



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?



EMERGENCY ALERTS



Emergency Alert

BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

The Offending Menu



BMD False Alarm

Amber Alert (CAE) - Kauai County Only

Amber Alert (CAE) Statewide

1. TEST Message

PACOM (CDW) - STATE ONLY

the option that was reportedly selected

Tsunami Warning (CEM) - STATE ONLY

DRILL - PACOM (CDW) - STATE ONLY

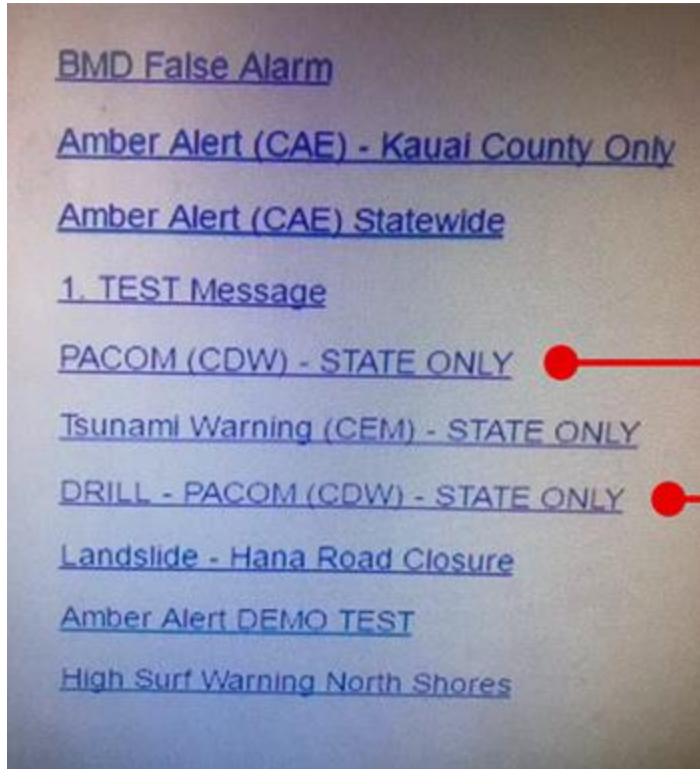
the option that should have been selected

Landslide - Hana Road Closure

Amber Alert DEMO TEST

High Surf Warning North Shores

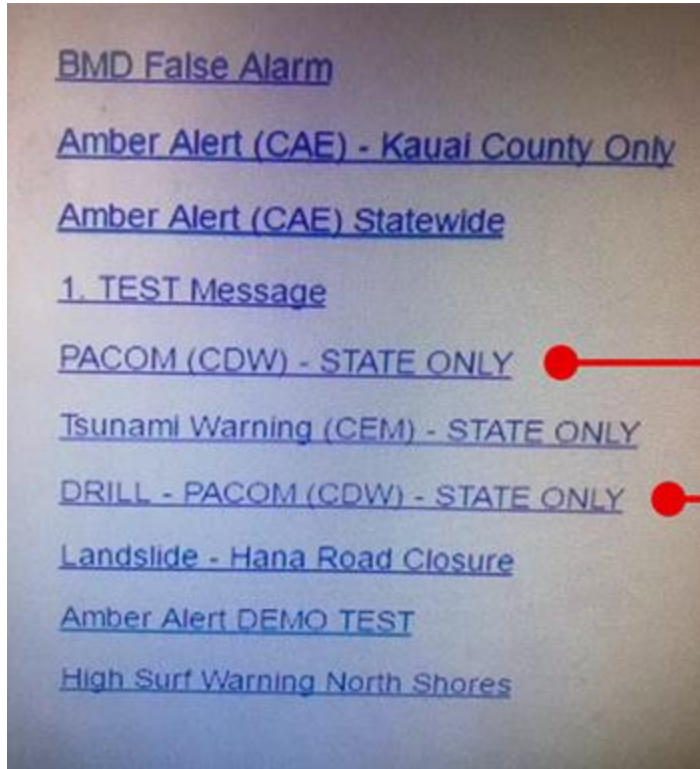
Put On Your Designer Hat and Dig In...



