

Case Study

Carbon Black Overview

Carbon Black is a cybersecurity software that provides endpoint security. The primary product is called the Carbon Black Cloud, which is a cloud-native platform designed to protect endpoints (such as computers and servers) from a variety of security threats. Key features and components of Carbon Black products include:

• Endpoint Detection and Response (EDR):

This functionality helps in detecting, investigating, and responding to advanced threats in real-time. It provides detailed visibility into activities across endpoints and aids in threat hunting and incident response.

• Next-Generation Antivirus (NGAV):

Combines traditional antivirus techniques with advanced machine learning and behavioral analysis to prevent malware and other malicious activities.

Threat Intelligence

Integrates global threat intelligence feeds to provide insights into the latest threats and helps in proactive threat hunting and defense.

Application Control

Allows organizations to lock down and control applications on endpoints to prevent unauthorized or malicious applications from running.

• Threat Hunting and Incident Response Tools

Provides tools for security teams to conduct thorough investigations and respond quickly to incidents.

• Real-Time Monitoring and Alerting

Continuously monitors endpoint activities and generates alerts for suspicious behaviors and potential threats.

The Carbon Black Cloud leverages a combination of behavioral analytics, machine learning, and cloud-based threat analysis to deliver comprehensive endpoint security.

My Role

In my role as Lead UX Designer for Carbon Black Alerts, I was responsible for leading improvements in the alerting experience. I collaborated closely with the product owner, UI and backend development teams, and the UX group to deliver customer value and functionality that aligned with Carbon Black's organizational initiative goals. Additionally, I was responsible for continuously refining the UX of CB Alerts, ensuring seamless integration and enhancement as new features were implemented in other areas.

Enhancing Carbon Black Alerting Experience

The Carbon Black Alerts Revamp Project set out to transform the user experience for enterprise corporate security analysts by revitalizing the Alerts section, the cornerstone of the CB endpoint protection software. This initiative was pivotal in bolstering early endpoint threat detection and mitigation capabilities.

By embracing agile methodology and fostering cross-functional collaboration, the project prioritized crafting a more intuitive, efficient, and user-centric alerts interface. The comprehensive redesign encompassed the development of new alert detail views, alert workflow states, alert grouping by threat ID, and the introduction of an auto-close alerts rule library, all while upholding stringent quality standards and ensuring a uniform UI across systems.

Project Context

Users within the Carbon Black Cloud platform have encountered numerous alerting challenges. Informed by extensive customer feedback, it became evident that users often struggle to effectively triage, scope, investigate, and remediate alerts within the platform. As we geared up for a significant UAE release in August 2023, we explored additional avenues for users to view, organize, and manage their alert queues within their SOC teams.

Project Goals

- 1. Increase ease-of-use of alert management in the CBC and reduce alert resolution friction
- 2. Introduce simplified alert workflow enhancements to customers with the goal of reducing users' timeto-value when investigating, triaging, and closing alerts
- 3. Surface relevant metadata to customers so they have the right level of information at their fingertips throughout the end-to-end alert triage and closure workflow

1	C	Car	rbon Blacl	k Clou	ld			Notifications >	Help >	
	A	LER Q	TS Search						3 hours	Search C
~ ~ ~	»	19 al	lerts				•	Group by	None	~ (?) Exp
and the second se	R III P		STATUS	SEV	TYPE/REASON	CREATED -	5 DEVICE ~	POLICY 3	WORKFLO	
			Policy applied	5	Watchlist Process sudo was detected by the report "Privilege Escalation - Sudoers in Cmdline" in 2 watchlists	06:10:20 Jan 27, 2022	Devicename	Watchlist name Report name	In progress	-4 💿 🔹
	C		🚱 Ran	5	CB Analytics The file opening for execute c:\users\bspeaker\desktop\20968\blockme.exe is not allowed.	02:50:09 Jan 27, 2022	Devicename	PolicyName Rule Name	In progress	-C () -
			🚱 Ran	5	CB Analytics The application sychost.exe attempted to perform a privilege escalation via a known User Account Control (UAC) bypass. A Terminate action was applied.	22:40:35 Jan 26, 2022	Devicename	PolicyName Rule Name	In progress	-4 0 -
			Policy applied	5	Watchlist Process vim basic was detected by the report "Privilege Escalation - Sudoers in Cmdline" in 2 watchlists	15:52:20 Jan 26, 2022	Devicename	Watchlist name Report name	In progress	-
				5	Watchlist Process snap-update-ns was detected by the report "Persistence - Modification of Boot-time Kernel Modules" in watchlist "Carbon Black Advanced Threats"	14:10:12 Jan 26, 2022	Devicename	Watchlist name Report name	In progress	-
			🚱 Ran	5	CB Analytics The application cmd.exe invoked another application (util.exe). A Deny Policy Action was applied	11:52:30 Jan 26, 2022	Devicename		In progress	-c 🕘 -
			Policy applied	5	Watchlist Process svchost.exe was detected by the report "sns-sqs" in watchlist "Jess-sns- sqs-test"	10:25:00 Jan 26, 2022	Devicename	Watchlist name Report name	In progress	-4 0 -
			Policy applied Ran Tags	5	USB Device Control Process rundli32.exe was detected by the report "Defense Evasion - Dil Load with Control_RunDil" in watchlist "Carbon Black Community"	09:42:08 Jan 26, 2022	Devicename	77 XXX	In progress	•C 🕘 •
			Policy applied	5	CB Analytics The application mcscript_inuse.exe attempted to perform ransomware behavior. A Deny action was applied.	07:23:46 Jan 26, 2022	Devicename	PolicyName Rule Name	In progress	-4
	Show	wing 1	1-10 of 19	Configure	The application mcscript_inuse.exe attempted to perform ransomware behavior. A Deny action was applied.	Jan 26, 2022	Devicenanie	Rule	Name	Name

