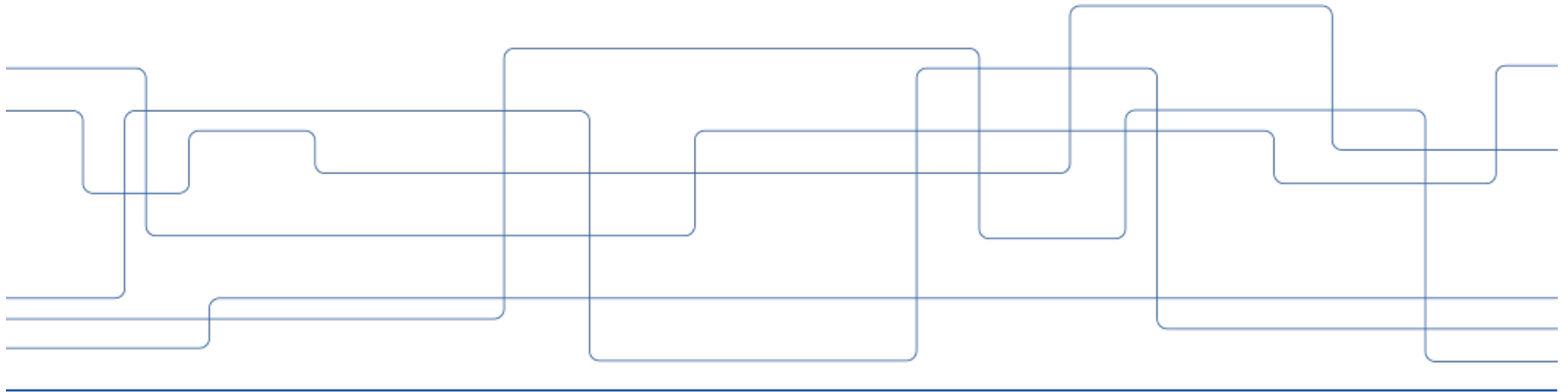




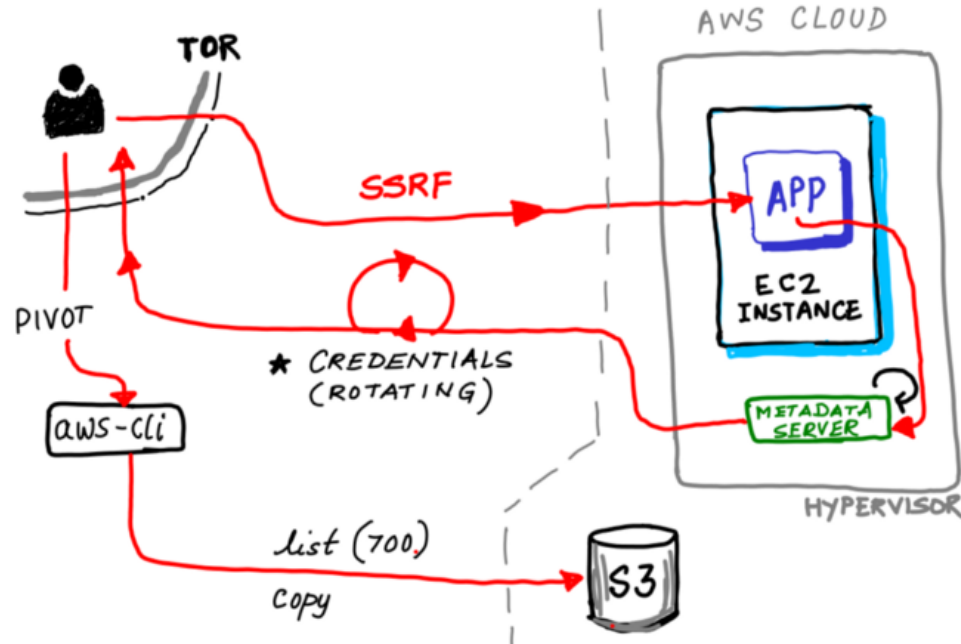
# CYBER SECURITY ASSESSMENT WITH ATTACK SIMULATIONS

Pontus Johnson

Professor



# Capital One Breach in Amazon AWS



Informal attack graph



# Risky Business Podcast on July 31, 2019



Adam Boileau & Patrick Gray



<https://risky.biz/RB550/>

# Risky Business Podcast on July 31, 2019



Adam Boileau & Patrick Gray

