abstract.security

THE COMPLETE DATA PLATFORM FOR SECURITY

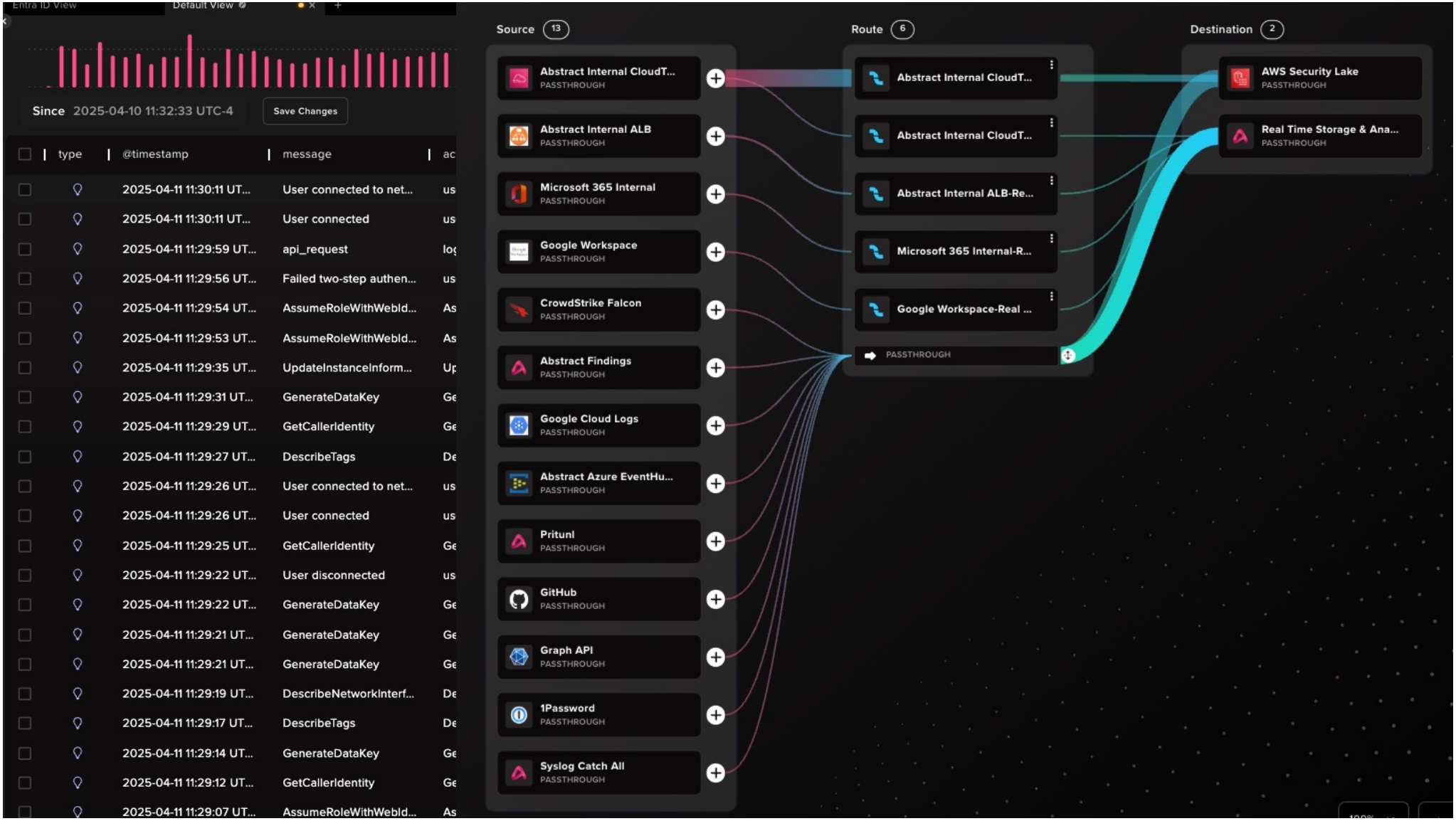
Guardians of the Cloud:

