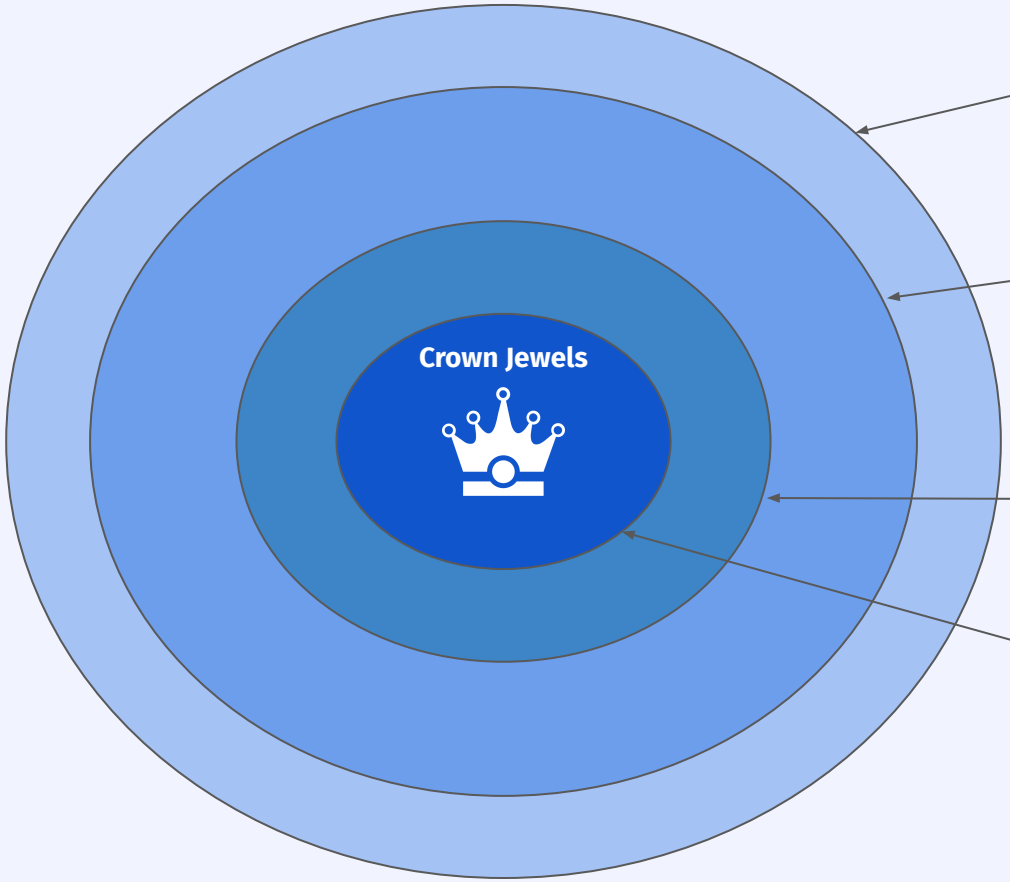
Threat Detection & Response (CADR)

+ Cloud Application Detection & Response (CDR, ADR)
+ CWPP
+ API security
+ Container security

Multi-Cloud, On-Premises and Air-Gapped

ARMO

ARMO Cloud Runtime Security Approach



All your potential vulnerabilities and misconfigurations: **hypothetical risk**

Your runtime-based exposure: **real risk**

Your **runtime based hardening** - Remediation, Seccomp profile, Network policy, Secrets mgmt, IAMs, RBAC etc

Your **application runtime anomalies and suspicious behavior** (zero days, unknown risk) - the gold security standard

ARMO

/Posture <-> Runtime Reinforcing Cycle

ARMO

Use Runtime information to continuously prioritize, remediate issues and shrink the attack surface

Configuration and Context (CSPM / KSPM)

Use Posture and Deep risk context to adapt runtime security policies and reduce alert fatigue

Runtime Information (eBPF, CDR/KDR/ADR)

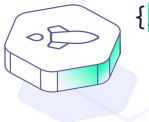
/The ARMO Behavioral Secret Sauce

{Containers & Workloads}

Container images & registries
SBOM
Manifest files & configurations
System calls
Networking
Files access
Process execution

