
cybr.com
Adversary Emulation
for the Cloud

FAQ

- Yes, this will be recorded and sent out!
- You can ask questions throughout the presentation and we'll answer as we can

Today's Agenda

- Quick intro
- Adversary simulation and purple teaming with Stratus Red Team
- Detection engineering with Grimoire
- Conclusion

Adversary Emulation for the Cloud



Christophe Limpalair

- 📽️ Founder and Trainer at Cybr
- 👨‍💻 8+ years of AWS experience
- 🥾 Originally from France, but currently live in Colorado and love hiking & skiing
- 🍻 I'm also a professional hobbyist *(current: home brewing, prior: growing mushrooms)*

Cybr.com/discord

Christophe Limpalair
linkedin.com/in/christophelimpalair

@ChristopheLimp
x.com/christophelimp

CYBR

Adversary Emulation for the Cloud



Christophe Tafani-Dereeper

- Cloud security & open source at DATADOG
- 🇨🇭🇫🇷
- Previously:

```
cloud security engineer
IT security engineer
SOC analyst/developer
freelance pentesting
Java backend development
```


Christophe Tafani-Dereeper
linkedin.com/in/christophelimpalair

@christophetd.fr
bsky.app/profile/christophetd.fr

CYBR

Adversary Emulation for the Cloud



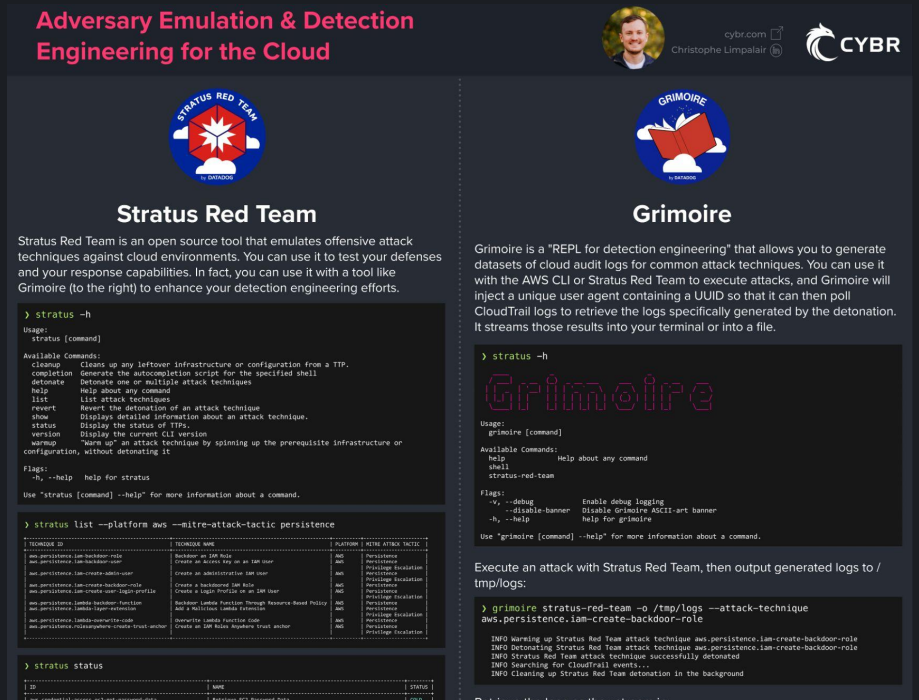


CYBR

Adversary Emulation for the Cloud

Reference Guide Cheat Sheet

Download: cybr.com/stratus-and-grimoire



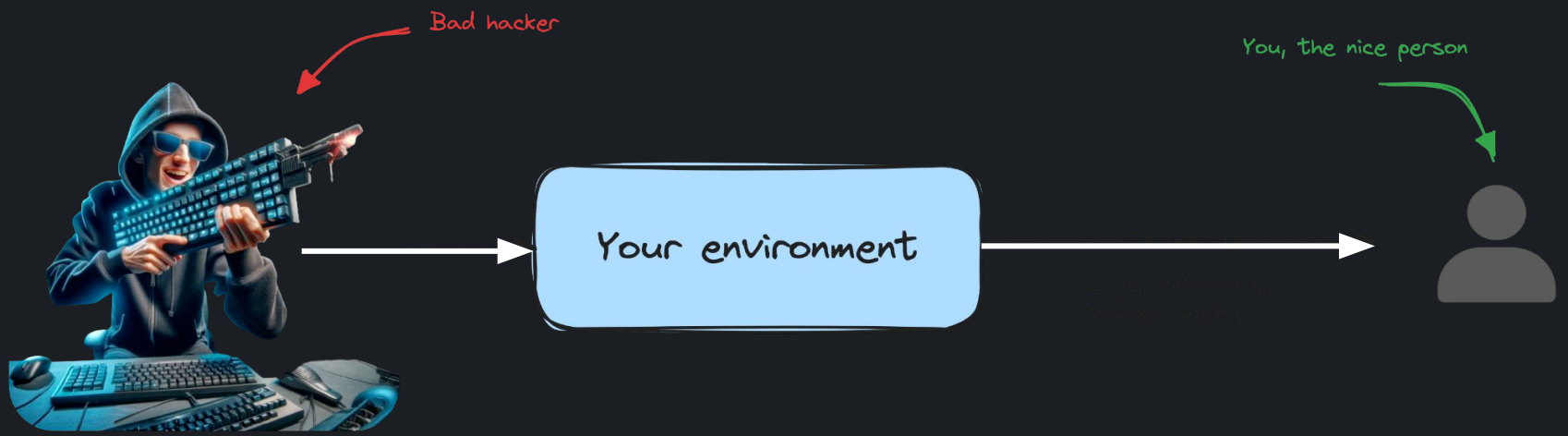
CYBR

Where we're going

- How to **detect** bad stuff? ("**Detection engineering**")
- How to **simulate** bad stuff? ("**Adversary emulation**")
- How to **empower defenders** to understand/reproduce bad stuff? ("**Purple teaming**")

CYBR

Setting the stage



Indicators of compromise

THREAT fox by ABUSE.ch

Browse IOCs | IOC Requests | Share IOCs | Request IOCs | Data | FAQ | About | Login

Browse Database

See search syntax see below, example: malware:ZLoader

Search

Search Syntax

Show entries

Search:

Date (UTC)	IOC	Malware	Tags	Reporter
2022-04-21 08:28	6965b12e280066a178c4d1a3262...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 08:23	http://198.187.30.47/p.php?id=1681...	Loki Password Stealer (PWS)	LokiBot	@abuse_ch
2022-04-21 08:20	http://genccagdas.com.tr/assets/do...	Emotet		@Cryptolaemus1
2022-04-21 08:20	https://fpd.cl/cgi-bin/N/	Emotet		@Cryptolaemus1
2022-04-21 08:20	http://djunreal.co.uk/site/ApOKpFad/	Emotet		@Cryptolaemus1
2022-04-21 08:19	fb8e2718a7369ce721eb63bfdd5a...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 08:12	d905e89224670a81d725dcd34f7e...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 08:05	20eb4527fabe44af4af095488a2b...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:58	50cc4992280830d59d81fd7c6f69...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:48	6732d35cbdd70baeed360a541141...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:41	a9d707010f8e1f4477451f7859545...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:34	4fd8d44dfa1f7371dc3c1e9850afed...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:27	7962a03b5353ff67acca99a7fb80...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:20	b4db67e12da58522b59f13aaa5a7f...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:13	41fa7d6a43c63a1bcdfc0bca0d19a...	Emotet	epoch4 exe	@Cryptolaemus1
2022-04-21 07:06	690bc5ccbf791426de612ee14ad8...	Emotet	epoch4 exe	@Cryptolaemus1

```
118  0022c1fe1d6b036de2a08d50ac5446a5;Kaspersky Carbanak APT Malware Hash http://goo.gl/
119  0155738045b331f44d300f4a7d08cf21;Kaspersky Carbanak APT Malware Hash http://goo.gl/
120  0275585c3b871405dd299d458724db3d;Kaspersky Carbanak APT Malware Hash http://goo.gl/
121  0ad4892ead67e65ec3dd4c978fce7d92;Kaspersky Carbanak APT Malware Hash http://goo.gl/
122  0ad6da9e62a2c985156a9c53f8494171;Kaspersky Carbanak APT Malware Hash http://goo.gl/
123  1046652e0aaa682f89068731fa5e8e50;Kaspersky Carbanak APT Malware Hash http://goo.gl/
124  10e0699f20e31e89c3becfd8bf24cb4c;Kaspersky Carbanak APT Malware Hash http://goo.gl/
125  1300432e537e7ba07840adecf38e543b;Kaspersky Carbanak APT Malware Hash http://goo.gl/
126  15a4eb525072642bb43f3c188a7c3504;Kaspersky Carbanak APT Malware Hash http://goo.gl/
127  16cda323189d8eba4248c0a2f5ad0d8f;Kaspersky Carbanak APT Malware Hash http://goo.gl/
128  1713e551b8118e45d6ea3f05ec1be529;Kaspersky Carbanak APT Malware Hash http://goo.gl/
129  1a4635564172393ae9f43eab85652ba5;Kaspersky Carbanak APT Malware Hash http://goo.gl/
130  1b9b9c8db7735f1793f981d0be556d88;Kaspersky Carbanak APT Malware Hash http://goo.gl/
131  1d1ed892f62559c3f8234c287cb3437c;Kaspersky Carbanak APT Malware Hash http://goo.gl/
132  1e127b92f7102fbd7fa5375e4e5c67d1;Kaspersky Carbanak APT Malware Hash http://goo.gl/
133  1e47e12d11580e935878b0ed78d2294f;Kaspersky Carbanak APT Malware Hash http://goo.gl/
134  1f43a8803498482d360befc6dfab4218;Kaspersky Carbanak APT Malware Hash http://goo.gl/
135  1fd4a01932df638a8c761abacffa0207;Kaspersky Carbanak APT Malware Hash http://goo.gl/
136  20f8e962b2b63170b228ccaff51aeb7d;Kaspersky Carbanak APT Malware Hash http://goo.gl/
137  26d6bb7a4e84bec672fc461487344829;Kaspersky Carbanak APT Malware Hash http://goo.gl/
138  2908afb4de41c64a45e1eb2503169108;Kaspersky Carbanak APT Malware Hash http://goo.gl/
139  2c6112e1e60f083467dc159ffb1ceb6d;Kaspersky Carbanak APT Malware Hash http://goo.gl/
140  2cba1a82a78f4dcbad1087c1b71588c9;Kaspersky Carbanak APT Malware Hash http://goo.gl/
141  2e2aa05a217aacf3105b4ba2288ad475;Kaspersky Carbanak APT Malware Hash http://goo.gl/
142  36cdf98bc79b6997dd4e3a6bed035dca;Kaspersky Carbanak APT Malware Hash http://goo.gl/
143  36dfd1f3bc58401f7d8b56af682f2c38;Kaspersky Carbanak APT Malware Hash http://goo.gl/
144  39012fb6f3a93897f6c5edb1a57f76a0;Kaspersky Carbanak APT Malware Hash http://goo.gl/
145  3dc8c4af51c8c367fbe7c7feef4f6744;Kaspersky Carbanak APT Malware Hash http://goo.gl/
146  407795b49789c2f9ca6eca1fbab3c73e;Kaspersky Carbanak APT Malware Hash http://goo.gl/
147  45691956a1ba4a8ecc912aeb9f1f0612;Kaspersky Carbanak APT Malware Hash http://goo.gl/
```