Proactive Policies for Securing the Cloud

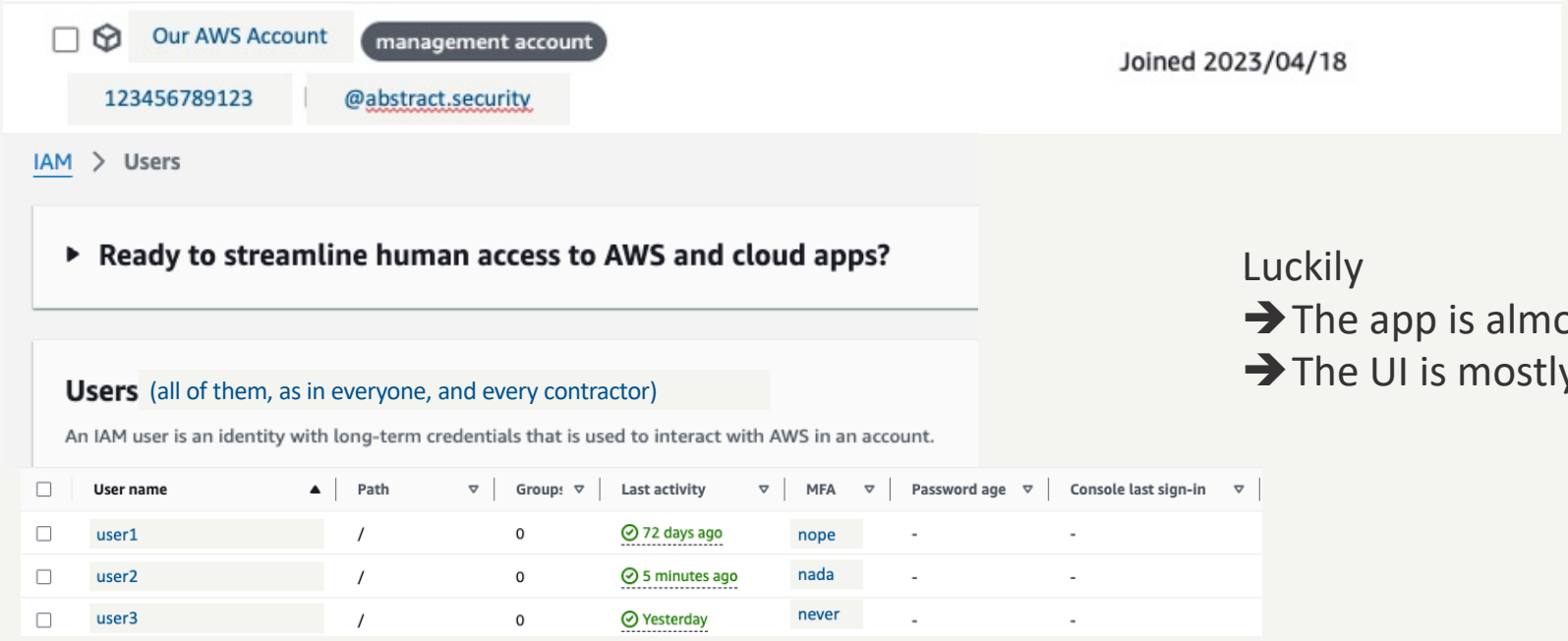
Aaron Shelmire
Co-Founder

Audience

- Security staff at Small to Mid Size Companies
- Large Enterprise – Nothing new here


Entra ID View
Default View
Since 2025-04-10 11:32:33 UTC-4
Save Changes
type
@timestamp
message
2025-04-11 11:30:11 UT... User connected to net...
2025-04-11 11:30:11 UT... User connected
2025-04-11 11:29:59 UT... api_request
2025-04-11 11:29:56 UT... Failed two-step authen...
2025-04-11 11:29:54 UT... AssumeRoleWithWebId...
2025-04-11 11:29:53 UT... AssumeRoleWithWebId...
2025-04-11 11:29:35 UT... UpdateInstanceInform...
2025-04-11 11:29:31 UT... GenerateDataKey
2025-04-11 11:29:29 UT... GetCallerIdentity
2025-04-11 11:29:27 UT... DescribeTags
2025-04-11 11:29:26 UT... User connected to net...
2025-04-11 11:29:26 UT... User connected
2025-04-11 11:29:25 UT... GetCallerIdentity
2025-04-11 11:29:22 UT... User disconnected
2025-04-11 11:29:22 UT... GenerateDataKey
2025-04-11 11:29:21 UT... GenerateDataKey
2025-04-11 11:29:21 UT... GenerateDataKey
2025-04-11 11:29:19 UT... DescribeNetworkInterf...
2025-04-11 11:29:17 UT... DescribeTags
2025-04-11 11:29:14 UT... GenerateDataKey
2025-04-11 11:29:12 UT... GetCallerIdentity
2025-04-11 11:29:07 UT... AssumeRoleWithWebId...
Source 13
Abstract Internal CloudT... PASSTHROUGH
Abstract Internal ALB PASSTHROUGH
Microsoft 365 Internal PASSTHROUGH
Google Workspace PASSTHROUGH
CrowdStrike Falcon PASSTHROUGH
Abstract Findings PASSTHROUGH
Google Cloud Logs PASSTHROUGH
Abstract Azure EventHu... PASSTHROUGH
Pritunl PASSTHROUGH
GitHub PASSTHROUGH
Graph API PASSTHROUGH
1Password PASSTHROUGH
Syslog Catch All PASSTHROUGH
Route 6
Abstract Internal CloudT...
Abstract Internal CloudT...
Abstract Internal ALB-Re...
Microsoft 365 Internal-R...
Google Workspace-Real ...
PASSTHROUGH
Destination 2
AWS Security Lake PASSTHROUGH
Real Time Storage & Ana... PASSTHROUGH

October ‘23



Luckily
➔ The app is almost all mocks
➔ The UI is mostly static images

AdministratorAccess -> As Far as the Eye Can See

On the Bright Side
➔ Everything is in IaC
➔ SecurityGroups on Everything

November

- EDR on all hosts.

- Separate AWS Accounts
- Org CloudTrail to S3
- SSO Identity Center
- WAF
- SAST Checking on PRs
- VPN
- Scan it all

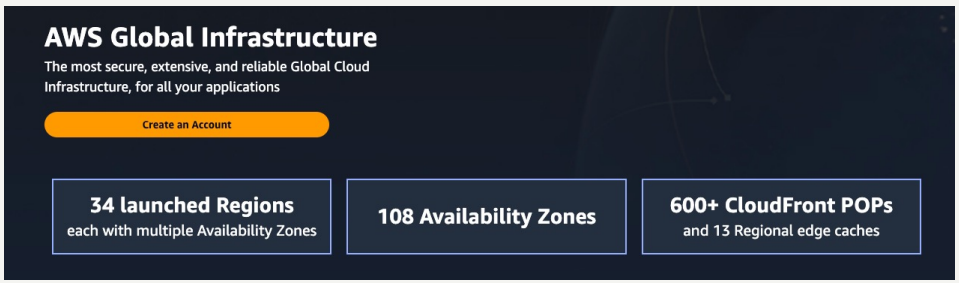
- Thanksgiving – we had thanks to give!