{Cloud & Kubernetes}

Cloud events logs
Cloud APIs
KubeAPI & Control plane
IAMs
VMs and Nodes
RBAC
CRDs



{Applications}

Code
Functions
Call stack
Stack traces
APIs
L4 & L7

ΔPD™

Application Profile DNA

Powered by

eBPF

Kubescape

ARMO

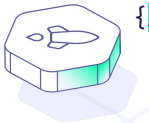
/The ARMO Behavioral Secret Sauce

{Containers & Workloads}

Container images & registries
SBOM
Manifest files & configurations
System calls
Networking
Files access
Process execution

{Cloud & Kubernetes}

Cloud events logs
Cloud APIs
KubeAPI & Control plane
IAMs
VMs and Nodes
RBAC
CRDs



{Applications}

Code
Functions
Call stack
Stack traces
APIs
L4 & L7

ΔPD™

Application Profile DNA

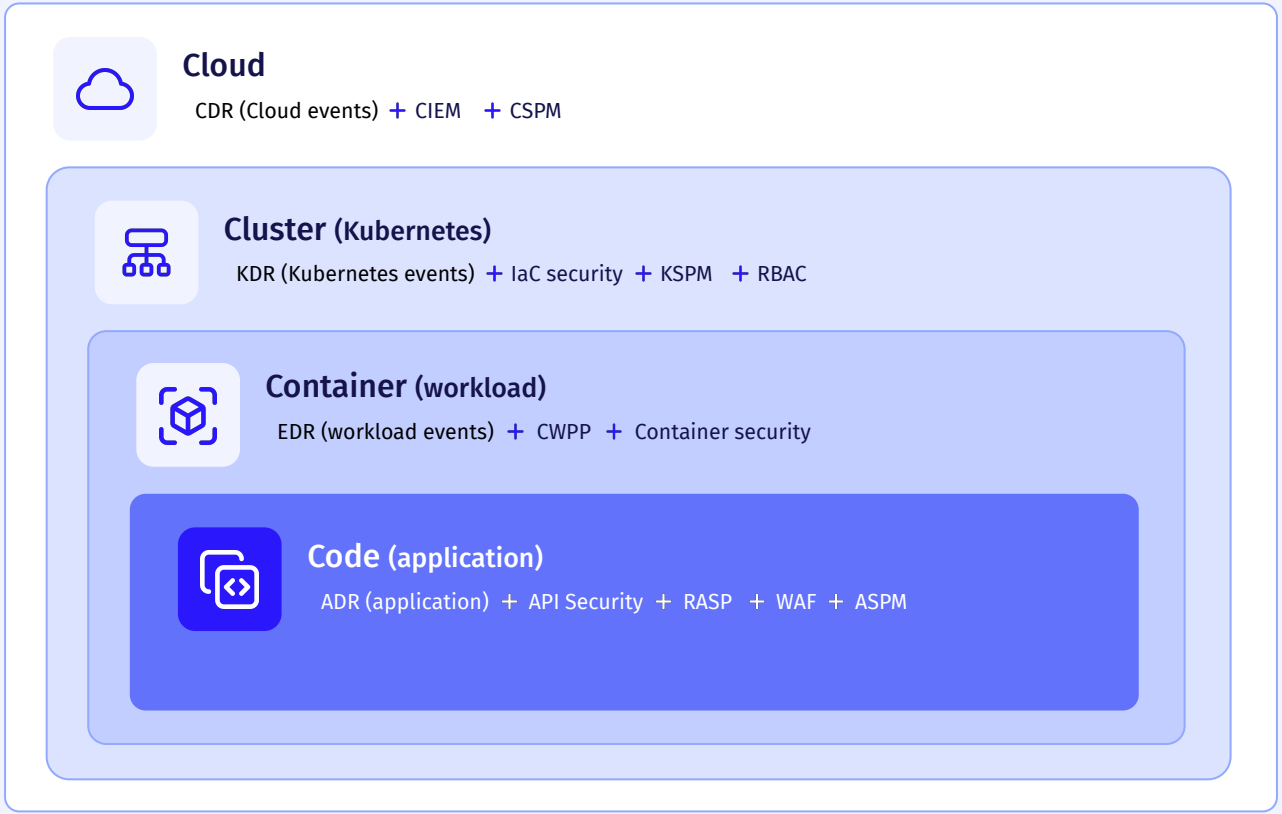
Powered by

eBPF Kubescape

- **Anomaly-based Threat detection** of first seen zero days with (almost) zero false positives
- **Automatic response** (incl. Soft quarantine) & real time **notifications**
- Unified Runtime incidents **visibility, explainability and traceability**
- **Runtime based Vulnerability mgmt -** prioritized relevant reachable, exploitable CVEs
- **Automated cloud hardening** without breaking application
- **Runtime based cloud posture & compliance** highly prioritized, low noise

ARMO

/The Cloud security layers



/xDRs only reveal part of the runtime incident story

+ **Unauthorized access** to S3 buckets
+ **New IAM role** created
+ And more...

+ **Unusual access** to K8s service account
+ **Unexpected process** execution
+ **Unexpected file** access
+ **Unexpected network** connection
+ And more...

+ **API call** with suspicious payload
+ **Function accesses** internet unexpectedly
+ And more...

/xDRs only reveal part of the runtime incident story

+ **Unauthorized access** to S3 buckets
+ **New IAM role** created
+ And more...

SOC <> DevOps

+ **Unusual access** to K8s service account
+ **Unexpected process** execution
+ **Unexpected file** access
+ **Unexpected network** connection
+ And more...

SOC <> Platform team

+ **API call** with suspicious payload
+ **Function accesses** internet unexpectedly
+ And more...