"Capital One are known for being really smart when it comes to this stuff, so when you see them getting owned by an attacker who falls into the category of Internet jerk, it does give you a moment."

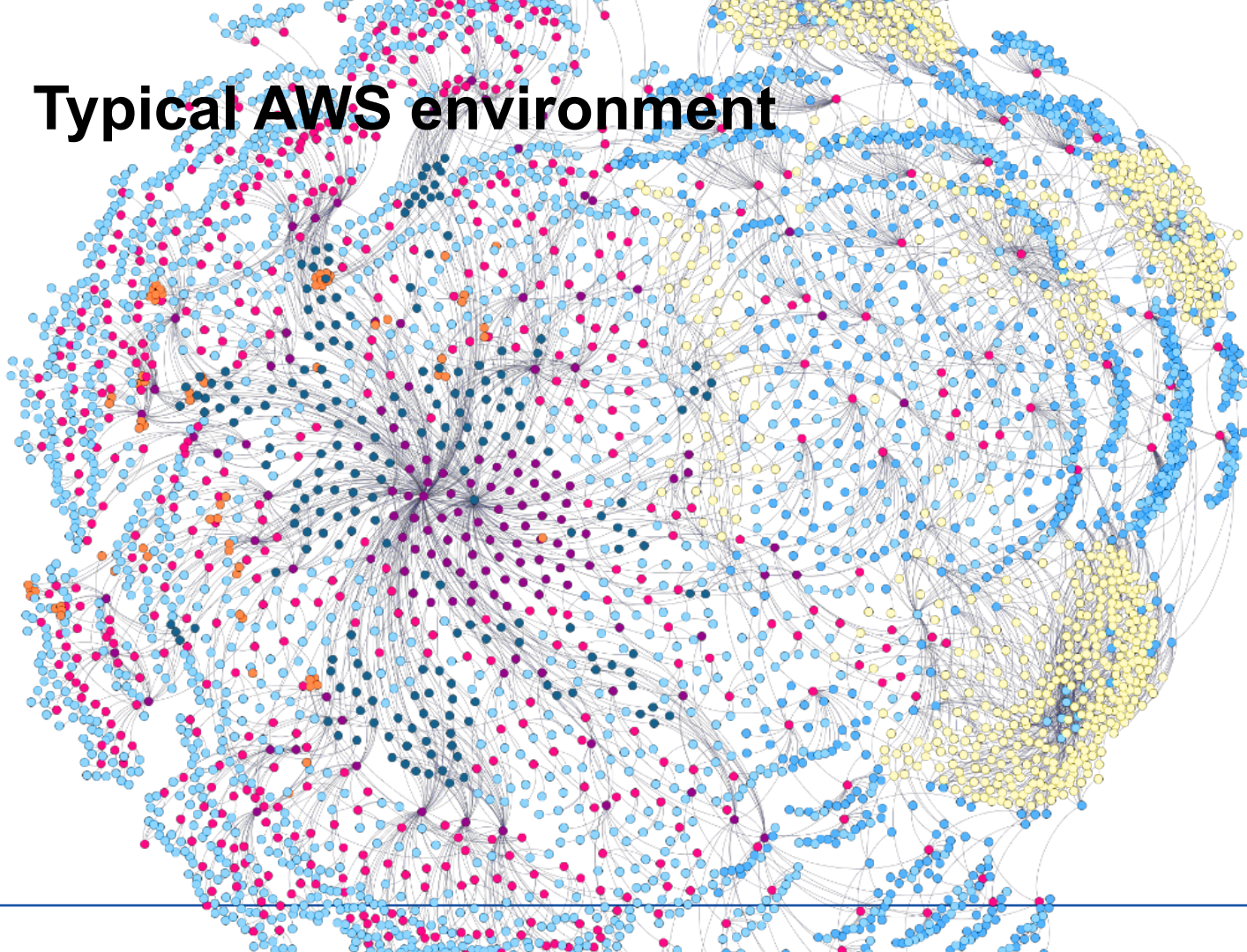
"Yes, part of the problem is that the Amazon product setup really is super complicated. You can build all sorts of amazing things at really big scale but doing it right consistently is really, really hard."

