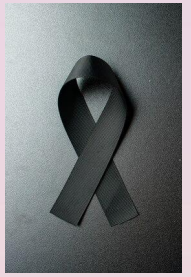


KubeCon | CloudNativeCon

North America 2023

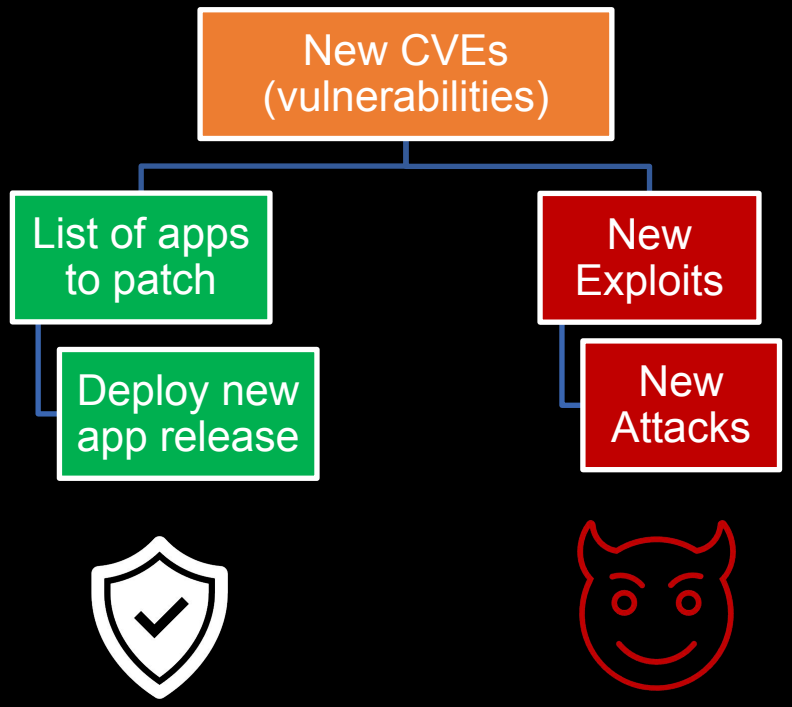
KubeCon | CloudNativeCon

North America 2023

All Cloud-Native Services Are Vulnerable — Block Exploits with Security Behavior Analytics

David Hadas, IBM Research
Roland Huß, Red Hat

Can we stop the cat and mouse cyber chase?



FIGHTING THE FRAUDSTERS: A GAME OF CAT AND MOUSE

Cybercrime is evolving in response to the coronavirus pandemic, but so too is the fight back

During the annual gathering of the Association of Certified Fraud Examiners last year, Jean-Francois Legault, MD and global head of cybersecurity at JP Morgan Chase, commented: "If you build a better mousetrap, it's highly likely that an adversary will build a better mouse."

Fraud has always been a cat-and-mouse game, where the good guys try to keep up and ahead of the increasingly sophisticated tactics of the bad guys. But during the pandemic, this battle has intensified.

Coronavirus-driven lockdowns, social distancing and people staying at home, with more free time and more disposable income, has led to mobile apps and online payment tools soaring in popularity with many fintechs reporting tremendous growth. However, just as quick to profit from the pandemic are fraudsters, who have gone where the money is to steal as quickly and easily as possible.

PANDEMIC-POWERED FRAUDULENT ATTACKS

According to fraud fighting firm **SEON**, rather than deterring fraudsters, the pandemic has, in many cases, empowered them. More traffic accordingly means more fraudulent behaviour.

In its latest report, *Fighting the Fraudsters in an Age of Pandemic*, SEON warns that: "As the world migrated online in record numbers to cope with restrictions on physical movement and interaction, within their numbers were those with nefarious intentions. As so much fraud is now perpetrated in cyberspace, many fraudsters saw an opportunity in enhanced traffic volumes, and they have been capitalising on it."

The report highlights that as cryptocurrency and online trading experienced growth during the early months of the pandemic, it also led to a spike in fraud. With sporting events postponed and cancelled, the popularity of eSports and iGaming has also grown – but so too has abuse in the sectors. While bonus abuse, multi-accounting and affiliate fraud were always persistent forms of attack, the popularity boom has also attracted the attention of more experienced and more ruthless fraudsters.

Daniel Sebes, SEON's eSports expert and business development manager, says: "We have found that fraudsters were registering multiple accounts and playing against themselves, using the bonuses provided by operators to generate cold, hard cash."

PHISHING ATTACKS

Security firm **F5** also reports on a drastic increase in phishing and spearphishing attacks. News about vaccines or elections have been leveraged to entice people to open emails from unknown sources, or even known sources who may have had their accounts breached and hijacked, to then spread malware and other malicious attack to steal user and corporate information or enable illicit access to sensitive networks, clouds, applications and data.

Keiron Shepherd, principal solutions engineer at F5, comments: "Cybercriminals are becoming very adept at misleading voters with disinformation. This includes propagating false news, using bots to drive social media engagement and the strategic leaks of incriminating emails or confidential documents."

"With data breaches reported on a near weekly basis in the national news, the view around cyber culture has changed considerably over the last few decades. We've gone from lone hackers in bedrooms to nation states weaponising zero-day attacks. More than ever, businesses and individuals are starting to understand that data is a valuable currency that needs to be protected."

ORGANISATIONS UNDER ATTACK

For its *Cybersecurity in the Remote Work Era: A Global Risk Report*, research firm **Ponemon Institute** – commissioned by password manager firm **Keeper Security** – surveyed IT security personnel from across the globe. Its report found that during the pandemic, many organisations have had exploits and malware that evaded their intrusion detection systems and anti-virus solutions – with credential theft and phishing, or social engineering, the most frequent types of cyberattacks.

It was also revealed that cyberattacks during Covid-19 are becoming more severe in terms of negative consequences, such as the impact on finances, with cyberattacks becoming more targeted and sophisticated. Fifty-eight per cent of those surveyed said that their organisations experienced a compromise that damaged IT infrastructure or stole IT assets.

Darren Guccione, CEO of password manager **Keeper Security**, says: "The past year has been a radical, cybersecurity wake-up call for the fintech industry. The pandemic exposed mass ill-preparedness across the entire finance sector with 70 per cent of companies experiencing a cyberattack in the last 12 months. With businesses entering 2021 having to face the double whammy of stringent lockdowns and challenges the new Brexit deal brings, it looks like things will still get worse for the sector on the cyber risk front before they eventually get better."

FIGHTING FRAUDSTERS

While the identification of threats is key to understanding exposure and risks, the increase in fraud during the pandemic has underlined the need for communication and collaborative action in the battle against cybercrime.

For **Tamás Kádár**, CEO and founder at **SEON**, it is crucial that businesses don't focus solely on their digital successes during the pandemic.

"The online space is busier than ever and companies are looking to remain competitive while they find their feet in the new normal. That being said, it's essential that they don't focus solely on bolstering conversions at the expense of security and vice versa. It is a balancing act. While security measures should be tightened, businesses should be conducting risk checks that cause minimal obstruction to customers and cause the least friction. Throughout the outbreak many businesses have had to adapt quickly to changing circumstances and they should be able to respond to fraud with the same haste.

> Cyberattacks in the pandemic are becoming more severe in terms of negative consequences, such as the impact on finances, with tactics becoming more targeted and sophisticated

"It's important to understand that there is no way of fighting fraud that can ever be 100 per cent successful. Every time a company like ours develops a new line of defence, the fraudsters begin looking for ways to bypass it. A solution we develop today might be outdated in just a few months' time. Unfortunately for the fraudsters however, though they may never stop, neither do we."

EMBRACING TECHNOLOGY

For **Darktrace**, an artificial intelligence company that specialises in cyber defence, while cyberattacks have evolved, the key to fighting them remains the same.

Dave Palmer, director of technology at **Darktrace**, says: "Static security – creating rules about what is 'good' and 'bad' simply can't keep pace. There is no silver bullet to cybersecurity but today we have technology available that can stop novel attacks at machine-speed. Finding the right people with the right skills to defend organisations is important, but they cannot handle the challenge alone. We need to augment teams with AI that can make decisions in seconds."

TAKING RESPONSIBILITY

According to **Tim Hickman**, partner and data protection lawyer at law firm **White & Case**, it is essential for any business to understand its legal and regulatory compliance responsibilities and identify the relevant cybersecurity risks, take a proactive approach wherever possible, and have a reactive plan in place where needed.

Hickman said: "In the wake of a cyber incident, establishing [an] initial snapshot assessment is incredibly important as it will drive not only the prioritisation of the response, but the entire process. If an incident is correctly identified as high risk at the onset, the response timeline will accelerate, with organisational resources deployed more appropriately. Principally, it's about damage limitation and controlling the incident, so understanding the mitigating factors that might help to reduce risk to the business is key."

Chris Huggett, senior vice president EMEA, at IT provider **Sungard AS**, says: "In today's IT-driven business world, assessing technology risks is a critical part of business continuity planning in every company across every industry. This is especially true when it comes to cybersecurity, where even the smallest IT footprint provides attackers with a gateway to global supply chains, and the ability to wreak havoc on countless stakeholders."

LESSONS LEARNED

Meanwhile, **Chris Hodson**, chief information security officer at security and systems management firm **Tanium**, believes that increased threats should be a "timely reminder for business leaders to incorporate resilience into their distributed workforce infrastructure if they're going to manage the security challenges of this new world of work effectively."

He adds: "Many of the issues that emerged at the start of lockdown resulted from considerably overestimating preparedness for the security challenges that came with shifting to a distributed working environment. Our research found that 85 per cent of business leaders thought they were prepared to manage the shift to widespread working from home. This confidence turned out to be ill-founded with 98 per cent admitting they faced security challenges in the transition away from the office.

"Even before the virus emerged, concern among IT leaders was growing with tool sprawl, shadow IT and legacy tech creating a slew of security challenges. Not only did widespread remote working exacerbate these existing issues, it also created a host of new security challenges, allowing cybercriminals to run amok during a period of deep confusion and uncertainty for businesses.

"Whether companies choose to permanently move their operations, return employees to the office, or some combination of both, implementing endpoint management and efficient security solutions should be a priority."

ALLOCATING RESOURCES

Keeper's Guccione agrees that with remote work poised to continue, the fintech sector needs to equip staff with the right cyber defence preparation at home, rather than waiting to reinstate security measures for a return to the office.

