How UI/UX Impact SOC Performance

Bruce Potter - CEO, Turngate gdead@turngate.io

#whoami

Don’t believe anything I say

- College dropout
- Can’t code
- No certs

30 years of cybersecurity experience

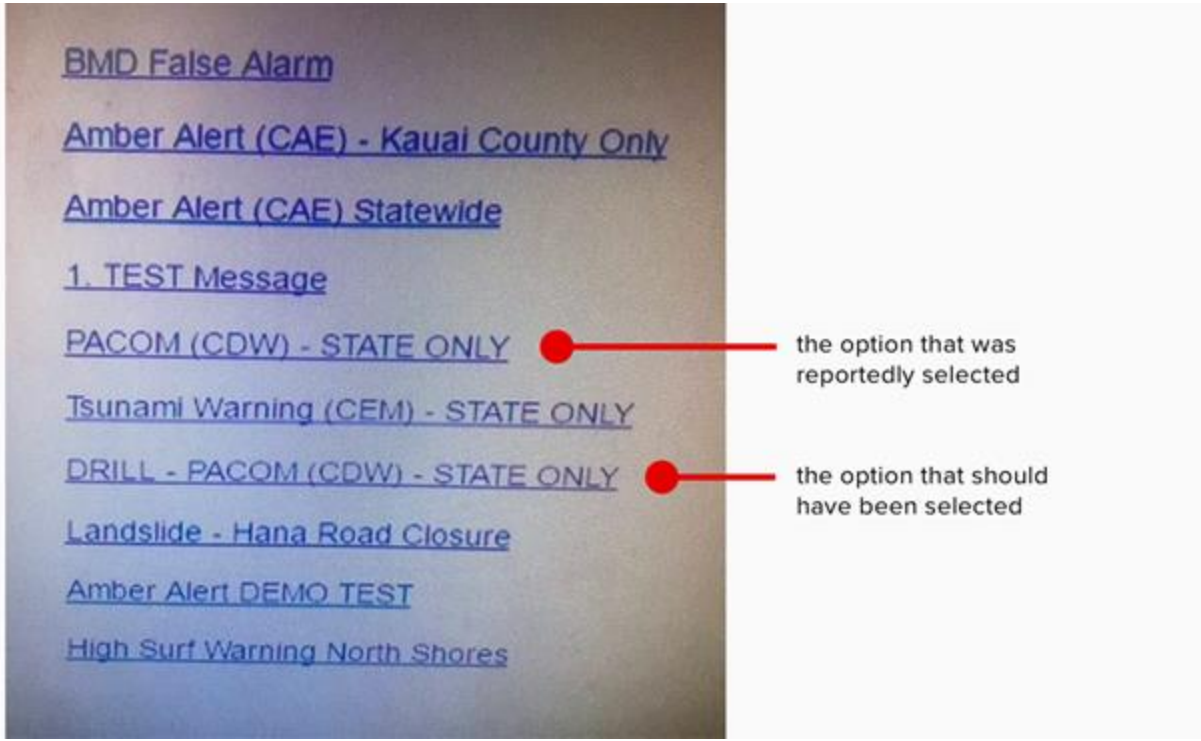
Run some companies, was a CISO a few times

Serve as Riker to ShmooCon’s Picard (Heidi)

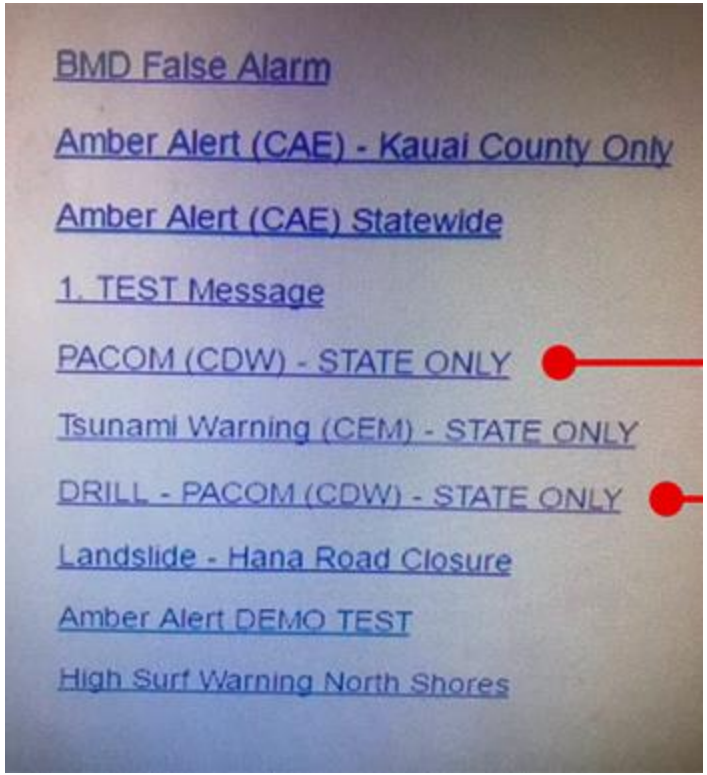
Currently CEO of Turngate, a SaaS and AI security operations product company

Why is UI/UX important?

The Offending Menu



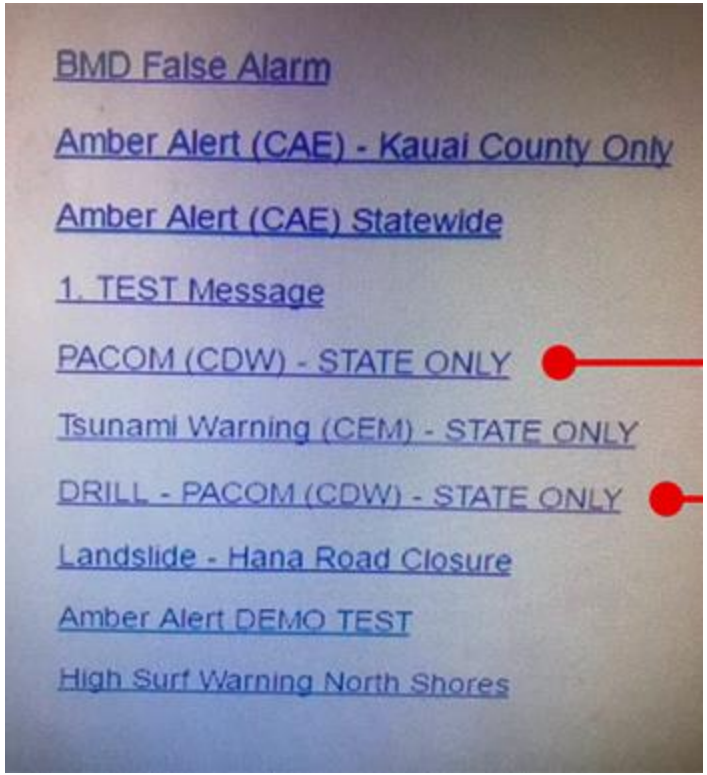
Put On Your Designer Hat and Dig In…



Categories of information represented:

- Plain Language Alert Name (*Amber, Tsunami, Thermonuclear War, etc*)
- Type of Alert (*Civil Defense, Child Abduction Emg., Civil Emergency Message*)
- Who will get the alert (*the whole state, Just a county, etc)*
- Status (*Real, Drill, "Oops, our bad"*)

Put On Your Designer Hat and Dig In…



How the information is represented:

- ALL CAPS
- Title Caps
- A single numbered bullet for some reason
- With the alert type and without the alert type
- Drills may be labeled as DRILL, DEMO TEST, TEST
- All fields are optional
  - $PlainName
  - $PlainName DEMO TEST
  - DRILL - $AlertType - $WhoGetsIt
  - 1. TEST Message

Fixing the Hawaii Emergency Alert System

First, build a simple Ontology of all alerts

Plain English Alert Name	Alert Type	Status	Recipient

Fixing the Hawaii Emergency Alert System

Next, build your list of alerts

Plain English Alert Name	Alert Type	Status	Recipient
Amber Alert	CAE	Live	Statewide
Amber Alert	CAE	Live	Kauai County
Amber Alert	CAE	Demo	Statewide
Amber Alert	CAE	Demo	Kauai County
False Alarm	BMD	Live	Statewide
High Surf Warning	CEM	Live	North Shores
And so on…			

Fixing the Hawaii Emergency Alert System

Now, decide on how to display the alerts

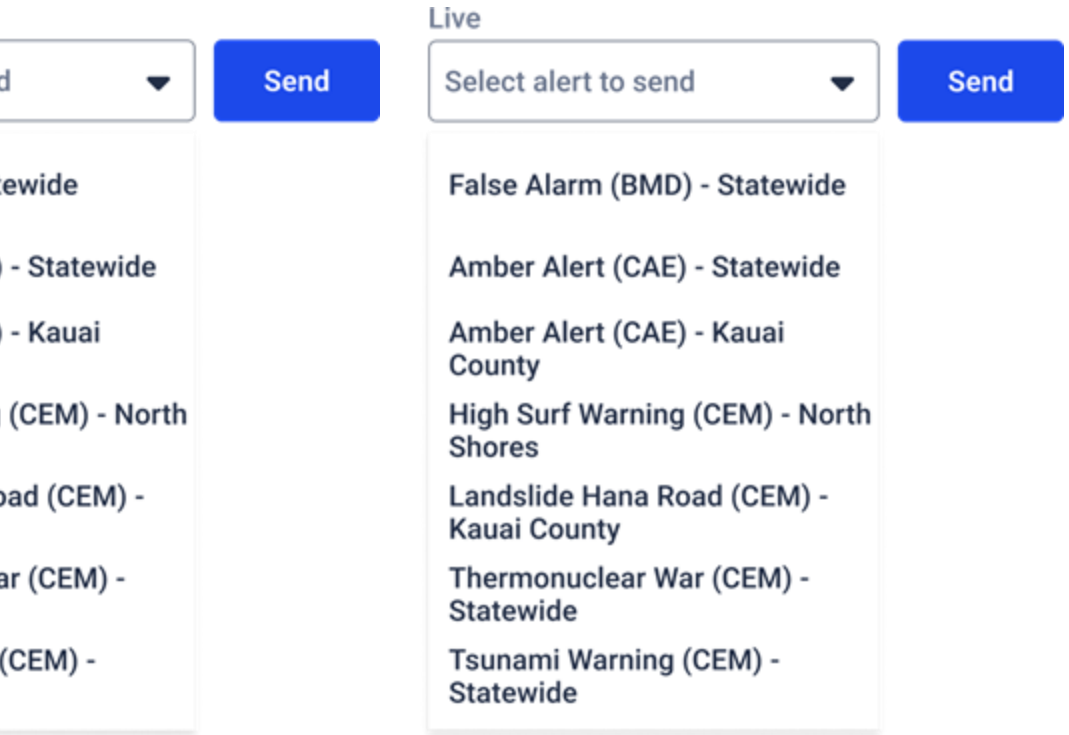
- Two menus (Demo and Live)
- All alerts have the same syntactic structure

  $PlainName ($Type) - $Recipient

All alerts requests generate an example alert with the exact wording. Alerts require positive affirmation of the user to be sent.

Plain English Alert Name	Alert Type	Status	Recipient
Amber Alert	CAE	Live	Statewide
Amber Alert	CAE	Live	Kauai County
Amber Alert	CAE	Demo	Statewide
Amber Alert	CAE	Demo	Kauai County
False Alarm	BMD	Live	Statewide
High Surf Warning	CEM	Live	North Shores
And so on…			

New and Improved Hawaii EAS Interface



Name this movie

Kujan:

It was Keaton's idea to rob the taxi service, wasn't it?

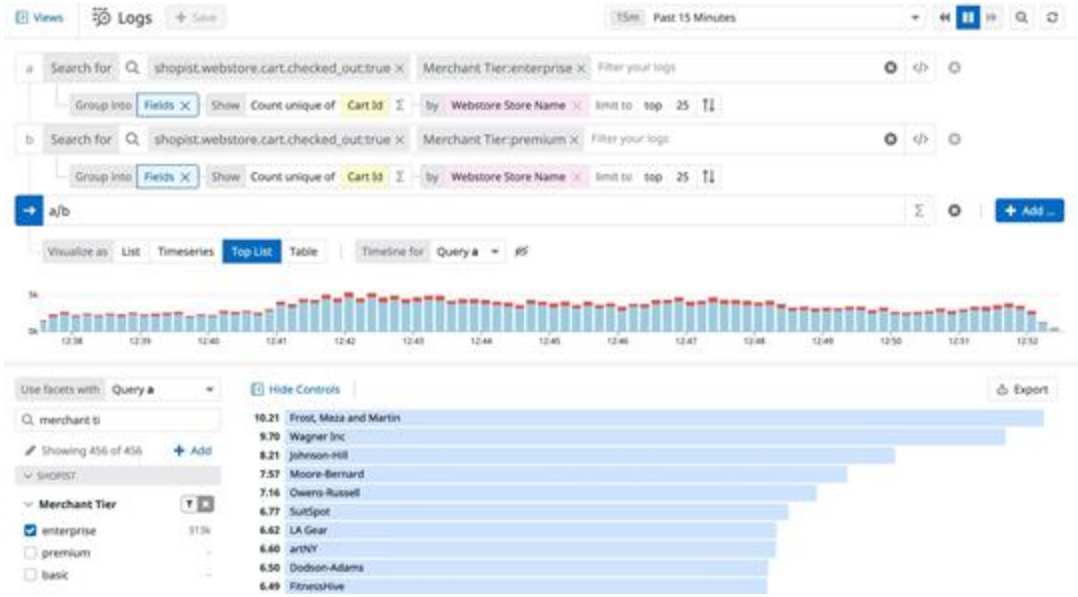
Verbal:

[sobbing] Yes, yes, it was all Keaton!
We followed him from the beginning!
I didn't know!