December – Plan: 1 big improvement a week

- New hire disappears w/ Laptop
- Re-appears with new version of our app …built in Vue.js…
- Negotiate -> Get Laptop Back, Repos Deleted
- **JumpCloud on all laptops.**

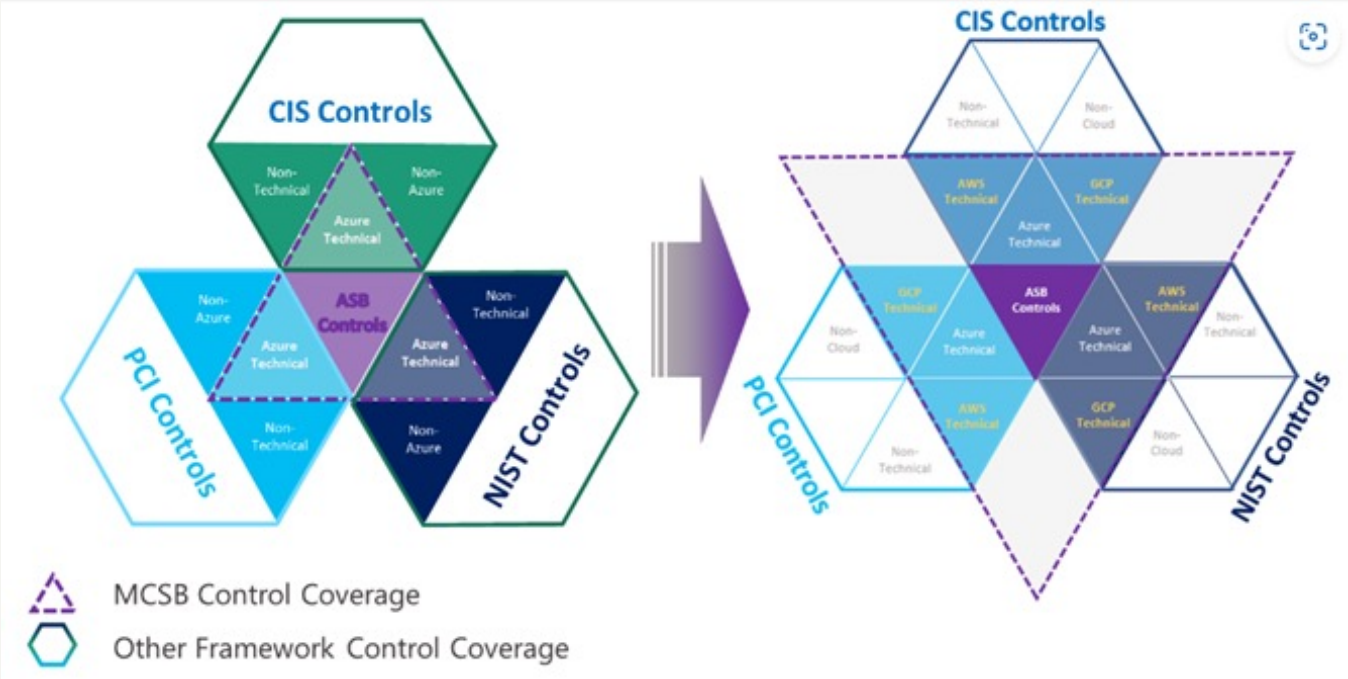

aws

CAF Category	Phase 1: Quick Wins	Phase 2: Foundational	Phase 3: Efficient	Phase 4: Optimized
Security governance	Assign Security contacts Select the region(s)	Identify security and regulatory requirements Cloud Security Training Plan	Perform threat modeling	Forming a Chaos Engineering (Resilience) Sharing security work and responsibility
Security assurance	Automate alignment with best practices using AWS Security Hub	Configuration monitoring with AWS Config	Create your reports for compliance (such as PCI-DSS)	
Identity and access management	Multi-Factor Authentication Avoid using Root and audit it Access and role analysis with IAM Access Analyzer	Centralized user repository Organization Policies - SCPs	Privilege review (Least Privilege) Tagging strategy Customer IAM: security of your customers	Context-based access control IAM Policy Generation Pipeline
Threat detection	Threat Detection with Amazon GuardDuty Audit API calls with AWS CloudTrail Remediate security findings found by AWS Trusted Advisor Billing alarms for anomaly detection	Investigate most Amazon GuardDuty findings	Integration with SIEM/SOAR Network Flows analysis (VPC Flow Logs)	Amazon Fraud Detector Integration with additional intelligence feeds
Vulnerability management		Manage vulnerabilities in your infrastructure and perform pentesting Manage vulnerabilities in your applications	Security Champions in Development	
Infrastructure protection	Limit access using Security Groups	Manage your instances with Fleet Manager Network segmentation - Public/Private Networks (VPCs) Multi-account management with AWS Control Tower	Image Generation Pipeline Anti-Malware/EDR Outbound Traffic Control Use abstract services	Process standardization with Service Catalog
Data protection	Amazon S3 Block Public Access Analyze data security posture with Amazon Macie	Data Encryption - AWS KMS Backups Discover sensitive data with Amazon Macie	Encryption in transit	
Application security	AWS WAF with managed rules	Involve security teams in development No secrets in your code - AWS Secrets Manager	WAF with custom rules Shield Advanced: Advanced DDoS Mitigation	DevSecOps Forming a Red Team (Attacker's Point of View)
Incident response	Act on Amazon GuardDuty findings	Define incident response playbooks - TableTop Exercises Redundancy using multiple Availability Zones	Automate critical and most frequently run Playbooks Automate deviation correction in configurations Using infrastructure as code (CloudFormation, CDK)	Automate most playbooks Amazon Detective: Root cause analysis Forming a Blue Team (Incident Response) Multi-region disaster recovery automation



- GuardDuty can cost $.10 - $.30 per day per region
- 34 regions
- $3792/yr for inactive regions

