Detection Challenges in Cloud Connected Credential Abuse Attacks

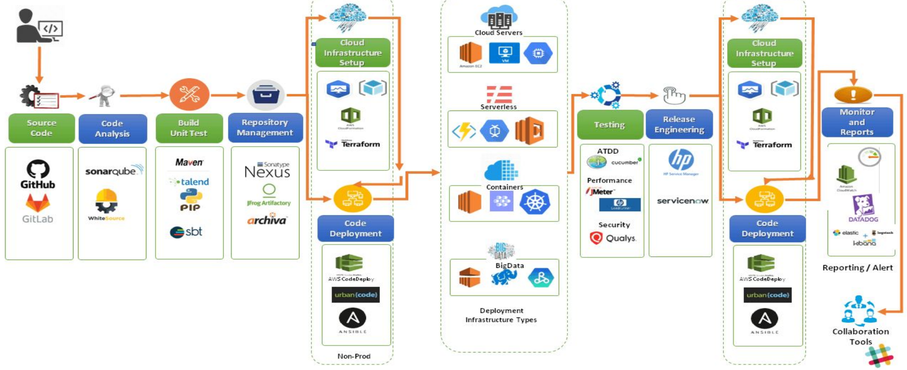
@rodsoto

$whoami

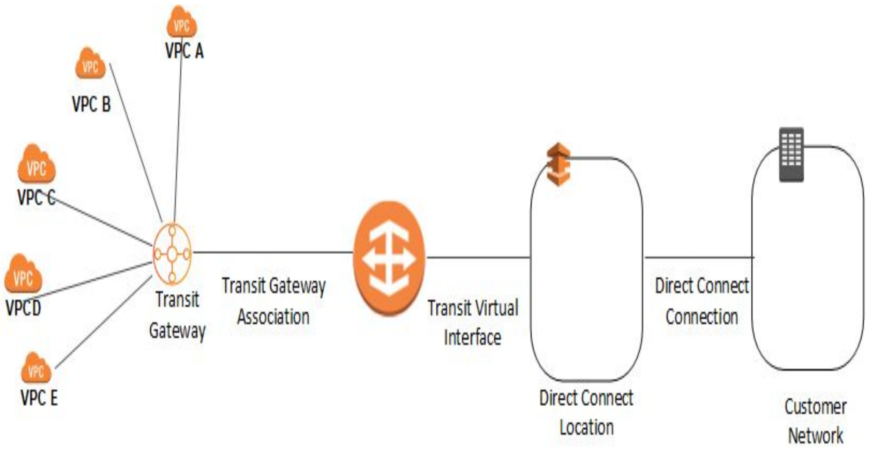
Rod Soto @rodsoto

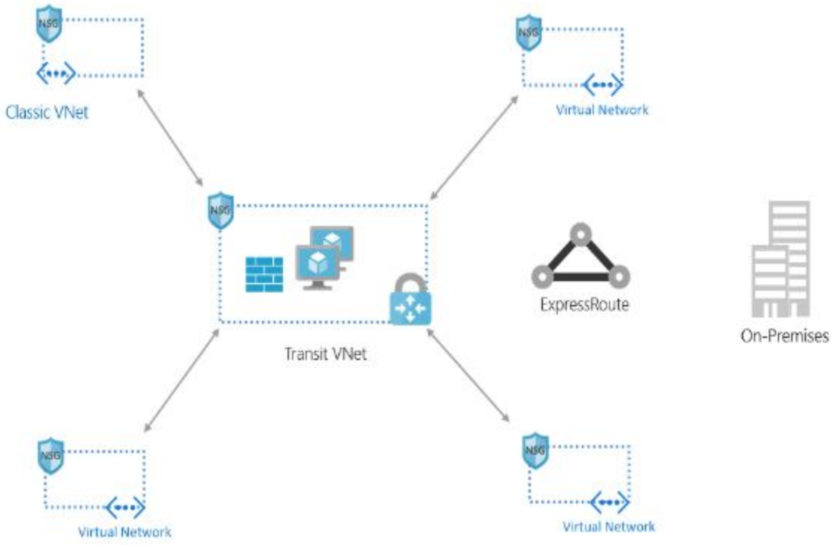
Principal Security Research Engineer at Splunk. Worked at Prolexic Technologies (now Akamai), and Caspida. Cofounder of Hackmiami and Pacific Hackers meetups and conferences. Creator of Kommand && KonTroll / NoQrtr-CTF.