"We can expect to see a rise in cybersecurity awareness training and general education covering online security," he says. "Presently, 34 per cent of those in the finance industry have no understanding of how to protect themselves against a cyberattack. The mass handling and management of financial assets makes fintech companies a prime target for cybercriminals. Increased budgets and resources should be allocated in order for fintech organisations to bolster internal controls and effectuate robust cybersecurity and incident response plans. In part, this will involve further investment in identity access management solutions that utilise a zero-trust framework, zero-knowledge security architecture and an enterprise password management platform that can tie into and strengthen their identity applications."

THE FIGHT CONTINUES

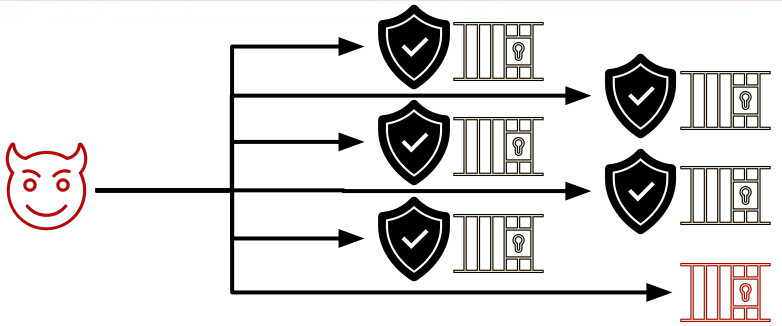
Cybersecurity is a never-ending cat-and-mouse game. As new services emerge and preventative technology evolves so too does fraud. Constant fine-tuning of fraud detection strategies and compliance is vital.

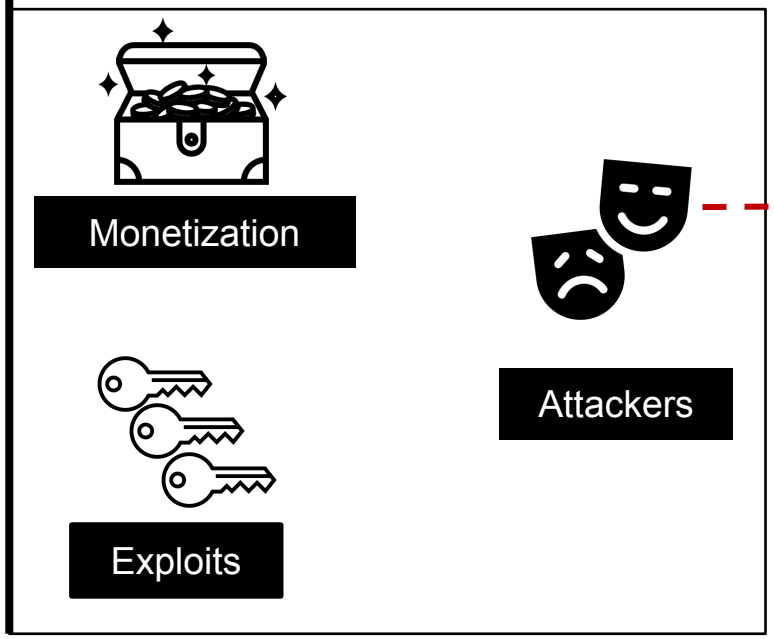
Businesses and individuals must arm themselves with the right tools, the right knowledge and be prepared to communicate in order to remain cyber resilient. The fight against fraud will continue... TFT

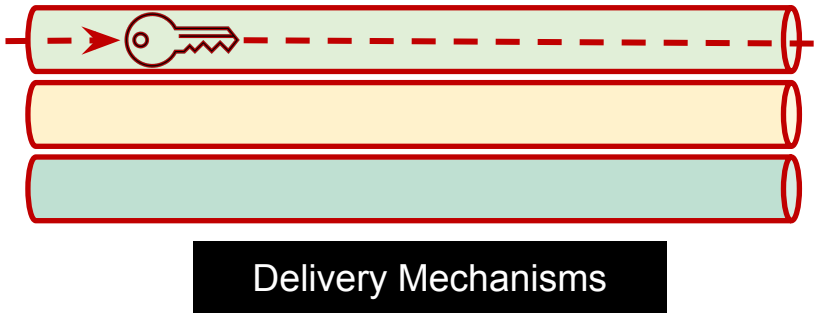
We lose in this game for a reason…

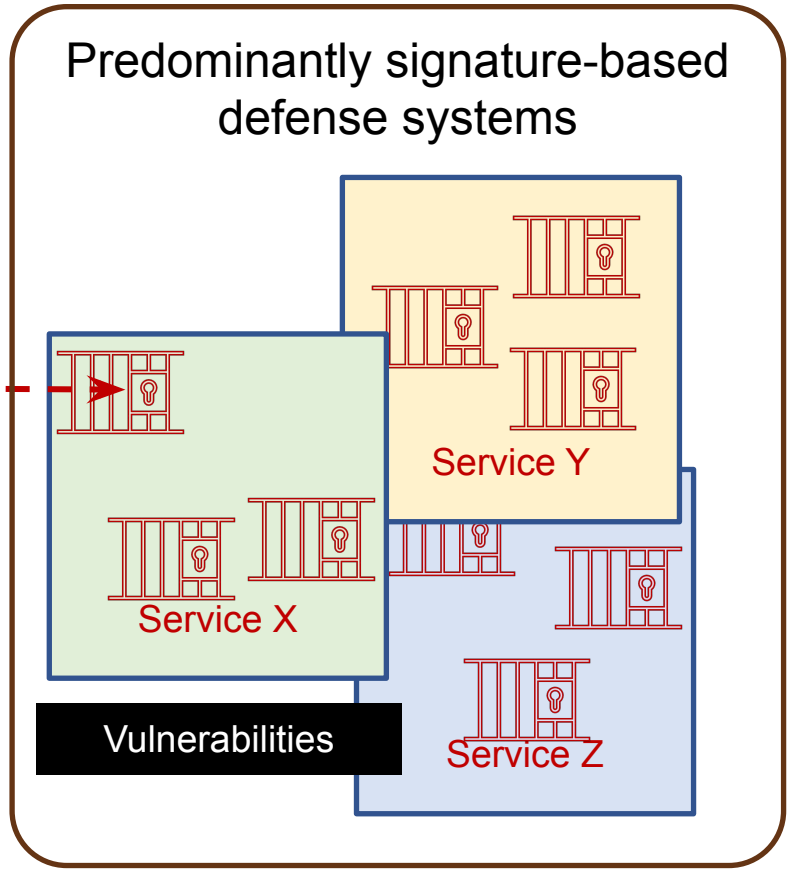
Today's rich hacking eco system includes an abundance of:

- Repetitive Vulnerabilities (same locks)
- Exploits (each a key for many locks)
- Delivery mechanisms
- Hackers (from beginners using tools embedded in Kali to professionals)
- Monetization methods and… lots of automation!!! => Great ROI









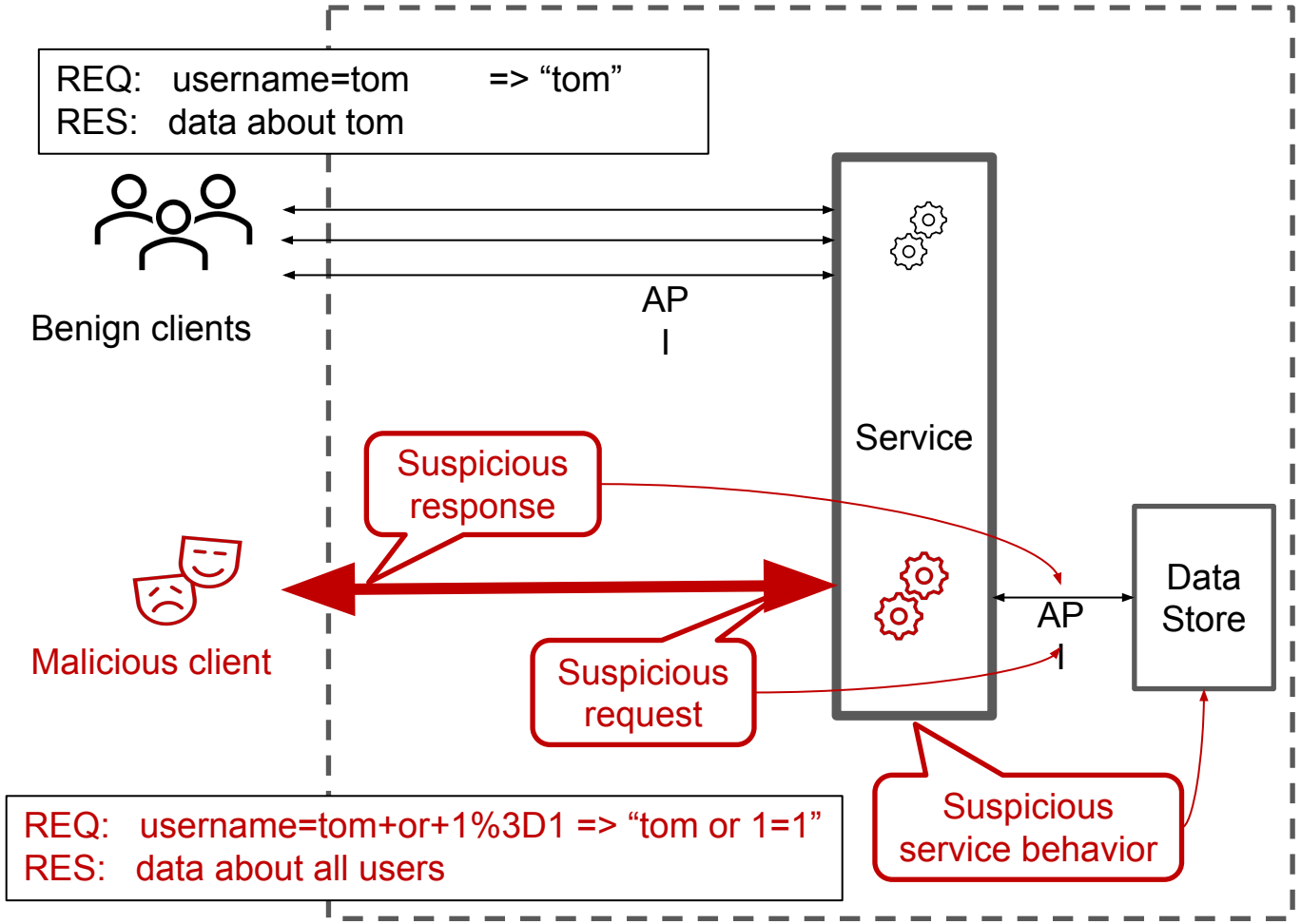
We should not rely on signatures


F. CLARK
IAD

Is this alien a Friend or Foo?