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
 - \$PlainText
 - \$PlainText 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

\$PlainText (\$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



Demo

Send

- System Test - Statewide
- Amber Alert (CAE) - Statewide
- Amber Alert (CAE) - Kauai County
- High Surf Warning (CEM) - North Shores
- Landslide Hana Road (CEM) - Kauai County
- Thermonuclear War (CEM) - Statewide
- Tsunami Warning (CEM) - Statewide

Live

Send

- False Alarm (BMD) - Statewide
- Amber Alert (CAE) - Statewide
- Amber Alert (CAE) - Kauai County
- High Surf Warning (CEM) - North Shores
- Landslide Hana Road (CEM) - Kauai County
- Thermonuclear War (CEM) - Statewide
- Tsunami Warning (CEM) - Statewide

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!

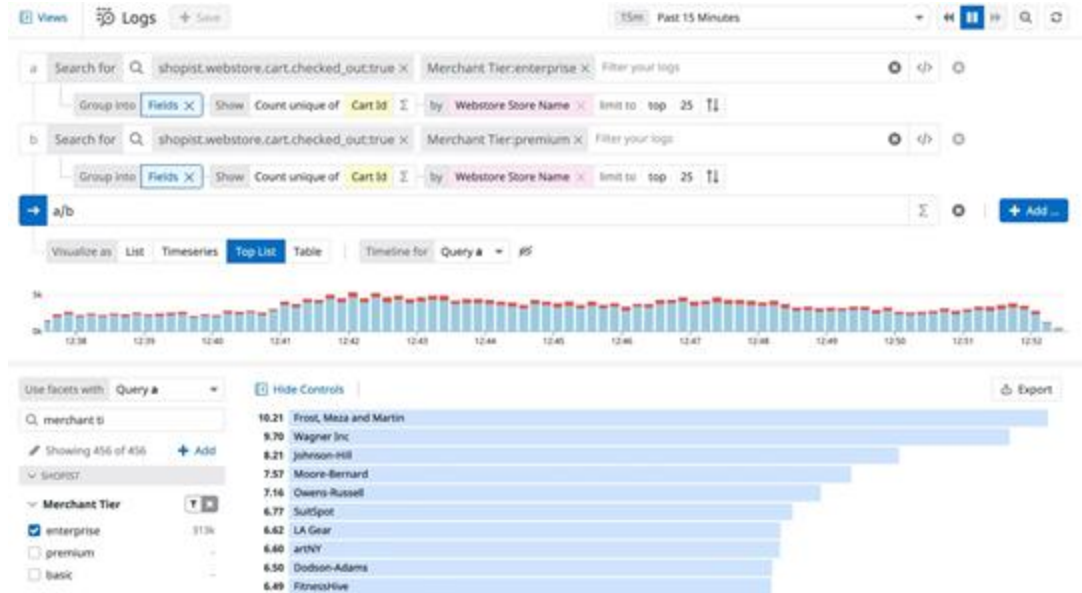
Anchoring and Confirmation Bias



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:

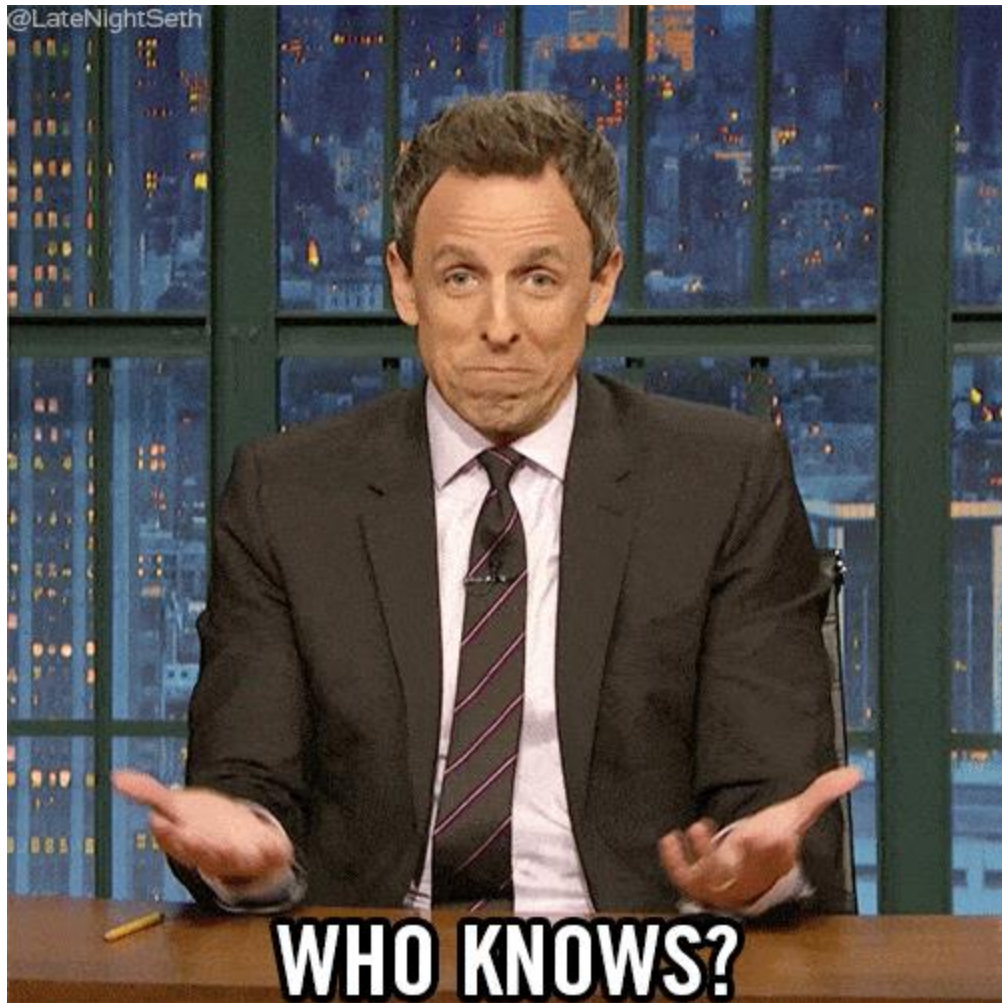
Base Score: 9.0 CRITICAL

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





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!



The screenshot displays a web interface for managing email sender lists. On the left is a dark sidebar menu with options like Dashboard, Tools, Log Search, Emergency Inbox, Archive, Security Awareness, Security Settings, Email, Filter Policies, **Sender Lists**, Spam Settings, Email Tagging, Disclaimers, Malicious Content, and Social Media. The main content area is titled 'Sender Lists' and contains two sections: 'Blocked Sender List' and 'Safe Sender List'. The 'Blocked Sender List' section has a text input field containing '*@anotherbaddomain.com' and a 'SAVE' button below it. The 'Safe Sender List' section has a text input field and a 'SAVE' button below it. Three callout boxes with blue borders and white backgrounds point to specific elements: one points to the 'Blocked Sender List' header, another points to the 'SAVE' button under the 'Blocked Sender List', and a third points to the 'SAVE' button under the 'Safe Sender List'.

There are two lists here. "Blocked" and "Safe" are now antonyms?

Holy shit don't forget to click "Save"

"Blocked" actually means "quarantined" I guess?

Block an email address or domain!



Dashboard

Tools

- Log Search
- Emergency Inbox
- Archive
- Security Awareness

Security Settings

- Email
- Filter Policies**
- Sender Lists**
- Spam Settings
- Email Tagging
- Disclaimers
- Malicious Content
- Social Media

Sender Lists

Blocked Sender List

*@anotherbadomain.com

Messages from addresses, domains or IP addresses that you include on the blocked sender list will be blocked.