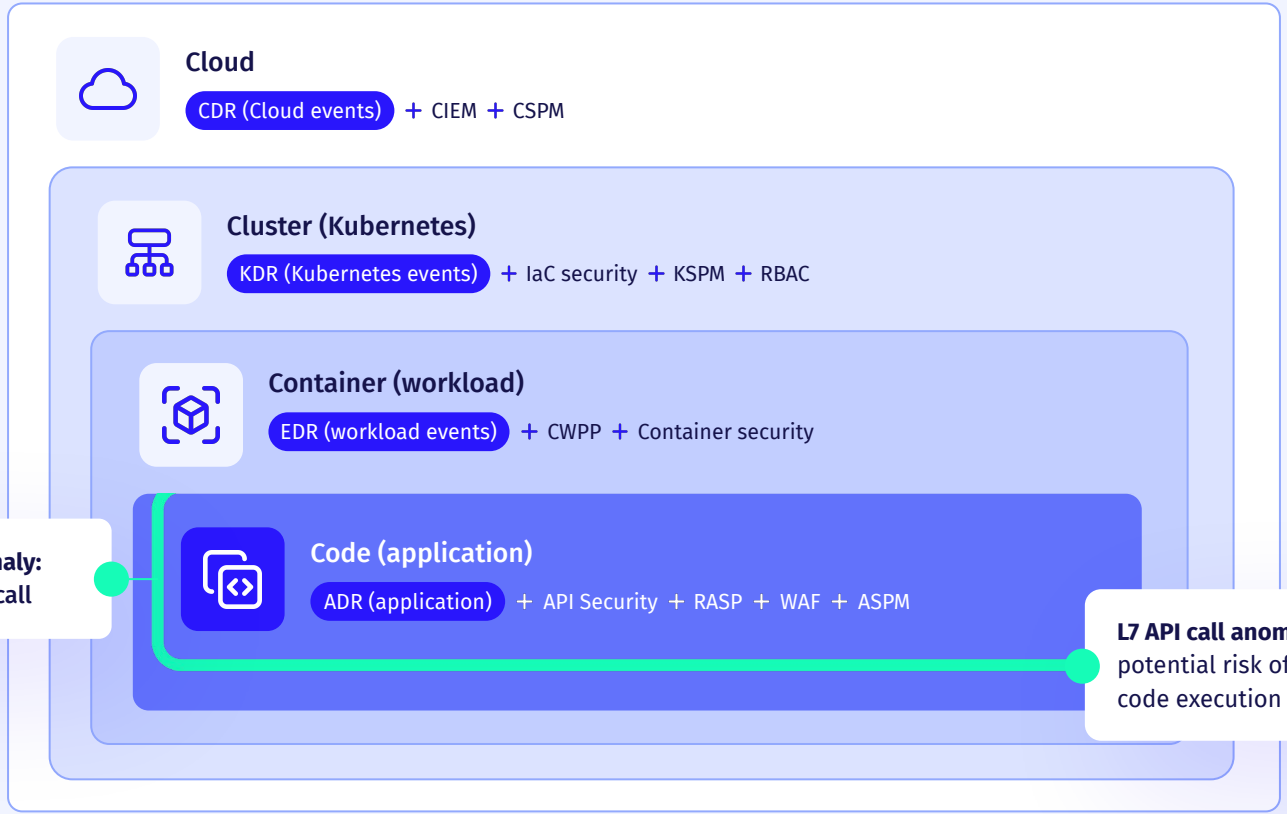
SOC <> App Dev

/Connecting the dots

Attacks are NEVER single dimension

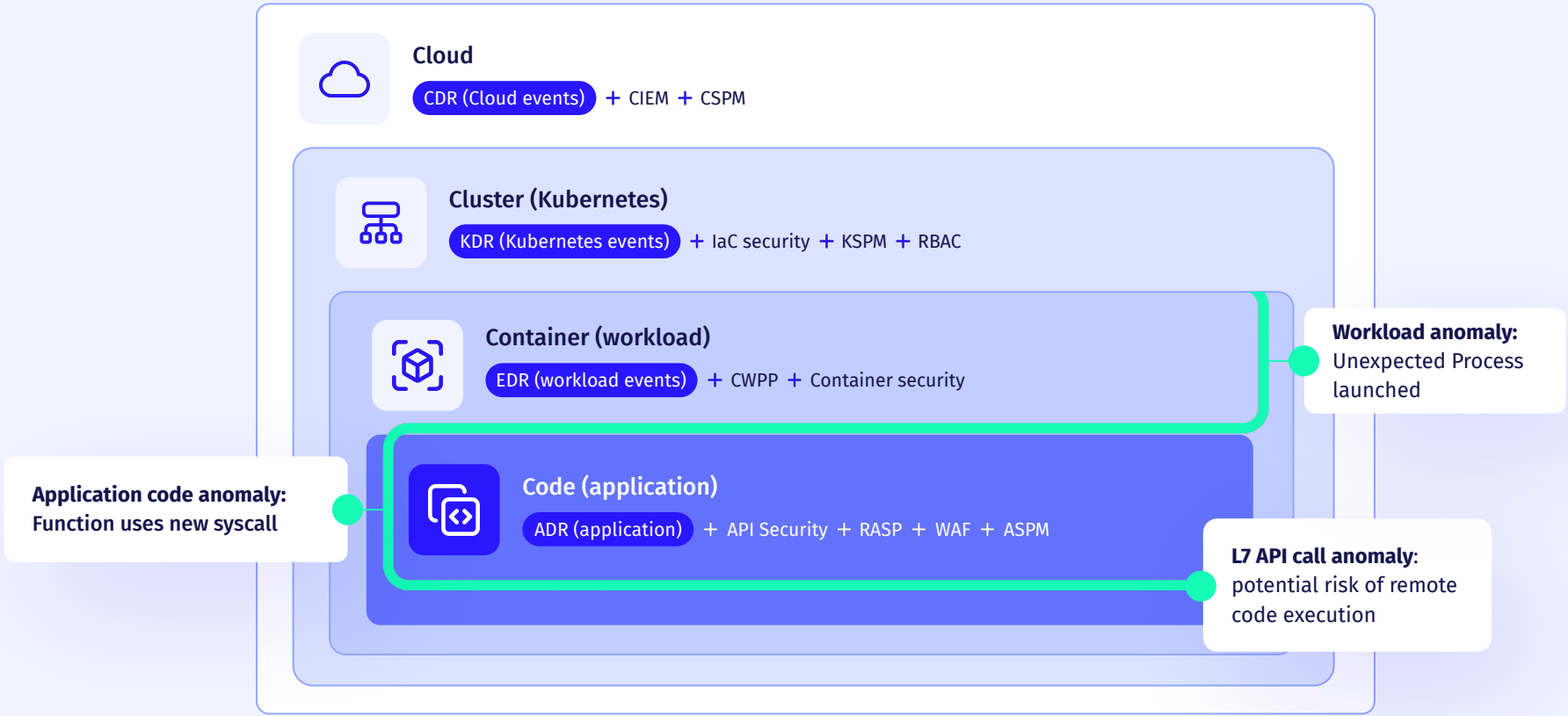
/Connecting the dots

Attacks are NEVER single dimension



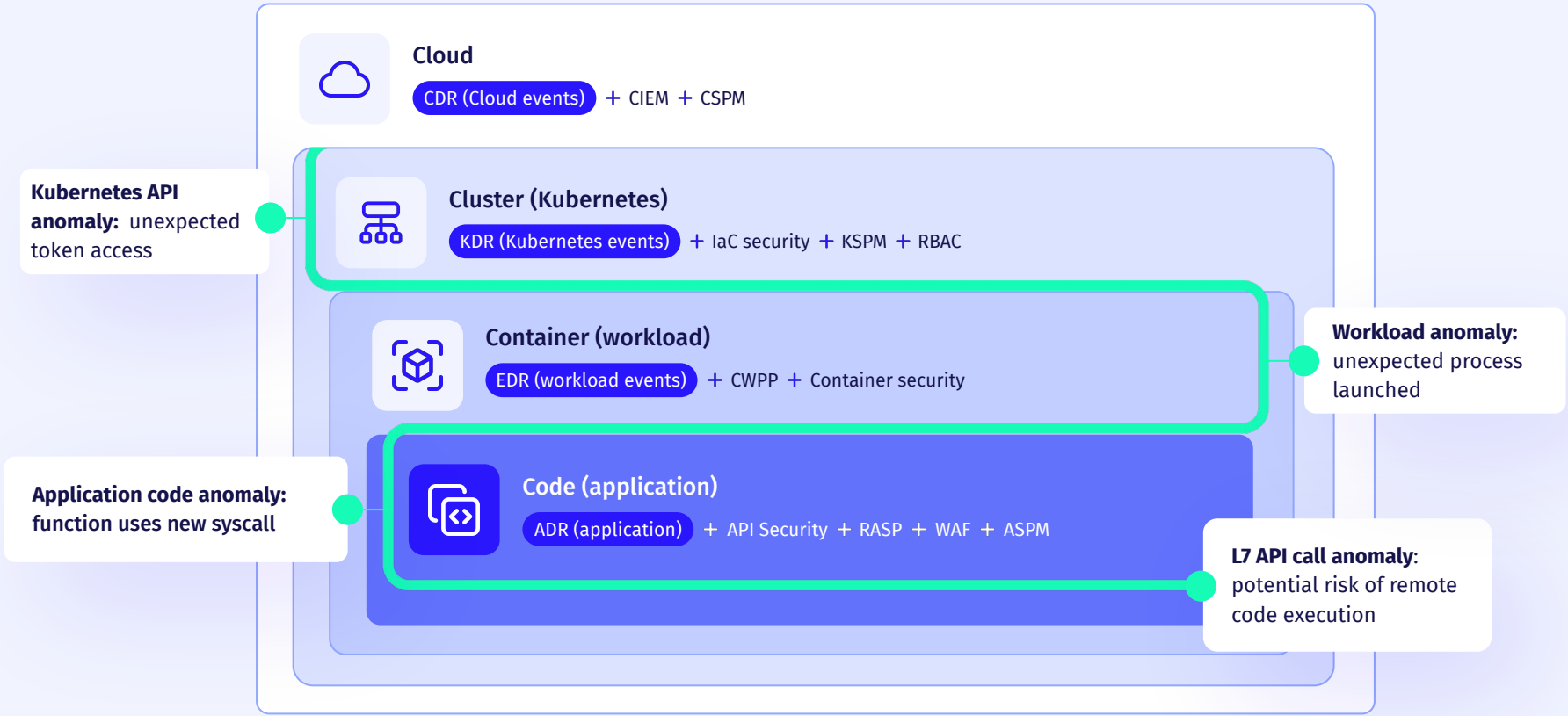
/Connecting the dots

Attacks are NEVER single dimension