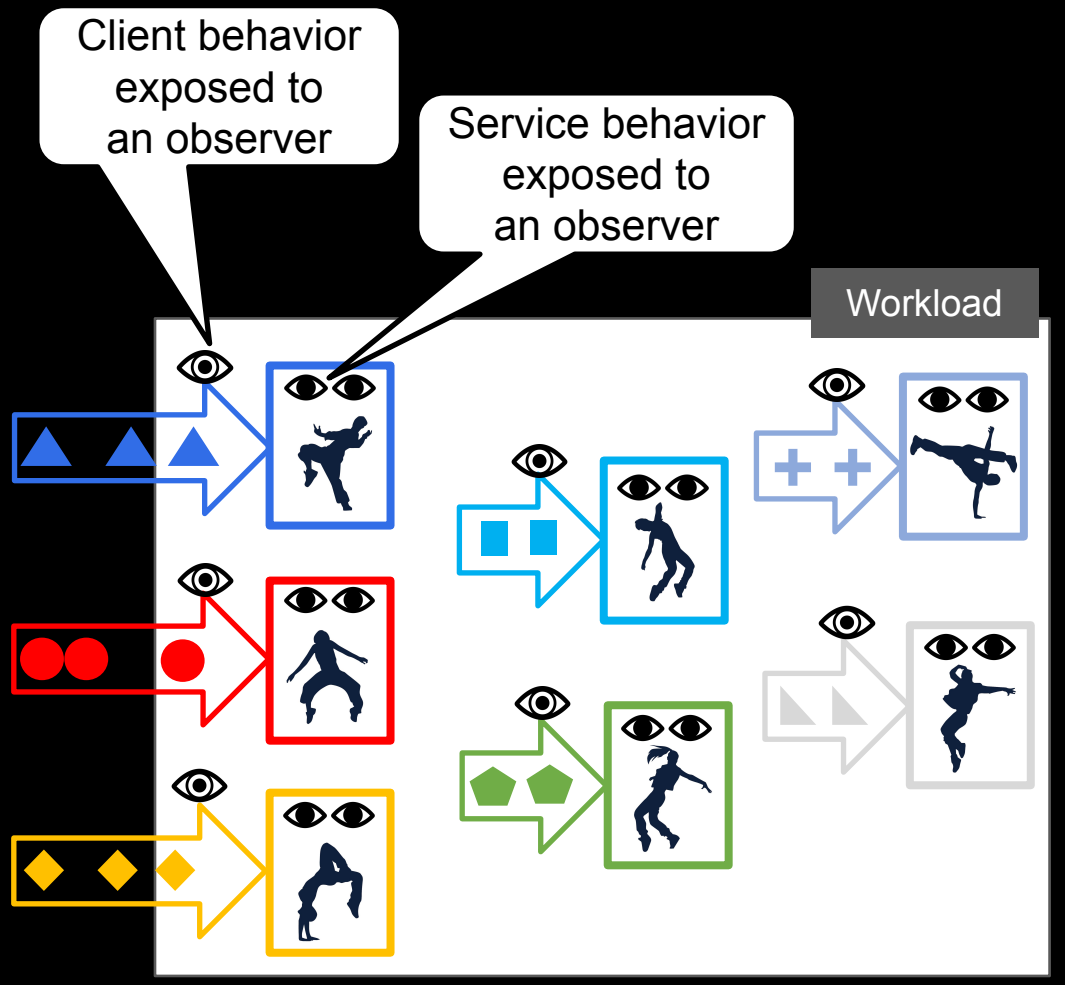
Security Behaviour Analytics

- CVEs in dependencies
- Business logic vulnerabilities –
  e.g SQL injection, poor user input verification



Example “Security Behaviour Analytics” performed on a simple workload

Cloud Native 12-factor apps:
Microservices, Serverless and Functions
are well suited to Security Behaviour Analytics



Per-service SBA can detect exploitation attempts that went unnoticed at the frontend services, came from lateral movement, or an insider.

Signatures are denylist (per cloud)

SBA uses an allowlist (per service value)

SBA is a per-service protection suite based on the behaviors associated with each specific service

- Analyzing client behavior - to stop the attack at its onset.
- Analyzing service behavior - to cover anything we missed + dormant malicious code + backdoors.

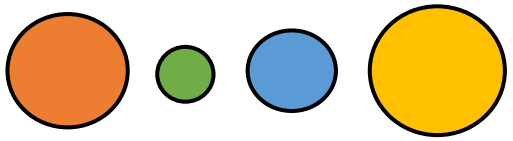
But how can we analyze behaviors?

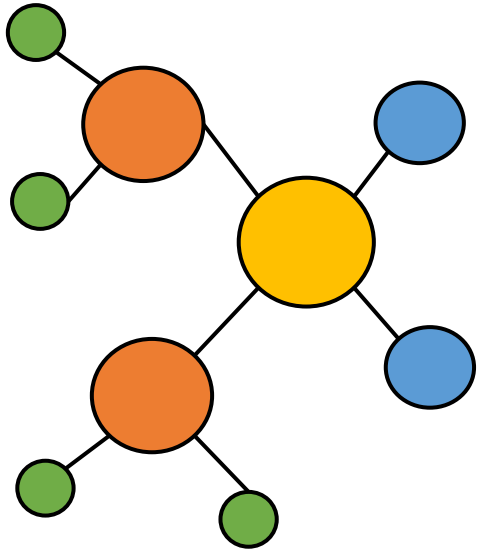
The Secret Sauce…

To perform SBA, we apply our knowledge about the basic ingredients of web exploits and construct an effective language of security indicators.

- Use of special characters, unreadable characters, Unicode regions
- Length
- Num of sequences

Indicators are atoms that compose exploits





Apply to every Key/Value

The security-related indicators are extracted from each and every key or value being transferred.

- Headers “Accept-Language: en-US,en;q=0.5”
- Headers “If-Modified-Since: Mon, 18 Jul 2016 02:36:04 GMT”
- Query String “name=joe” or “page=2”
- Json Body

```
{
  "data": [{
    "type": "articles",
    "id": "1",
    "attributes": {
      "title": "JSON:API paints my bikeshed!",
      "body": "The shortest article. Ever.",
      "created": "2015-05-22T14:56:29.000Z",
```

We first establish the normal behavior in each kind of interaction,
then detect when a key/value is being used abnormally for the delivery of an exploit.

Using SBA

Client behavior

- **Profile client requests**
  Identify requests that contain key/value pairs showing indicators not appearing in normal **requests** for this service

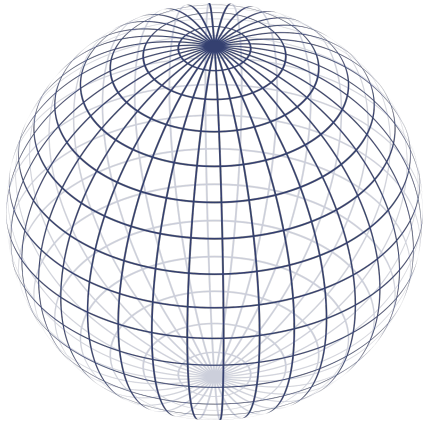
Service behavior

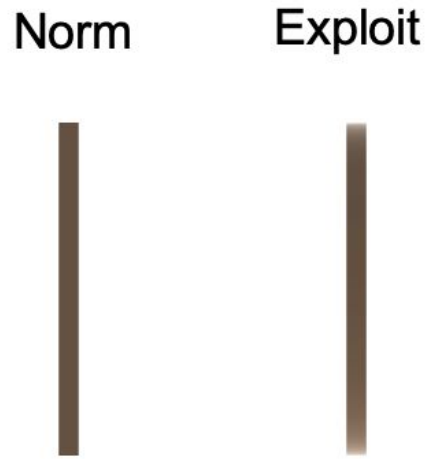
- **Profile cloud-service responses**
  Identify requests that contain key/value pairs showing indicators not appearing in normal **responses** of this service
- **Profile cloud-service runtime behavior**
  Identify service that show runtime indicators not appearing normally by this service

Is this really a game changer?

Why is this a game changer?

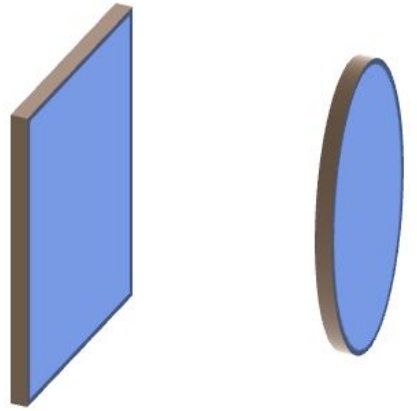
Developing new exploits when SBA is applied
- Let's assume I can create an exploit indistinguishable from a normal key/value





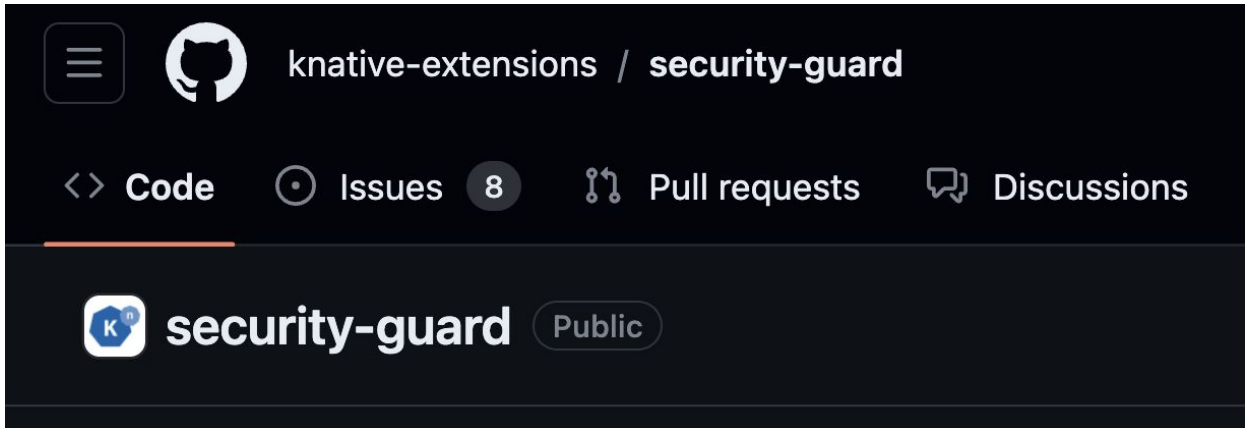
Adding indicators

Adding more dimensions to distinguish between exploit and norm
- Identify between exploit and normal key/value
- Use for all key/values



Where are we on the journey for SBA?