To add addresses, domains (e.g., *@domain.com, *@*.domain.com) or IP addresses to the list, type them in the text box and use a link, comma or semicolon to separate entries. IP addresses may contain wildcards (e.g., 10.20.*.20, 10.*.*.10.*.5.*) and CIDR notation (e.g., 10.0.0.0/24). Click the save button to save your changes.

Safe Sender List

Enter your Safe sender list separated by commas.

Messages from addresses, domains or IP addresses that you include on the safe sender list will not be blocked.

To add addresses, domains (e.g., *@domain.com, *@*.domain.com) or IP addresses to the list, type them in the text box and use a link, comma or semicolon to separate entries. IP addresses may contain wildcards (e.g., 10.20.*.20, 10.*.*.10.*.5.*) and CIDR notation (e.g., 10.0.0.0/24). Click the save button to save your changes.

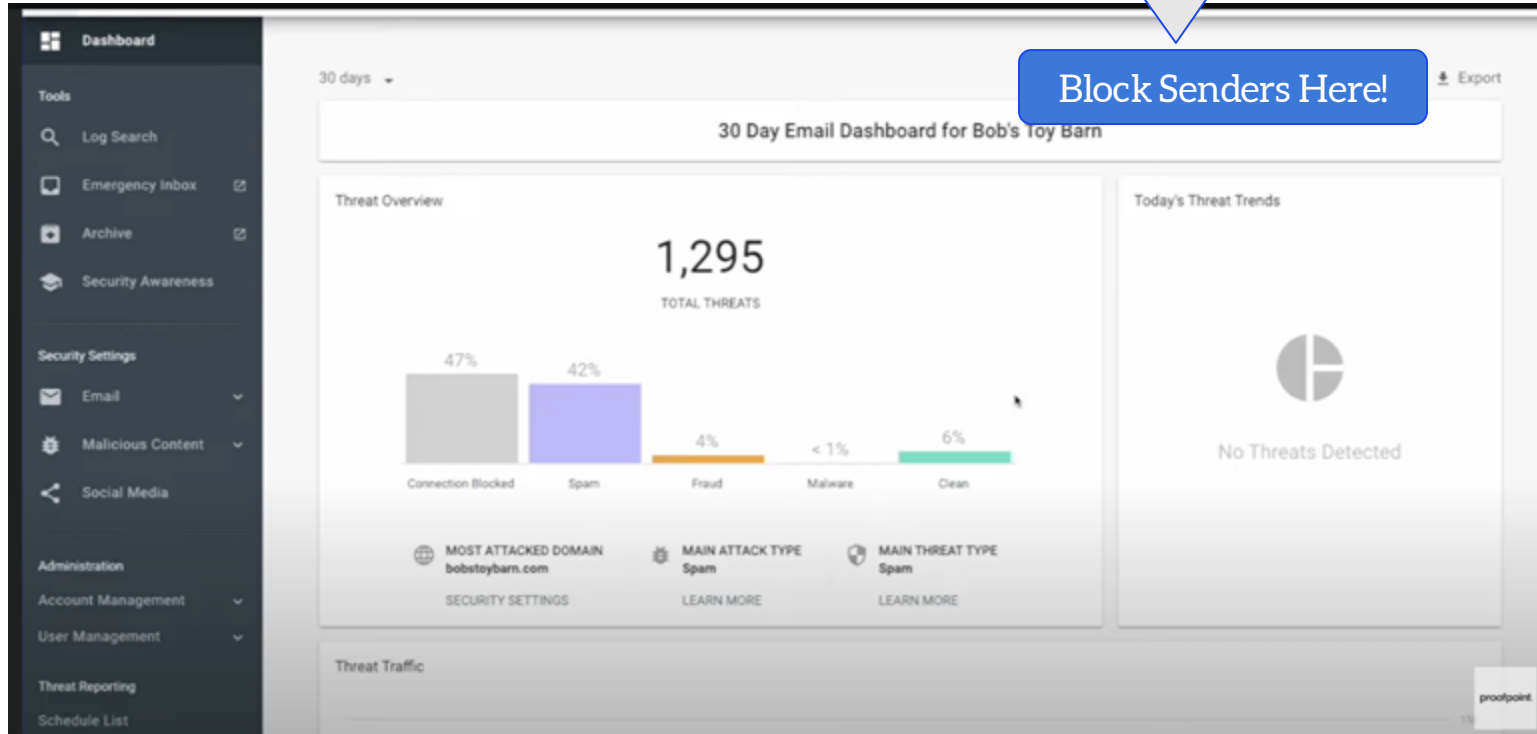
SAVE

proofpoint

Oh, you wanted to see a list of already Blocked senders? HAHAHA. That's somewhere else completely? Why would it be here?

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...



Endpoint security | Policies > Windows > Default (Windows)

Endpoint security

- Quarantined files
- On-demand scans
- Remediation

Firewall ^

- Activity
- Policies
- Rule groups
- Network locations

USB device control ^

- Activity
- Files written to USB
- Policies

Configure ^

- Prevention policies Updated
- Exclusions
- IOC management

https://falcon.us-2.crowdstrike.com/policies/device-control

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?



Endpoint security | Firewall | Policies > Windows > Default (Window)

Bookmarks

Recently visited

Endpoint security

Counter Adversary Operations

Fusion SOAR

Foundry

Asset inventory

Dashboards and reports

Host setup and management

CrowdStrike Store

Audit logs

Support and resources

Data connectors

Endpoint security

Monitor ^

- Activity dashboard
- Endpoint detections