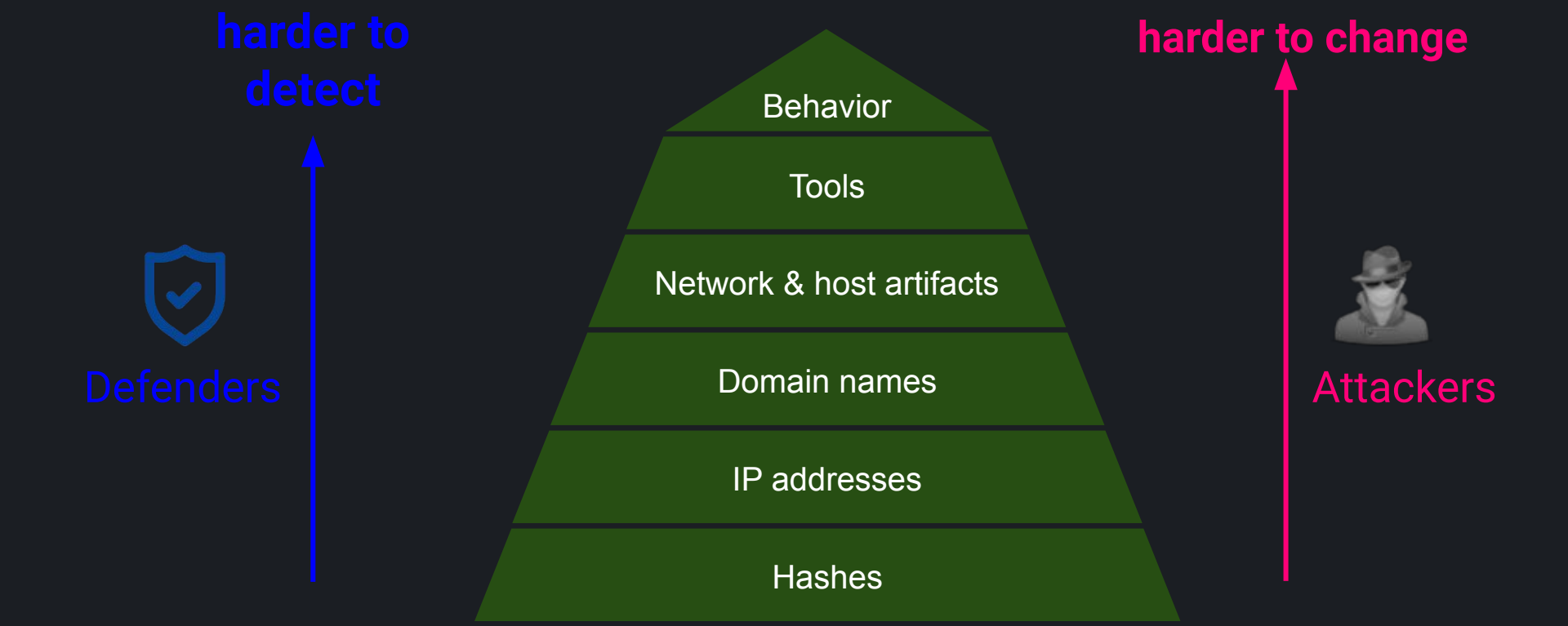
CYBR

(Cloud) indicators of compromise

- Docker image names
- AWS account ID
- AMI ID
- User agent, IP address

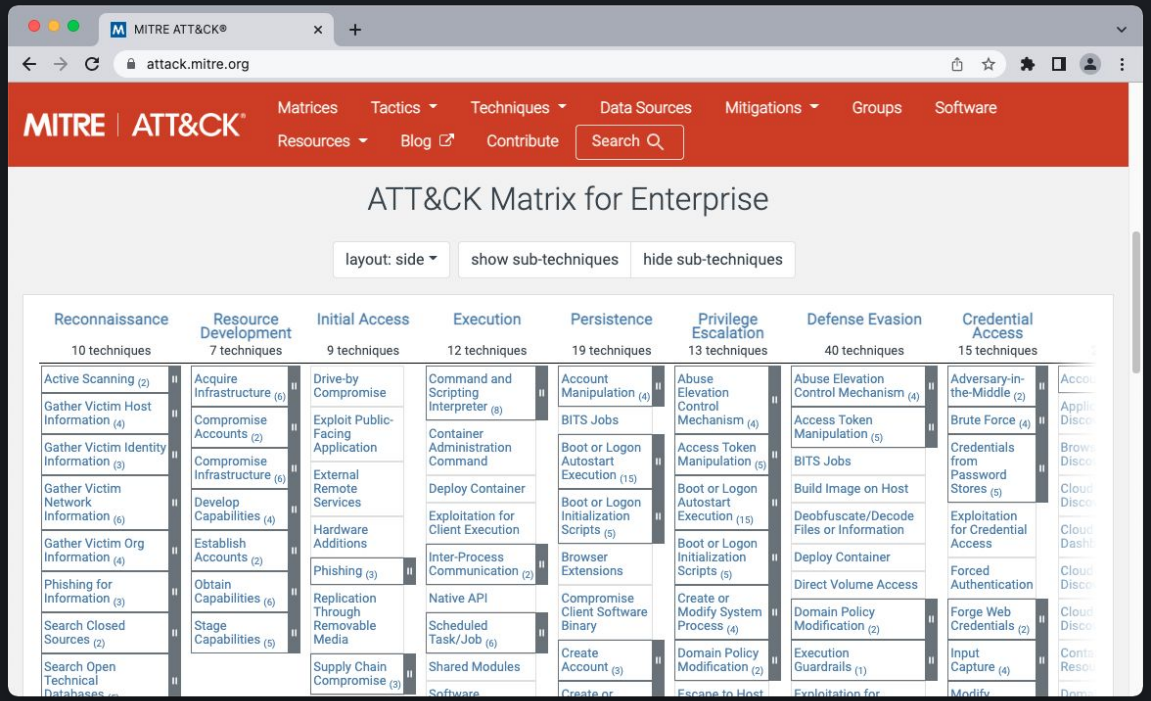
CYBR

The Pyramid of Pain



As: an attacker,
I want to: ???
So that I can: ???

Modeling attacker behavior



Modeling attacker behavior

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear contaienr logs	List K8s secrets	Access the K8s API server	Access cloud resources
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	cluster-admin binding	Delete K8s events	Mount service principal	Access Kubelet API	Container service account
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from proxy server	Application credentials in configuration files	Instance Metadata API	Application credentials in configuration files

https://microsoft.github.io/Threat-Matrix-for-Kubernetes/

CYBR

Modeling attacker behavior



Reconnaissance	Initial Access	Execution	Privilege Escalation	Persistence	Credential Access	Impact
Port Mapping	Valid Credentials	Virtual Machine Scripting	Privileged Identity Management Role	Account Manipulation	Steal Managed Identity JsonWebToken	SAS URI Generation
IP Discovery	Password Spraying	Unmanaged Scripting	Elevated Access Toggle	Account Creation	Steal Service Principal Certificate	File Share Mounting
Public Accessible Resource	Malicious Application Consent	Managed Device Scripting	Local Resource Hijack	HTTP Trigger	Service Principal Secret Reveal	Replication
Gather User Information			Principal Impersonation	Watcher Tasks	Azure KeyVault Dumping	Soft-Delete Recovery
Gather Application Information			Azure AD Application	Scheduled Jobs	Resource Secret Reveal	Azure Backup Delete
Gather Role Information				Network Security Group Modification		
Gather Resource Data				External Entity Access		
Gather Victim Data				Azure Policy		

https://microsoft.github.io/Azure-Threat-Research-Matrix/

CYBR

Modeling attacker behavior



Accessing the AWS Console using programmatic credentials	aws
Creating a new backdoor IAM role	aws
Using Amazon SES to send spam	aws

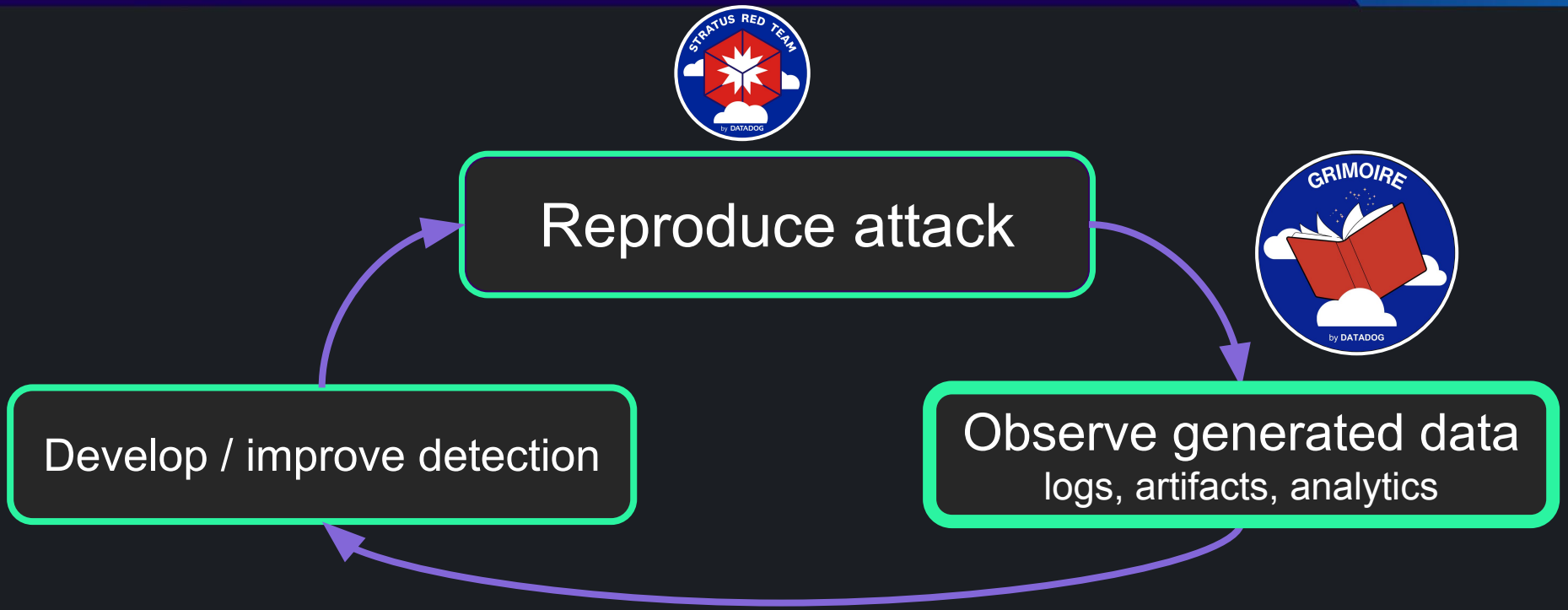
Creating a new IAM user	aws
Stealing EC2 instance credentials through the Instance Metadata Service	aws
Adversary-in-the-middle phishing	A