Security-Guard



knative.dev/security-guard

2021 IBM Research project

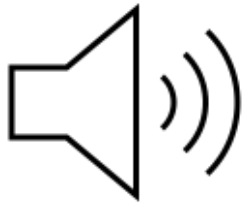
2022 Open Sourced as a CNCF Knative extension

2023 Add support for Vanilla Kubernetes
Work as part of the Tag Security Zero Trust effort

Show me!

Demo

See Video at
https://youtu.be/qq8fDbrTzE4

(Turn speakers on) 

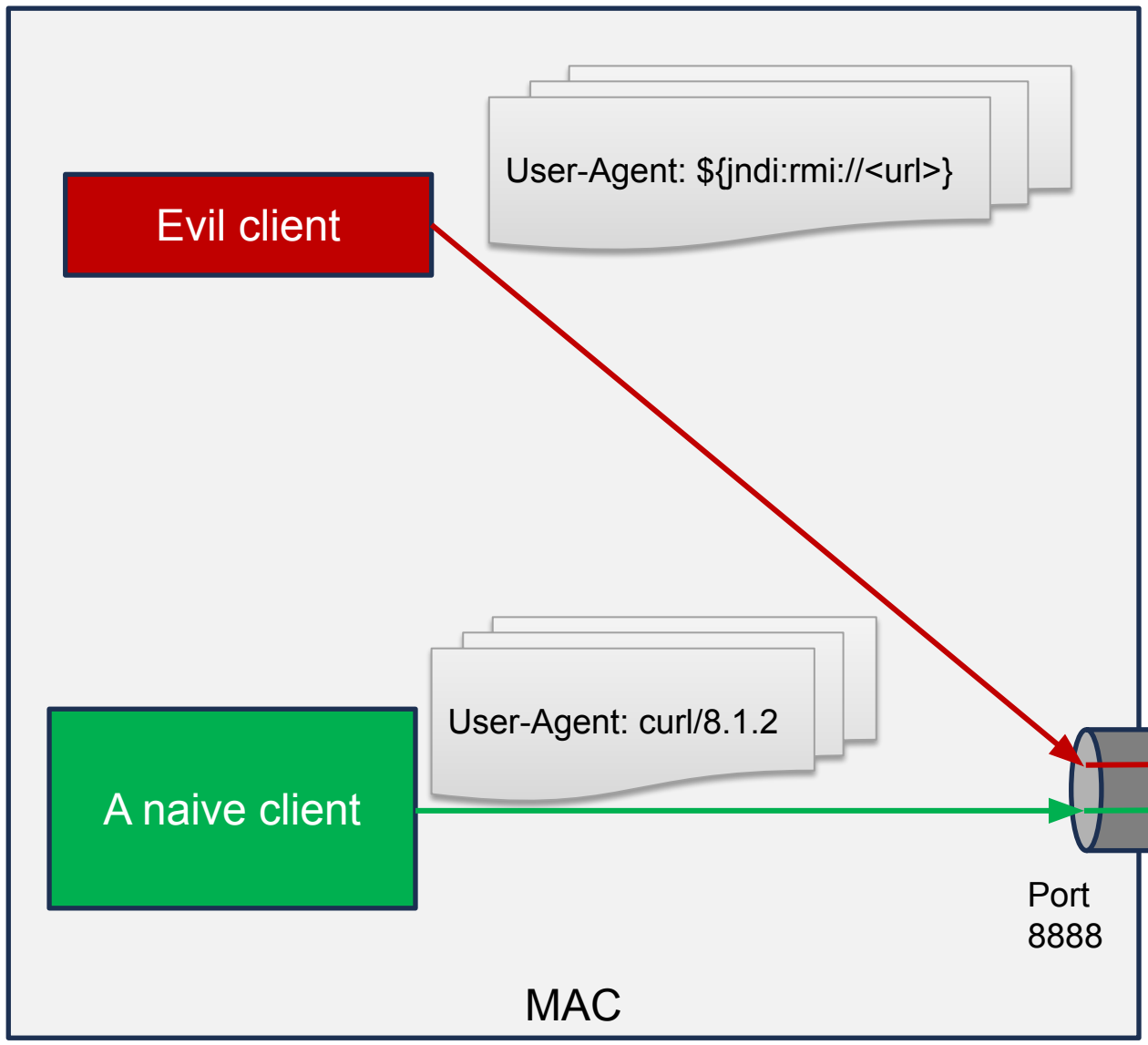
A Log4Shell vulnerable Java app is exploited.

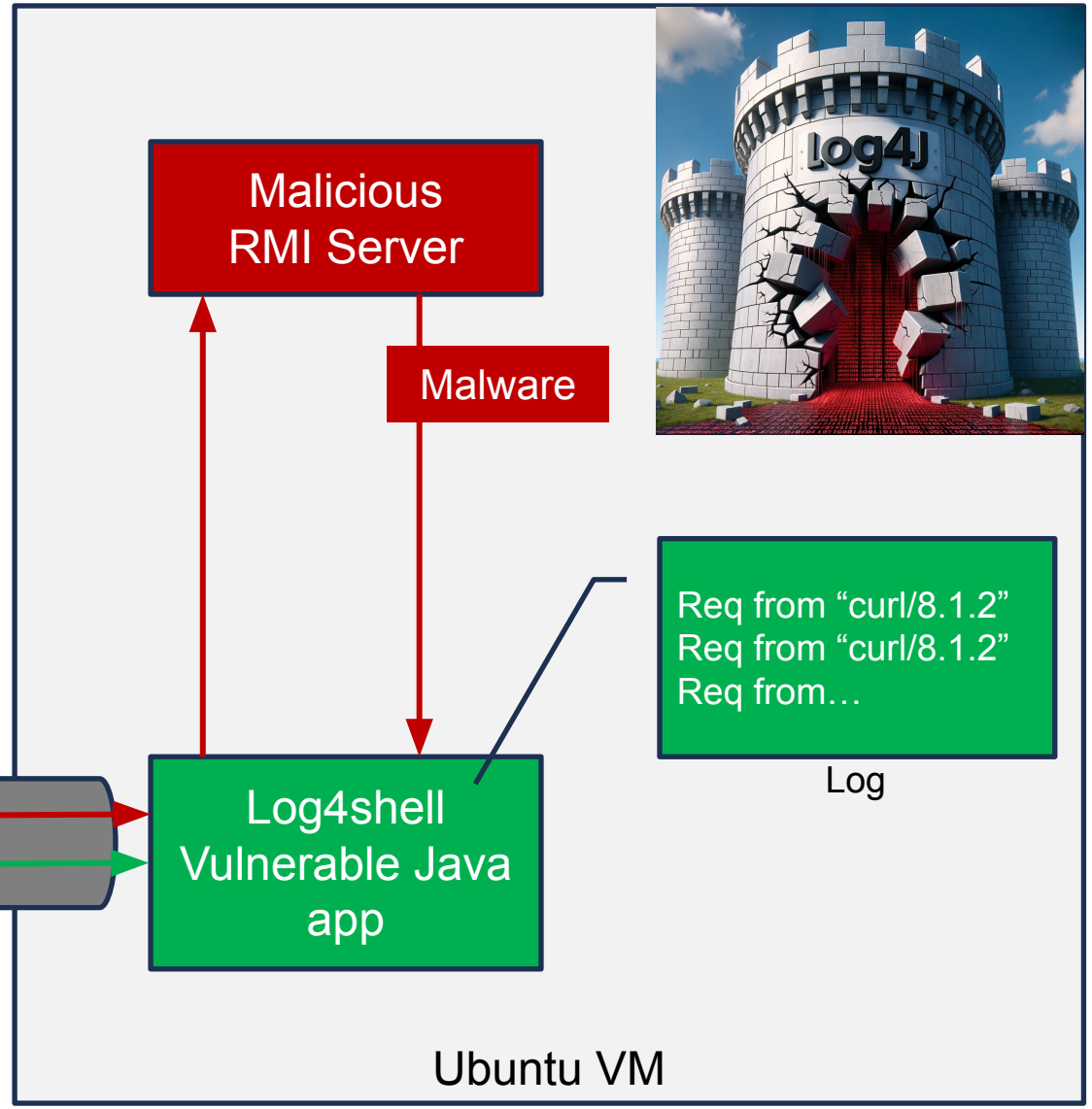
The exploit directs the app to retrieve malware from a malicious RMI server.

Malware mimics a “WannaCry” ransomware attack

(Demo)

What if we deployed SBA prior to Log4Shell?





(Demo)

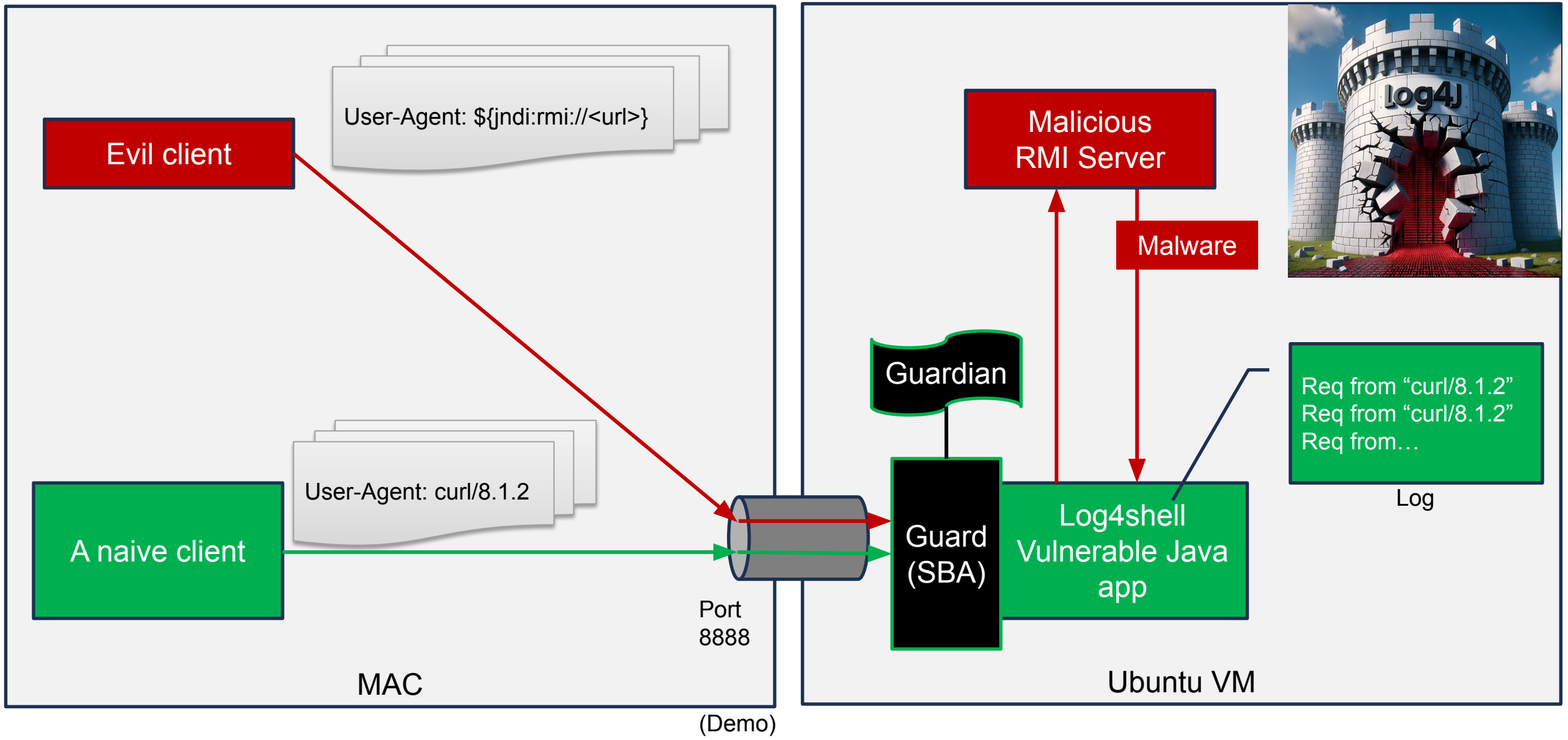
Guard performs Security Behavior Analytics (SBA)