Azure Security Benchmark



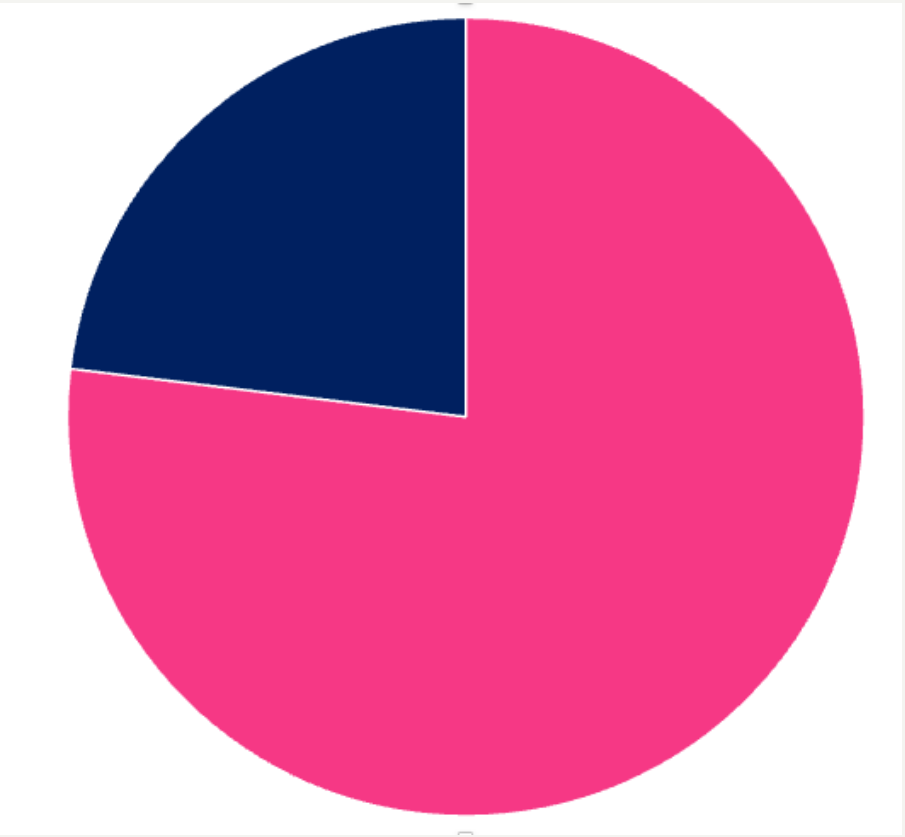
- Providing a **single control framework** to **easily meet** the **security controls** across clouds
- Providing consistent user experience for monitoring and enforcing the multi-cloud security benchmark in Defender for Cloud
- Staying aligned with Industry Standards (e.g., CIS, NIST, PCI)