Anchoring and Confirmation Bias

Anchoring - Prioritizing your first impression

Confirmation bias - Focusing on data that confirms your belief



Cybersecurity tools are AWFUL at both of these.

Framing effect

How information is presented can impact decision making.

- Vader betrayed and murdered your father

  vs

- Vader is your father but was a REALLY different person before

- You have 50 vulnerable hosts

  vs

- You have no vulnerable hosts with external reachability and 50 out of 10,000 internal hosts are vulnerable

This applies to visual representation of data as well.

Goals of Good UI/UX (in Cybersecurity)

Maximize velocity to the objective

Maximize likelihood of correct outcome

Minimize bias through proper presentation of data and user elements

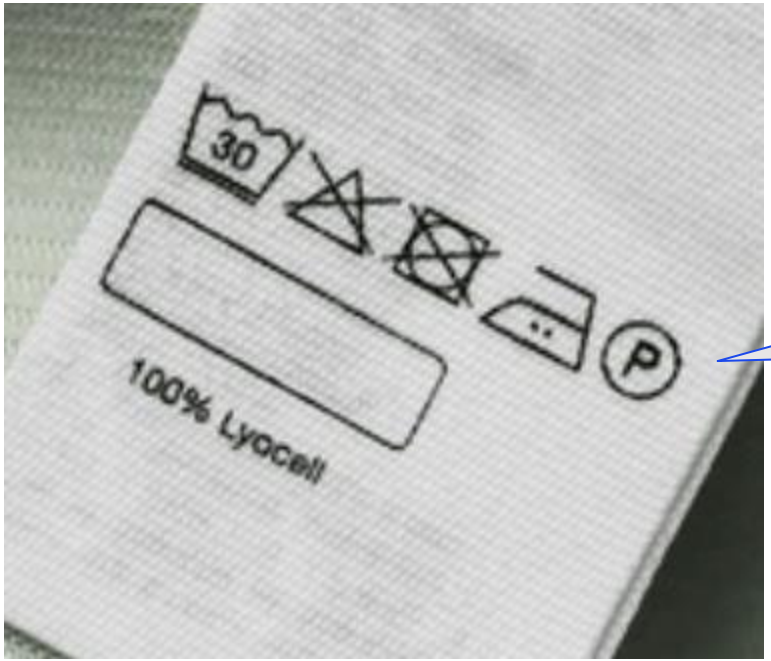
Minimize need for tool-specific training

Which way is this pointing?

Should you stop or not stop?

Or am I not allowed to do a Heisman pose here?

How do I wash this?



Can I park here?

Speaking of condensing a lot of information into a small space… what does this mean?

CVSS v3.1 Severity and Metrics:

Base Score: 9.0 CRITICAL

Vector: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Impact Score: 6.0

Exploitability Score: 2.2


@LateNightSeth
WHO KNOWS?

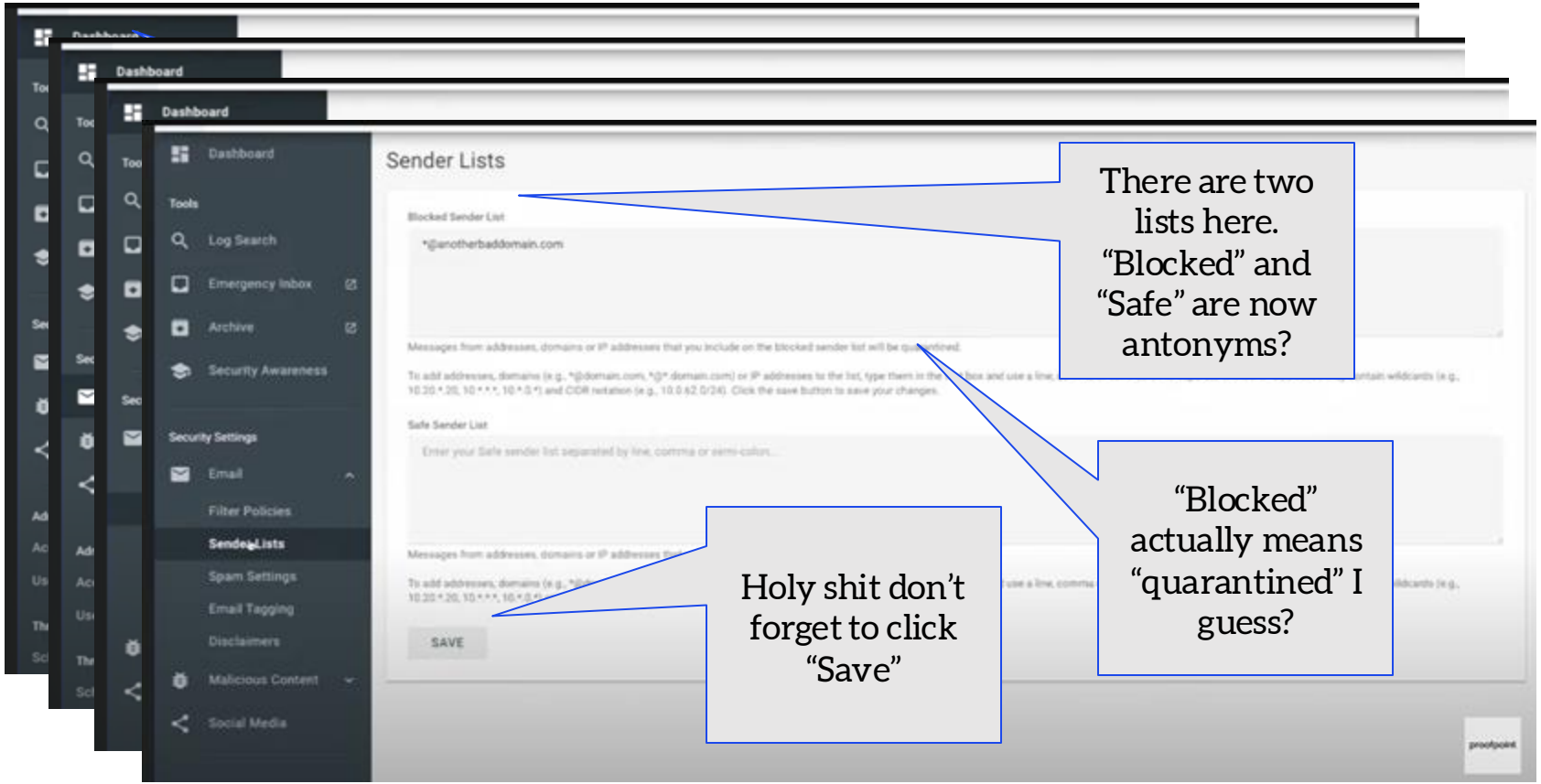
Thinking about cybersecurity UX

Email Security Gateways

What's the most common thing an administrator needs to do to their ESG?