https://securitylabs.datadoghq.com/cloud-security-atlas/

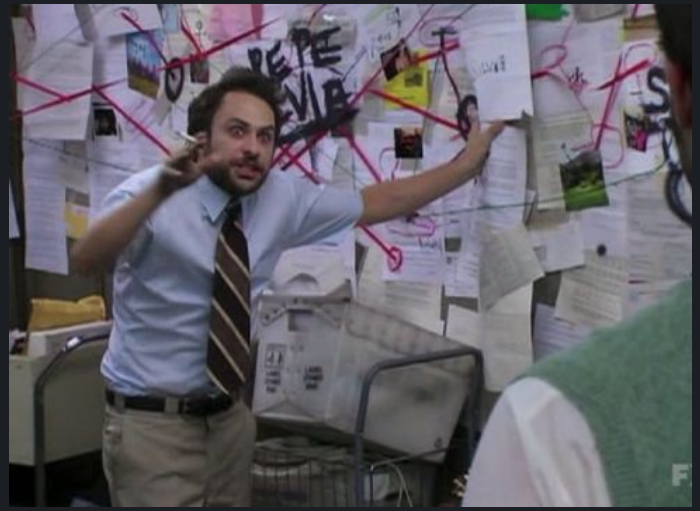
CYBR

Purple teaming




STRATUS RED TEAM
by DATADOG
Reproduce attack
GRIMOIRE
by DATADOG
Develop / improve detection
Observe generated data
logs, artifacts, analytics

The problem with cloud purple teaming

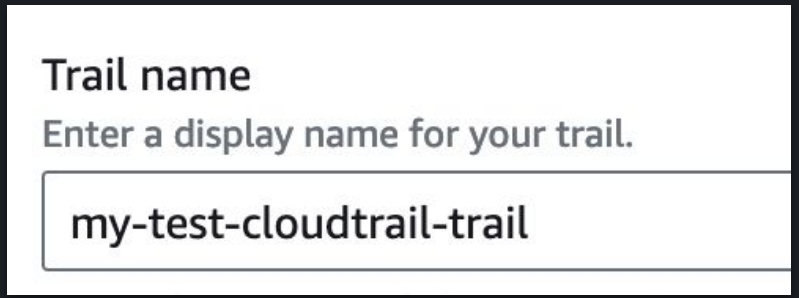


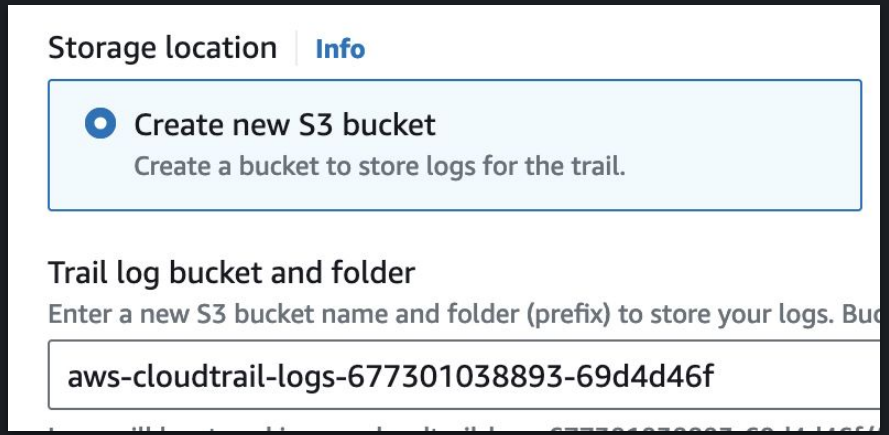
Challenging to handle pre-requisite infrastructure

CYBR

T1562.008: Impair Defenses: Disable or Modify Cloud Logs

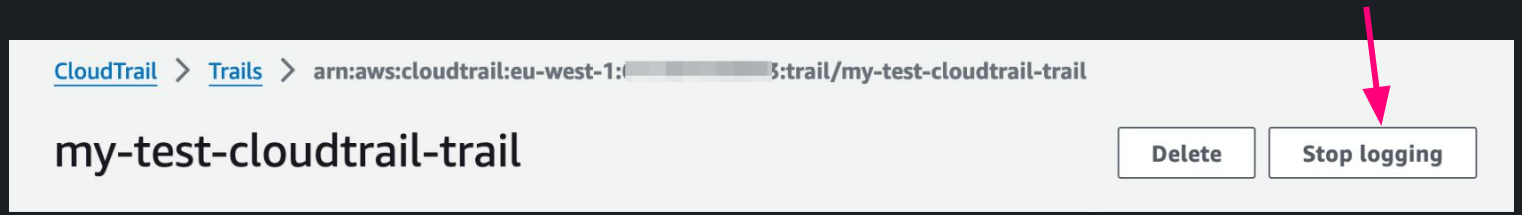
a.k.a "Disable CloudTrail logging"