Azure

Development Azure account

Average $10k/month

All Cloud Recommendations + $3,300k

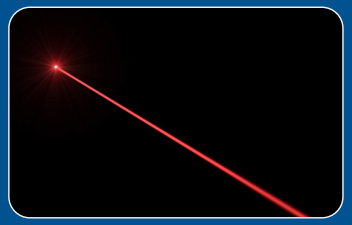



THERE'S GOT TO BE A
BETTER WAY

What if we…

Survey real threats

Limit Actions



Laser focus monitoring

What are the real Threats here

Bug Bounty Actors

- Most frequent and common
- Fake Bug Bounties – new to me…

Ransomware & Extortion

- Dis-Organized and Organized Groups
- Fast Moving, Highly Destructive

Resource Theft or Exhaustion

- Access to some privileged token
- Cryptomine or Run up your bill

Exposed Data

- Whoops someone published it out
- Website with debug flags on

What are the real Threats here

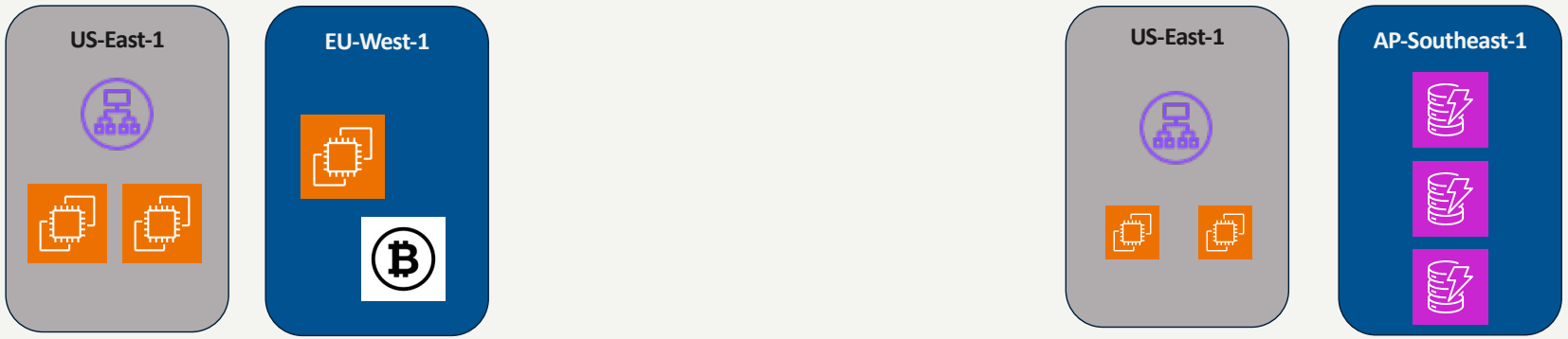
Bug Bounty Actors

- Most frequent and common
- Fake Bug Bounties – new to me…

Ransomware & Extortion

- Dis-Organized and Organized Groups
- Fast Moving, Highly Destructive

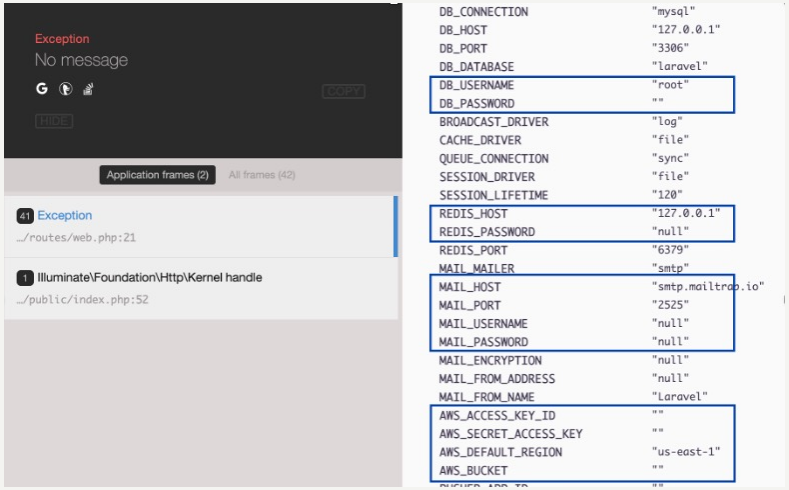
What are the real Threats here



Resource Theft or Exhaustion

- Access to some privileged token
- Cryptomine or Run up your bill

What are the real Threats here



Exposed Data

- Whoops someone published it out
- Website with debug flags on

What are the real Threats here

Bug Bounty Actors

- Most frequent and common
- Fake Bug Bounties – new to me…

Ransomware & Extortion

- Dis-Organized and Organized Groups
- Fast Moving, Highly Destructive

Resource Theft or Exhaustion

- Access to some privileged token
- Cryptomine or Run up your bill

Exposed Data

- Whoops someone published it out
- Website with debug flags on

How do we Protect our resources and Limit Attack Surface

Protect

Service Control Policies & Azure Policies

- Limit Risky Actions
- Limit Regions

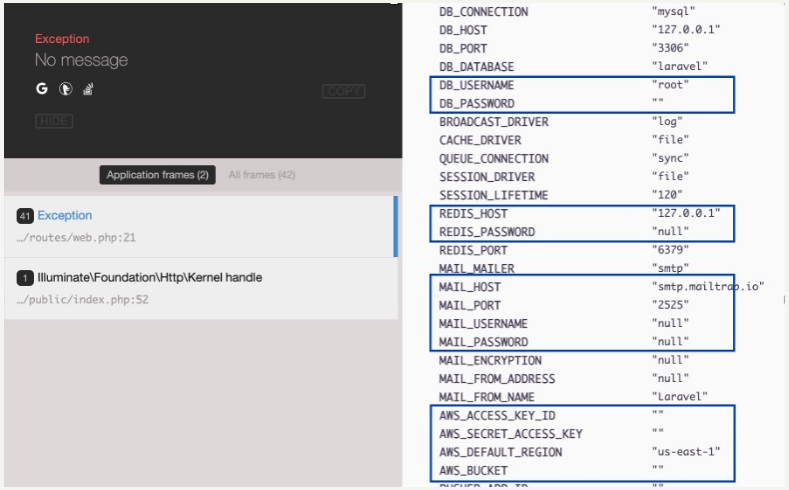
- Limit Services
- Standardized Resource Policies (tagging)

- Require MFA for resource deletion
- Prevent Disabling Controls and Monitoring

- Deny peering (SAML / IDP / VPC)
- Deny Internet Gateway Creation

AWS Protection

The real Threats



Exposed Data

- Whoops someone published it out
- Website with debug flags on

Protect: public disclosure whoops & Account Takeover

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:LeaveOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "account:PutContactInformation",
        "account:PutChallengeQuestions",
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:CloseAccount",
        "billing:UpdateBillingPreferences",
        "billing:PutContractInformation",
        "billing:UpdateIAMAccessPreference",
        "invoicing:PutInvoiceEmailD
        "payments:DeletePaymentInst
        "payments:UpdatePaymentPref
        "tax:BatchPutTaxRegistratio
        "tax:DeleteTaxRegistration"
        "tax:PutTaxInheritance"
      ],
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutBucketPublicAccessBlock",
        "s3:PutAccountPublicAccessBlock"
      ],
      "Resource": "*",
      "Effect": "Deny"
    }
  ]
}
```

Protect

Service Control Policies & Azure Policies

- **Limit Risky Actions**
- Deny Internet Gateway Creation

- Deny peering (SAML / IDP / VPC)
- Standardized Resource Policies (tagging)

- Limit Regions
- Limit Services

- Require MFA for resource deletion
- Prevent Disabling Controls and Monitoring

Protect: shield dev sites from public

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictVPCPeering",
      "Action": [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:CreateVpcPeeringConnection"
      ],
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
```

Protect

Service Control Policies & Azure Policies

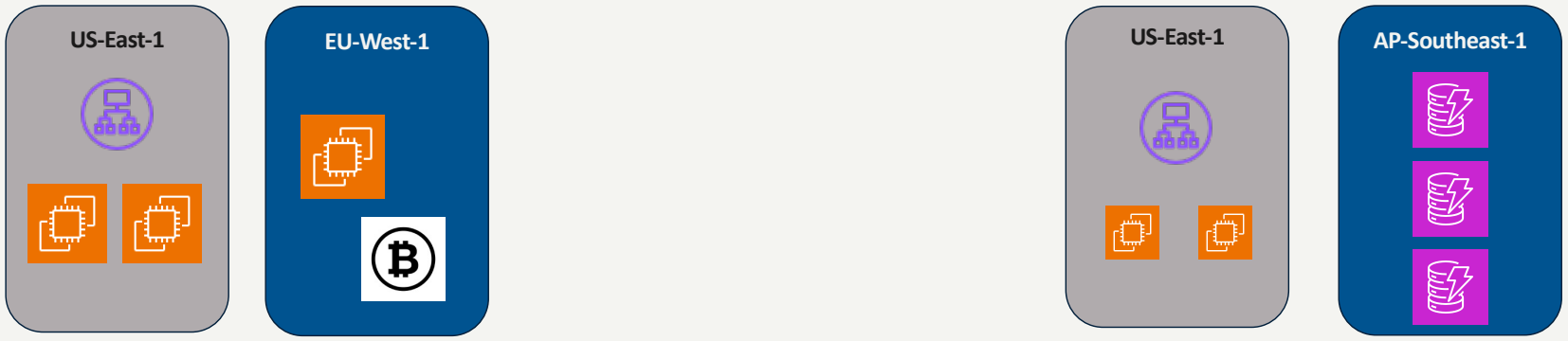
- Limit Risky Actions
- **Deny Internet Gateway Creation**

- **Deny peering (SAML / IDP / VPC)**
- Standardized Resource Policies (tagging)