How the cloud permeates inside the perimeter

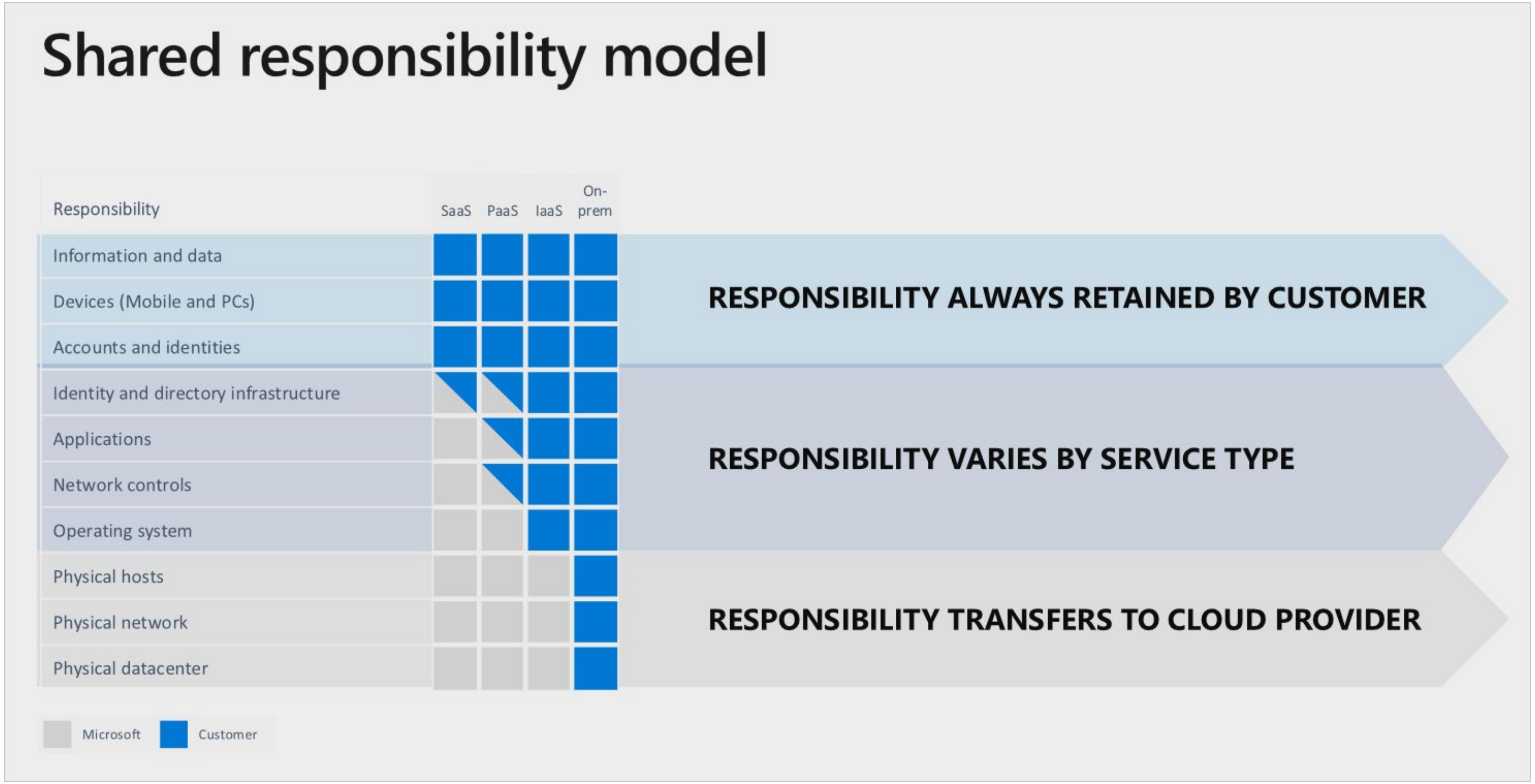


Amazon transit gateway / Azure vnet





The hot potato of security ownership



Shared responsibility model

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	⬜	⬜	⬜	🟦

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

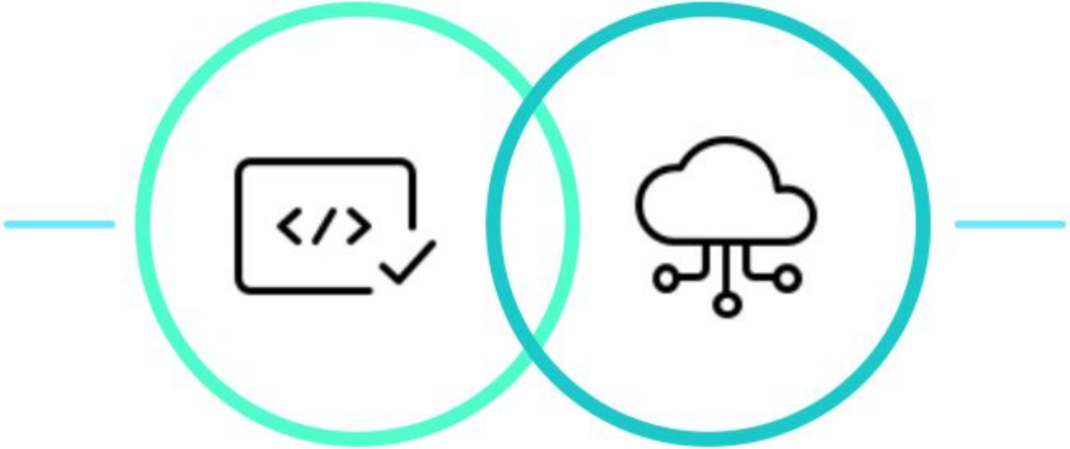
RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

⬜ Microsoft 🟦 Customer

CLOUD REAL ESTATE + PERIMETER

Converged Perimeter



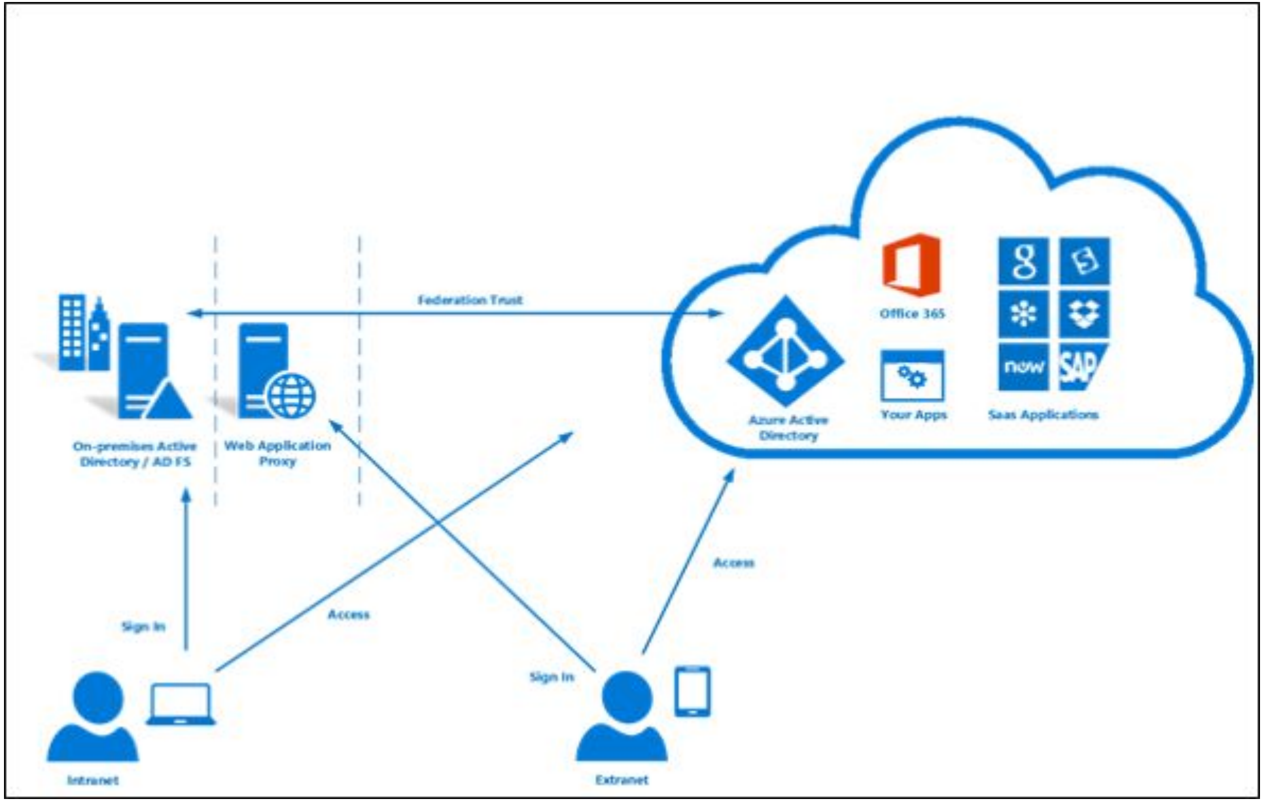
Behind Internet Gateway
DevOps
ITOps

Cloud
Storage
Compute
Databases

It's not a vulnerability it’s a feature

SSH Key Pairs
Slack Tokens
SAML Tokens
Email
IAM secrets
Key Pairs
X.509 Certs
API Keys (AWS, GCP, Azure)

Federated environments



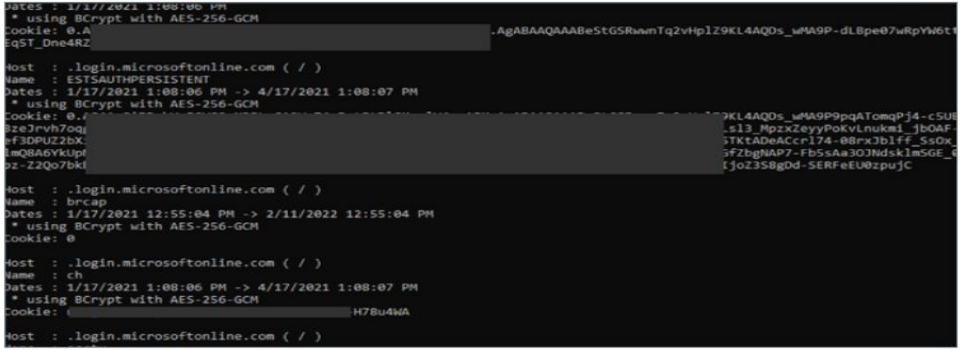
Federated Environments

- Formal connection of perimeter and cloud real estate resources
- Increase in Cloud utilization (Move of on-premise resources to the cloud)
- Increases resource availability and geographical reach
- Requires standards that allow passage of data, identification, authentication (Tokens, Certificates, Passwords, API Keys)
- Formal federations (Trust between cloud/perimeter) aim to implement stricter control on access
- You can have informal federations