Learns normal traffic

Identify and block Exploits

(Demo)

What if we deployed SBA prior to Log4Shell?



Guard blocks Log4Shell exploit although it never seen one before!!!

Guard ML builds a per app “Guardian” object defining what is normal in each key/value.

(Demo)

Getting real….

A CNCF Knative open-source tool*

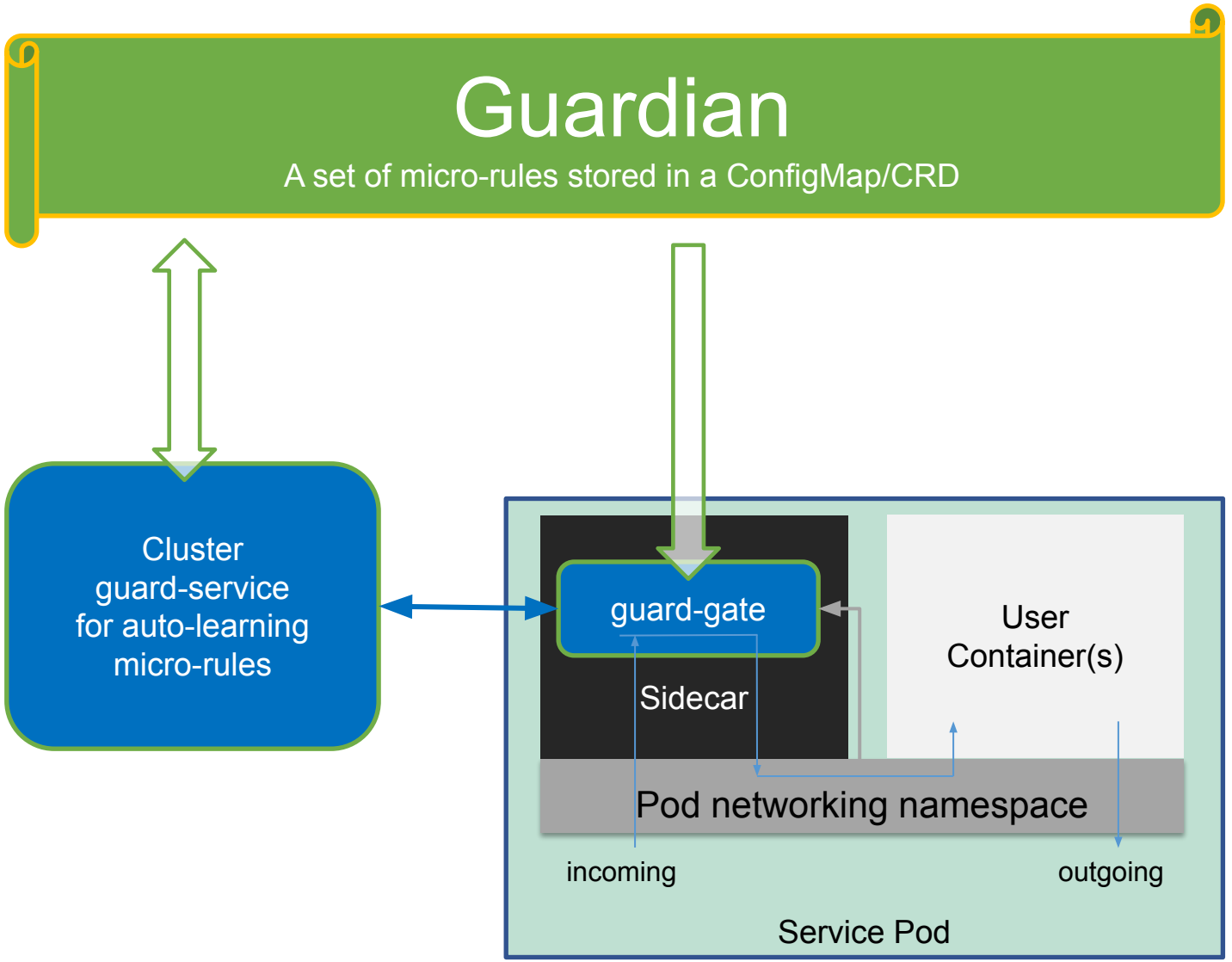
Guard: SBA for Cloud Native clusters

Guard-gate

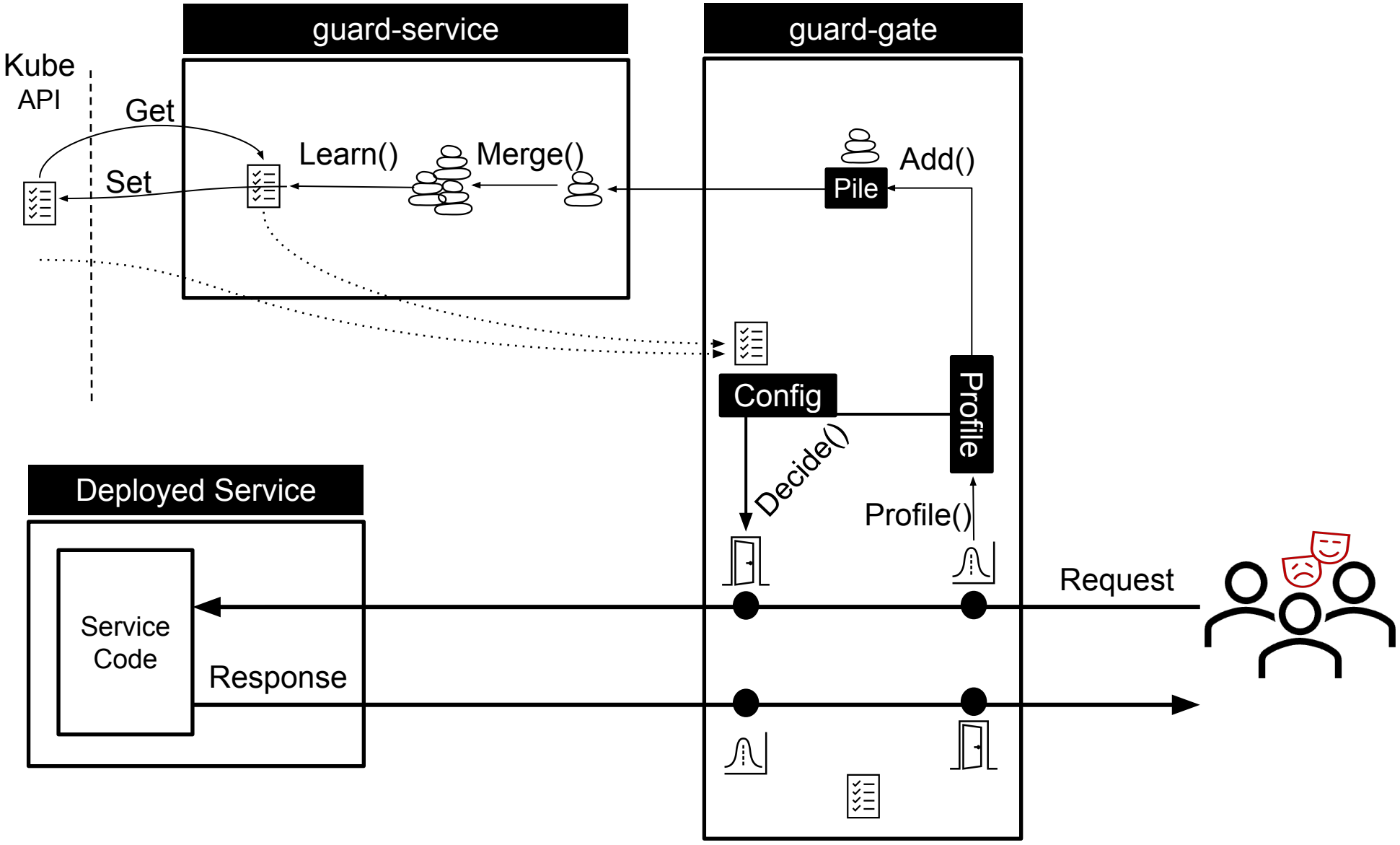
- Profile requests, responses, user containers
- Decide if profile meets Guardian micro-rules
- Pile profiles and send to guard-service to enable ML

Guard-service (ML)

- Auto-learn micro-rules and update Guardian:



*Can be used as a sidecar with Vanila Kubernetes


guard-service
guard-gate
Kube
API
Get
Set
Learn()
Merge()
Add()
Pile
Config
Profile
Decide()
Profile()
Deployed Service
Service
Code
Response
Request

ML keeps me in the dark!

