Application Security: The New Attack Vectors

Daniel Shechter, CEO, Miggo Security

Meet the Speaker

- Daniel Shechter - Co-founder and CEO of Miggo Security
- Trying to find a vaccination to the current application attacks plague
- Redefining AppSec for the modern “shared responsibility” state

Part 1:

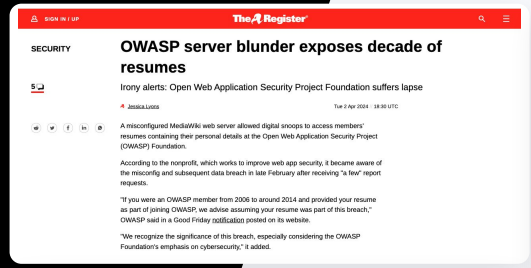
Attackers ❤ Applications

MIGGO | NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

80%

Of cyber attacks are targeting the application layer

Verizon DBIR, 2023



SIGN IN / UP — The Register

SECURITY

OWASP server blunder exposes decade of resumes

Irony alerts: Open Web Application Security Project Foundation suffers lapse

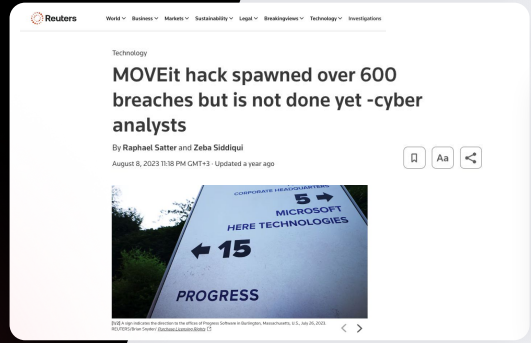
Jessica Lyons — Tue 2 Apr 2024 · 18:30 UTC

A misconfigured MediaWiki web server allowed digital snoops to access members' resumes containing their personal details at the Open Web Application Security Project (OWASP) Foundation.

According to the nonprofit, which works to improve web app security, it became aware of the misconfig and subsequent data breach in late February after receiving "a few" report requests.

"If you were an OWASP member from 2006 to around 2014 and provided your resume as part of joining OWASP, we advise assuming your resume was part of this breach," OWASP said in a Good Friday notification posted on its website.

"We recognize the significance of this breach, especially considering the OWASP Foundation's emphasis on cybersecurity," it added.



Reuters — World · Business · Markets · Sustainability · Legal · Breakingviews · Technology · Investigations

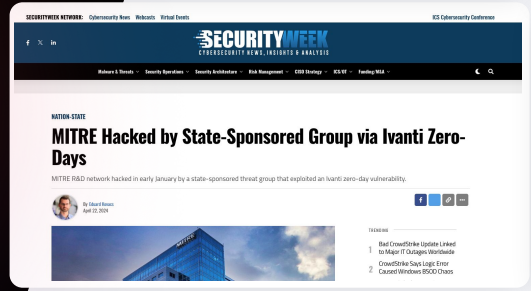
Technology

MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts

By Raphael Satter and Zeba Siddiqui

August 8, 2023 11:18 PM GMT+3 · Updated a year ago

[1/2] A sign indicates the direction to the offices of Progress Software in Burlington, Massachusetts, U.S., July 25, 2023. REUTERS/Brian Snyder / Purchase Licensing Rights



SECURITYWEEK NETWORK: Cybersecurity News · Webcasts · Virtual Events · ICS Cybersecurity Conference

SECURITYWEEK — CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats · Security Operations · Security Architecture · Risk Management · CISO Strategy · ICS/OT · Funding/M&A

NATION-STATE

MITRE Hacked by State-Sponsored Group via Ivanti Zero-Days

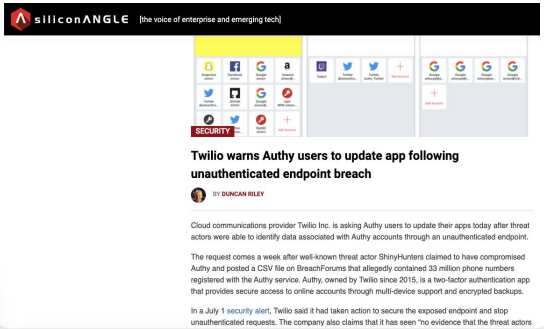
MITRE R&D network hacked in early January by a state-sponsored threat group that exploited an Ivanti zero-day vulnerability.

By Eduard Kovacs, April 22, 2024

TRENDING

1 Bad CrowdStrike Update Linked to Major IT Outages Worldwide

2 CrowdStrike Says Logic Error Caused Windows BSOD Chaos



siliconANGLE [the voice of enterprise and emerging tech]

SECURITY

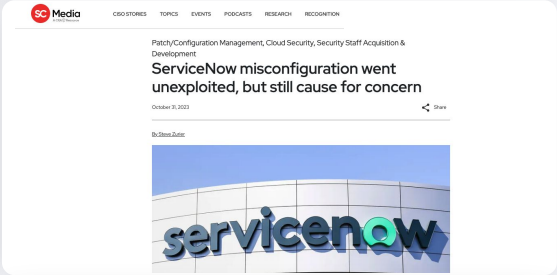
Twilio warns Authy users to update app following unauthenticated endpoint breach

BY DUNCAN RILEY

Cloud communications provider Twilio Inc. is asking Authy users to update their apps today after threat actors were able to identify data associated with Authy accounts through an unauthenticated endpoint.

The request comes a week after well-known threat actor ShinyHunters claimed to have compromised Authy and posted a CSV file on BreachForums that allegedly contained 33 million phone numbers registered with the Authy service. Authy, owned by Twilio since 2015, is a two-factor authentication app that provides secure access to online accounts through multi-device support and encrypted backups.