- Quarantined files
- On-demand scans
- Remediation

Firewall ^

Activity

- Policies
- Rule groups
- Network locations

USB device control ^

- Activity
- Files written to USB
- Policies

https://falcon.us-2.crowdstrike.com/activity-v2/firewall/events

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...**

Findings

A finding is a security is

Search filters: AWS account ID is [] Resource type is AwsEc2SecurityGroup Workflow status is NEW Workflow status is NOTIFIED Add filters

Columns: Severity, Work status, Record State, Region, Company, Product, Title, Resource, Compliance Status, Updated at

All this information could be displayed in 1/4 the space...

...so that this isn't 5 lines tall

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
CRITICAL	NEW	ACTIVE	us-east-1	AWS	Security Hub	EC2.19 Security should not allow unrestricted a ports with high			13 minutes ago
HIGH	NEW	ACTIVE	us-east-1	AWS	Security Hub	4.1 Ensure no groups allow from 0.0.0.0/22			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

Also, is Amazon's numbering convention for findings actually important?

Findings

A finding is a security issue or a failed security check.

Actions ▾

Workflow status ▾

Create insight

< 1 >

<input type="checkbox"/>	Severity ▾	Workflow status ▾	Record State ▾	Region ▾	Company	Product	Title ▾	Resource	Compliance Status ▾	Updated at ▾
<input type="checkbox"/>	■ HIGH	NEW	ACTIVE	us-east-1	AWS	Security Hub	EC2.18 Security groups should only allow unrestricted in traffic for authentication ports	EC2 Security		13 minutes ago <input type="checkbox"/>
<input type="checkbox"/>	■ CRITICAL	NEW	ACTIVE	us-east-1	AWS	Security Hub	EC2.19 Security should not allow unrestricted access to ports with high priority			13 minutes ago <input type="checkbox"/>
<input type="checkbox"/>	■ HIGH	NEW	ACTIVE	us-east-1	AWS	Security Hub	4.1 Ensure no groups allow i from 0.0.0.0/0			13 minutes ago <input type="checkbox"/>