"A company that has some of the best people in the business for doing this stuff still got popped via their Amazon stuff because it is so complicated."



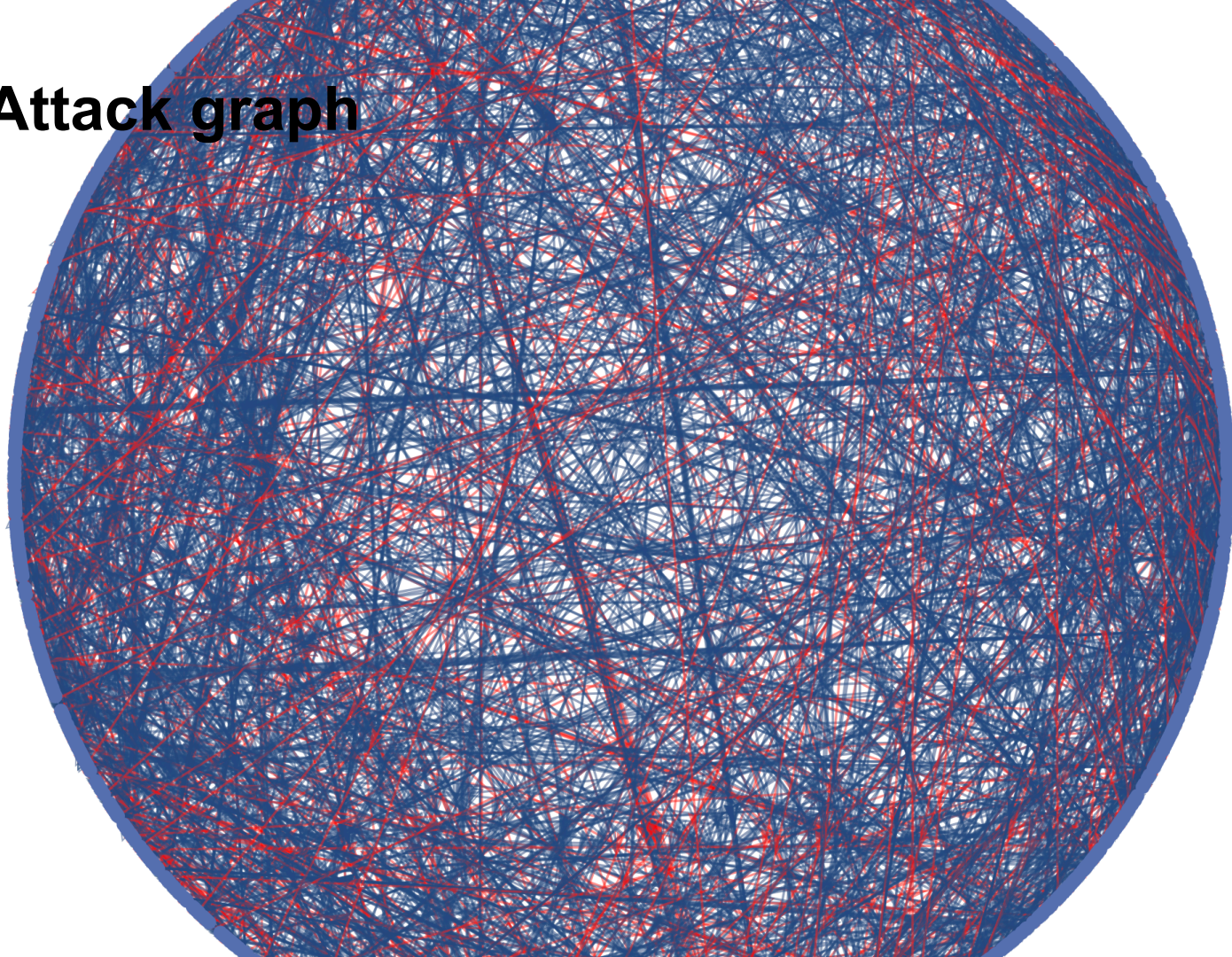


# Typical AWS environment





# Attack graph



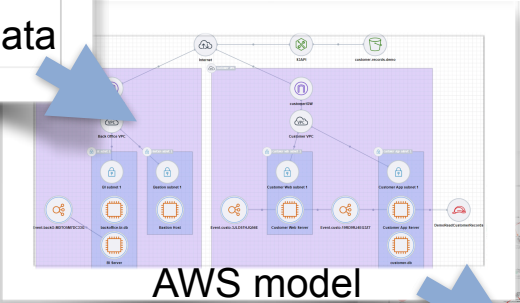


# Simulating cyber attacks

## Simulation results

The shortest paths an attacker can use to compromise assets of value

AWS config data  
& vuln scan



Attack graph

Shortest paths

The easiest way for an attacker to reach the most valuable assets

Mitigation	
Asset	Mitigation
Asset 1	Mitigation 1
Asset 2	Mitigation 2
Asset 3	Mitigation 3
Asset 4	Mitigation 4
Asset 5	Mitigation 5
Asset 6	Mitigation 6
Asset 7	Mitigation 7
Asset 8	Mitigation 8
Asset 9	Mitigation 9
Asset 10	Mitigation 10
Asset 11	Mitigation 11
Asset 12	Mitigation 12
Asset 13	Mitigation 13
Asset 14	Mitigation 14
Asset 15	Mitigation 15
Asset 16	Mitigation 16
Asset 17	Mitigation 17
Asset 18	Mitigation 18
Asset 19	Mitigation 19
Asset 20	Mitigation 20
Asset 21	Mitigation 21
Asset 22	Mitigation 22
Asset 23	Mitigation 23
Asset 24	Mitigation 24
Asset 25	Mitigation 25
Asset 26	Mitigation 26
Asset 27	Mitigation 27
Asset 28	Mitigation 28
Asset 29	Mitigation 29
Asset 30	Mitigation 30
Asset 31	Mitigation 31
Asset 32	Mitigation 32
Asset 33	Mitigation 33
Asset 34	Mitigation 34
Asset 35	Mitigation 35
Asset 36	Mitigation 36
Asset 37	Mitigation 37
Asset 38	Mitigation 38