In a July 1 security alert, Twilio said it had taken action to secure the exposed endpoint and stop unauthenticated requests. The company also claims that it has seen "no evidence that the threat actors



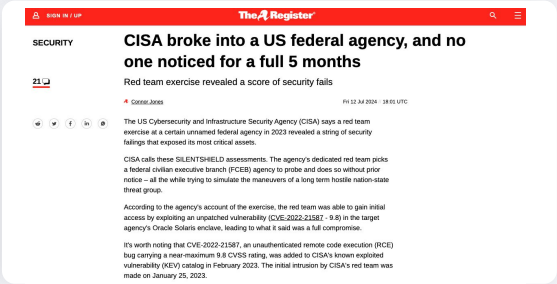
SC Media — CISO STORIES · TOPICS · EVENTS · PODCASTS · RESEARCH · RECOGNITION

Patch/Configuration Management, Cloud Security, Security Staff Acquisition & Development

ServiceNow misconfiguration went unexploited, but still cause for concern

October 31, 2023 · Share

By Steve Zurier



SIGN IN / UP — The Register

SECURITY

CISA broke into a US federal agency, and no one noticed for a full 5 months

Red team exercise revealed a score of security fails

Connor Jones — Fri 12 Jul 2024 · 18:01 UTC

The US Cybersecurity and Infrastructure Security Agency (CISA) says a red team exercise at a certain unnamed federal agency in 2023 revealed a string of security failings that exposed its most critical assets.

CISA calls these SILENTSHIELD assessments. The agency's dedicated red team picks a federal civilian executive branch (FCEB) agency to probe and does so without prior notice – all the while trying to simulate the maneuvers of a long term hostile nation-state threat group.

According to the agency's account of the exercise, the red team was able to gain initial access by exploiting an unpatched vulnerability (CVE-2022-21587 - 9.8) in the target agency's Oracle Solaris enclave, leading to what it said was a full compromise.

It's worth noting that CVE-2022-21587, an unauthenticated remote code execution (RCE) bug carrying a near-maximum 9.8 CVSS rating, was added to CISA's known exploited vulnerability (KEV) catalog in February 2023. The initial intrusion by CISA's red team was made on January 25, 2023.

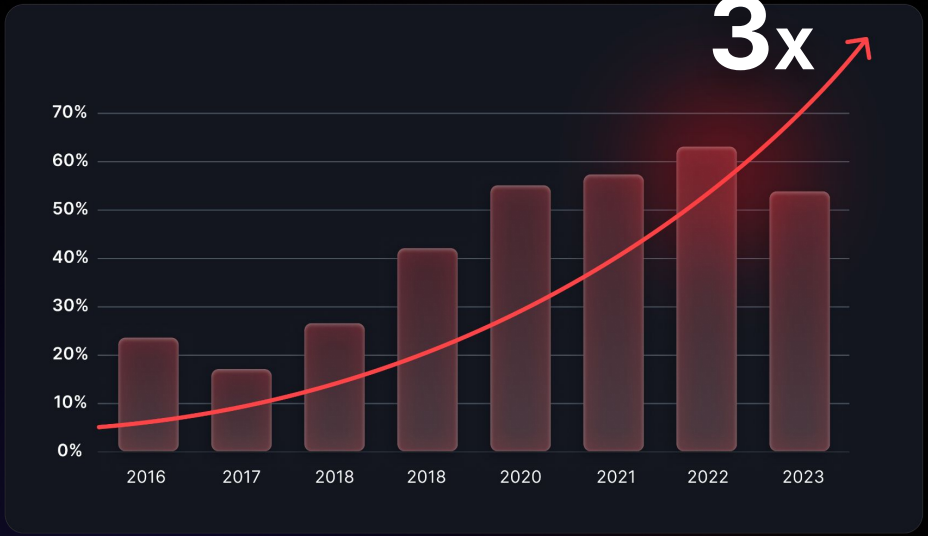

AppSec
SQL Injection
Ivanti,
MoveIT
imgflip.com

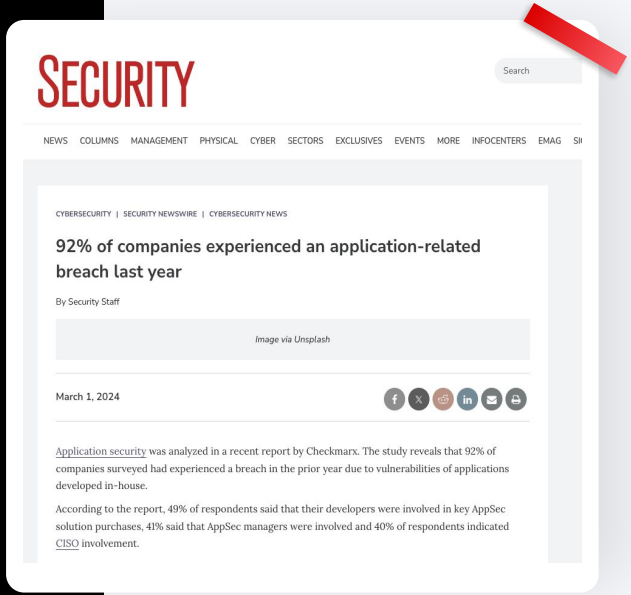
MIGGO | NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

Successful application breaches **tripled** over the last few years

% of breaches initiated by web applications

2016-2023, DBIR





SECURITY

Search

NEWS COLUMNS MANAGEMENT PHYSICAL CYBER SECTORS EXCLUSIVES EVENTS MORE INFOCENTERS EMAG

CYBERSECURITY | SECURITY NEWSWIRE | CYBERSECURITY NEWS

92% of companies experienced an application-related breach last year

By Security Staff

Image via Unsplash

March 1, 2024

Application security was analyzed in a recent report by Checkmarx. The study reveals that 92% of companies surveyed had experienced a breach in the prior year due to vulnerabilities of applications developed in-house.