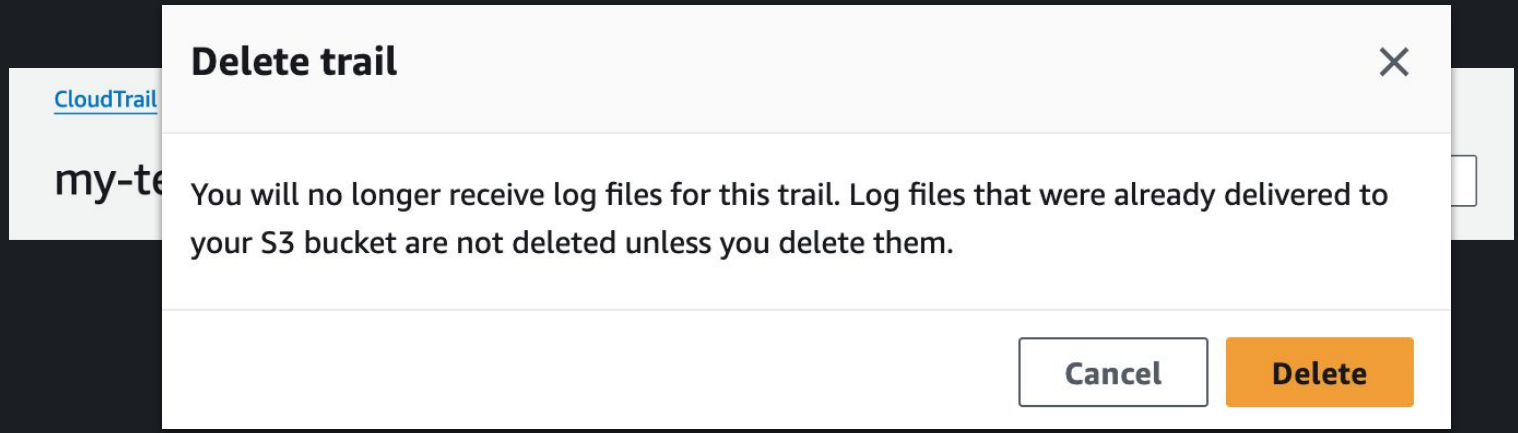
CYBR

T1562.008: Impair Defenses: Disable or Modify Cloud Logs



T1562.008: Impair Defenses: Disable or Modify Cloud Logs

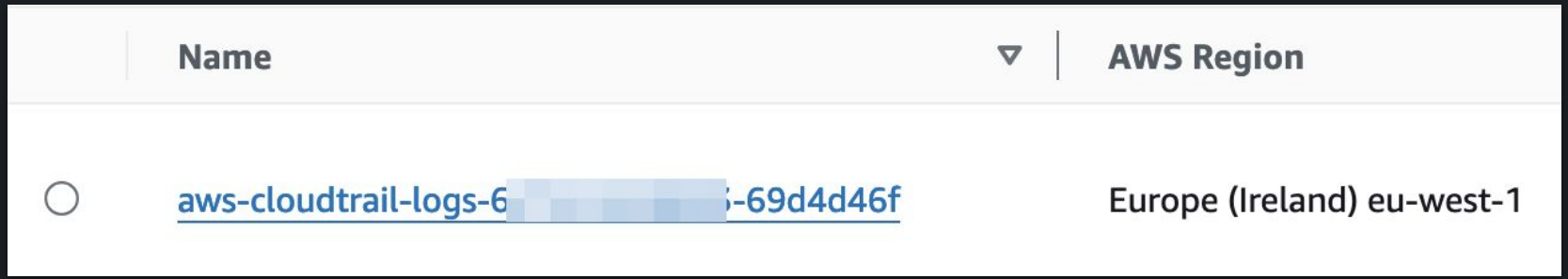
Cleaning up our test



CYBR

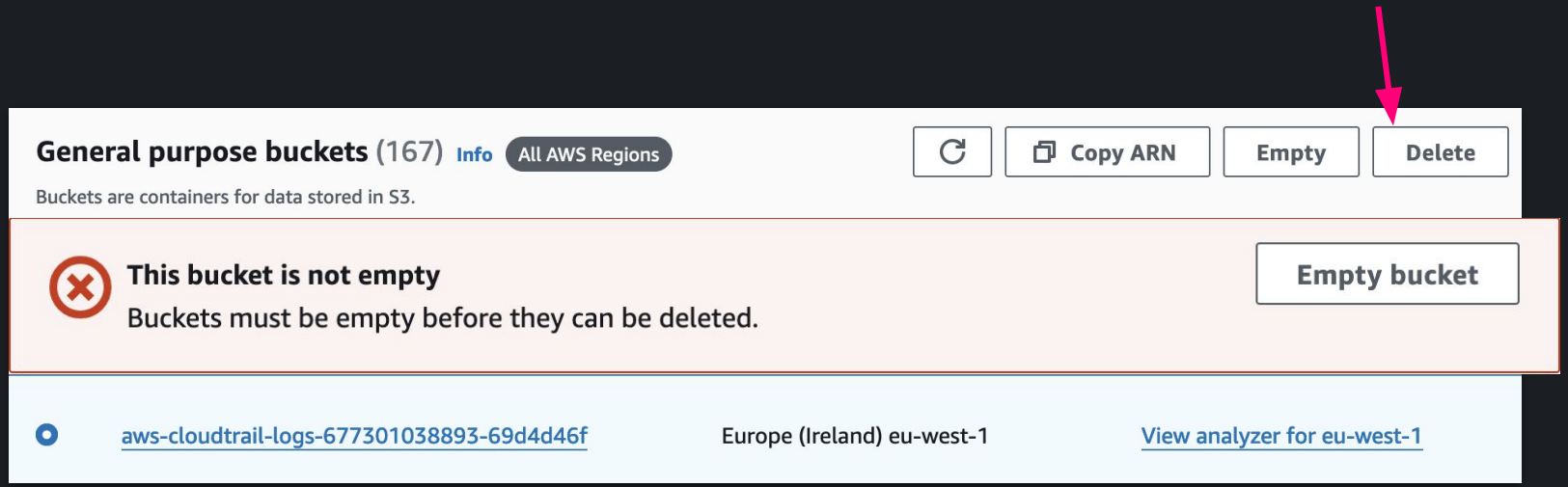
T1562.008: Impair Defenses: Disable or Modify Cloud Logs