Block an email address or domain!

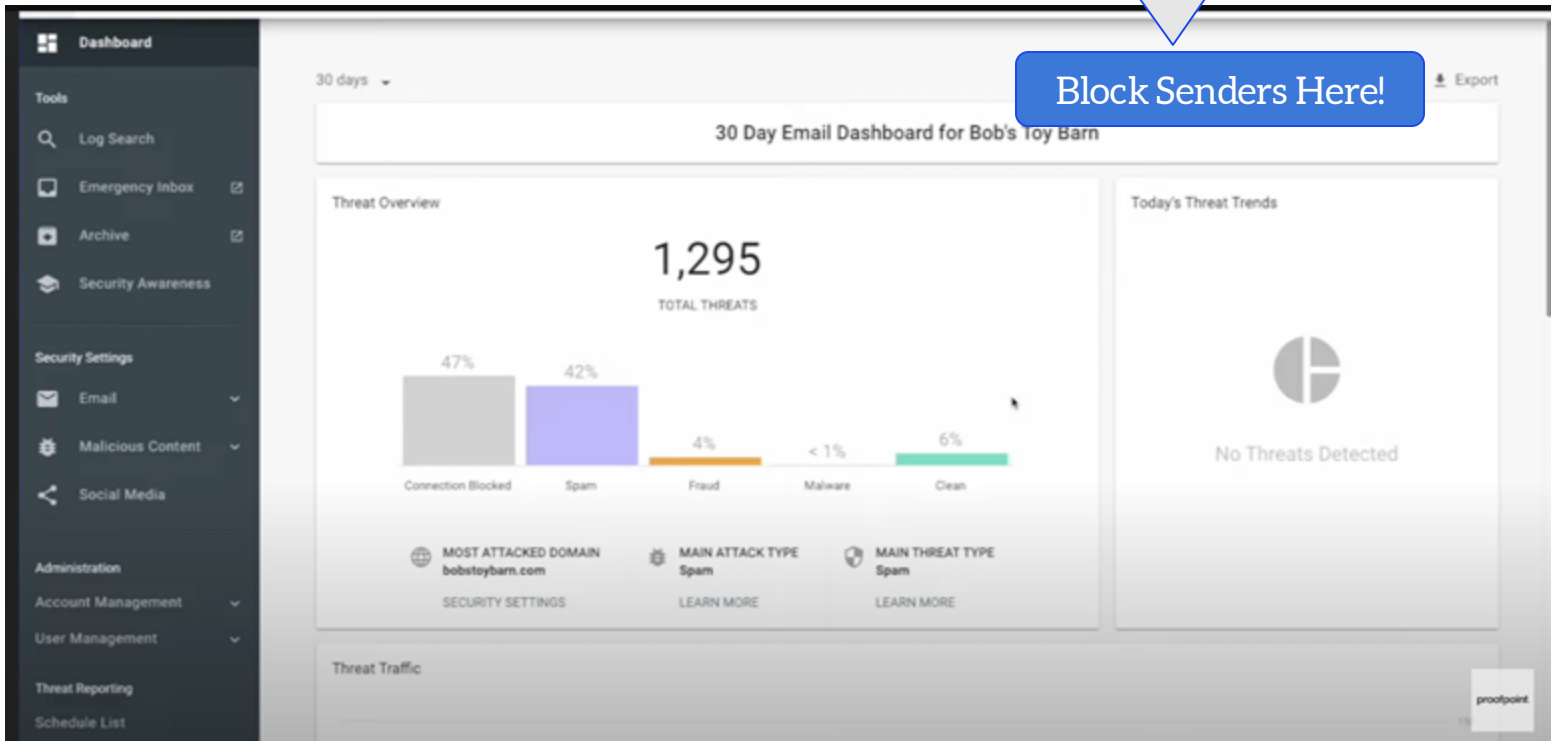
Block an email address or domain!



Block an email address or domain!

How about this?

Bonus points if your RUM tooling identifies common behaviors and updates this automatically



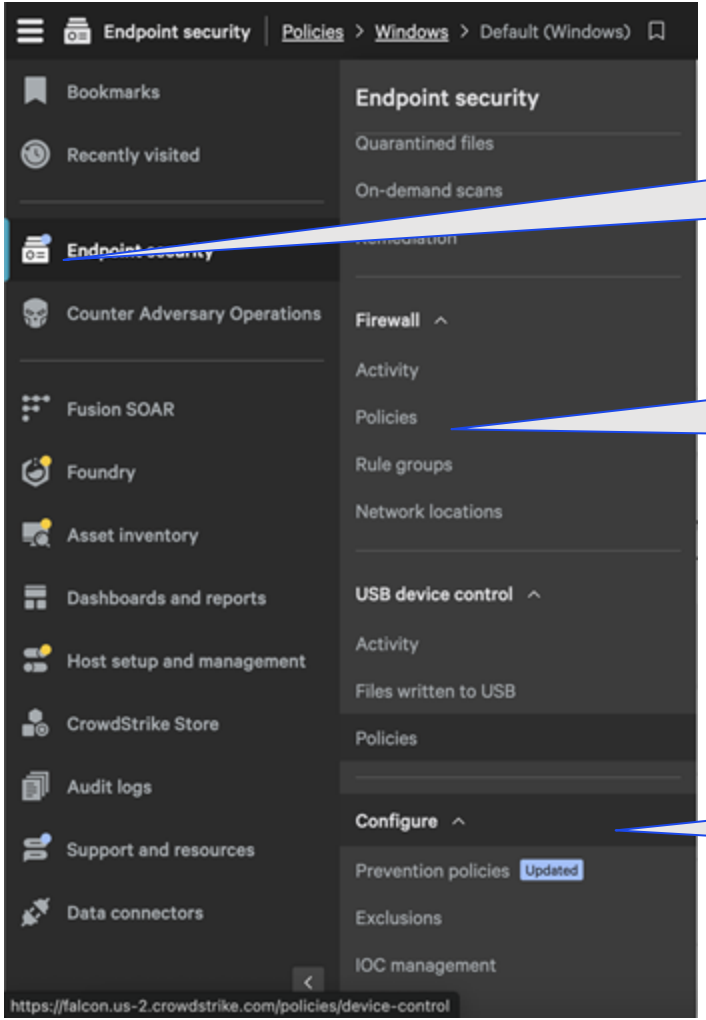
BTW, blocking an email address in postfix

```
$ sudo vi /etc/postfix/blocked_senders
$ sudo postmap blocked_senders
```