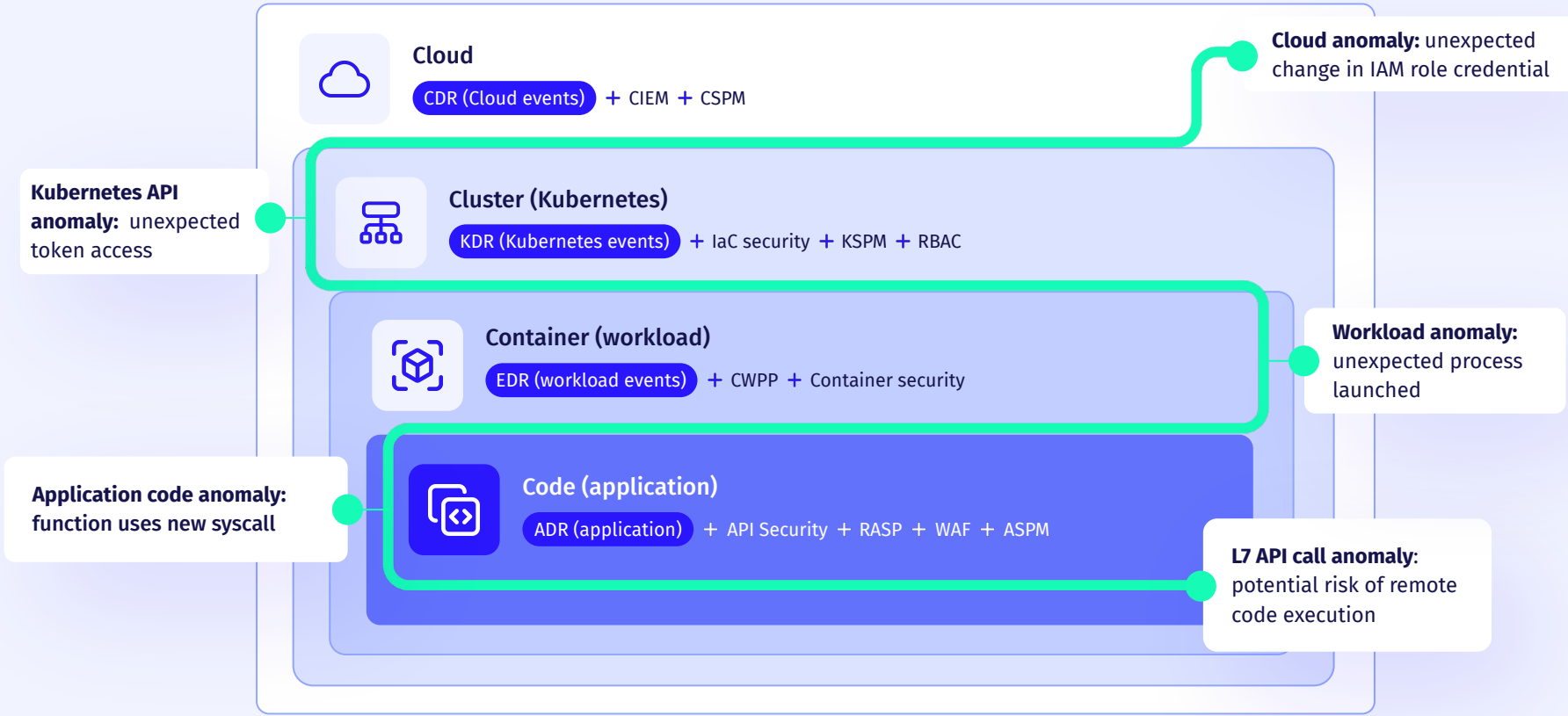
/Connecting the dots

Attacks are NEVER single dimension



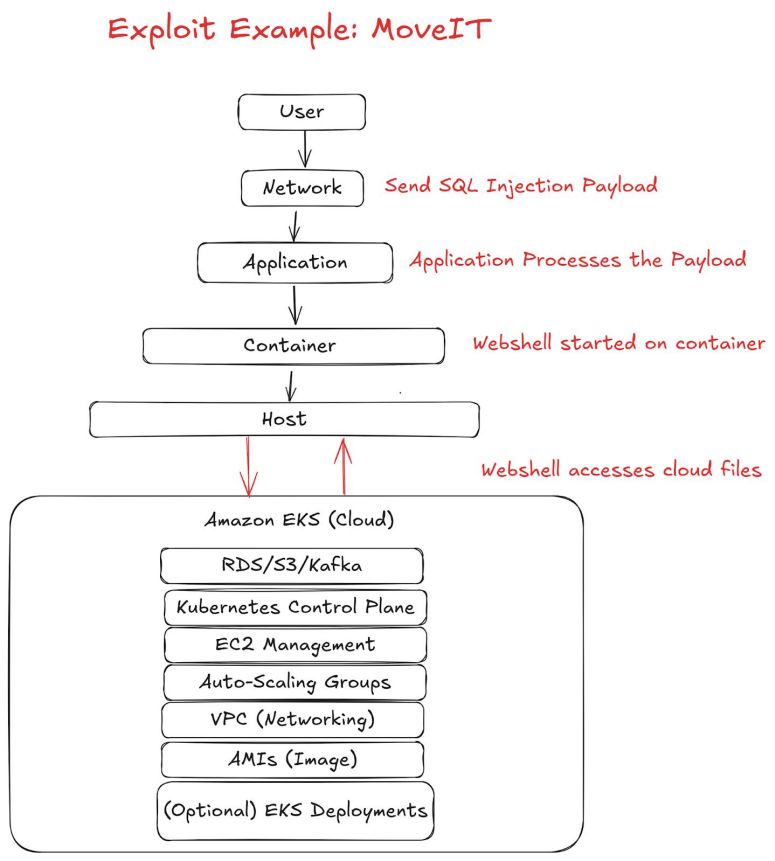
/Connecting the dots

Attacks are NEVER single dimension



/Connecting the dots

Attacks are NEVER single dimensional



/ Static based (Rules) Detection & Response Doesn’t Scale

Static vs Anomaly Detection

MITRE Based

MITRE STATS: [Tactic: 14+ **] [** Technique: 60+ **] [**Sub-Technique: 150+**] [Patterns: Infinite]**

Static Detector

Static Rule 1

Tactic: Execution

Technique: Command & Script Interpreter

Sub-Technique: PowerShell

Pattern: Static (curl, nmap, netcat etc)

Static Rule 2

Static Rule 3

Static Rule 4

Static Rule N (~100k rules)

Static (Rules based) Detection:

- **Explosion** of rules
- **Blind** to zero-days
- **Complex** and Opaque
- **High** false positive rate
- **Constant** rule and exception tuning

/ Static based (Rules) Detection & Response Doesn't Scale

Static vs Anomaly Detection

MITRE Based

MITRE STATS: [Tactic: 14+ **] [** Technique: 60+ **] [**Sub-Technique: 150+**] [Patterns: Infinite]**

Static Detector

Static Rule 1

Tactic: Execution

Technique: Command & Script Interpreter

Sub-Technique: PowerShell

Pattern: Static (curl, nmap, netcat etc)

Static Rule 2

Static Rule 3

Static Rule 4

Static Rule N (~100k rules)