According to the report, 49% of respondents said that their developers were involved in key AppSec solution purchases, 41% said that AppSec managers were involved and 40% of respondents indicated CISO involvement.

Part 2:

Modern applications don’t make security simpler

Applications Open Doors, and Attackers Exploit the Complexity

1

Distribution

Interdependencies between code, infra, and 3rd parties expand the attack surface

2

Velocity

Rapid changes introduce vulnerabilities faster than patches can be applied

3

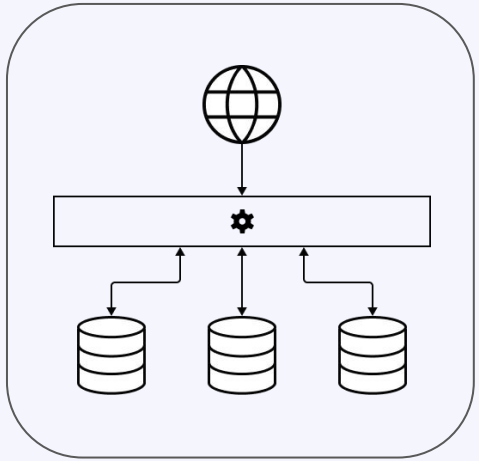
Dependency

"Shared responsibility" model blurs ownership, leading to detection and remediation gaps

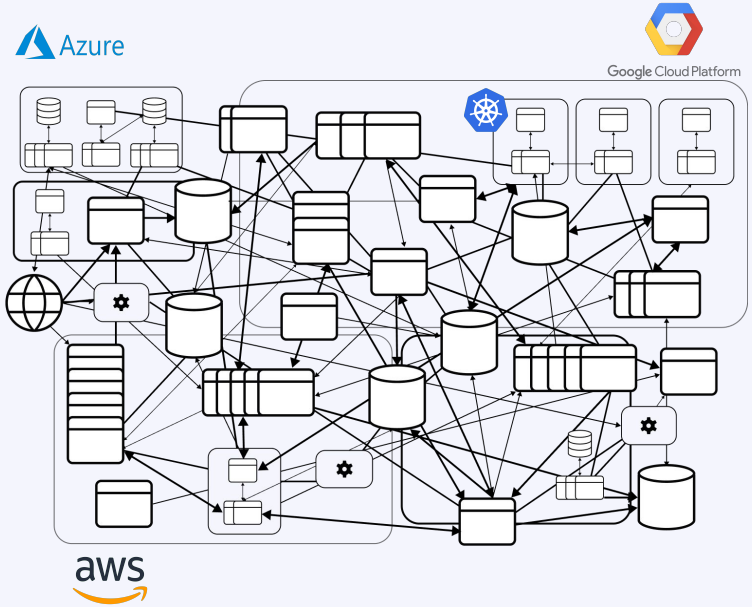
Most organizations are unaware of their true vulnerabilities, and blind to an actual application attack

1 Increased and distributed attack surface

Apps before the cloud ...

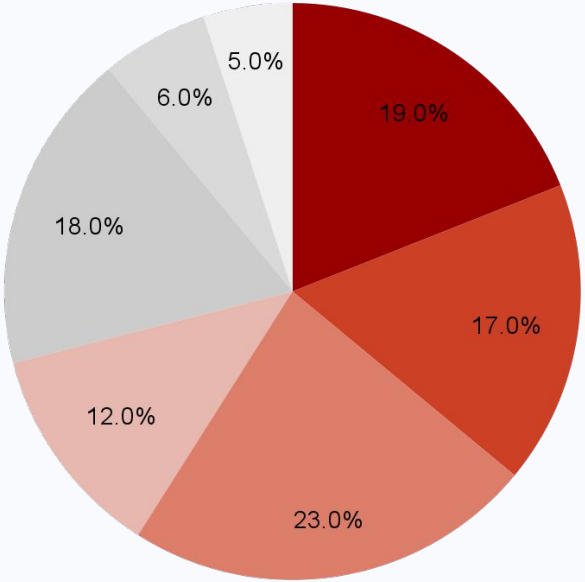


...Apps in the Cloud



2 Rapidly changing environment

Code deployment cycles[1]



71%

Deploy new code once a week or daily

1. Crowdstrike State of Application Security Report 2024

3 Third-parties took over the party - “Shared Responsibility”

3rd-party Applications

argo

GitLab

Jenkins

Metabase

rocket.chat

Backstage

3rd-party APIs

The bottom line:

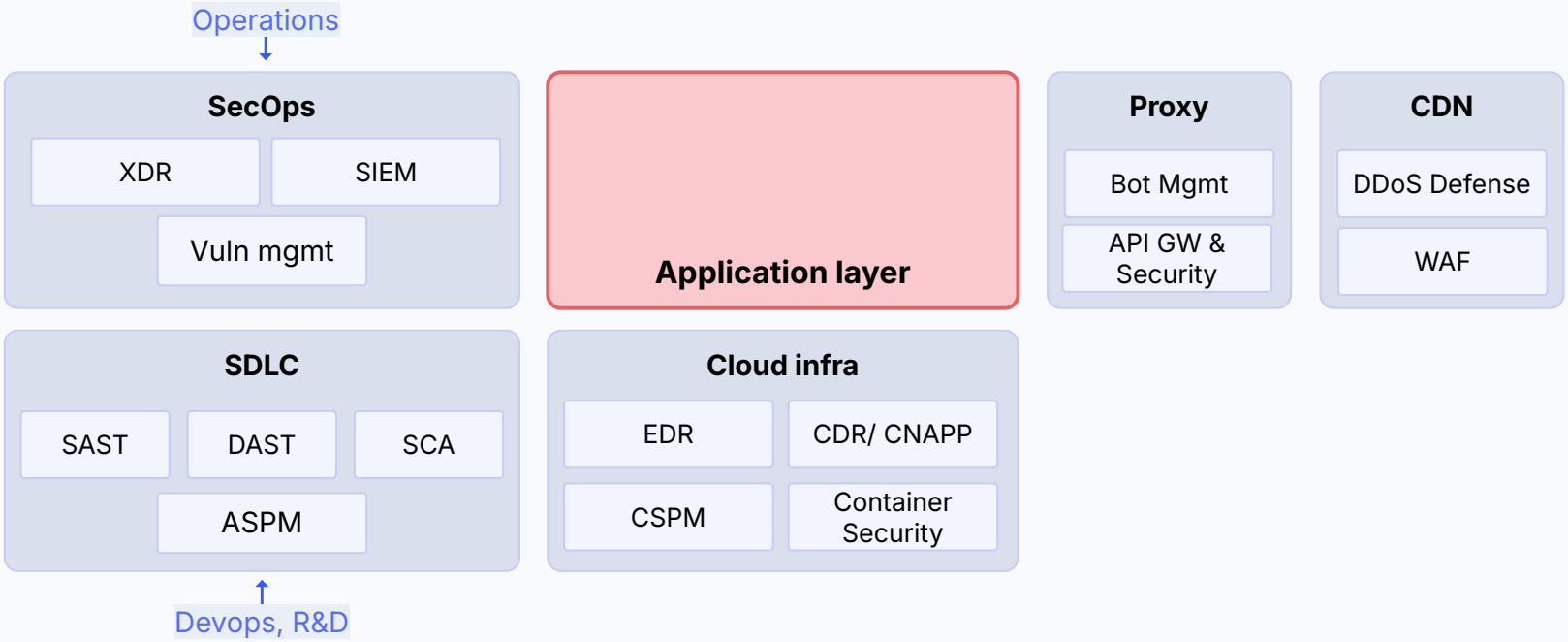
Modern application environments are exponentially more complicated to stay in control of,
due to the ever increasing amount of interdependent connections

Do you have good grasp of how your application ecosystem works?

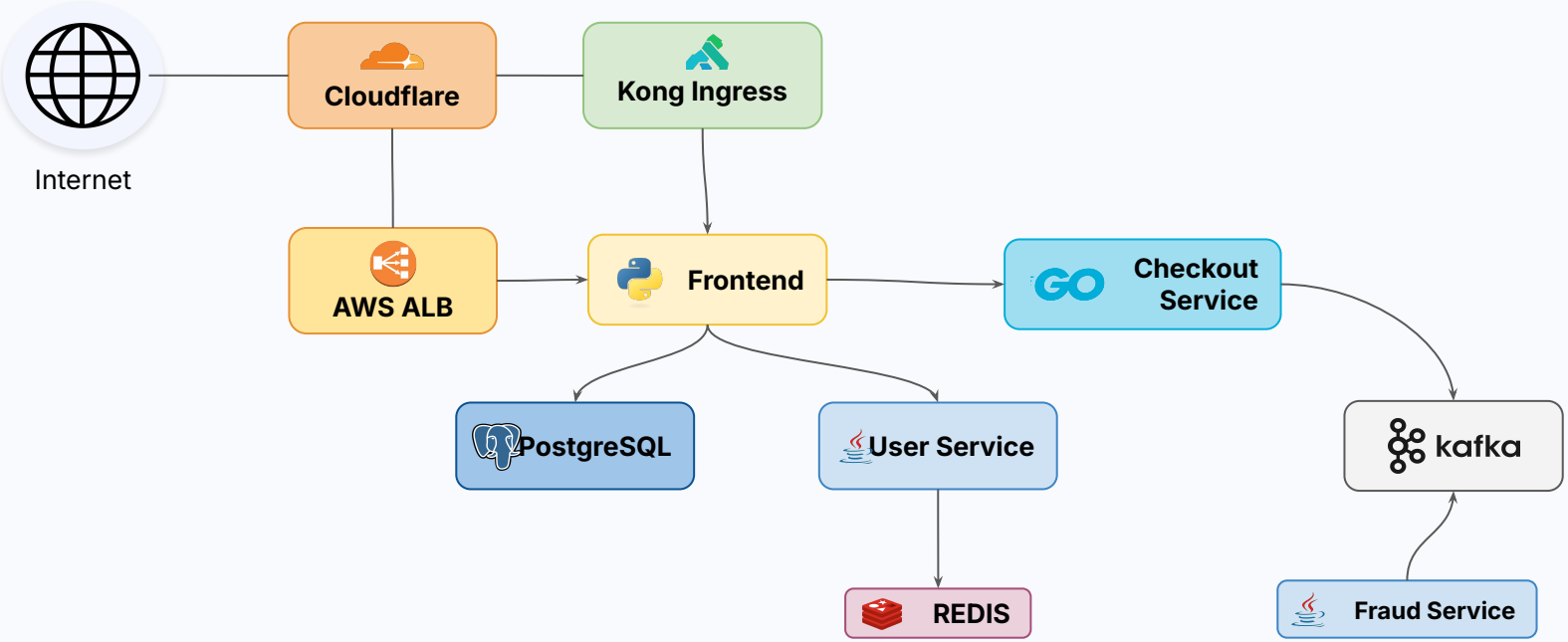
Part 3:

Attackers exploit slow patching cycles and lack of application runtime context to bypass detections

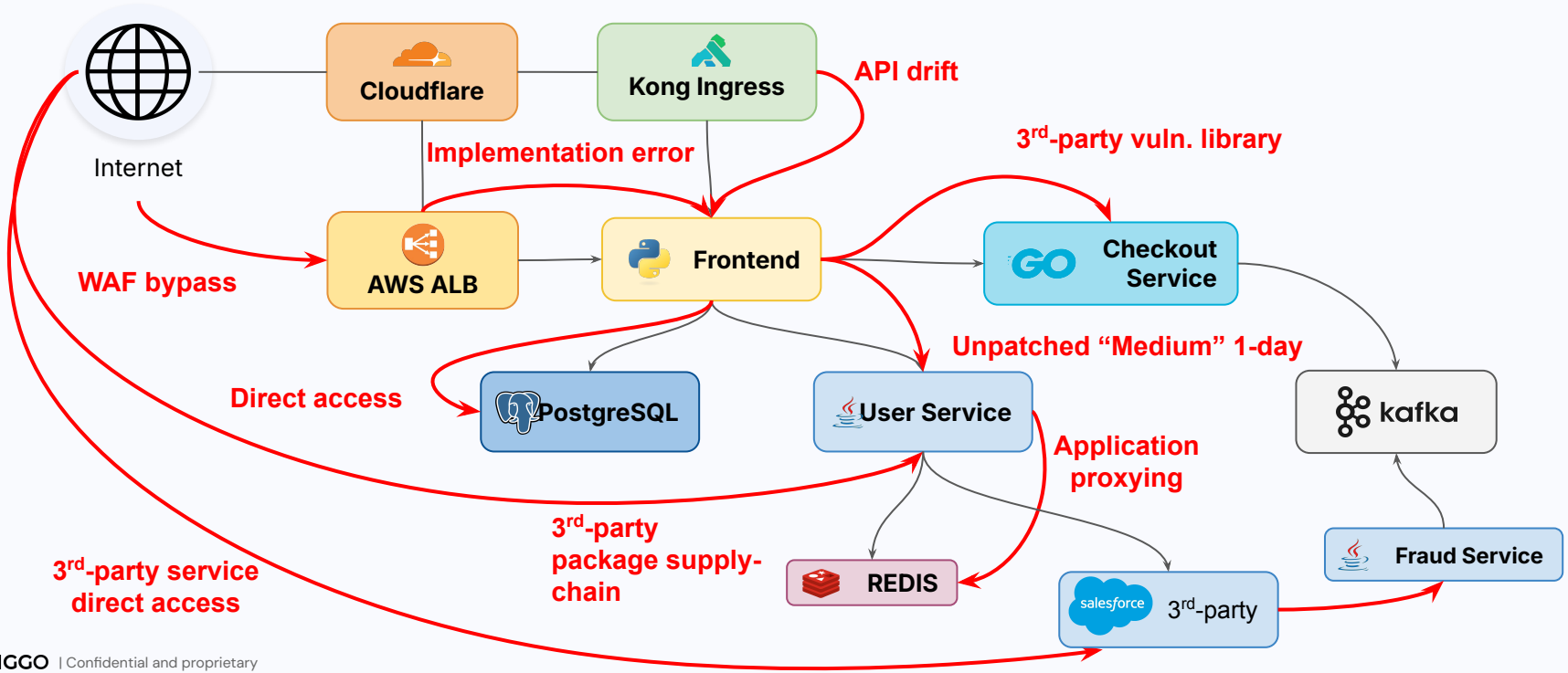
Multiple solutions around the application layer have no visibility into the in-application interactions and context in runtime



Attacker view: Exploiting drifts, interdependency, trust chains and low patching velocity



Attacker view: Exploiting drifts, interdependency, trust chains and low patching velocity



Unlocked: New attack primitives in every stage

Initial access

- Distributed Architecture: Request smuggling
- Application drifts: unintentional internet exposure
- 3rd party dependencies: unmonitored packages and subprocessors
- WAF Gaps: Coverage and config issues

Exploitation

- Unpatched 1-days
- Misconfigured APIs: Weak/Missing Auth
- Supply Chain Risks: Zero-days in third-party components
- “Shared Responsibility”: Misunderstandings create security gaps