Like, there's a top level file of "don't accept emails" that you just edit and then run a simple command to make it active

And if you're good you can do it in one command

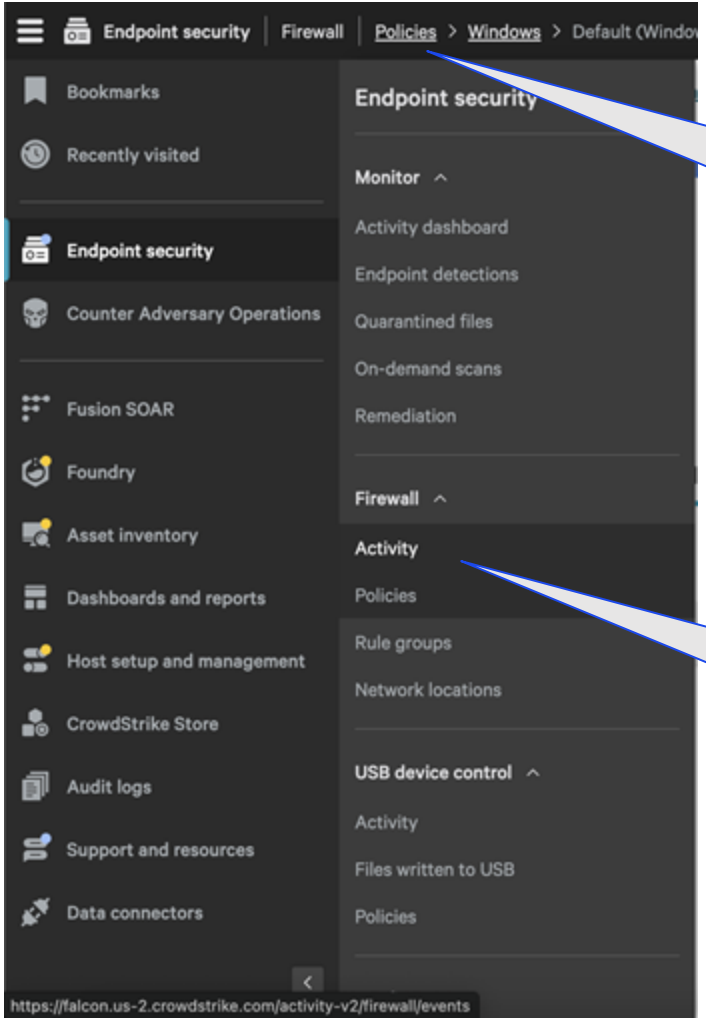
Let’s administer Falcon…



WTF do Yellow and Blue dots mean

What's the difference between a "Policy" and "Rule Group" in a firewall? Why is it meaningful at this level?

Why is this section labeled "configure"? Don't most of these options allow me to configure something?



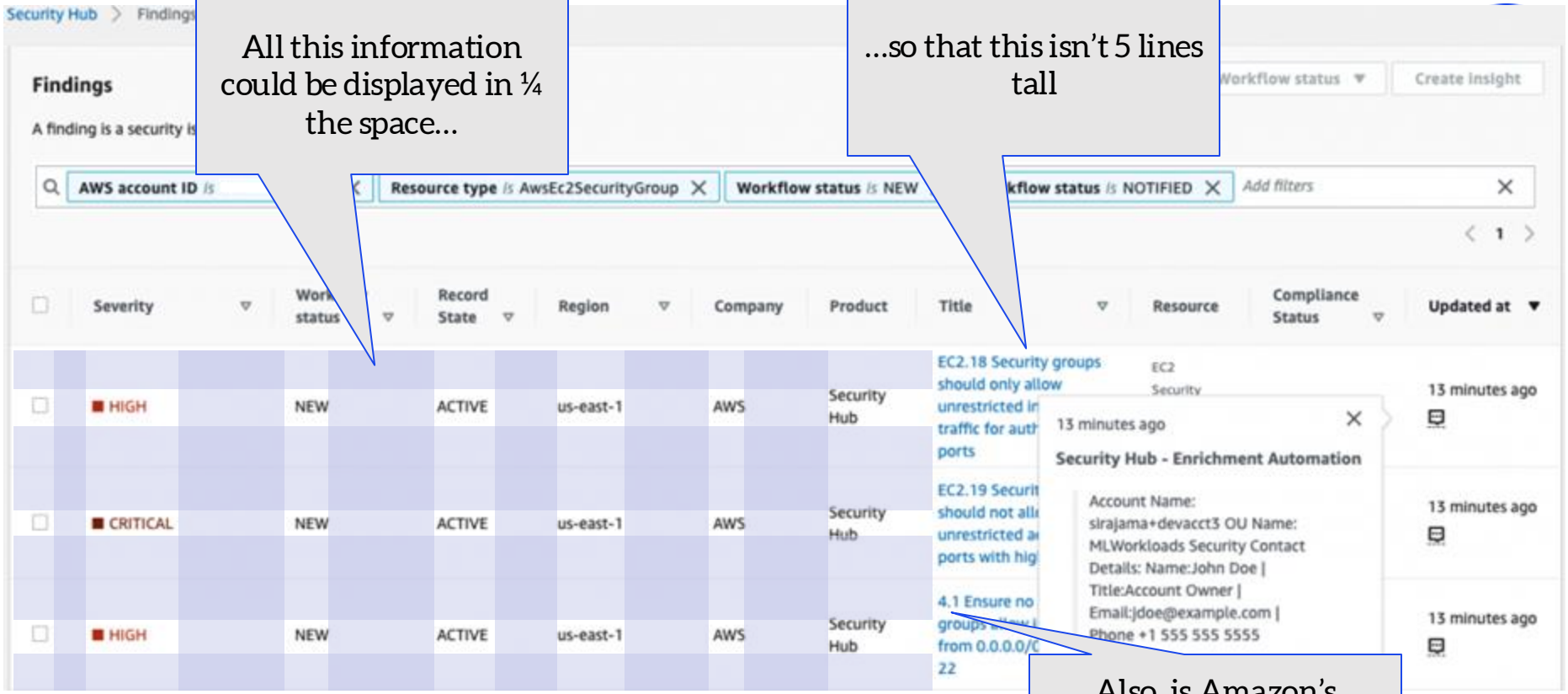
The top nav bar allows me to navigate to the top.. almost