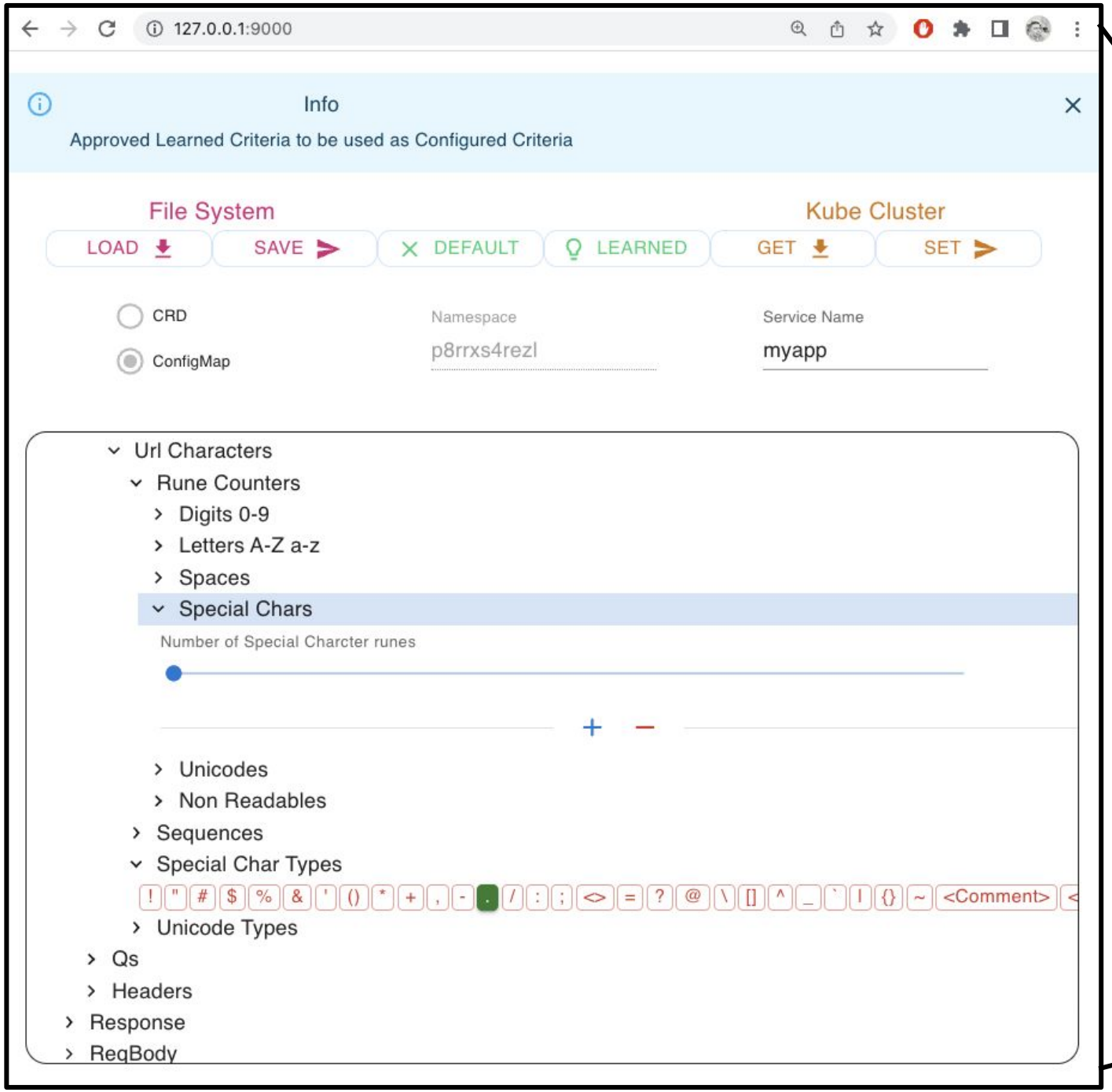
We need ML with Human Oversight

ML used for cyber security needs to offer human oversight

- Humans should be able to understand and justify the ML decisions
- Humans should be able to tune the Guardian for their needs (Set Micro-rules)

ML need to quickly learn what deviates from the norm

- Guard uses an ensemble of small (quick) learners rather than a multi-dimensional learner



CRD object
guard.security.knative.dev

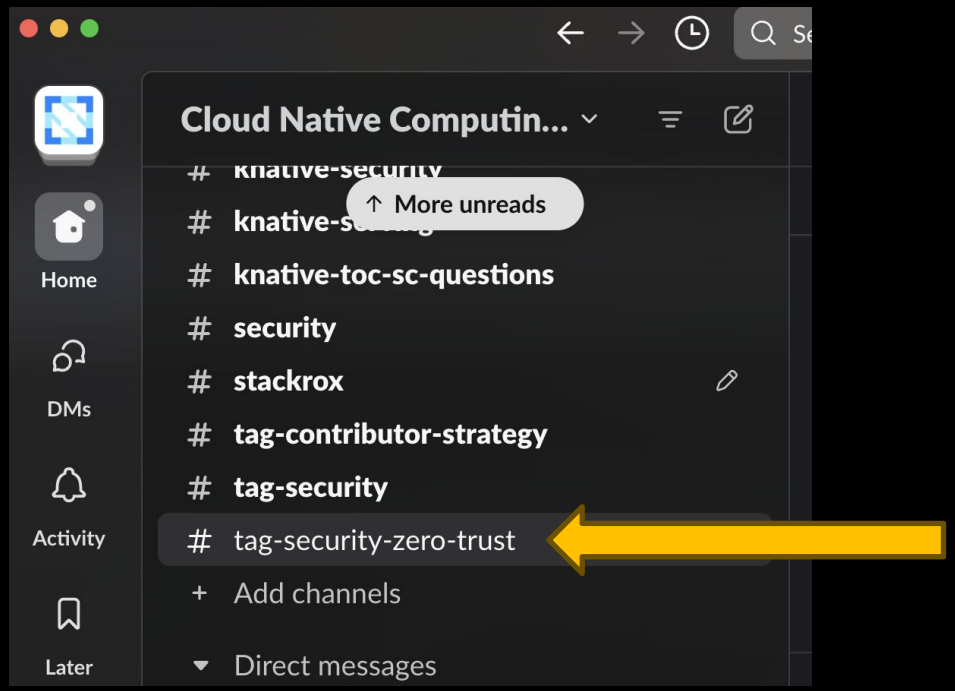
```
    unicodeFlags: null
    unicodes: 0
  User-Agent:
    digits: 19
    flags: 8434816
    letters: 36
    nonreadables: 0
    schars: 17
    sequences: 33
    spaces: 12
    unicodeFlags: null
    unicodes: 0
  X-Forwarded-For:
    digits: 14
    flags: 5120
    letters: 0
```

What is the relationship of SBA to “Zero Trust”?

Tag-Security is working on a whitepaper -
Applying “Zero Trust” for Cloud Native environments

The white paper advocates SBA technologies to protect the cloud

Why is SBA needed when designing a Zero Trust Architecture?



Zero Trust: Everyone is a suspect

Always verify, never trust

- Eliminate implicit trust
- Continually monitor behavior to verify trustworthiness
- Minimize explicit trust