Asset 39	Mitigation 39
Asset 40	Mitigation 40
Asset 41	Mitigation 41
Asset 42	Mitigation 42
Asset 43	Mitigation 43
Asset 44	Mitigation 44
Asset 45	Mitigation 45
Asset 46	Mitigation 46
Asset 47	Mitigation 47
Asset 48	Mitigation 48
Asset 49	Mitigation 49
Asset 50	Mitigation 50
Asset 51	Mitigation 51
Asset 52	Mitigation 52
Asset 53	Mitigation 53
Asset 54	Mitigation 54
Asset 55	Mitigation 55
Asset 56	Mitigation 56
Asset 57	Mitigation 57
Asset 58	Mitigation 58
Asset 59	Mitigation 59
Asset 60	Mitigation 60
Asset 61	Mitigation 61
Asset 62	Mitigation 62
Asset 63	Mitigation 63
Asset 64	Mitigation 64
Asset 65	Mitigation 65
Asset 66	Mitigation 66
Asset 67	Mitigation 67
Asset 68	Mitigation 68
Asset 69	Mitigation 69
Asset 70	Mitigation 70
Asset 71	Mitigation 71
Asset 72	Mitigation 72
Asset 73	Mitigation 73
Asset 74	Mitigation 74
Asset 75	Mitigation 75
Asset 76	Mitigation 76
Asset 77	Mitigation 77
Asset 78	Mitigation 78
Asset 79	Mitigation 79
Asset 80	Mitigation 80
Asset 81	Mitigation 81
Asset 82	Mitigation 82
Asset 83	Mitigation 83
Asset 84	Mitigation 84
Asset 85	Mitigation 85
Asset 86	Mitigation 86
Asset 87	Mitigation 87
Asset 88	Mitigation 88
Asset 89	Mitigation 89
Asset 90	Mitigation 90
Asset 91	Mitigation 91
Asset 92	Mitigation 92
Asset 93	Mitigation 93
Asset 94	Mitigation 94
Asset 95	Mitigation 95
Asset 96	Mitigation 96
Asset 97	Mitigation 97
Asset 98	Mitigation 98
Asset 99	Mitigation 99
Asset 100	Mitigation 100