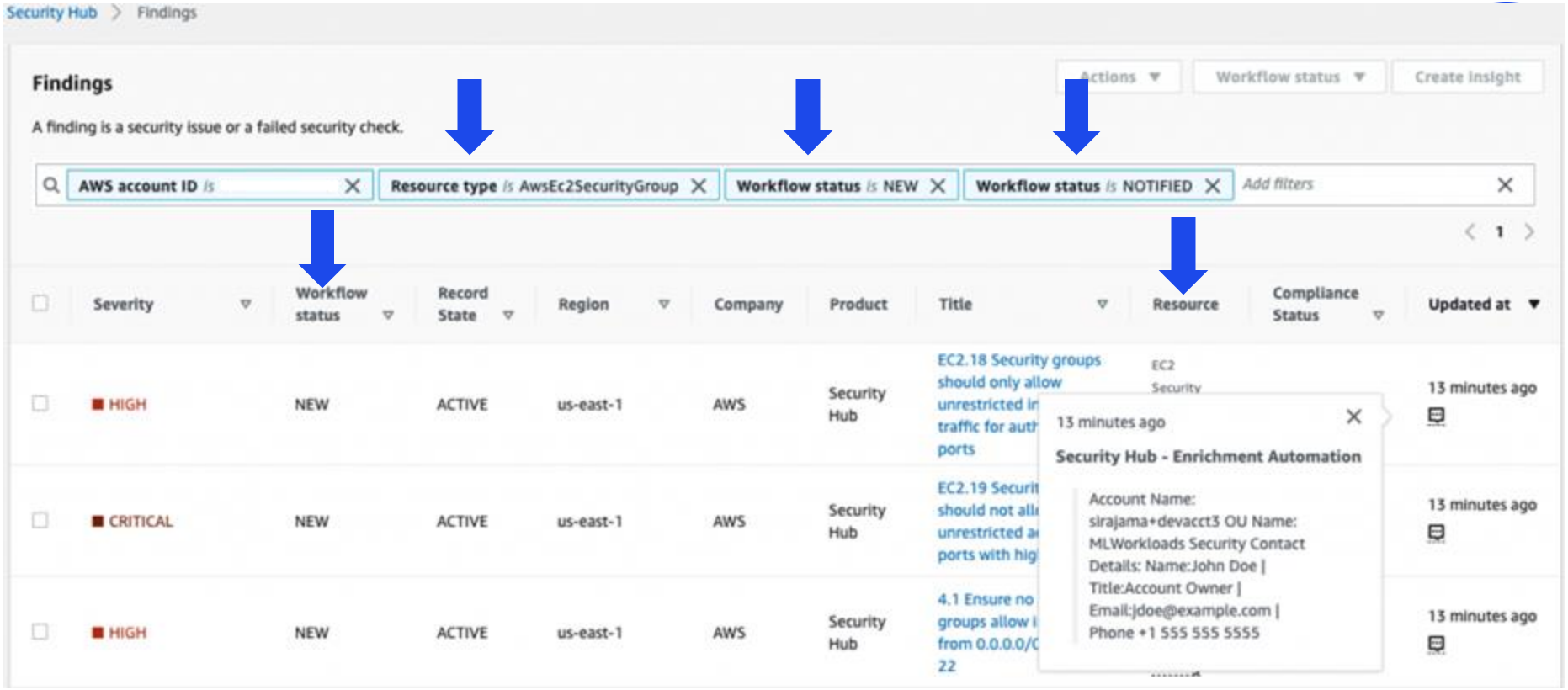
I have to click on the hamburger to to get back to here to select “Activity”... shouldn’t the “Firewall” nav bar allowed me to do that too?