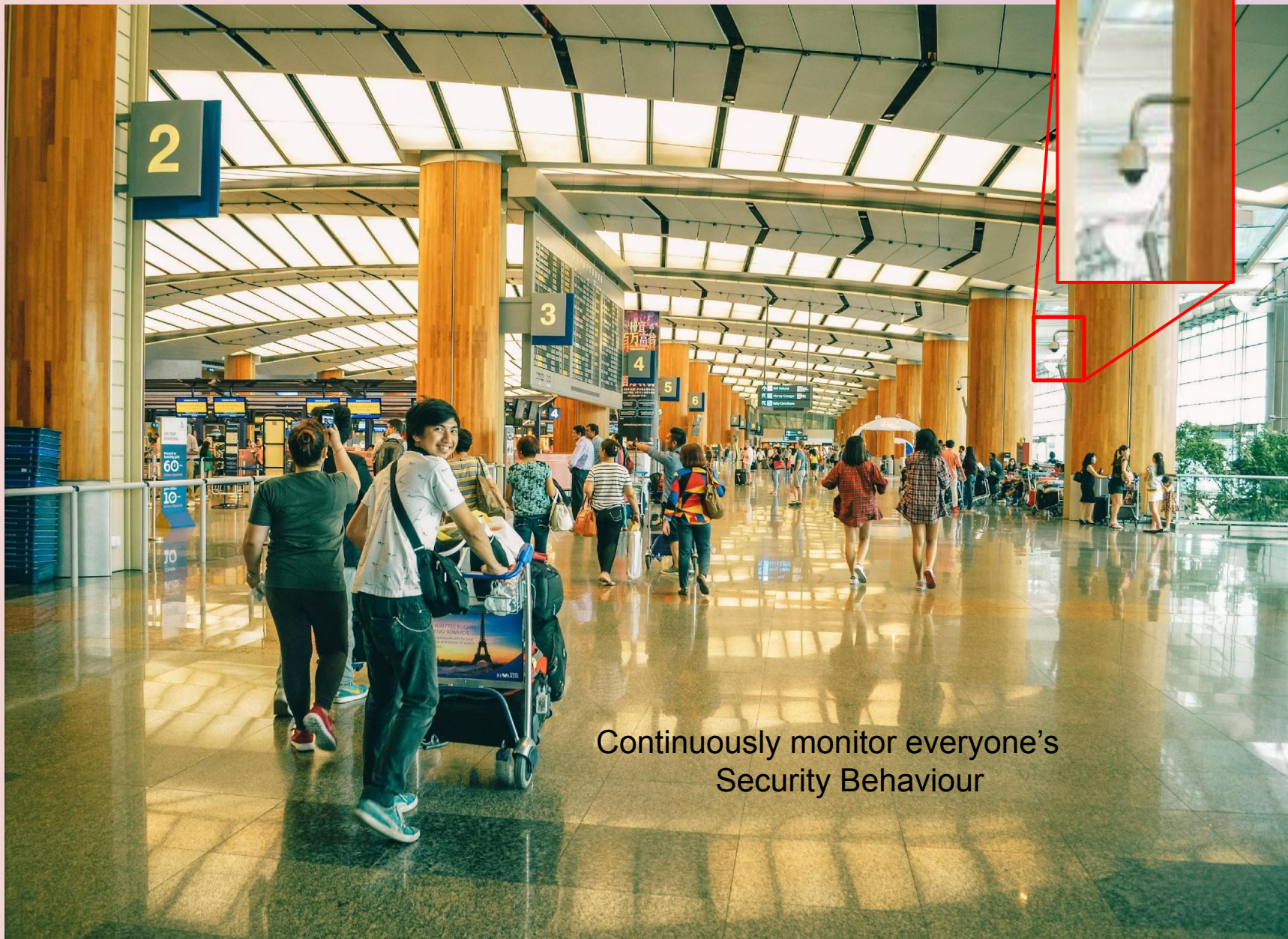
Zero Trust: Everything will go wrong

Assume a breach

- Any Client may be breached
- Any Service may be breached

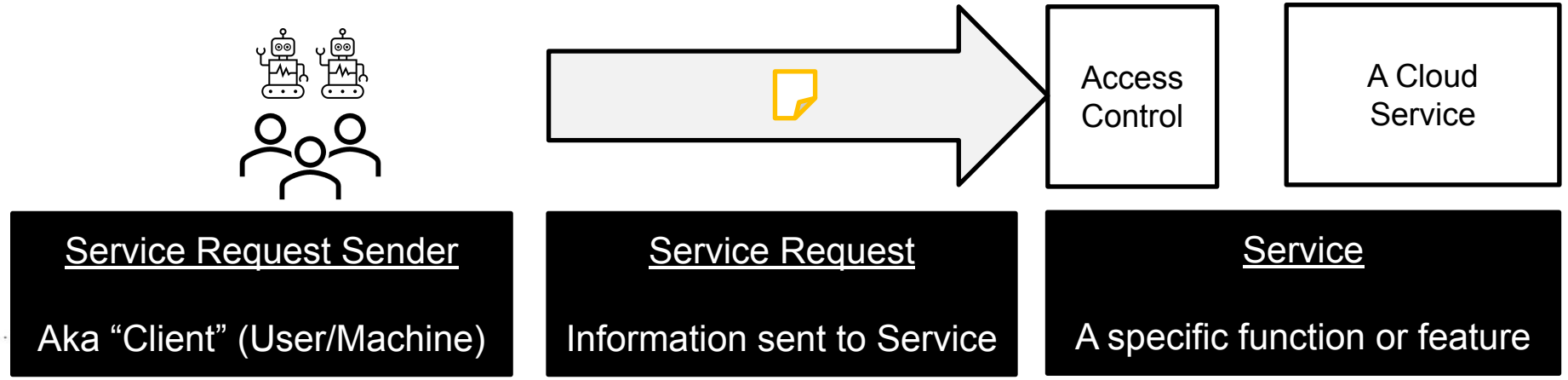
Protect the perimeter

Zero Trust



Continuously monitor everyone's
Security Behaviour

"*Zero Trust*" under Cloud Native

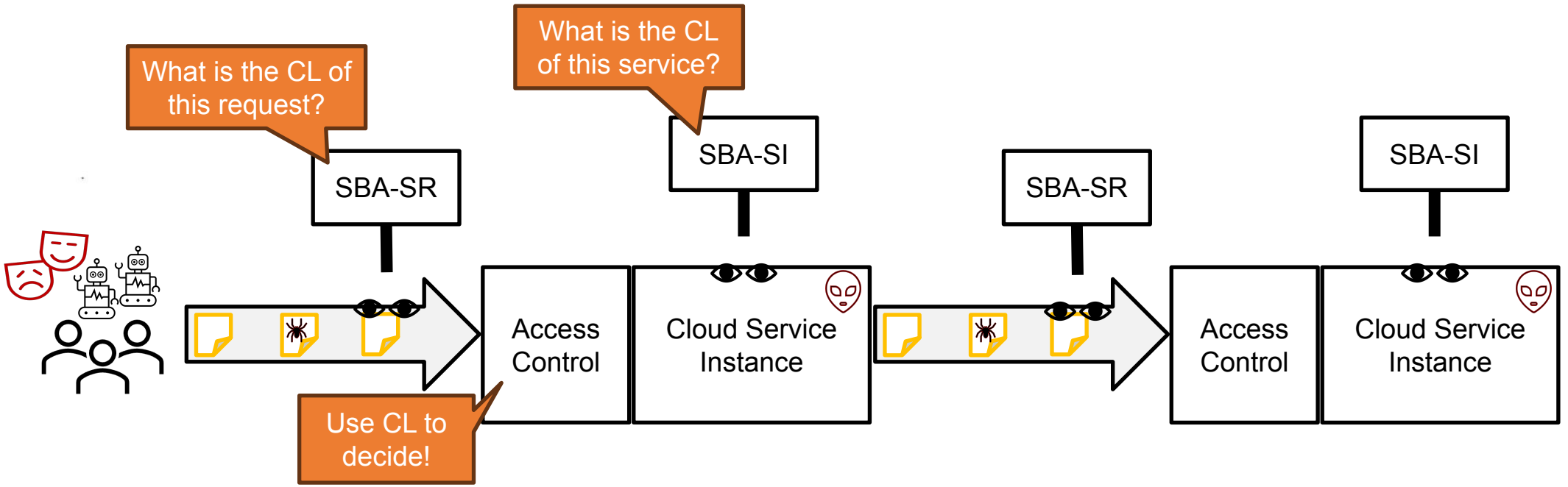


***Zero Trust requires an "Active Observer"* to evaluate if we can trust:**

- **The Service Request Sender**
- **The Service Request**
- **The Service**

SBA is the "*Zero Trust*" Active Observer

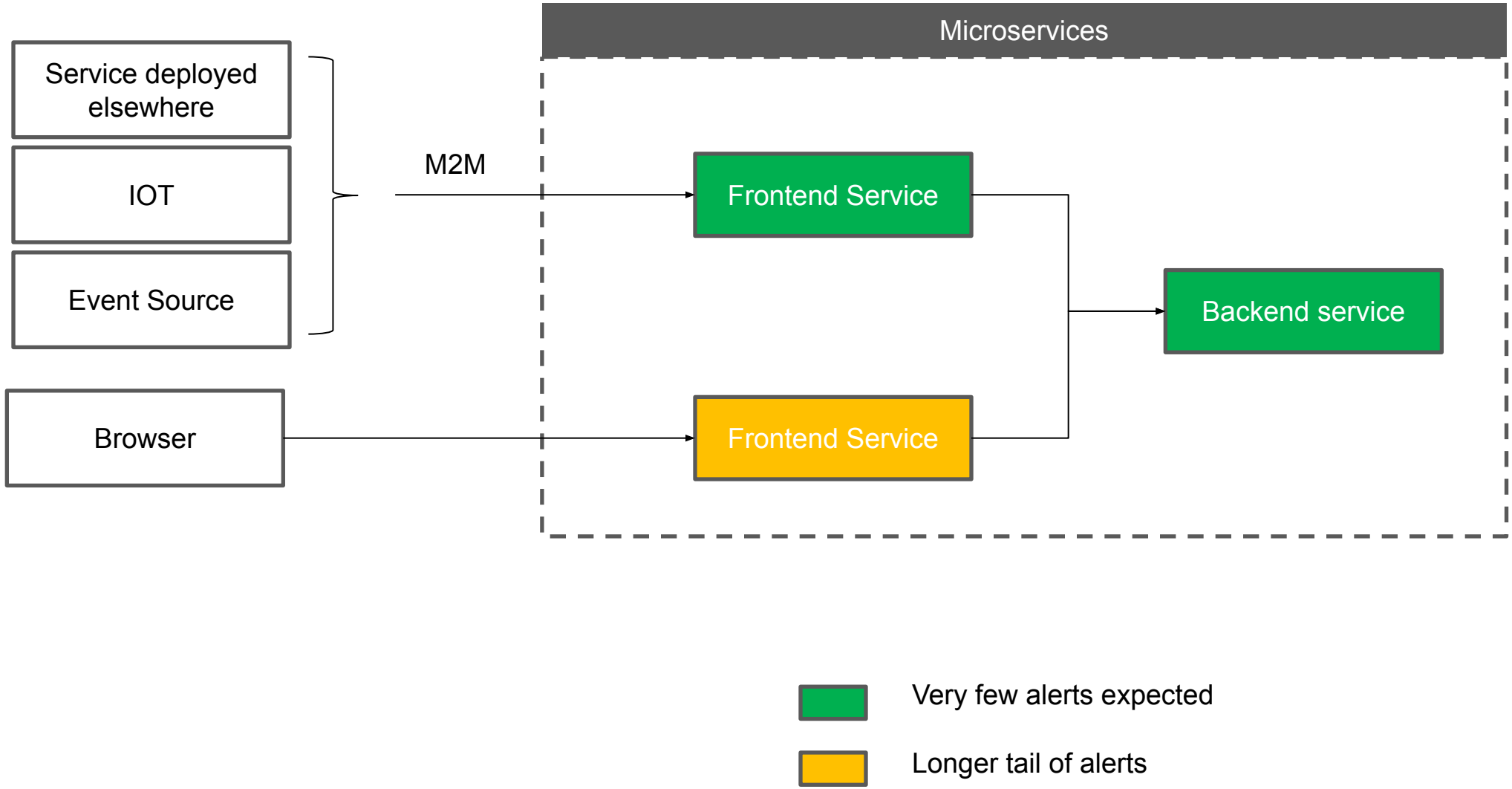
The "Active Observer"* evaluates our *Confidence Levels (CL)