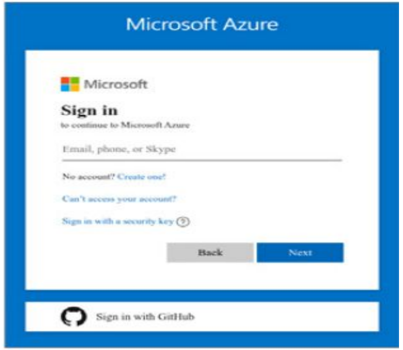
Converged perimeter risks scenarios

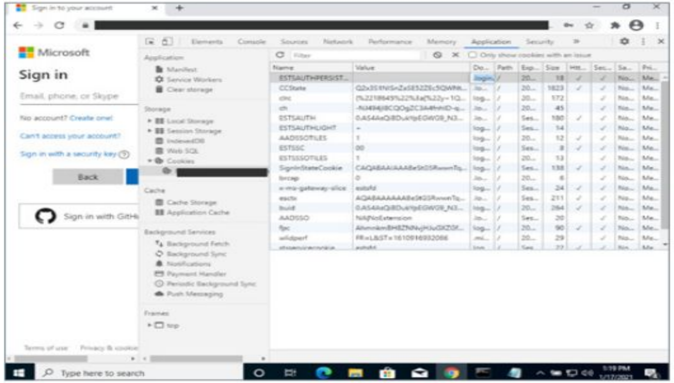
- Credential leakage in public repositories
- Use of vulnerable components from cloud (Open source libraries, containers)
- Exposure of cloud apps and infrastructure may lead to internal access
- Re-use of federated credentials (Golden SAML, Oauth Token hijack, Pass The Cookie)
- Pivoting from Cloud Providers to internal or converged perimeter resources

Examples of Cloud Connected Credential Abuse Attacks

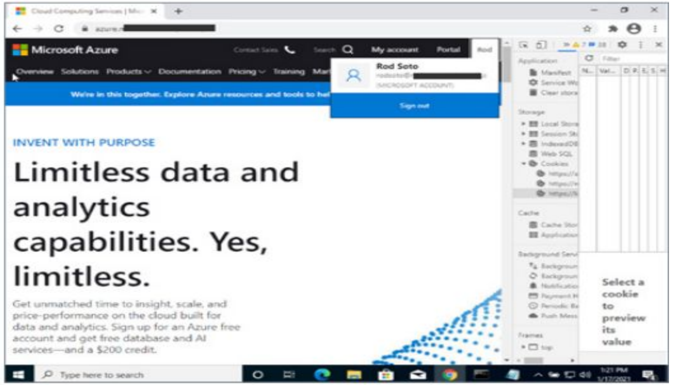


```
Dates : 1/17/2021 1:08:06 PM
 * using BCrypt with AES-256-GCM
Cookie: 0.A[redacted].AgABAAQAAABeStGSRwwnTq2vHplZ9KL4AQDs_wMA9P-dLBpe07wRpYW6t
EqST_Dne4RZ[redacted]

Host  : .login.microsoftonline.com ( / )
Name  : ESTSAUTHPERSISTENT
Dates : 1/17/2021 1:08:06 PM -> 4/17/2021 1:08:07 PM
 * using BCrypt with AES-256-GCM
Cookie: 0.[redacted]9KL4AQDs_wMA9P9pqATomqPj4-cSUE
3zeJrvh7oq                                                           .sl3_MpzxZeyyPoKvLnukmi_jbOAF-
ef3DPUZ2bX                                                           5TKtADeACcrl74-08rxJblff_SsOx_
lmQ8A6YkUp                                                           5fZbgNAP7-Fb5sAa3OJNdsklmSGE_
pz-Z2Qo7bk                                                           IjoZ3S8gDd-SERFeEU0zpujC

Host  : .login.microsoftonline.com ( / )
Name  : brcap
Dates : 1/17/2021 12:55:04 PM -> 2/11/2022 12:55:04 PM
 * using BCrypt with AES-256-GCM
Cookie: 0

Host  : .login.microsoftonline.com ( / )
Name  : ch
Dates : 1/17/2021 1:08:06 PM -> 4/17/2021 1:08:07 PM
 * using BCrypt with AES-256-GCM
Cookie: [redacted]H78u4WA

Host  : .login.microsoftonline.com ( / )
```





Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Sa...	Pri...
ESTSAUTHPERSIST...		login...	/	20...	18	✓	✓	No...	Me...
CCState	Q2x3S1NISnZaSES2ZEc5QWNt...	.lo...	/	20...	1823	✓	✓	No...	Me...
clrc	{%2218849%22%3a{%22y=1Q...	log...	/	20...	172		✓	No...	Me...
ch	-NJ494jI8CQOgZC3A4fnhID-q...	.lo...	/	20...	45		✓	No...	Me...
ESTSAUTH	0.AS4AeQiBDuaYpEGWG8_N3...	.lo...	/	Ses...	180	✓	✓	No...	Me...
ESTSAUTHLIGHT	+	log...	/	Ses...	14		✓	No...	Me...
AADSSOTILES	1	log...	/	20...	12	✓	✓	No...	Me...
ESTSSC	00	log...	/	Ses...	8	✓	✓	No...	Me...
ESTSSSOTILES	1	log...	/	20...	13		✓	No...	Me...
SigninStateCookie	CAQABAAIAAAABeStGSRwwnTq...	log...	/	Ses...	138	✓	✓	No...	Me...
brcap	0	.lo...	/	20...	6		✓	No...	Me...
x-ms-gateway-slice	estsfd	log...	/	Ses...	24	✓	✓	No...	Me...
esctx	AQABAAAAAAABeStGSRwwnTq...	.lo...	/	Ses...	211	✓	✓	No...	Me...
buid	0.AS4AeQiBDuaYpEGWG8_N3...	log...	/	20...	284	✓	✓	No...	Me...
AADSSO	NA|NoExtension	.lo...	/	Ses...	20		✓	No...	Me...
fpc	AhmnkmBH8ZNNvjHJuGXZGf...	log...	/	20...	90	✓	✓	No...	Me...
wlidperf	FR=L&ST=1610916932086	.mi...	/	20...	29		✓	No...	Me...
stsservicecookie	estsfd	log...	/	Ses...	22	✓	✓	No...	Me...