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

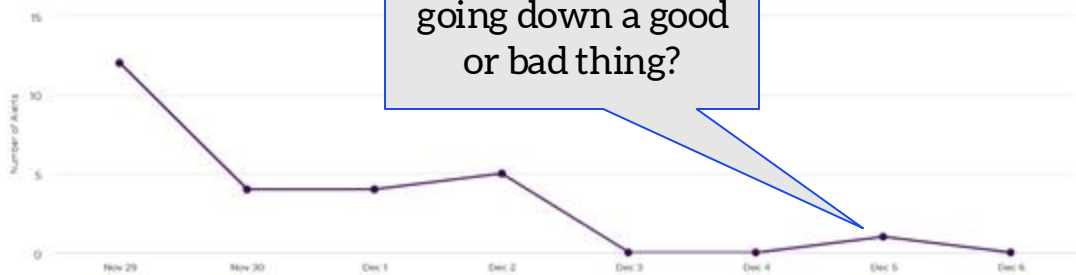


Is Carbon Black paying for fonts by the point size?

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

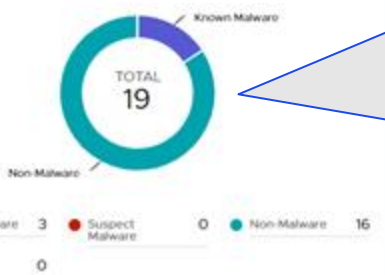


Is alert volume going down a good or bad thing?

Endpoint Status



Prevented Malware



Cool stat. What about malware that wasn't prevented?

Top Alerted Applications

APPLICATION	ALERTS
powershell.exe	11

Top Alerted Assets

ASSET	POLICY	ALERTS
VMWTD\cbw10malware-01	Virtual Desko...	13

And apparently blocking malware doesn't generate an alert? I'd love to know HOW it even landed on an endpoint, shit.

Apache - Web Server Operations

LIVE MODE [From Panel]



Top 10

#	bot...	count
1	Goog	199,198
2	facel	199,157
3	ibaid	105,927
4	Exab	105,893
5	Ezoo	53,223
6	Yand	53,126

Histograms are meaningless without velocity info



Gonna do anything about this?



Top 5 Clients Causing 4xx Errors

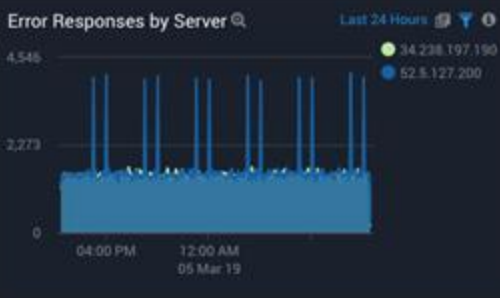
Last 24 Hours

#	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

Top Ser

#	error	count
1	mod... local (13)	78,828
2	mod... link	68,188
3	PHP /var... line 642	47,504
4	PHP Notice: Undefined index: head... line 353	41,656
5	File does not exist: /usr/h/docs	28,662

Histograms are meaningless without velocity info



Top 5 URIs causing 404 Responses

#	url	count
1	/blog/index.php	33,536
2	/_js/master.js	26,383
3	/abouts/	22,804
4	/testimonials/ref-vfjg_sdsd_4	20,722
5	./downloads/Case_Study.pdf	20,543





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		9 0	
Error	accountid: 11111111111 errorcode: InternalServerError eventname: query awsregion: us-east-1		9 0	
Error	accountid: 951234567898 errorcode: InternalServerError eventname: query awsregion: us-east-1		9 0	
Error	accountid: 11111111111 errorcode: SomeLimitExceeded eventname: SomeDynamoDBEvent awsregion: ...		9 0	
Error	accountid: 123456789033 errorcode: SomeLimitExceeded eventname: SomeDynamoDBEvent awsregi...		9 0	

 Current score  Benchmark score

D

F

C

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