SR - Service Request
SI - Service Instance

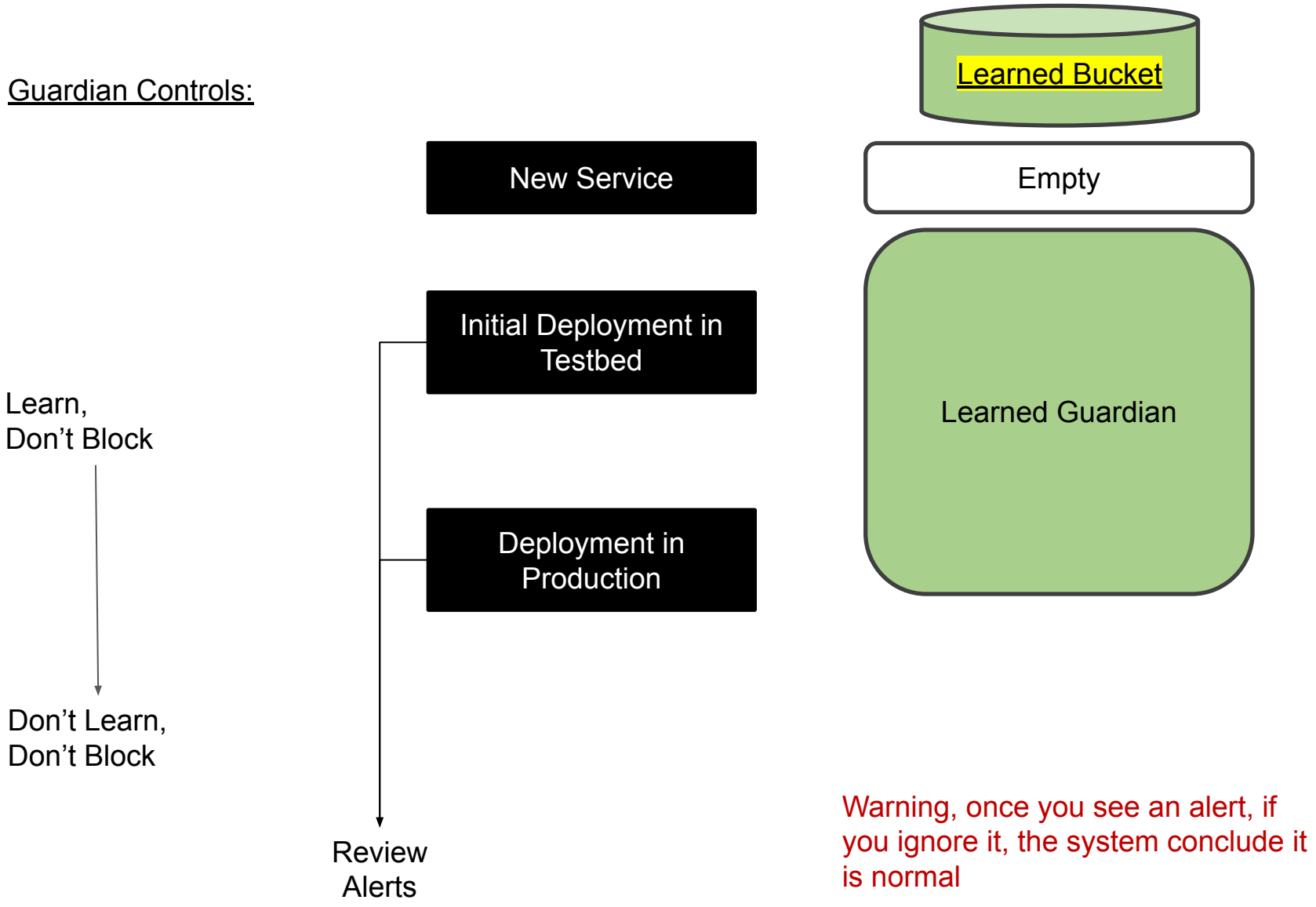
How can I manage
a Guardian for each service?

Guard: Microservive deployment implications



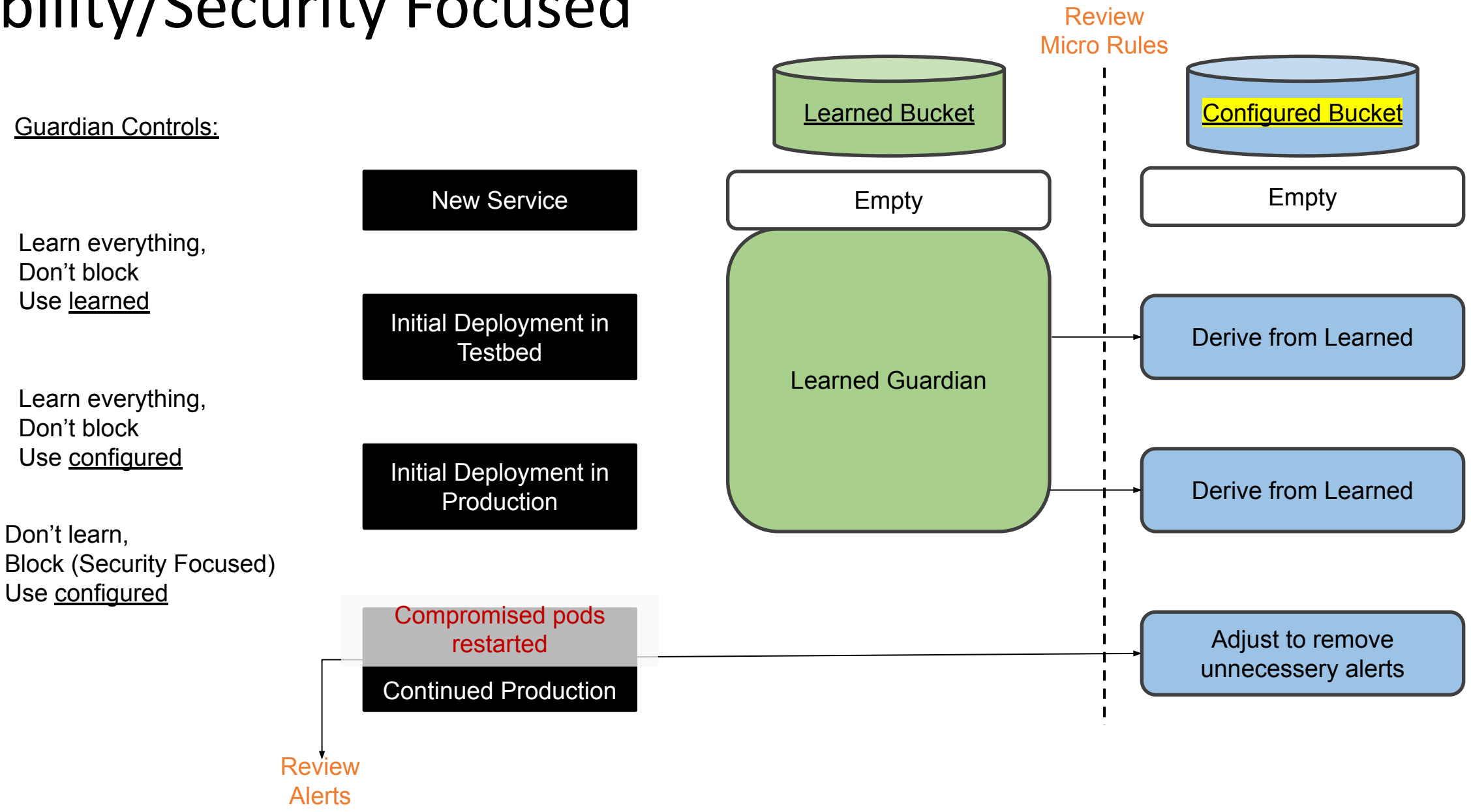
Using Guard:

Operations Focused



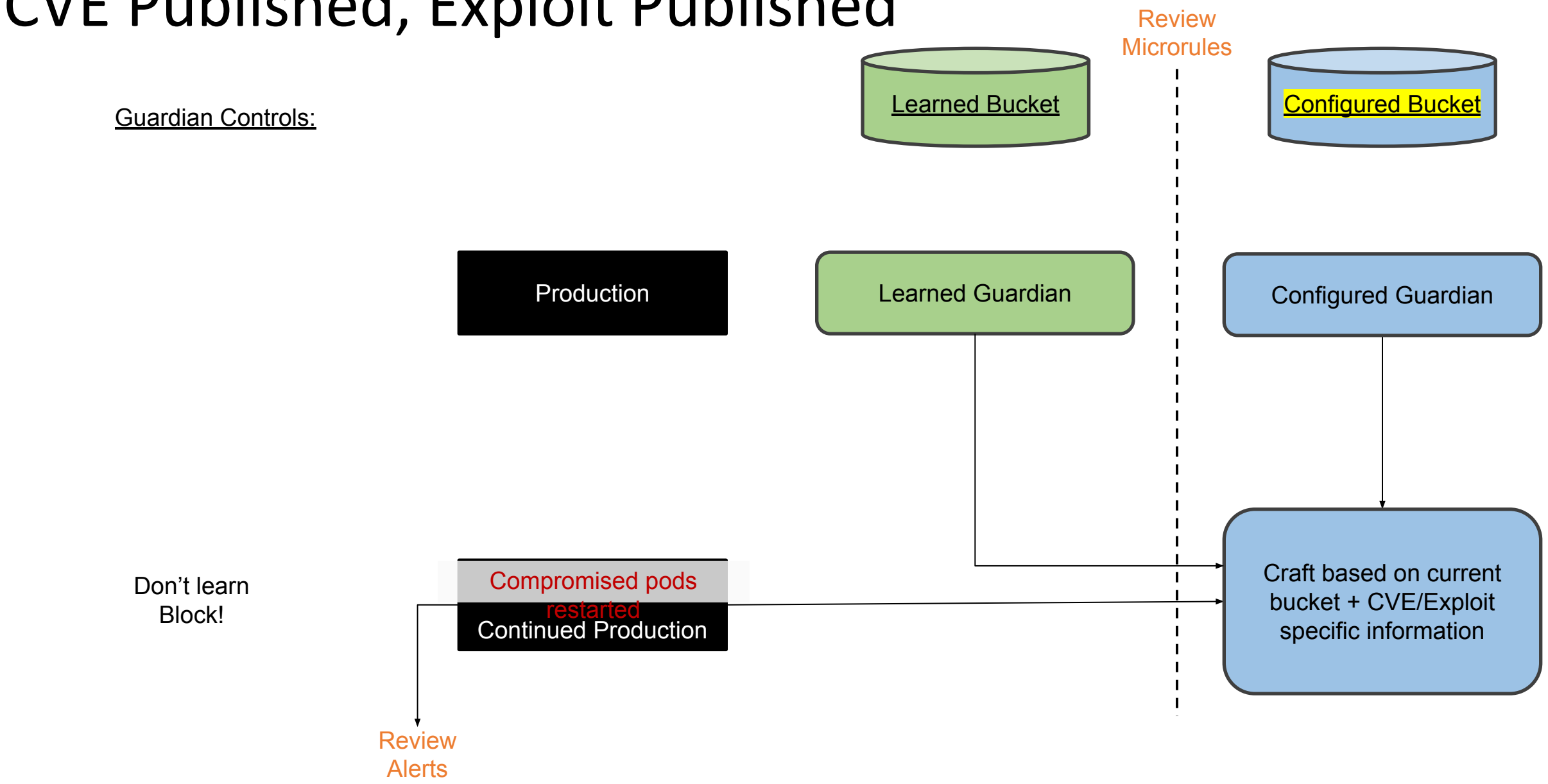
Warning, once you see an alert, if you ignore it, the system conclude it is normal

Using Guard:
Visibility/Security Focused



Using Guard:

CVE Published, Exploit Published



Some believe that proprietary security is safer…

Strength in Open-Source: Security Through Community

Limited to company's own expertise
- Less agile to new threats

Outrun others in the community
- …Remain insecure & hope for the best

Let’s face it together - Collective intelligence of Cloud Native (CN) Community
- Make CN safer than any other technology - join forces & face the challenges
- Agility to adapt, Community-driven updates

Make CN security as strong as the community behind it.

Please scan the QR Code above
to leave feedback on this session