We're in this together. Explore Azure resources and tools to hel

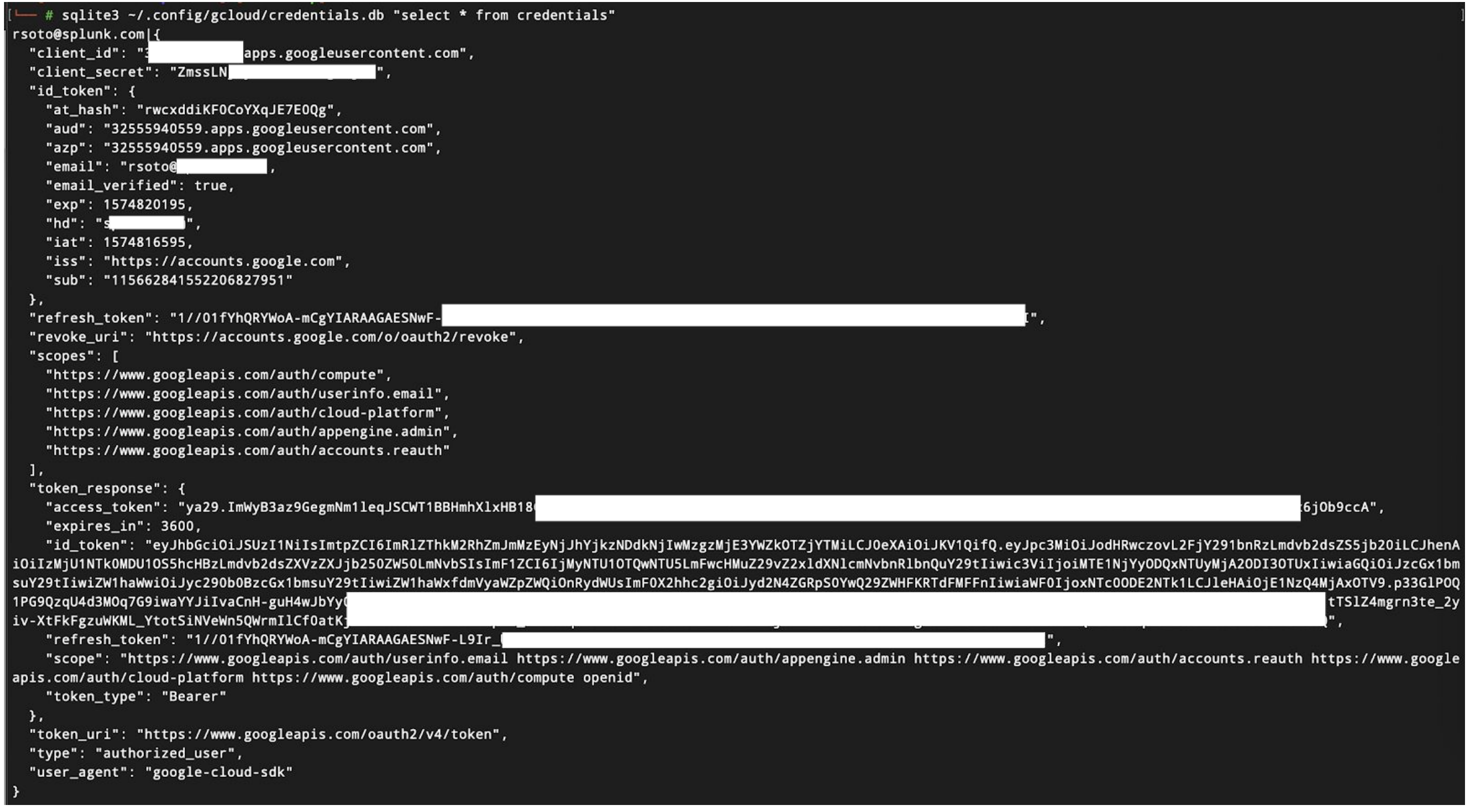
INVENT WITH PURPOSE

Limitless data and analytics capabilities. Yes, limitless.

Get unmatched time to insight, scale, and price-performance on the cloud built for data and analytics. Sign up for an Azure free account and get free database and AI services—and a $200 credit.

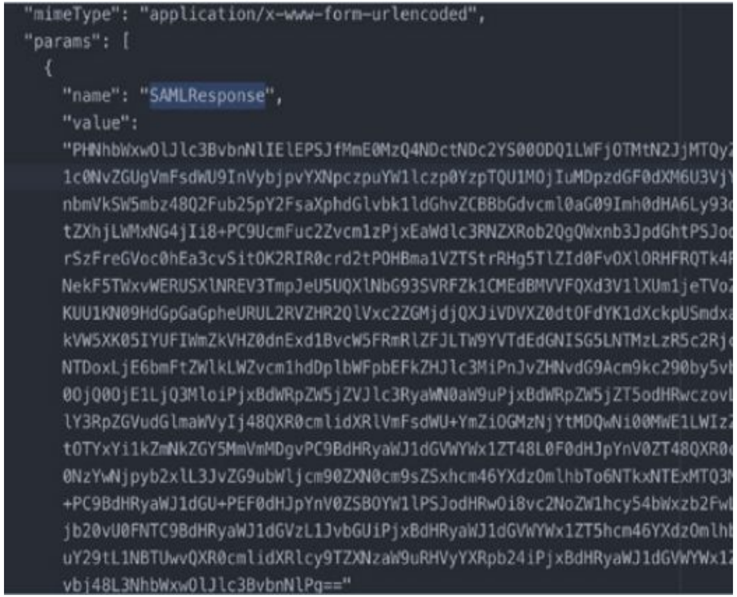
Select a cookie to preview its value

Oauth token hijack

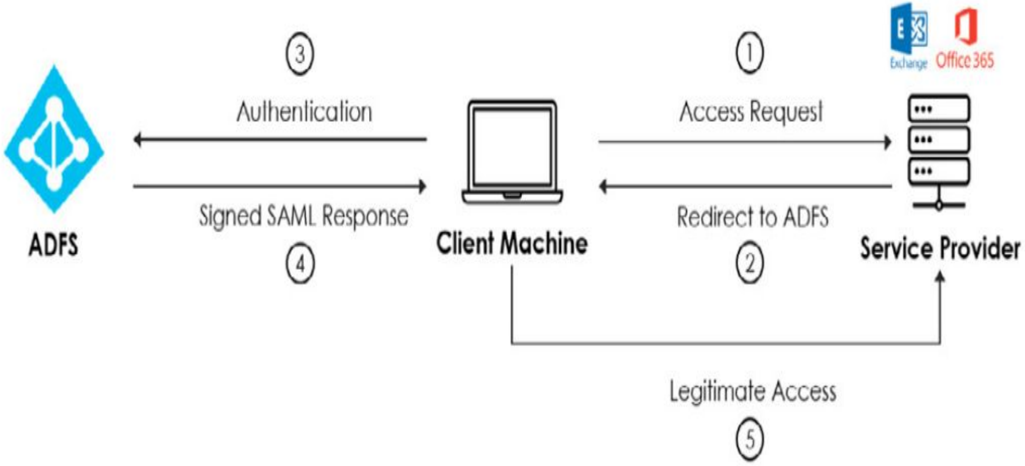


```
└─ # sqlite3 ~/.config/gcloud/credentials.db "select * from credentials"
rsoto@splunk.com|{
  "client_id": "[redacted]apps.googleusercontent.com",
  "client_secret": "ZmssLN[redacted]",
  "id_token": {
    "at_hash": "rwcxddiKF0CoYXqJE7E0Qg",
    "aud": "32555940559.apps.googleusercontent.com",
    "azp": "32555940559.apps.googleusercontent.com",
    "email": "rsoto@[redacted],
    "email_verified": true,
    "exp": 1574820195,
    "hd": "[redacted]",
    "iat": 1574816595,
    "iss": "https://accounts.google.com",
    "sub": "115662841552206827951"
  },
  "refresh_token": "1//01fYhQRYWoA-mCgYIARAAGAESNwF-[redacted]",
  "revoke_uri": "https://accounts.google.com/o/oauth2/revoke",
  "scopes": [
    "https://www.googleapis.com/auth/compute",
    "https://www.googleapis.com/auth/userinfo.email",
    "https://www.googleapis.com/auth/cloud-platform",
    "https://www.googleapis.com/auth/appengine.admin",
    "https://www.googleapis.com/auth/accounts.reauth"
  ],
  "token_response": {
    "access_token": "ya29.ImWyB3az9GegmNm1leqJSCWT1BBHmhXlxHB18[redacted]6jOb9ccA",
    "expires_in": 3600,
    "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6ImRlZThkM2RhZmJmMzEyNjJhYjkzNDdkNjIwMzgzMjE3YWZkOTZjYTMiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2FjY291bnRzLmdvb2dsZS5jb20iLCJhenA
iOiIzMjU1NTk0MDU1OS5hcHBzLmdvb2dsZXVzZXJjb250ZW50LmNvbSIsImF1ZCI6IjMyNTU1OTQwNTU5LmFwcHMuZ29vZ2xldXNlcmNvbnRlbnQuY29tIiwic3ViIjoiMTE1NjYyODQxNTUyMjA2ODI3OTUxIiwiaGQiOiJzcGx1bm
suY29tIiwiZW1haWwiOiJyc290b0BzcGx1bmsuY29tIiwiZW1haWxfdmVyaWZpZWQiOnRydWUsImF0X2hhc2giOiJyd2N4ZGRpS0YwQ29ZWHFKRTdFMFFnIiwiaWF0IjoxNTc0ODE2NTk1LCJleHAiOjE1NzQ4MjAxOTV9.p33GlPOQ
1PG9QzqU4d3MOq7G9iwaYYJiIvaCnH-guH4wJbYy[redacted]tTSlZ4mgrn3te_2y
iv-XtFkFgzuWKML_YtotSiNVeWn5QWrmIlCf0atK",
    "refresh_token": "1//01fYhQRYWoA-mCgYIARAAGAESNwF-L9Ir_[redacted]",
    "scope": "https://www.googleapis.com/auth/userinfo.email https://www.googleapis.com/auth/appengine.admin https://www.googleapis.com/auth/accounts.reauth https://www.google
apis.com/auth/cloud-platform https://www.googleapis.com/auth/compute openid",
    "token_type": "Bearer"
  },
  "token_uri": "https://www.googleapis.com/oauth2/v4/token",
  "type": "authorized_user",
  "user_agent": "google-cloud-sdk"
}
```