Woops

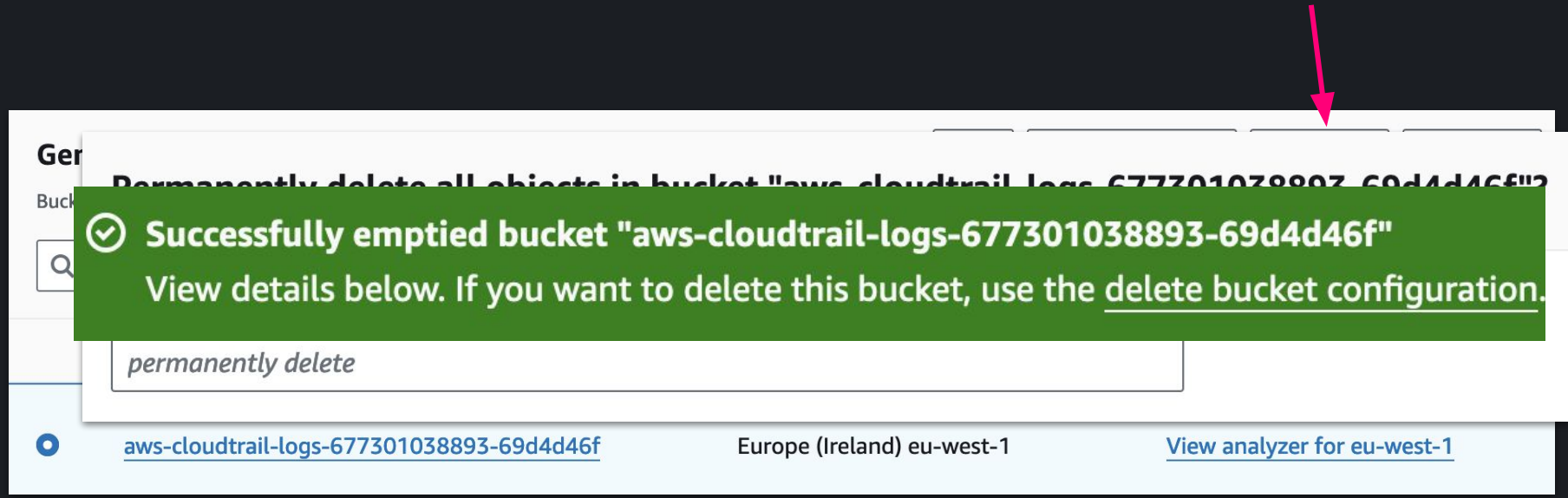


CYBR

T1562.008: Impair Defenses: Disable or Modify Cloud Logs

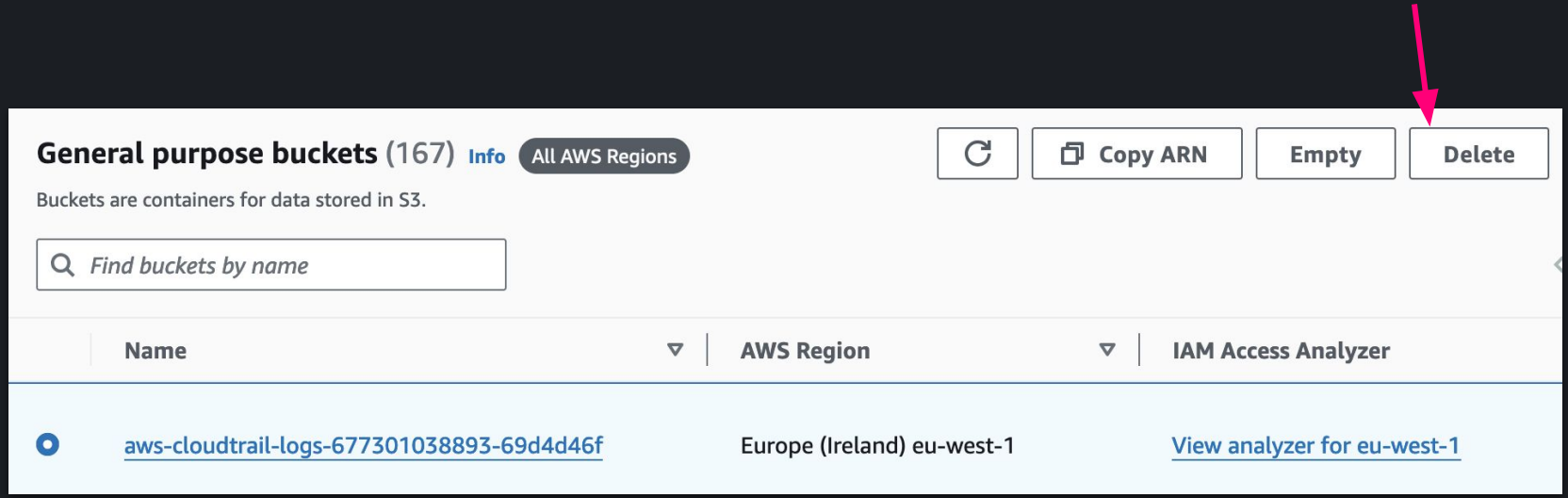


T1562.008: Impair Defenses: Disable or Modify Cloud Logs



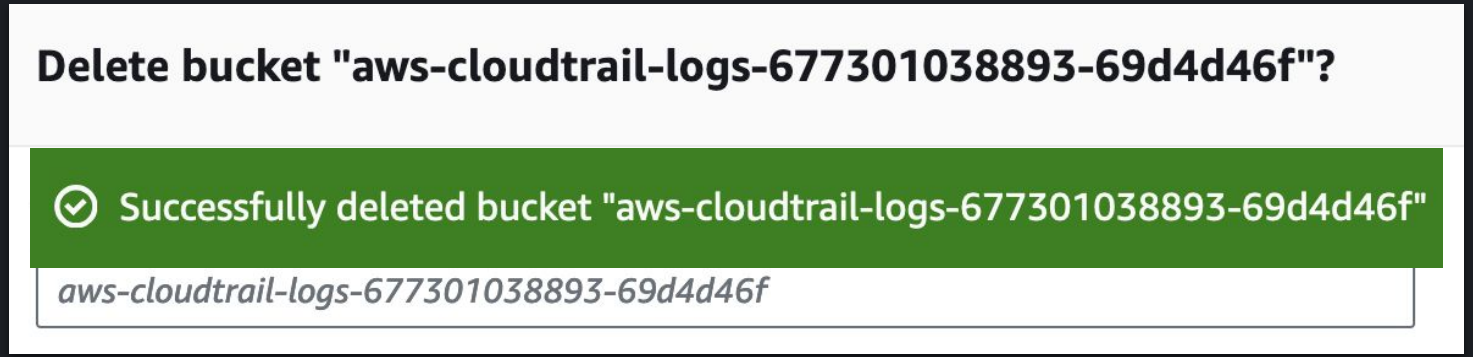
CYBR

T1562.008: Impair Defenses: Disable or Modify Cloud Logs



CYBR

T1562.008: Impair Defenses: Disable or Modify Cloud Logs



T1562.008: Impair Defenses: Disable or Modify Cloud Logs

- Setting up the right cloud infrastructure
- Complaining about the documentation
- Actually testing your threat detection



CYBR

Stratus Red Team



stratus-red-team Public

Granular, Actionable Adversary Emulation for the Cloud

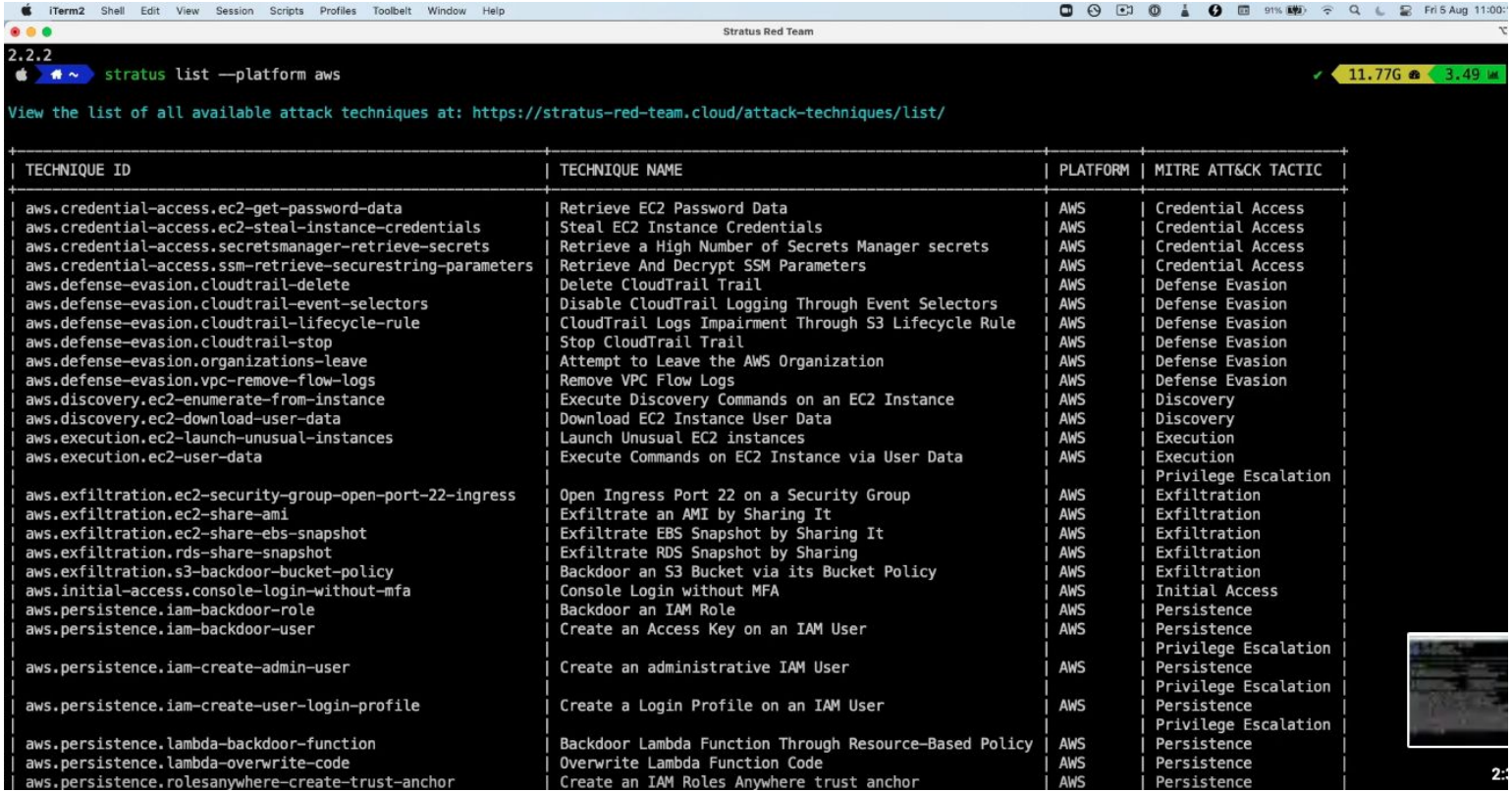
Go 1.8k 214

- *"Atomic Red Team for the Cloud"*
- Written in Go
- Packaged with cloud-native attacks