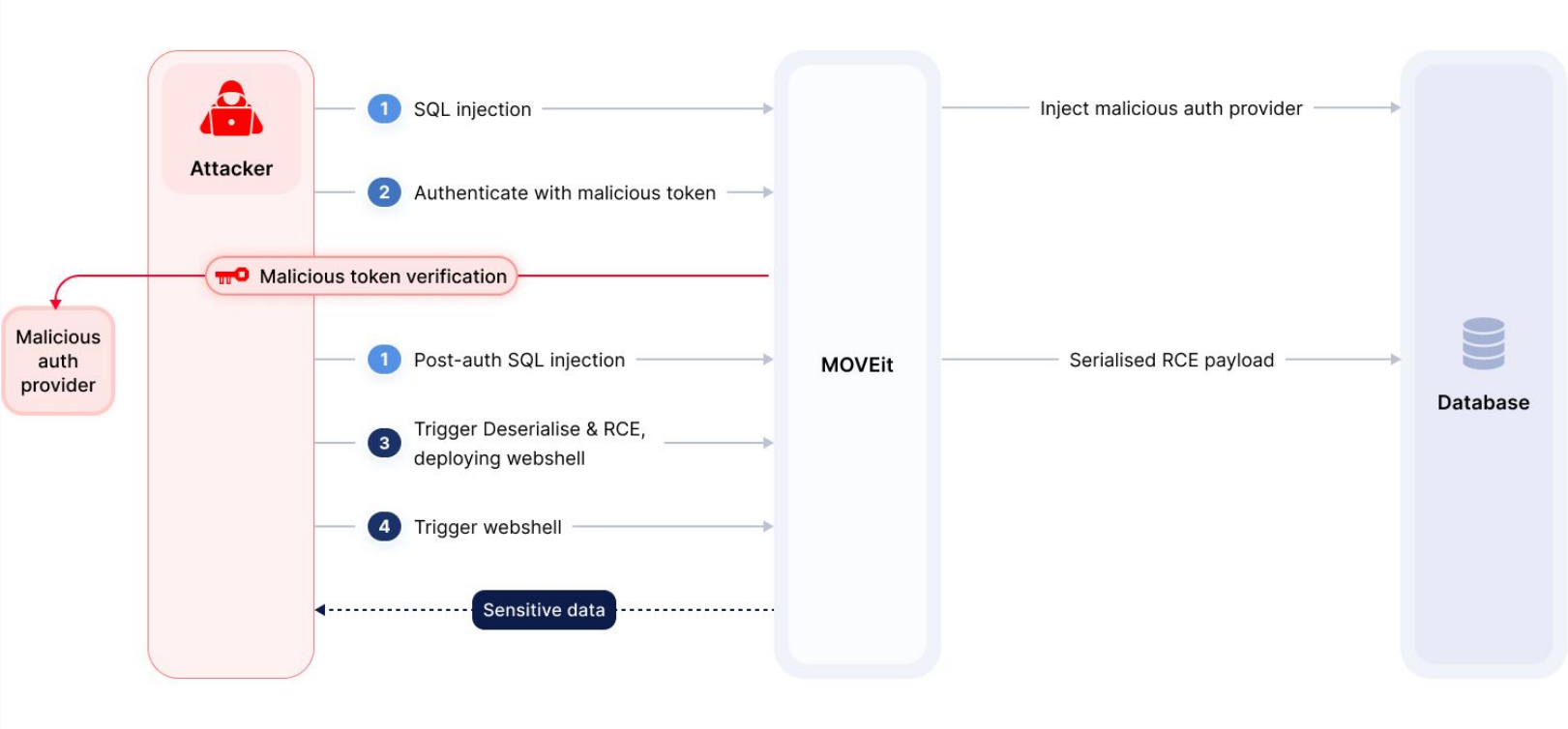
Lateral Movement

- Application Proxying: "Living-off-the-land" within apps
- Web Shells: invisible hold in the environment

Impact

- Data Exfiltration: Theft of sensitive information
- Ransomware attacks

Real world Example: The MOVEit Breach



1

Bypassing WAF through smuggling SQLi parts: unfold only within the App

NewProcessCreation

Service: **moveit-trial** | Duration: **2.39ms** | Start Time: **125.76ms**

Tags

	N0KCk7CiAgICB9CiAgICByZXR1cm47Cn0KPC9zY3JpcHQ+ > C:\Windows\Temp\bfile && certutil -decode C:\Windows\Temp\bfile C:\MOVEitTransfer\wwwroot\human2.aspx
io.miggo.instrumentation.processexec.filename	cmd
io.miggo.instrumentation.processexec.stacktrace	at OpenTelemetry.AutoInstrumentation.Instrumentations.ProcessExec.ProcessExecInstrumentation.OnMethodBegin[TTarget](TTarget instance, ProcessStartInfo info) at ProcessExecInstrumentation.OnMethodBegin(Process , ProcessStartInfo&) at OpenTelemetry.AutoInstrumentation.CallTarget.Handlers.BeginMethodHandler`3.Invoke(TTarget instance, TArg1& arg1) at System.Diagnostics.Process.StartWithShellExecuteEx(ProcessStartInfo startInfo) at System.Diagnostics.Process.Start(ProcessStartInfo startInfo) at System.Comparison`1.Invoke(T x, T y) at System.Collections.Generic.ComparisonComparer`1.Compare(T x, T y) at System.Collections.Generic.SortedSet`1.AddIfNotPresent(T item) at System.Collections.Generic.SortedSet`1.OnDeserialization(Object sender) at System.Runtime.Serialization.ObjectManager.RaiseDeserializationEvent() at System.Runtime.Serialization.Formatters.Binary.ObjectReader.Deserialize(HeaderHandler handler, __BinaryParser serParser, Boolean fCheck, Boolean isCrossAppDomain, IMethodCallMessage methodCallMessage) at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean fCheck, Boolean isCrossAppDomain, IMethodCallMessage methodCallMessage) at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean fCheck, IMethodCallMessage methodCallMessage)