SAML Forging

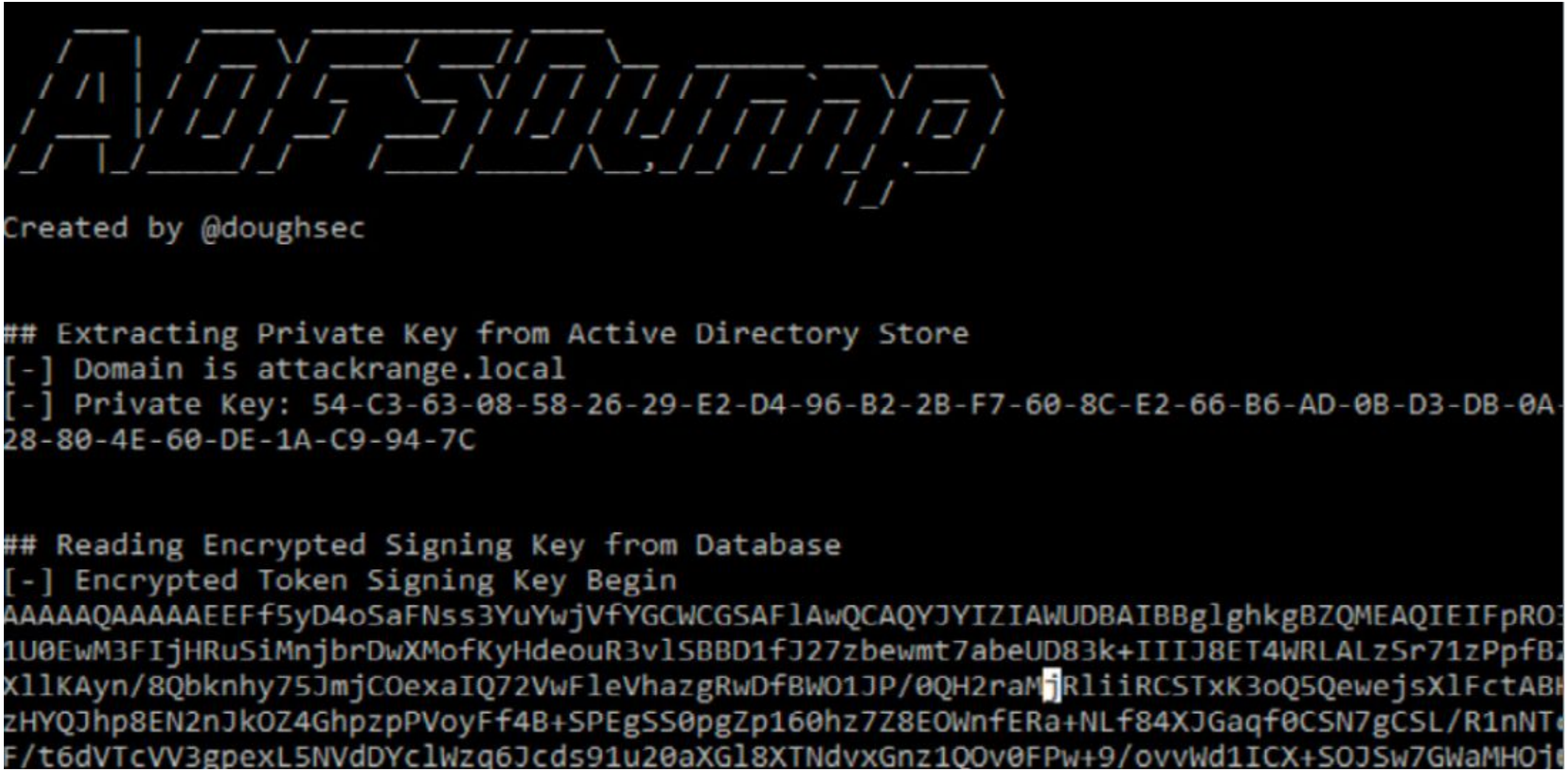


```
"mimeType": "application/x-www-form-urlencoded",
"params": [
  {
    "name": "SAMLResponse",
    "value":
    "PHNhbWxwOlJlc3BvbnNlIElEPSJfMmE0MzQ4NDctNDc2YS00ODQ1LWFjOTMtN2JjMTQy
    1c0NvZGUgVmFsdWU9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpzdGF0dXM6U3Vj
    nbmVkSW5mbz48Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBBbGdvcml0aG09Imh0dHA6Ly93
    tZXhjLWMxNG4jIi8+PC9UcmFuc2Zvcm1zPjxEaWdlc3RNZXRob2QgQWxnb3JpdGhtPSJo
    rSzFreGVoc0hEa3cvSitOK2RIR0crd2tPOHBma1VZTStrRHg5TlZId0FvOXlORHFRQTk4
    NekF5TWxvWERUSXlNREV3TmpJeU5UQXlNbG93SVRFZk1CMEdBMVVFQXd3V1lXUm1jeTVo
    KUU1KN09HdGpGaGpheURUL2RVZHR2QlVxc2ZGMjdjQXJiVDVXZ0dtOFdYK1dXckpUSmdx
    kVW5XK05IYUFIWmZkVHZ0dnExd1BvcW5FRmRlZFJLTW9YVTdEdGNISG5LNTMzLzR5c2Rj
    NTDoxLjE6bmFtZWlkLWZvcm1hdDplbWFpbEFkZHJlc3MiPnJvZHNvdG9Acm9kc290by5v
    0OjQ0OjE1LjQ3MloiPjxBdWRpZW5jZVJlc3RyaWN0aW9uPjxBdWRpZW5jZT5odHRwczov
    lY3RpZGVudGlmaWVyIj48QXR0cmlidXRlVmFsdWU+YmZiOGMzNjYtMDQwNi00MWE1LWIz
    tOTYxYi1kZmNkZGY5MmVmMDgvPC9BdHRyaWJ1dGVWYWx1ZT48L0F0dHJpYnV0ZT48QXR0
    0NzYwNjpyb2xlL3JvZG9ubWljcm90ZXN0cm9sZSxhcm46YXdzOmlhbTo6NTkxNTExMTQ3
    +PC9BdHRyaWJ1dGU+PEF0dHJpYnV0ZSBOYW1lPSJodHRwOi8vc2NoZW1hcy54bWxzb2Fw
    jb20vU0FNTC9BdHRyaWJ1dGVzL1JvbGUiPjxBdHRyaWJ1dGVWYWx1ZT5hcm46YXdzOmlh
    uY29tL1NBTUwvQXR0cmlidXRlcy9TZXNzaW9uRHVyYXRpb24iPjxBdHRyaWJ1dGVWYWx1
    vbj48L3NhbWxwOlJlc3BvbnNlPg=="
```