- Limit Regions
- Limit Services

- Require MFA for resource deletion
- Prevent Disabling Controls and Monitoring

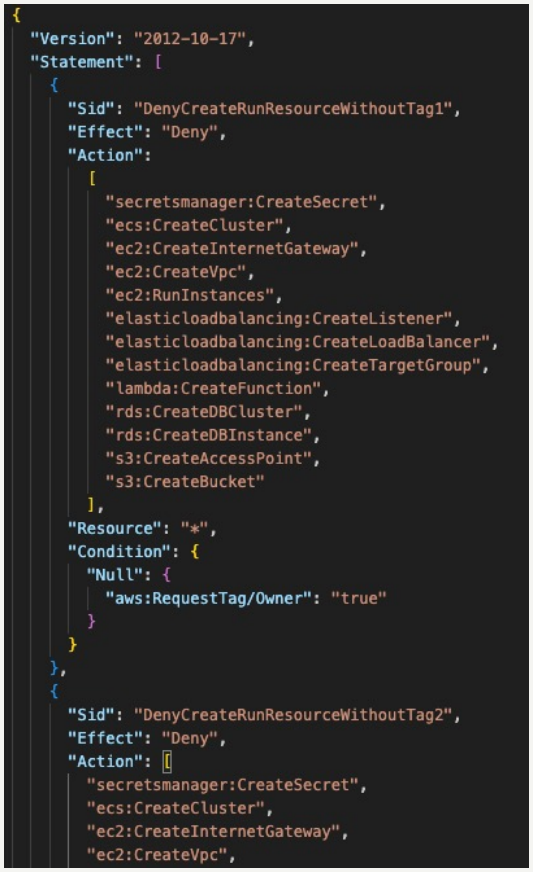
The real Threats



Resource Theft or Exhaustion

- Access to some privileged token
- Cryptomine or Run up your bill

Protect: provides easier response & frustrates actors



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateRunResourceWithoutTag1",
      "Effect": "Deny",
      "Action":
        [
          "secretsmanager:CreateSecret",
          "ecs:CreateCluster",
          "ec2:CreateInternetGateway",
          "ec2:CreateVpc",
          "ec2:RunInstances",
          "elasticloadbalancing:CreateListener",
          "elasticloadbalancing:CreateLoadBalancer",
          "elasticloadbalancing:CreateTargetGroup",
          "lambda:CreateFunction",
          "rds:CreateDBCluster",
          "rds:CreateDBInstance",
          "s3:CreateAccessPoint",
          "s3:CreateBucket"
        ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Owner": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateRunResourceWithoutTag2",
      "Effect": "Deny",
      "Action": [
        "secretsmanager:CreateSecret",
        "ecs:CreateCluster",
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
```

Protect

Service Control Policies & Azure Policies

- Limit Risky Actions
- Deny Internet Gateway Creation

- Deny peering (SAML / IDP / VPC)
- **Standardized Resource Policies (tagging)**

- Limit Regions
- Limit Services

- Require MFA for resource deletion
- Prevent Disabling Controls and Monitoring

Protect: reduce monitor costs & focus attention

1. Limit Ability to Enable Regions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource": "*"
    }
  ]
}
```

34

17 regions still enabled

2. Limit Actions to Specific Regions

```
    ],
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "aws:RequestedRegion": [
          "us-east-1",
          "us-east-2",
          "us-west-1",
          "us-west-2",
          "eu-west-1",
          "us-west-2"
        ]
      },
```

Protect

Service Control Policies & Azure Policies

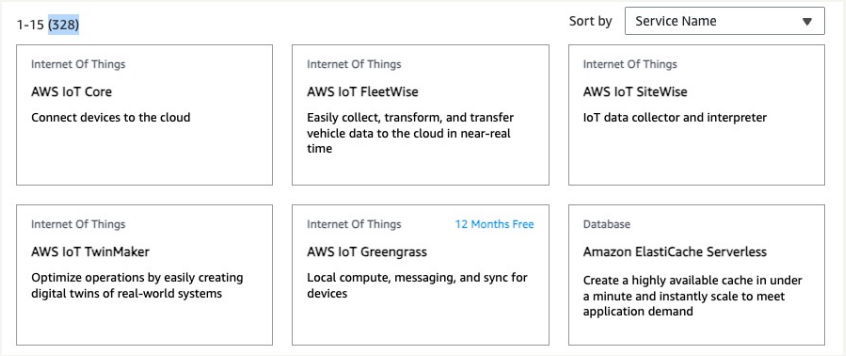
- Limit Risky Actions
- Deny Internet Gateway Creation

- Deny peering (SAML / IDP / VPC)
- Standardized Resource Policies (tagging)

- **Limit Regions**
- Limit Services

- Require MFA for resource deletion
- Prevent Disabling Controls and Monitoring

How should we Protect our resources



There are 328 Services in AWS

Protect

Service Control Policies & Azure Policies

- Limit Risky Actions
- Deny Internet Gateway Creation

- Deny peering (SAML / IDP / VPC)
- Standardized Resource Policies (tagging)

- Limit Regions
- **Limit Services**

- Require MFA for resource deletion
- Prevent Disabling Controls and Monitoring

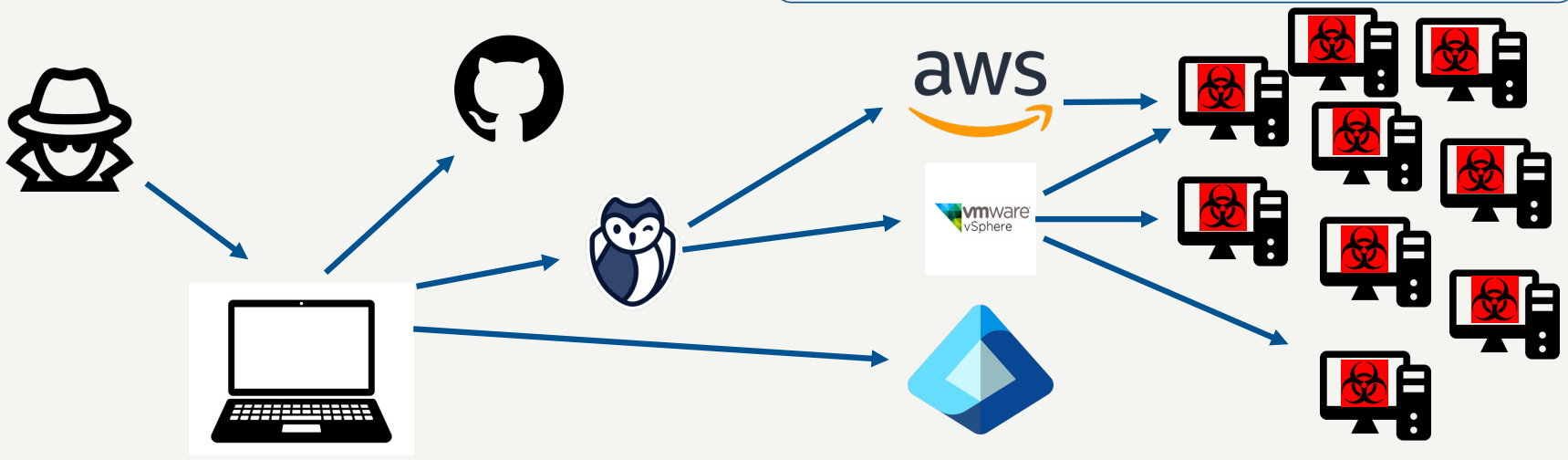
The real Threats: Ransomware & Extortion