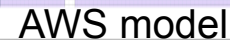
Mitigations

## conforms

(Meta-Attack Language)

# AWS Model Lang

# AWS config data & vuln scan



# AWS Domain-Specific Language (DSL) in MAL

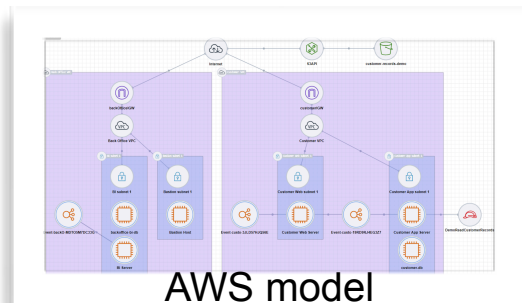
```
[...]  
asset EC2Instance extends Instance  
{  
}  
[...]  
asset S3Bucket extends Resource  
{  
[...]  
}  
[...]  
associations {  
S3Bucket [s3Bucket] 1 <-- Storage --> * [s3Objects] S3Object  
[...]
```



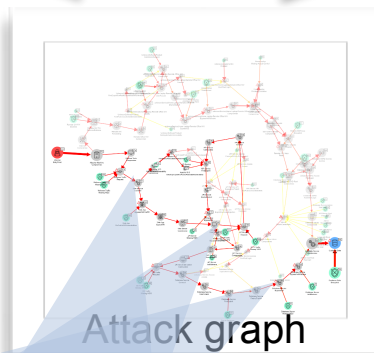
# Attack graph generation



AWS Model Lang

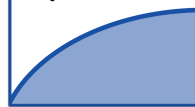


AWS model



Attack graph

Local time to  
compromise



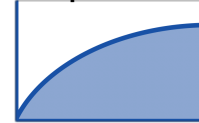


# AWS Domain-Specific Language (DSL) in MAL

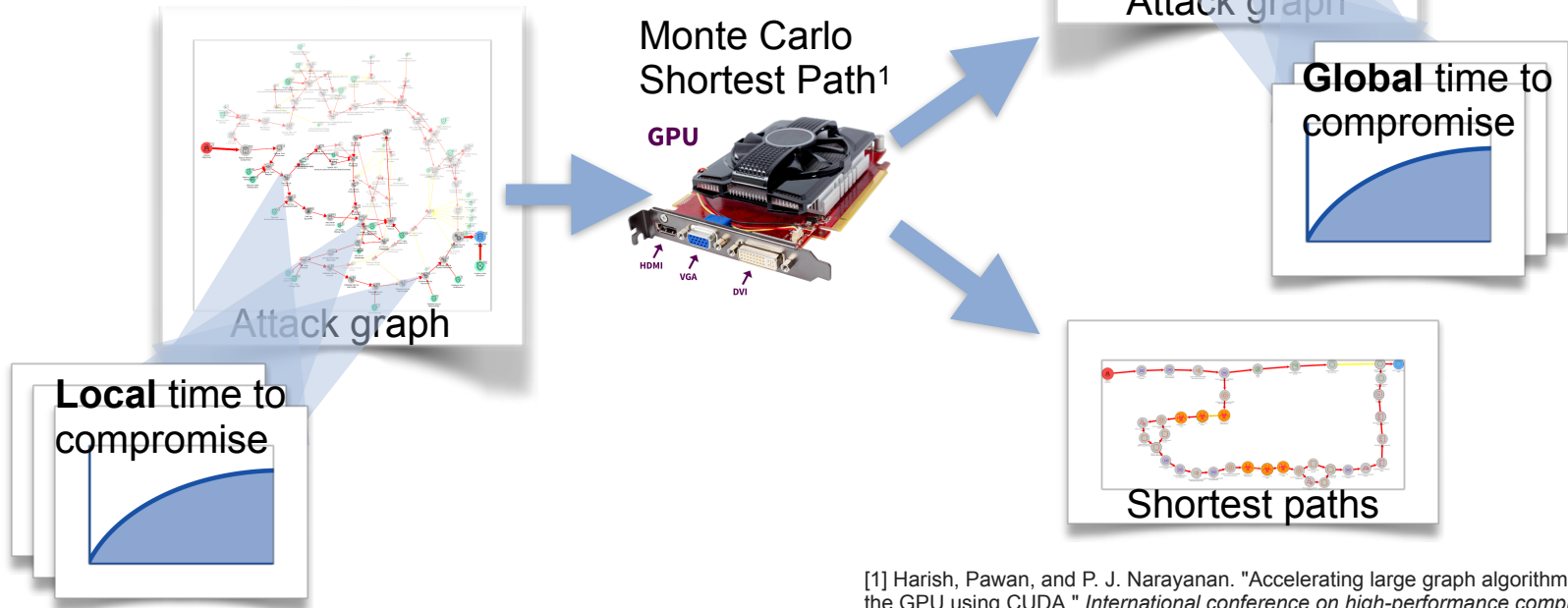
```
asset IAMIdentity extends Identity
{
  | assume
  -> policies.satisfy,
    statements.satisfy,
  [...]