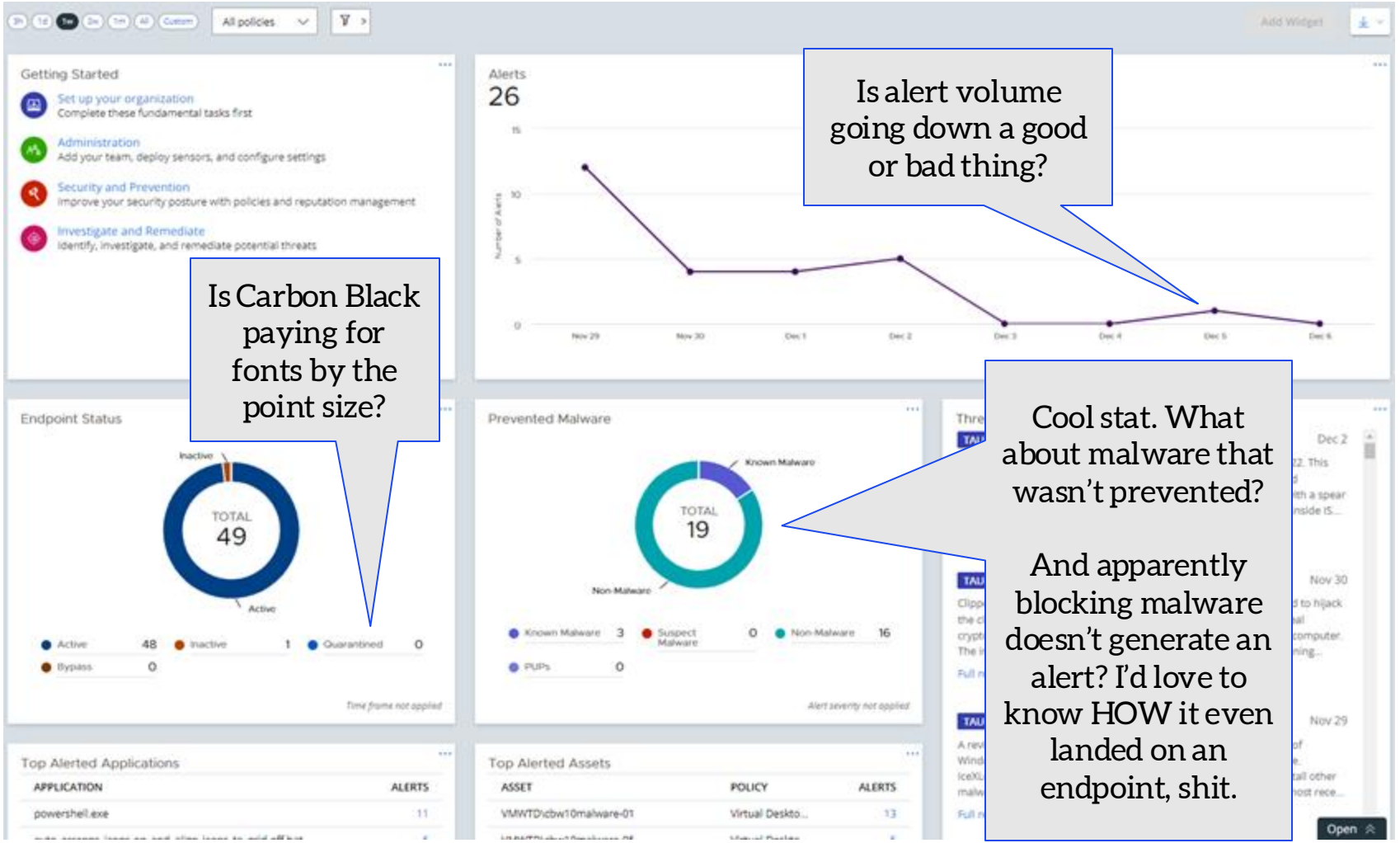
In fairness, this isn’t much better

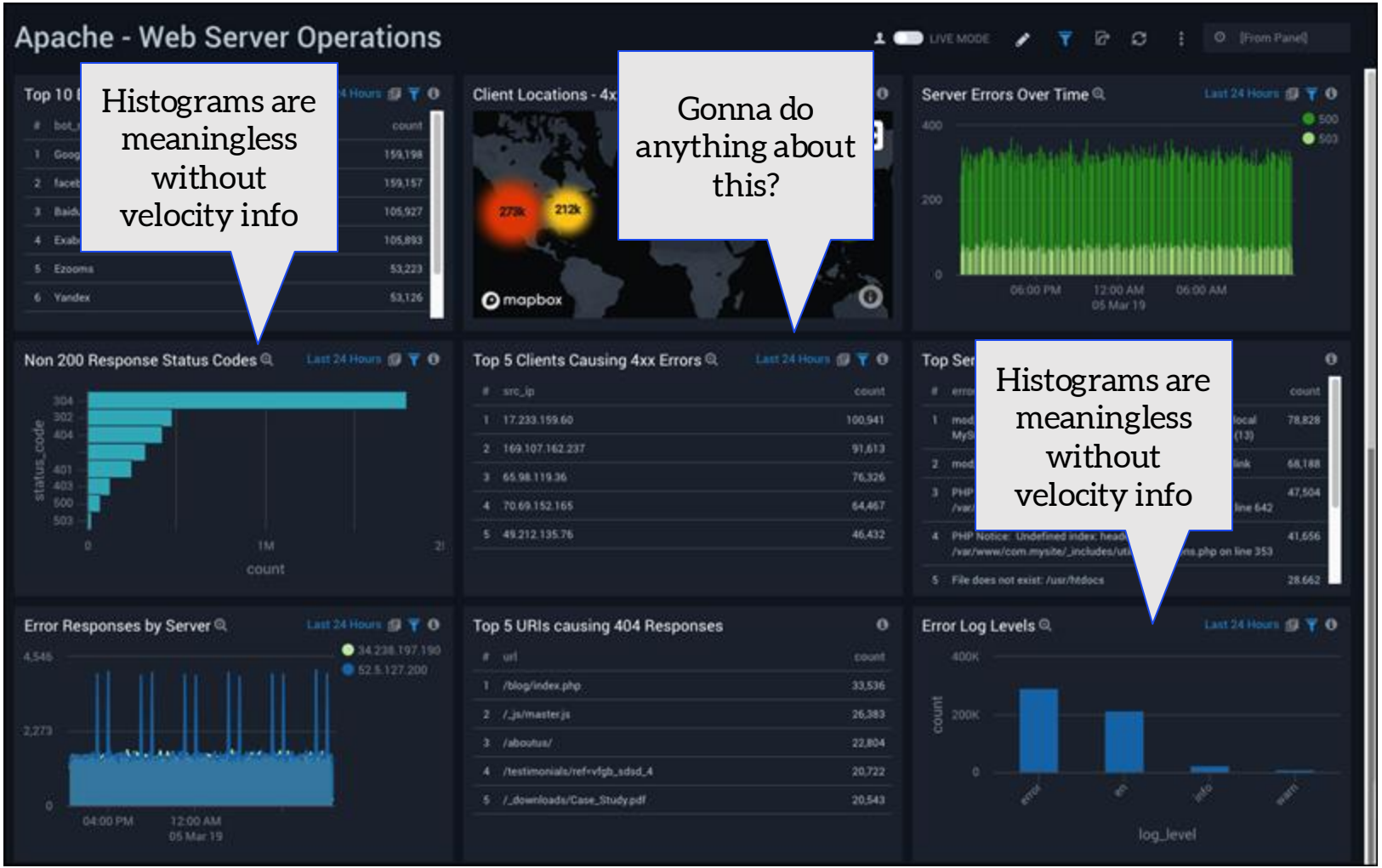
```
$ sudo iptables -A INPUT -s 192.168.1.10 -j DROP
$ sudo sudo iptables -A INPUT -s 192.168.1.10 -j DROP
```

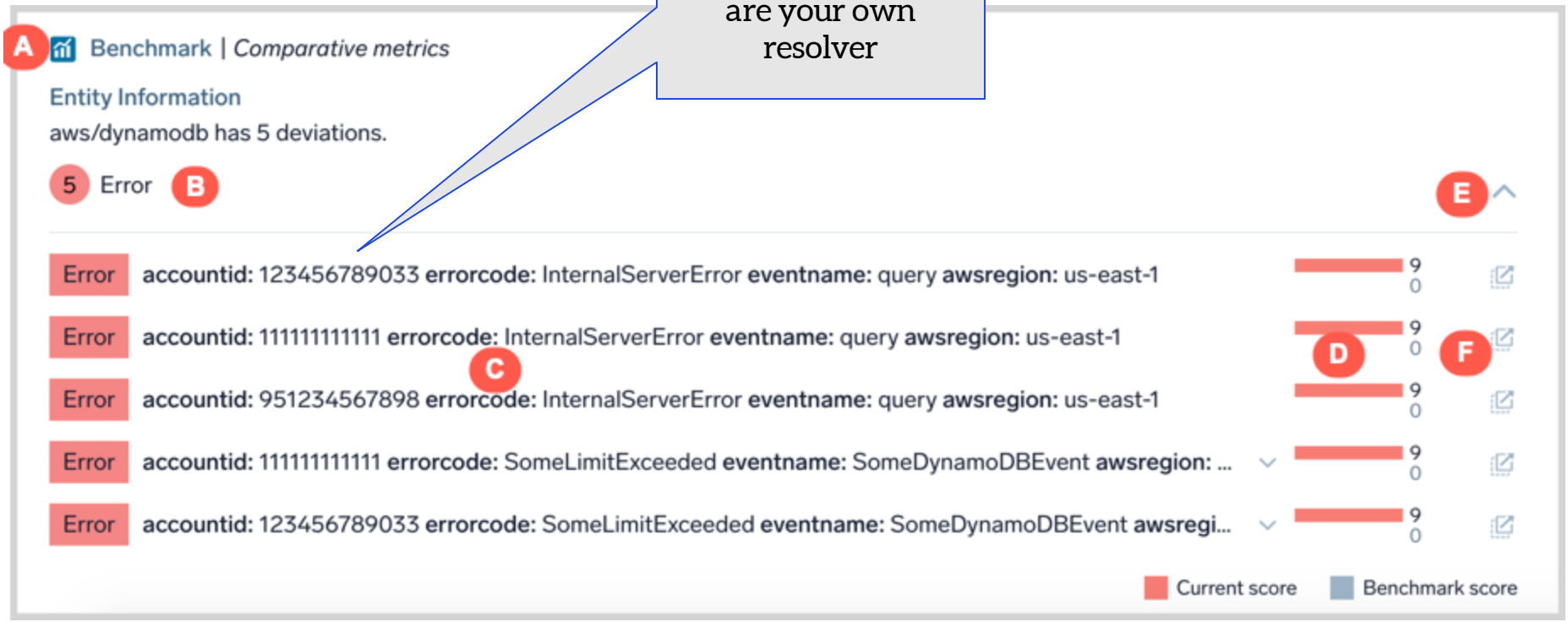
Thinking about whitespace and information density…