Bug Bounty Actors

- Most frequent and common
- Fake Bug Bounties – new to me…

Ransomware & Extortion

- Dis-Organized and Organized Groups
- Fast Moving, Highly Destructive



Protect: prevents stopping resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "autoscaling:DeleteAutoScalingGroup",
        "cloudwatch:DeleteAlarms",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ecs:DeleteCluster",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBCluster"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Protect

Service Control Policies & Azure Policies

- Limit Risky Actions
- Deny Internet Gateway Creation

- Deny peering (SAML / IDP / VPC)
- Standardized Resource Policies (tagging)

- Limit Regions
- Limit Services

- **Require MFA for resource deletion**
- Prevent Disabling Controls and Monitoring

Protect: maintain visibility

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudtrail:DeleteTrail",
        "cloudtrail:PutEventSelectors",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail"
      ],
```

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty:DeleteDetector",
    "guardduty:DeleteFilter",
    "guardduty:DeleteInvitations",
    "guardduty:DeleteIPSet",
    "guardduty:DeleteMembers",
```

Protect

Service Control Policies & Azure Policies

- Limit Risky Actions
- Deny Internet Gateway Creation

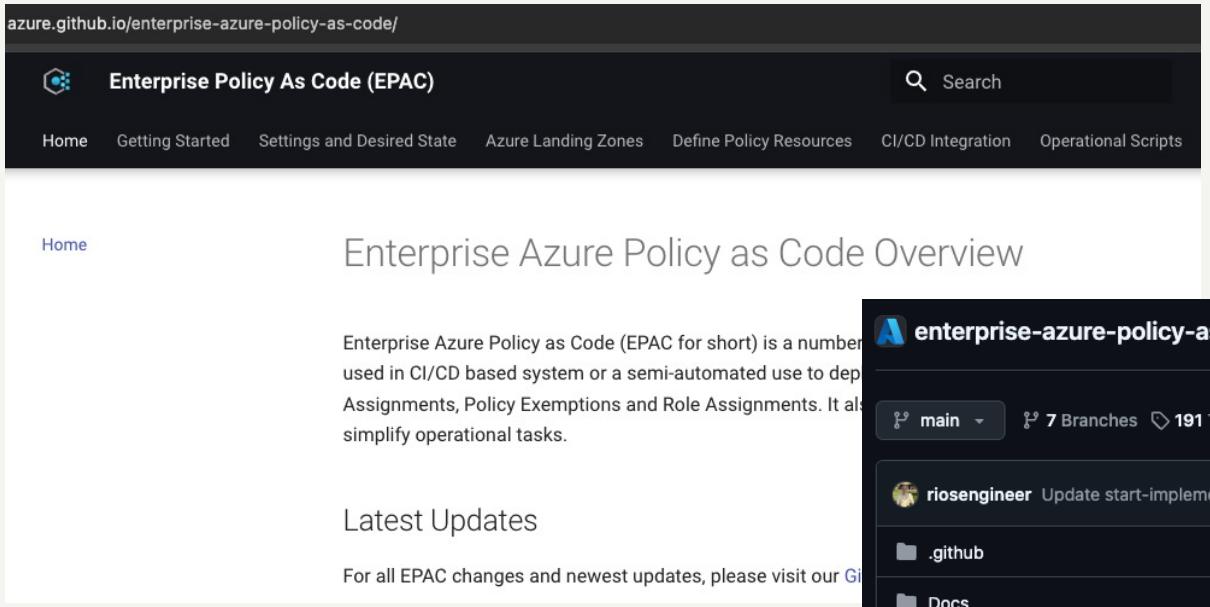
- Deny peering (SAML / IDP / VPC)
- Standardized Resource Policies (tagging)

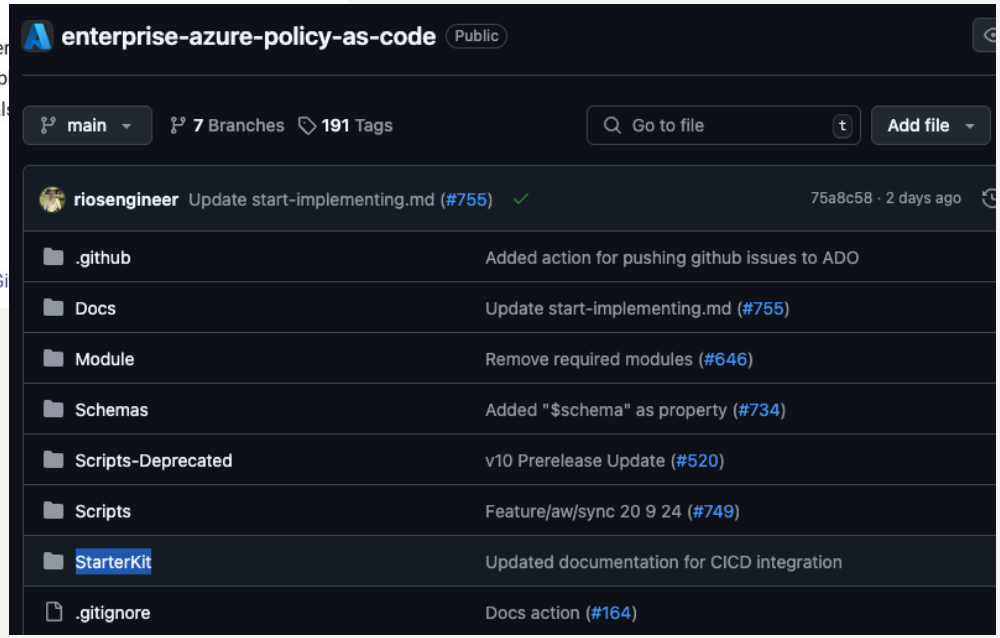
- Limit Regions
- Limit Services

- Require MFA for resource deletion
- **Prevent Disabling Controls and Monitoring**