Anomaly Detector

Rule 1: Anomalous **Process** Execution

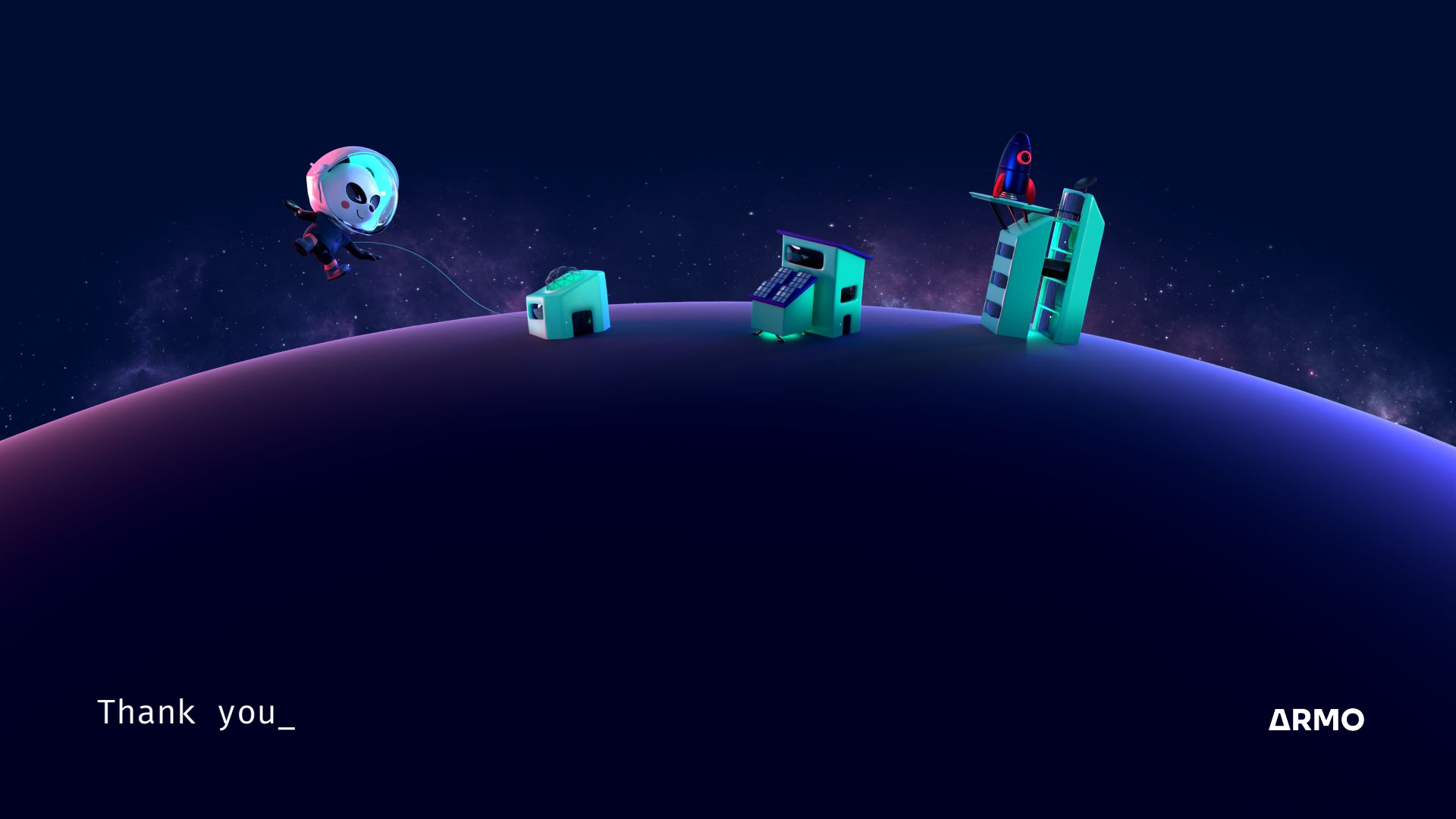
Tactic: Execution
Techniques : Process Injection Command and Scripting Interpreter System Binary Proxy Execution

Tactic: Privilege Escalation
Techniques : Exploitation for Privilege Escalation

Rule 2: Anomalous **Network Activity**

Tactic: Command and Control (C2)
Techniques : Application Layer Protocol Web Service

Tactic: Exfiltration
Techniques :
Data Exfiltration Over C2 Channel
Exfiltration Over Non-C2 Protocol


Thank you_
ARMO