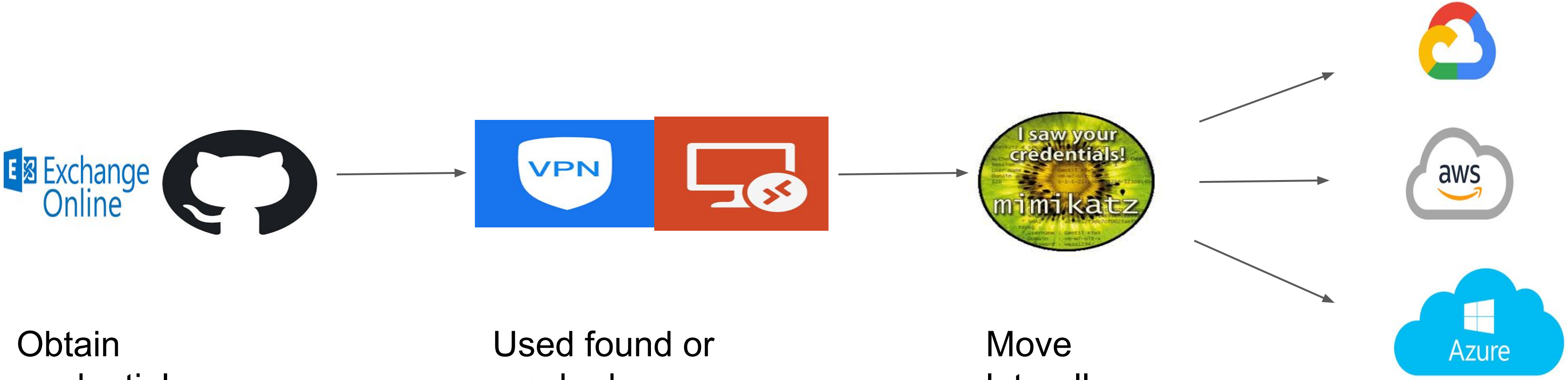
Source: Sygnia Advisory – Detection of Golden SAML attacks

Post exploitation tools



```
Created by @doughsec


## Extracting Private Key from Active Directory Store
[-] Domain is attackrange.local
[-] Private Key: 54-C3-63-08-58-26-29-E2-D4-96-B2-2B-F7-60-8C-E2-66-B6-AD-0B-D3-DB-0A-
28-80-4E-60-DE-1A-C9-94-7C


## Reading Encrypted Signing Key from Database
[-] Encrypted Token Signing Key Begin
AAAAAQAAAAAEEFf5yD4oSaFNss3YuYwjVfYGCWCGSAFlAwQCAQYJYIZIAWUDBAIBBglghkgBZQMEAQIEIFpRO
1U0EwM3FIjHRuSiMnjbrDwXMofKyHdeouR3vlSBBD1fJ27zbewmt7abeUD83k+IIIJ8ET4WRLALzSr71zPpfB
XllKAyn/8Qbknhy75JmjCOexaIQ72VwFleVhazgRwDfBWO1JP/0QH2raMjRliiRCSTxK3oQ5QewejsXlFctAB
zHYQJhp8EN2nJkOZ4GhpzpPVoyFf4B+SPEgSS0pgZp160hz7Z8EOWnfERa+NLf84XJGaqf0CSN7gCSL/R1nNT
F/t6dVTcVV3gpexL5NVdDYclWzq6Jcds91u20aXGl8XTNdvxGnz1QOv0FPw+9/ovvWd1ICX+SOJSw7GWaMHOj
```

Exploitation Circle Cloud App/Service / perimeter secrets

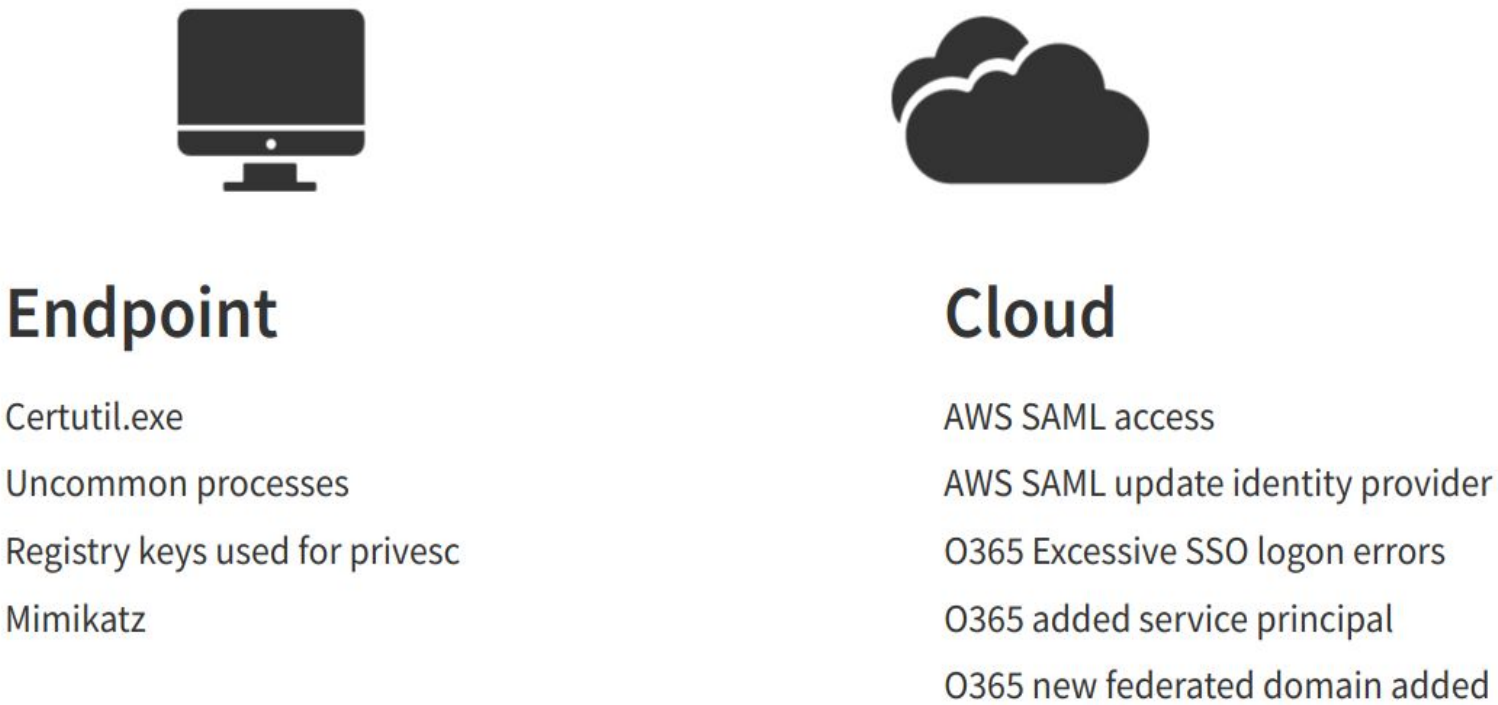


Obtain credentials either leaked, or from misconfigured federated services

Used found or cracked credentials to access VPN/RDP with no MFA

Move laterally, extract more secrets (SAML, Cookies, Passwords, Hashes, Certificates)

So how do we approach these attacks?