  abstractAsset HighComplexityVulnerability extends Vulnerability
  {
    & abuse [ExponentialDistribution(x_hcv)]
    -> exploits.impact
  }
  [...]
```

Local time to  
compromise



# Attack graph computation



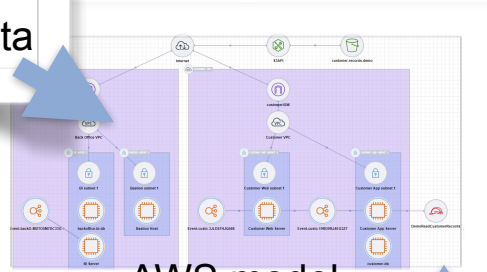
[1] Harish, Pawan, and P. J. Narayanan. "Accelerating large graph algorithms on the GPU using CUDA." *International conference on high-performance computing*. Springer, Berlin, Heidelberg, 2007.



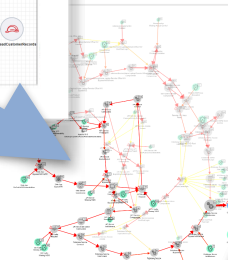


# AWS config data & vuln scan

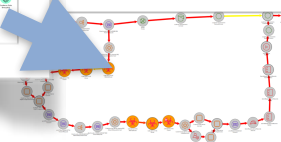
# AWS config data & vuln scan



## AWS model



## Attack graph




## Shortest paths

[illegible]

# Mitigations

Home About Learn more Who uses MAL? **Get Started**



# MAL

## Meta Attack Language

*The open source platform for creation of cyber threat modeling systems*

**Get Started →**

<https://mal-lang.org>