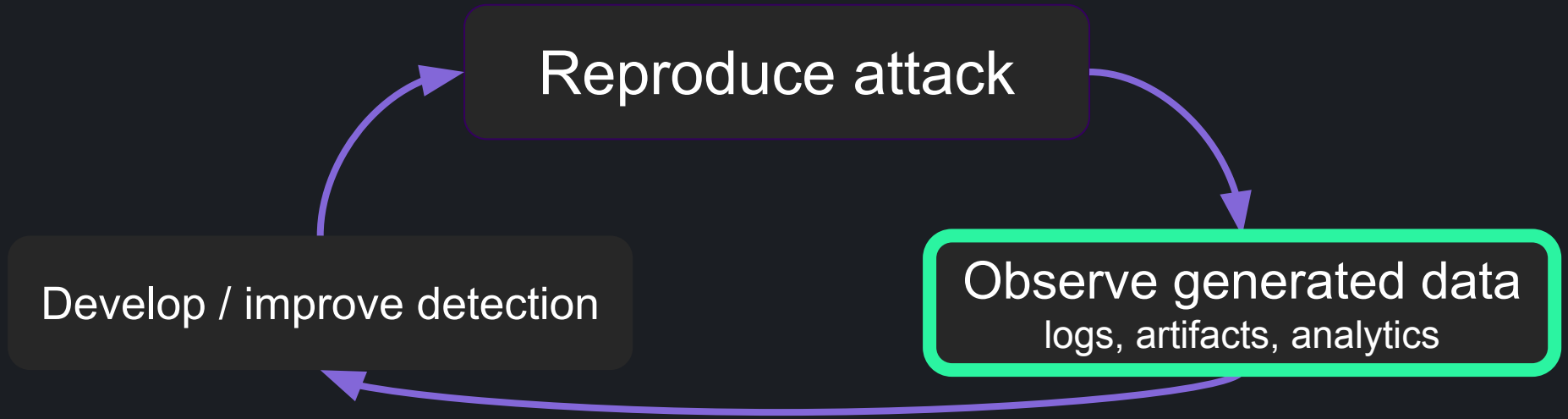
CYBR

Demo

CYBR



https://www.youtube.com/watch?v=GJENDhzO7j4


Reproduce attack
Observe generated data
logs, artifacts, analytics
Develop / improve detection

CYBR


Attack
Cloud environment
????

Grimoire



grimoire Public

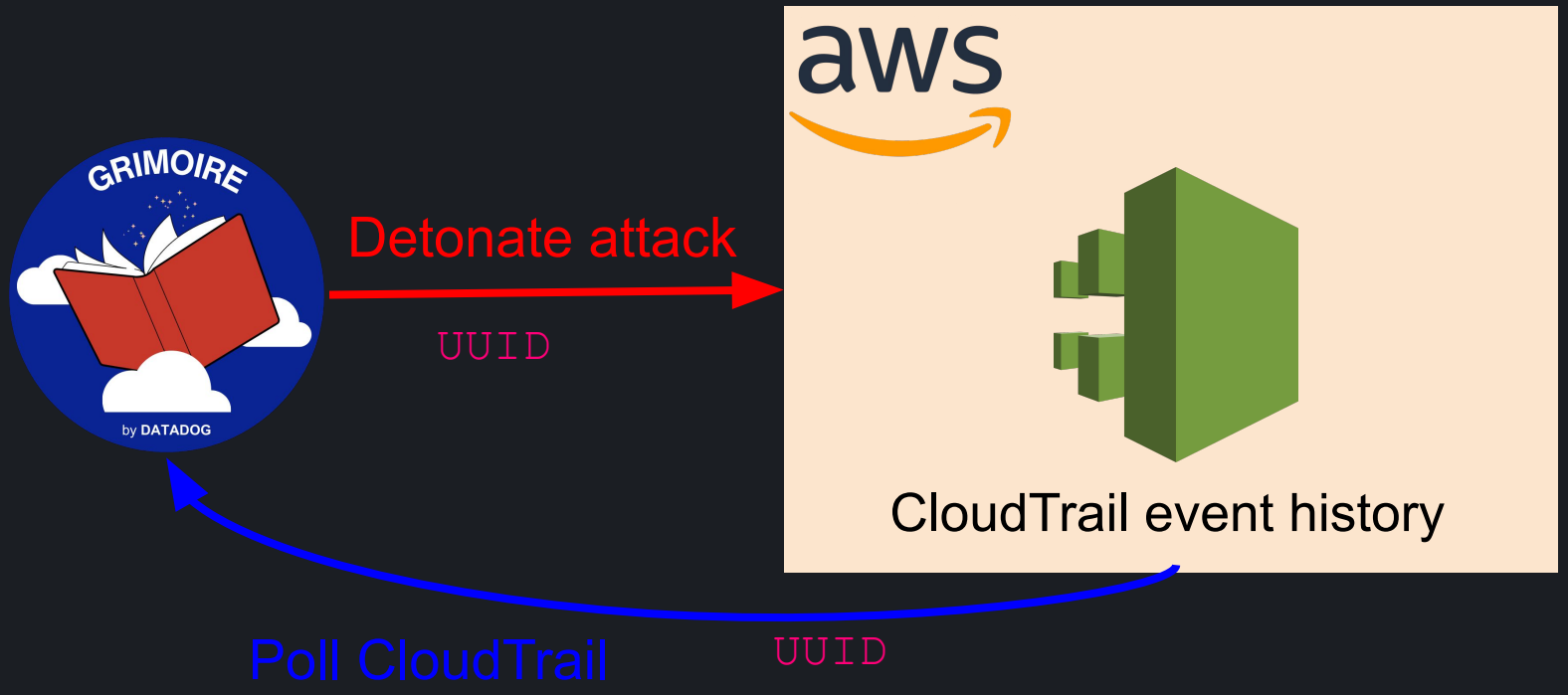
Generate datasets of cloud audit logs for common attacks