Endpoint

Certutil.exe

Uncommon processes

Registry keys used for privesc

Mimikatz

Cloud

AWS SAML access

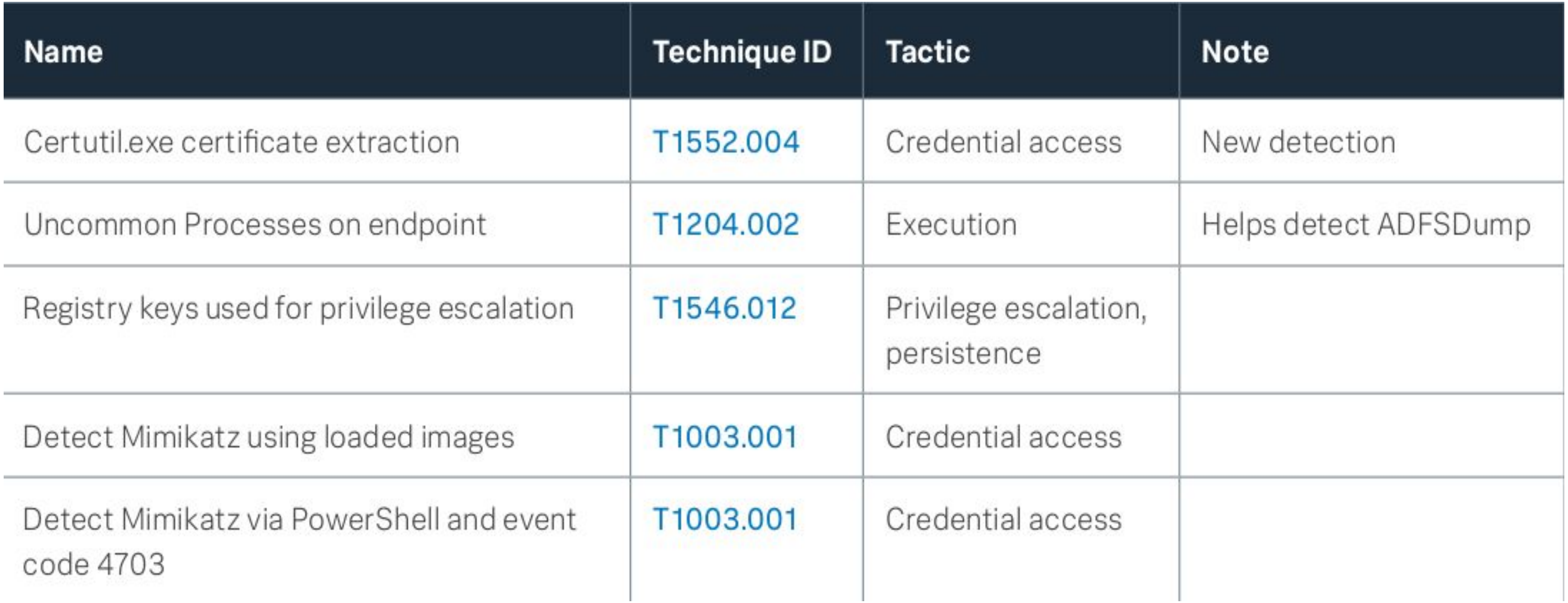
AWS SAML update identity provider

O365 Excessive SSO logon errors

O365 added service principal

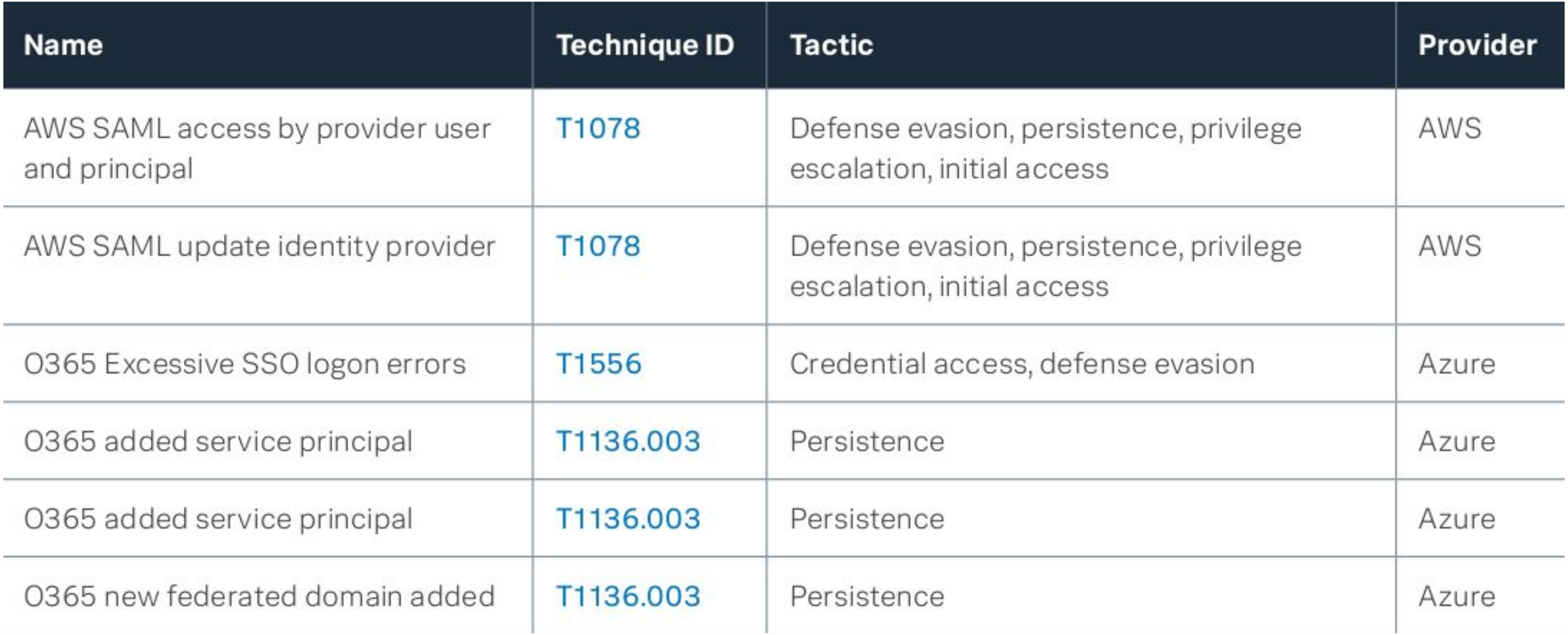
O365 new federated domain added

Detections by TTPs - Endpoint



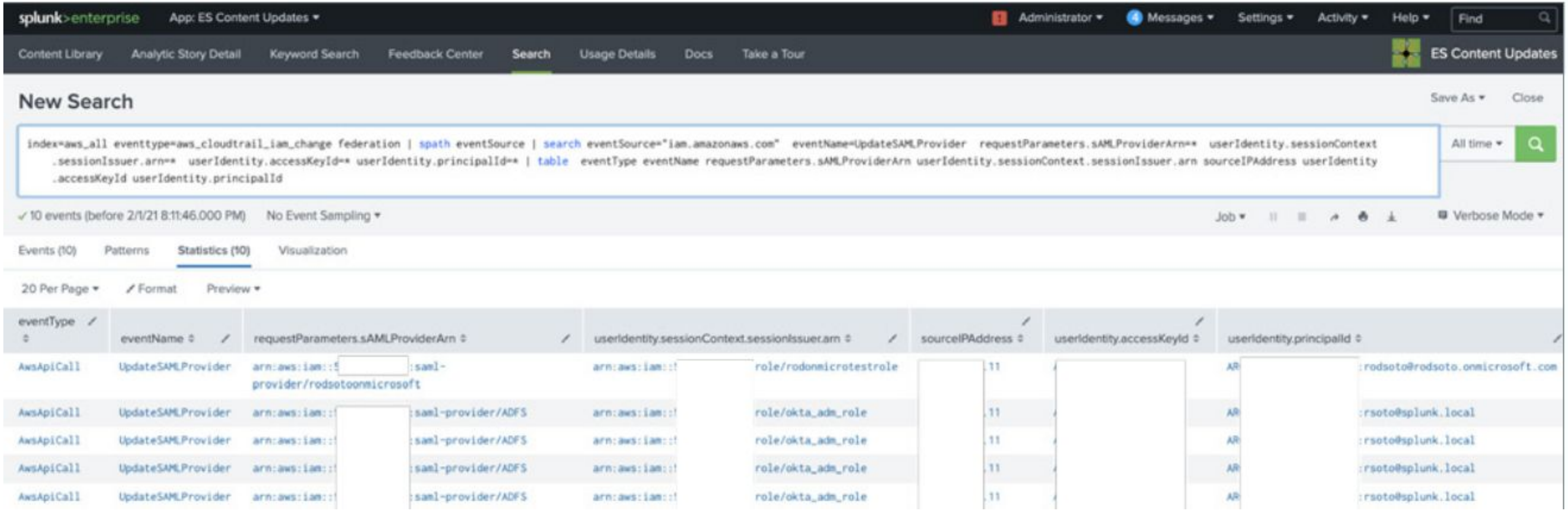
Name	Technique ID	Tactic	Note
Certutil.exe certificate extraction	T1552.004	Credential access	New detection
Uncommon Processes on endpoint	T1204.002	Execution	Helps detect ADFSDump
Registry keys used for privilege escalation	T1546.012	Privilege escalation, persistence	
Detect Mimikatz using loaded images	T1003.001	Credential access	
Detect Mimikatz via PowerShell and event code 4703	T1003.001	Credential access	