Security Hub
Findings
Findings
A finding is a security is
Workflow status
Create insight
AWS account ID is
Resource type is AwsEc2SecurityGroup
Workflow status is NEW
kflow status is NOTIFIED
Add filters
1
Severity
Work status
Record State
Region
Company
Product
Title
Resource
Compliance Status
Updated at
HIGH
NEW
ACTIVE
us-east-1
AWS
Security Hub
EC2.18 Security groups should only allow unrestricted in traffic for auth ports
EC2
Security
13 minutes ago
13 minutes ago
Security Hub - Enrichment Automation
Account Name: sirajama+devacct3 OU Name: MLWorkloads Security Contact Details: Name:John Doe | Title:Account Owner | Email:jdoe@example.com | Phone +1 555 555 5555
CRITICAL
EC2.19 Securit should not all unrestricted a ports with hig
13 minutes ago
HIGH
4.1 Ensure no groups from 0.0.0.0/0 22
13 minutes ago
All this information could be displayed in ¼ the space…
…so that this isn't 5 lines tall
Also, is Amazon's numbering convention for findings actually important?


Security Hub
Findings
Findings
A finding is a security issue or a failed security check.
Actions
Workflow status
Create insight
AWS account ID is
Resource type is AwsEc2SecurityGroup
Workflow status is NEW
Workflow status is NOTIFIED
Add filters
1
Severity
Workflow status
Record State
Region
Company
Product
Title
Resource
Compliance Status
Updated at
HIGH
NEW
ACTIVE
us-east-1
AWS
Security Hub
EC2.18 Security groups should only allow unrestricted in traffic for auth ports
EC2
Security
13 minutes ago
13 minutes ago
Security Hub - Enrichment Automation
Account Name: sirajama+devacct3 OU Name: MLWorkloads Security Contact Details: Name:John Doe | Title:Account Owner | Email:jdoe@example.com | Phone +1 555 555 5555
CRITICAL
NEW
ACTIVE
us-east-1
AWS
Security Hub
EC2.19 Securit should not all unrestricted a ports with hig
13 minutes ago
HIGH
NEW
ACTIVE
us-east-1
AWS
Security Hub
4.1 Ensure no groups allow i from 0.0.0.0/0 22
13 minutes ago


All policies
Getting Started
Set up your organization
Complete these fundamental tasks first
Administration
Add your team, deploy sensors, and configure settings
Security and Prevention
Improve your security posture with policies and reputation management
Investigate and Remediate
Identify, investigate, and remediate potential threats
Alerts
26
Is alert volume going down a good or bad thing?
Is Carbon Black paying for fonts by the point size?
Endpoint Status
TOTAL
49
Inactive
Active
Active 48
Inactive 1
Quarantined 0
Bypass 0
Prevented Malware
TOTAL
19
Known Malware
Non-Malware
Known Malware 3
Suspect Malware 0
Non-Malware 16
PUPs 0
Cool stat. What about malware that wasn't prevented?
And apparently blocking malware doesn't generate an alert? I'd love to know HOW it even landed on an endpoint, shit.
Top Alerted Applications
APPLICATION
ALERTS
powershell.exe
Top Alerted Assets
ASSET
POLICY
ALERTS
VMWTD\cbw10malware-01
Virtual Deskto...
Open


Apache - Web Server Operations
LIVE MODE
[From Panel]
Histograms are meaningless without velocity info
Client Locations - 4x
Gonna do anything about this?
279k
212k
mapbox
Server Errors Over Time
Last 24 Hours
500
503
400
200
0
06:00 PM
12:00 AM
05 Mar 19
06:00 AM
Non 200 Response Status Codes
Last 24 Hours
304
302
404
401
403
500
503
status_code
0
1M
count
Top 5 Clients Causing 4xx Errors
Last 24 Hours
src_ip count
1 17.233.159.60 100,941
2 169.107.162.237 91,613
3 65.98.119.36 76,326
4 70.69.152.165 64,467
5 49.212.135.76 46,432
Histograms are meaningless without velocity info
count
78,828
68,188
47,504
41,656
5 File does not exist: /usr/htdocs 28,662
Error Responses by Server
Last 24 Hours
4,546
2,273
0
34.238.197.190
52.5.127.200
04:00 PM
12:00 AM
05 Mar 19
Top 5 URIs causing 404 Responses
url count
1 /blog/index.php 33,536
2 /_js/master.js 26,383
3 /aboutus/ 22,804
4 /testimonials/ref=vfgb_sdsd_4 20,722
5 /_downloads/Case_Study.pdf 20,543
Error Log Levels
Last 24 Hours
400K
200K
0
count
log_level


Memorize IP's and Account ID's. You are your own resolver
A
Benchmark | Comparative metrics
Entity Information
aws/dynamodb has 5 deviations.
5 Error
B
E
Error accountid: 123456789033 errorcode: InternalServerError eventname: query awsregion: us-east-1
Error accountid: 111111111111 errorcode: InternalServerError eventname: query awsregion: us-east-1
C
D
F
Error accountid: 951234567898 errorcode: InternalServerError eventname: query awsregion: us-east-1
Error accountid: 111111111111 errorcode: SomeLimitExceeded eventname: SomeDynamoDBEvent awsregion: ...
Error accountid: 123456789033 errorcode: SomeLimitExceeded eventname: SomeDynamoDBEvent awsregi...
9
0
Current score
Benchmark score

Why is this important?

Poorly designed products require far **more training** and **specialized knowledge** to use than products that think of the UX first.

Poor UI leads to poor outcomes. If you're screwing around in Photoshop it's frustrating. If you're screwing around in your EDR you may apply the wrong policy and leave your enterprise vulnerable.

Seconds matter in security incidents. Don't make me click or think more than I need to.

Questions?

Assuredly I’m out of time by now…

@gdead | gdead@turngate.io