Go ☆ 185 Apache-2.0 14 5 0

CYBR

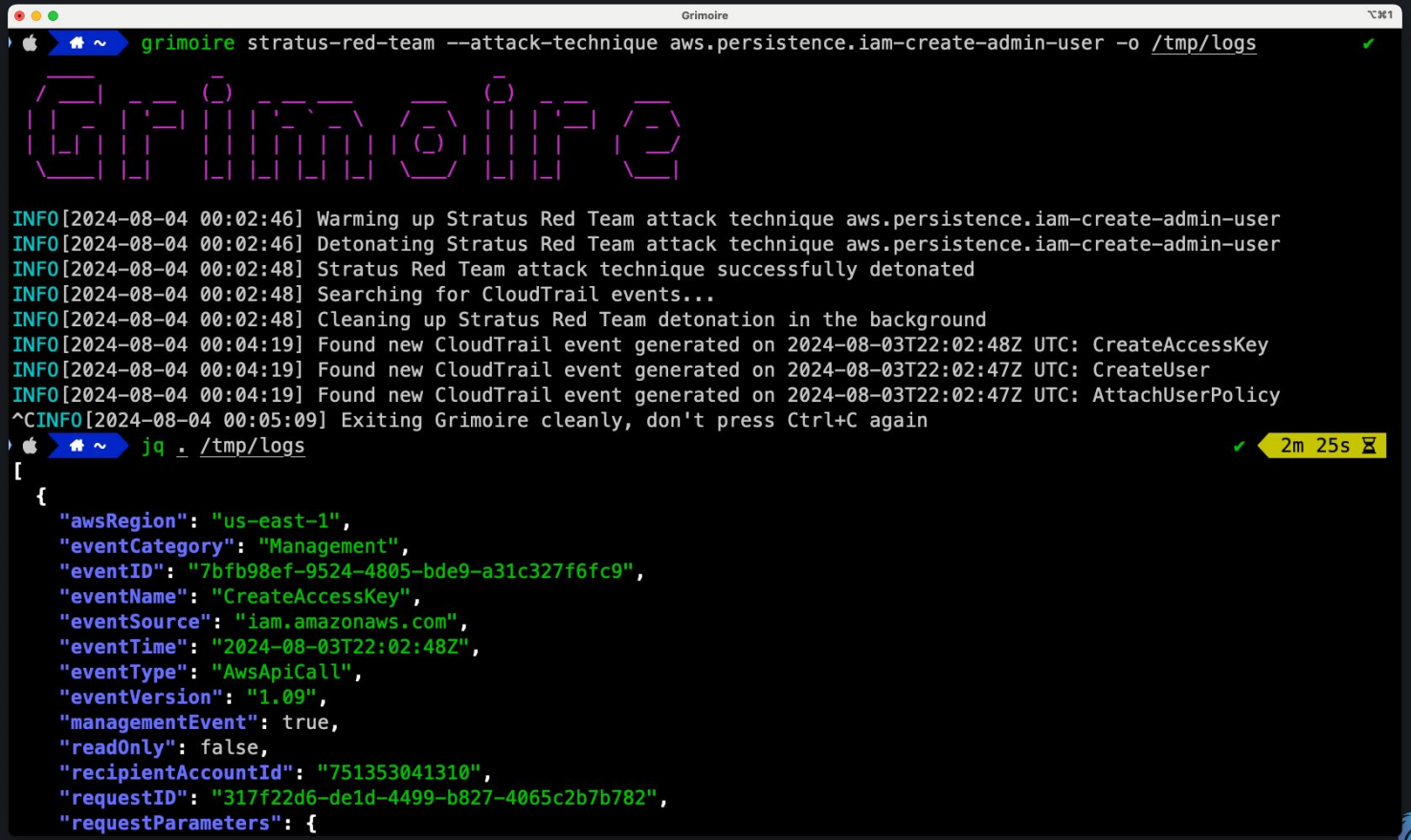
Grimoire


GRIMOIRE
by DATADOG
Detonate attack
UUID
aws
CloudTrail event history
Poll CloudTrail
UUID

Demo

CYBR

Demo


Grimoire
~ grimoire stratus-red-team --attack-technique aws.persistence.iam-create-admin-user -o /tmp/logs
INFO[2024-08-04 00:02:46] Warming up Stratus Red Team attack technique aws.persistence.iam-create-admin-user
INFO[2024-08-04 00:02:46] Detonating Stratus Red Team attack technique aws.persistence.iam-create-admin-user
INFO[2024-08-04 00:02:48] Stratus Red Team attack technique successfully detonated
INFO[2024-08-04 00:02:48] Searching for CloudTrail events...
INFO[2024-08-04 00:02:48] Cleaning up Stratus Red Team detonation in the background
INFO[2024-08-04 00:04:19] Found new CloudTrail event generated on 2024-08-03T22:02:48Z UTC: CreateAccessKey
INFO[2024-08-04 00:04:19] Found new CloudTrail event generated on 2024-08-03T22:02:47Z UTC: CreateUser
INFO[2024-08-04 00:04:19] Found new CloudTrail event generated on 2024-08-03T22:02:47Z UTC: AttachUserPolicy
^CINFO[2024-08-04 00:05:09] Exiting Grimoire cleanly, don't press Ctrl+C again
~ jq . /tmp/logs
2m 25s
[
{
"awsRegion": "us-east-1",
"eventCategory": "Management",
"eventID": "7bfb98ef-9524-4805-bde9-a31c327f6fc9",
"eventName": "CreateAccessKey",
"eventSource": "iam.amazonaws.com",
"eventTime": "2024-08-03T22:02:48Z",
"eventType": "AwsApiCall",
"eventVersion": "1.09",
"managementEvent": true,
"readOnly": false,
"recipientAccountId": "751353041310",
"requestID": "317f22d6-de1d-4499-b827-4065c2b7b782",
"requestParameters": {

CYBR

Demo



CYBR


STRATUS RED TEAM
by DATADOG
GRIMOIRE
by DATADOG

Cloud audit logs dataset

Detonation logs NEW!

The following CloudTrail events are generated when this technique is detonated[1]:

- `ec2:DescribeInstances`
- `ec2:StartInstances`
- `ec2:ModifyInstanceAttribute`
- `ec2:StopInstances`

View raw detonation logs >

1. These logs have been gathered from a real detonation of this technique in a test environment using Grimoire, and anonymized using LogLicker.

CYBR

Cloud audit logs dataset

View raw detonation logs


```
[
   {
      "awsRegion": "ca-northsouth-2r",
      "eventCategory": "Management",
      "eventID": "759fa0d5-d7d6-4de3-97f0-c469d1a0f92c",
      "eventName": "DescribeInstances",
      "eventSource": "ec2.amazonaws.com",
      "eventTime": "2024-08-01T12:04:24Z",
      "eventType": "AwsApiCall",
      "eventVersion": "1.09",
      "managementEvent": true,
      "readOnly": true,
      "recipientAccountId": "309303190113",
      "requestID": "a9c78483-c047-4215-94c6-89794dd3b44e",
      "requestParameters": {
         "filterSet": {},
         "instancesSet": {
            "items": [
               {
                  "instanceId": "i-DDd6c7B0e18F0E35f"
               }
            ]
         }
      },
```

Wrapping up

Adversary Emulation for the Cloud

Lab: https://cybr.com/try-stratus

CYBR

Adversary Emulation for the Cloud

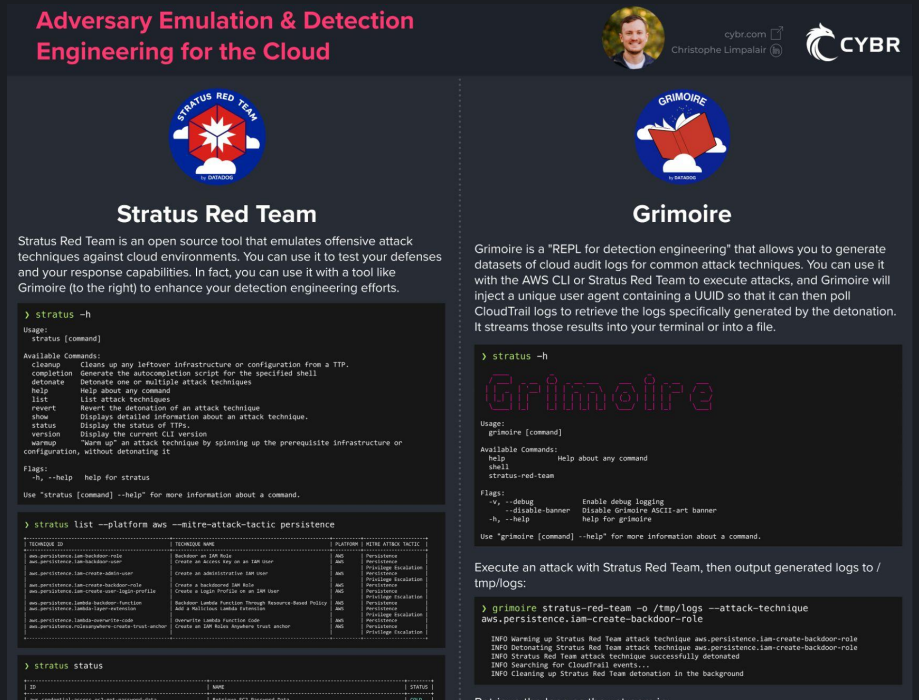
Contributions welcome!

CYBR

Adversary Emulation for the Cloud

Reference Guide Cheat Sheet

Download: cybr.com/stratus-and-grimoire



CYBR





Thank you for attending!

Any questions?

Christophe Limpalair
linkedin.com/in/christophelimpalair

Christophe Tafani-Dereeper
linkedin.com/in/christophetafanidereeper



Live training webinars
https://cybr.com/webinars