Detection by TTPs - Cloud



Name	Technique ID	Tactic	Provider
AWS SAML access by provider user and principal	T1078	Defense evasion, persistence, privilege escalation, initial access	AWS
AWS SAML update identity provider	T1078	Defense evasion, persistence, privilege escalation, initial access	AWS
O365 Excessive SSO logon errors	T1556	Credential access, defense evasion	Azure
O365 added service principal	T1136.003	Persistence	Azure
O365 added service principal	T1136.003	Persistence	Azure
O365 new federated domain added	T1136.003	Persistence	Azure

Investigation example - AWS update SAML provider



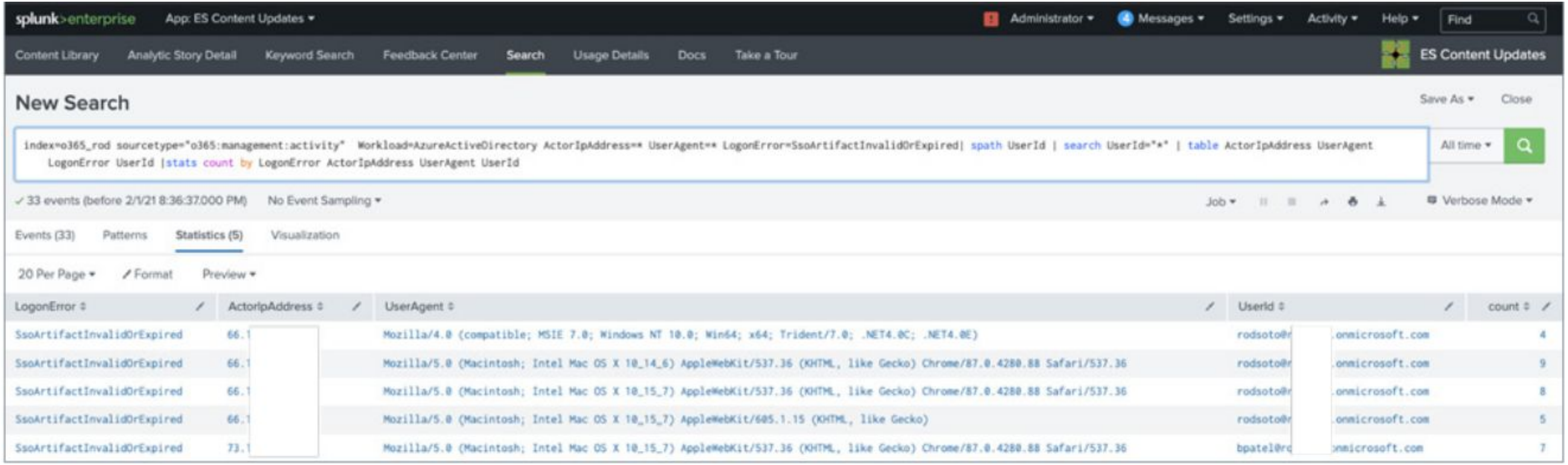
New Search

```
index=aws_all eventtype=aws_cloudtrail_iam_change federation | spath eventSource | search eventSource="iam.amazonaws.com"  eventName=UpdateSAMLProvider  requestParameters.sAMLProviderArn=*  userIdentity.sessionContext
    .sessionIssuer.arn=*  userIdentity.accessKeyId=* userIdentity.principalId=* | table  eventType eventName requestParameters.sAMLProviderArn userIdentity.sessionContext.sessionIssuer.arn sourceIPAddress userIdentity
    .accessKeyId userIdentity.principalId
```

✓ 10 events (before 2/1/21 8:11:46.000 PM)   No Event Sampling ▾

eventType	eventName	requestParameters.sAMLProviderArn	userIdentity.sessionContext.sessionIssuer.arn	sourceIPAddress	userIdentity.accessKeyId	userIdentity.principalId
AwsApiCall	UpdateSAMLProvider	arn:aws:iam::[redacted]:saml-provider/rodsotoonmicrosoft	arn:aws:iam::[redacted]role/rodonmicrotestrole	[redacted].11	[redacted]	AR[redacted]:rodsoto@rodsoto.onmicrosoft.com
AwsApiCall	UpdateSAMLProvider	arn:aws:iam::[redacted]:saml-provider/ADFS	arn:aws:iam::[redacted]role/okta_adm_role	[redacted].11	[redacted]	AR[redacted]:rsoto@splunk.local
AwsApiCall	UpdateSAMLProvider	arn:aws:iam::[redacted]:saml-provider/ADFS	arn:aws:iam::[redacted]role/okta_adm_role	[redacted].11	[redacted]	AR[redacted]:rsoto@splunk.local
AwsApiCall	UpdateSAMLProvider	arn:aws:iam::[redacted]:saml-provider/ADFS	arn:aws:iam::[redacted]role/okta_adm_role	[redacted].11	[redacted]	AR[redacted]:rsoto@splunk.local
AwsApiCall	UpdateSAMLProvider	arn:aws:iam::[redacted]:saml-provider/ADFS	arn:aws:iam::[redacted]role/okta_adm_role	[redacted].11	[redacted]	AR[redacted]:rsoto@splunk.local

Detection - excessive SSO errors



New Search

```
index=o365_rod sourcetype="o365:management:activity"  Workload=AzureActiveDirectory ActorIpAddress=* UserAgent=* LogonError=SsoArtifactInvalidOrExpired| spath UserId | search UserId="*" | table ActorIpAddress UserAgent
    LogonError UserId |stats count by LogonError ActorIpAddress UserAgent UserId
```

✓ 33 events (before 2/1/21 8:36:37.000 PM)   No Event Sampling ▾

LogonError	ActorIpAddress	UserAgent	UserId	count
SsoArtifactInvalidOrExpired	66.1[redacted]	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)	rodsoto@r[redacted].onmicrosoft.com	4
SsoArtifactInvalidOrExpired	66.1[redacted]	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	rodsoto@r[redacted].onmicrosoft.com	9
SsoArtifactInvalidOrExpired	66.1[redacted]	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	rodsoto@r[redacted].onmicrosoft.com	8
SsoArtifactInvalidOrExpired	66.1[redacted]	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko)	rodsoto@r[redacted].onmicrosoft.com	5
SsoArtifactInvalidOrExpired	73.1[redacted]	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	bpatel@rc[redacted]onmicrosoft.com	7

Q&A

@rodsoto

rodsoto.net