3

Taking advantage of serialization vulnerability for RCE

NewProcessCreation

Service: **moveit-trial** | Duration: **2.39ms** | Start Time: **125.76ms**

Tags

	N0KCk7CiAgICB9CiAgICByZXR1cm47Cn0KPC9zY3JpcHQ+ > C:\Windows\Temp\bfile && certutil -decode C:\Windows\Temp\bfile C:\MOVEitTransfer\wwwroot\human2.aspx
io.miggo.instrumentation.processexec.filename	cmd
io.miggo.instrumentation.processexec.stacktrace	at OpenTelemetry.AutoInstrumentation.Instrumentations.ProcessExec.ProcessExecInstrumentation.OnMethodBegin[TTarget](TTarget instance, ProcessStartInfo info) at ProcessExecInstrumentation.OnMethodBegin(Process , ProcessStartInfo&) at OpenTelemetry.AutoInstrumentation.CallTarget.Handlers.BeginMethodHandler`3.Invoke(TTarget instance, TArg1& arg1) at System.Diagnostics.Process.StartWithShellExecuteEx(ProcessStartInfo startInfo) at System.Diagnostics.Process.Start(ProcessStartInfo startInfo) at System.Comparison`1.Invoke(T x, T y) at System.Collections.Generic.ComparisonComparer`1.Compare(T x, T y) at System.Collections.Generic.SortedSet`1.AddIfNotPresent(T item) at System.Collections.Generic.SortedSet`1.OnDeserialization(Object sender) at System.Runtime.Serialization.ObjectManager.RaiseDeserializationEvent() at System.Runtime.Serialization.Formatters.Binary.ObjectReader.Deserialize(HeaderHandler handler, __BinaryParser serParser, Boolean fCheck, Boolean isCrossAppDomain, IMethodCallMessage methodCallMessage) at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean fCheck, Boolean isCrossAppDomain, IMethodCallMessage methodCallMessage) at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean fCheck, IMethodCallMessage methodCallMessage)

How could an external tool identify an anomaly?

3

Utilizing App WebShell to proxy “legitimate” requests

/human2.aspx

Tags: http.client_ip = ::1 | http.client_port = 52803 | http.host = localhost | http.metho

Process: host.name = EC2AMAZ-1ISV33E | io.miggo.project.id = 828BECFC-A565-4

1.89ms

1.74ms

MiggoSession

Tags

io.miggo.instrumentation.session.is_new_session	true
io.miggo.instrumentation.session.session_id	anhrckutnlfiwsgqp5tgs5fp
span.kind	internal

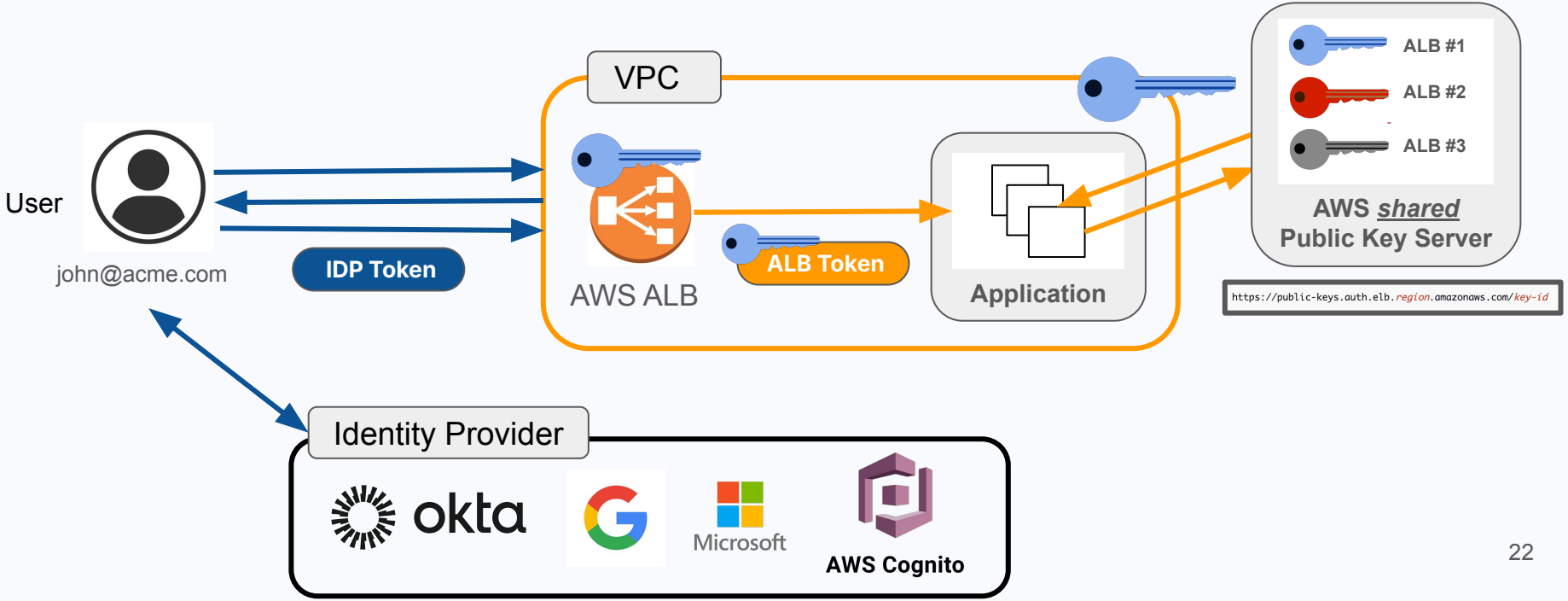
mysql.Execute

Service: **moveit-trial** | Duration: **4.22ms**

Tags

db.connection_string	server=localhost;database=moveittransfer;user id=moveittransfer;minpoolsize=5;maxpoolsize=500;connectiontimeout=8;characterset=utf8
db.name	moveittransfer
db.statement	select f.id, f.instid, f.folderid, filesize, f.Name as Name, u.LoginName as uploader, fr.FolderPath , fr.name as fname from folders fr, files f left join users u on f.UploadUsername = u.Username where f.FolderID = fr.ID
db.system	mysql
db.user	moveittransfer

Real world example:
Shared responsibility authentication bypass in AWS

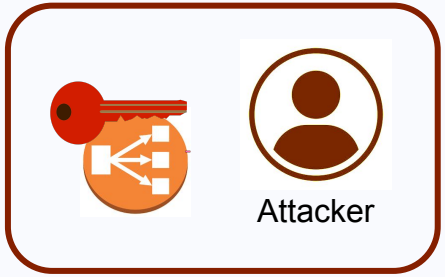


Shared responsibility = who's accountable?