Azure

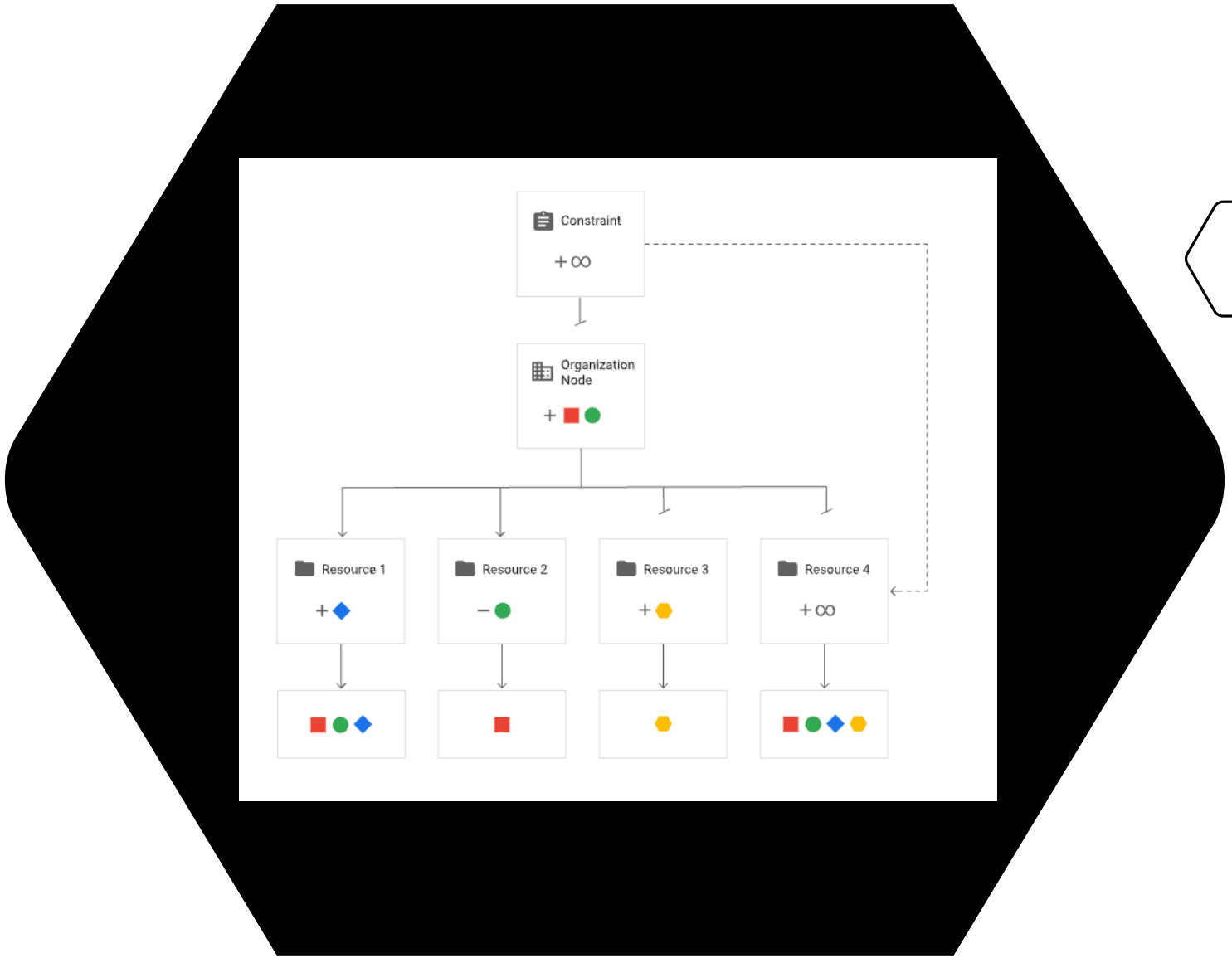
Azure Enterprise Policy As Code





Smaller Organizations

- While designed for medium and large Enterprises, EPAC can and should be used by small organizations implementing fully-automated DevOps deployments of every Azure resource (known as Infrastructure as Code). Your DevOps maturity level will be well suited for EPAC.
- If your DevOps (CI/CD) maturity is lower, Azure Landing Zones direct implementation of Policies might be a better choice.
- For extremely small Azure customers with one or two subscriptions Microsoft Defender for Cloud automated Policy Assignments for built-in Policies is sufficient.


Constraint
+∞
Organization Node
+
Resource 1
+
Resource 2
−
Resource 3
+
Resource 4
+∞

Policies Gotchas

AWS

- 5 SCPs
- Definitions
- Default Regions and Services
- Don’t block iam:*

GCP

- Limit Regions
- InheritFromParent = False
- Policy Conflicts
- RestoreDefault

Azure

- 500 Policies!
- 2,500 definitions
- Deny Resources not actions
- Not fully implemented

SOC2 (Type 2) Compliant

Received our Type 2 on Monday!!!


Yesterday
Steven Montalbano 8:17 PM
do you have god mode in our gcp organization?
I'm trying to deploy sentinel one and running into a policy that needs to be disabled and I dont have the access to do so

- Cloud Security Frameworks are way too complex and cost far too much

- Reduction, Standardization, and Simplification offer a better way

- Implement these controls
  - Focus your attention