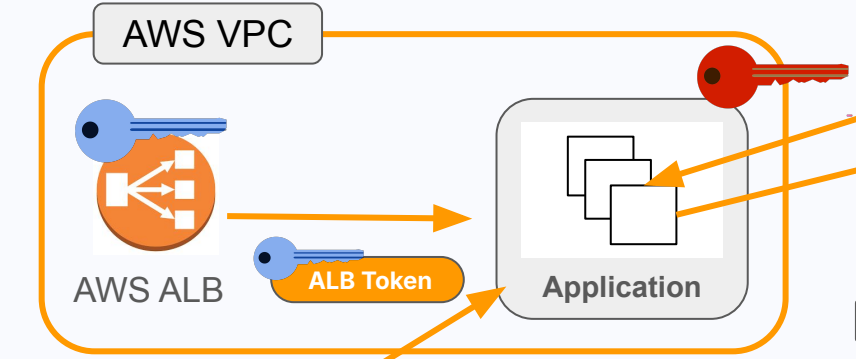
Signer Misconfig - exploiting shared keys

No ALB "Signer" Validation

- Per-Application code change
- +95% are vulnerable

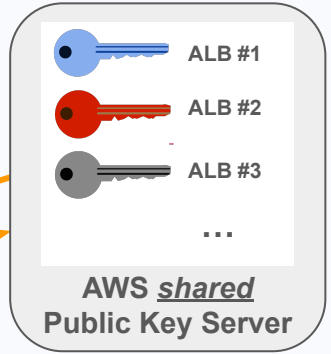



```
email:  john@acme.com
scope:  openid email
kid:    <kid>
issuer: Attacker IDP
signer:
```




```
email:  .....
scope:  .....
kid:    ......
issuer: <IDP>
signer:
```

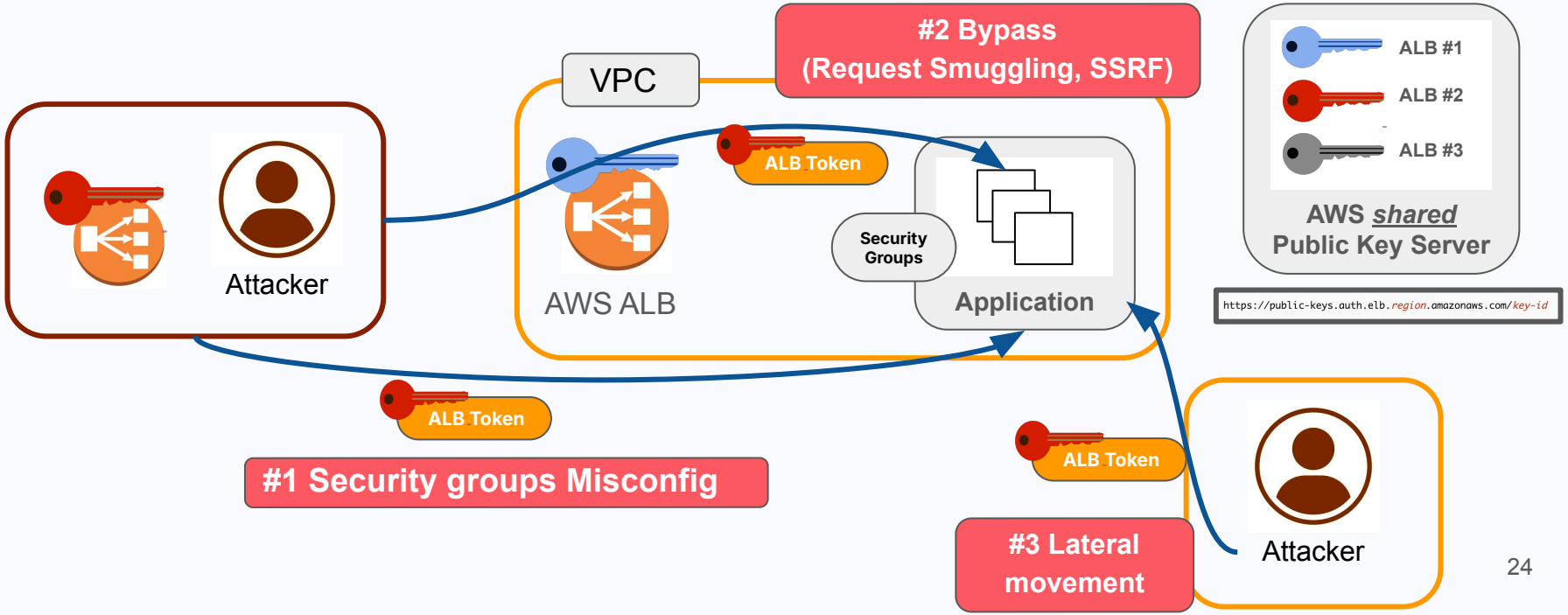
ALB Token



https://public-keys.auth.elb.region.amazonaws.com/key-id

Bypassing authentication through implementation vulnerability and misconfiguration

- How can an attacker exploit this?



Enhancing Application Security in a Distributed Environment

1. **Enhance real-time visibility** across your application environment to increase control and reduce blind spots.
2. **Identify and monitor interdependency weak points** in critical functions to prevent unintended drifts in structure and behavior
3. **Focus on runtime application security,** addressing actual risks over static vulnerabilities to minimize exploitable gaps.
4. **Automate threat detection and response to mitigate exploitation** caused by slow patching cycles and unknown threats.

Let's stop application breaches

NY metro joint cyber security conference
September 2024

www.miggo.io