We refined our project goals into more granual list of objectives:

- 1. Incorporate new alert metadata such as process command line and username, parent and child process information, netconn data, additional device fields, MITRE categorization, and more
- 2. New customizable alert facets and table columns
- 3. In-product alert workflow management, allowing the analyst to mark alerts as "In Progress"
- 4. Classify alerts as True or False Positive
- 5. Better note management with the ability to add notes to both individual alerts as well as threats
- 6. Enhanced Alert History visibility which shows a history of all alert state transitions (ie. Open -> In Progress), comments, determination, closure information, etc.

Alert ID History & Threat ID History



EPIC 1: Alert Workflow

User Stories, Design Requirements

In delineating the enhanced alert experience, I've drawn upon previous customer research and design insights, where customers expressed a desire for alert workflow states. This allows the team of analysts to collaborate on alert resolution progress effectively.

User Epic: As a Customer, I want to be able to transition an alert between Open, In Progress, and Closed states, while maintaining a comprehensive history of alert workflow activity within my environment.

As a cross-functional alert team comprising of product owner, content writer, UX researcher, UI devs and sometimes backend devs, we unearthed various edge cases during our exploration, necessitating further refinement of design requirements. We conducted weekly design reviews to deliberate technical specifications and assess their impact on our design trajectory.

Semi-structured Interview + Usability Testing

We validated the workflow UX design by user research study that was Semi-structured interview + usability testing. We had 5 participants (1 internal, 1 Partner, 3 Customers) The study was based on an interactive prototype that I've created for research task flows I sat in all research sessions and notated customer feedback.

Key findings:

- Overall, new improvements were very well received by participants
- Ratings were 6+ for meeting their requirements and 7 for ease of use across the board

Design Validation UXR > Research Prototyping

- New features did not prevent participants from completing their tasks and were mostly a value added
- Some hindrance but no major obstructions to completing the tasks
- Needing to click or go into Alerts ID history to view who is working on an alert because did not know "In progress" was clickable
- Having Close being separate from Determination
- Not being able to use alert_id key in search



EPIC 2: Group Alerts by Threat ID

Background

Customers have reported experiencing alert fatigue due to the CBC system generating thousands of alerts based on the root alert trigger. With the introduction of Threat ID, the CBC system can now group similar alerts into a Threat ID alert group, thereby reducing the number of alerts users need to mitigate.

Customer Pain Points

1. Lack of Clarity at a Glance:

- It's not immediately clear that alerts are grouped.
- The grouping criteria are not transparent.

2. Confusing Alert Details:

- The group right rail takes sample data from one alert and displays an "Alert Detail" card instead of an aggregate of data across the group, which is confusing for users.
- 3. Visibility Issues:
- There is no clear indication of how many alerts are in a group from the initial grouped table view.
- 4. Unhelpful Labeling:
- Generic labels such as "results" in group navigation do not help users understand that the list represents groups of alerts.

Approach

- To address these issues, we undertook the following steps:
- 1. Design Workshops:
- Conducted workshops to brainstorm solutions and align on design direction.
- 2. User Research:
- Gathered insights from existing user feedback and additional user interviews to understand pain points in detail.
- 3. Prototyping and Testing:
- Created prototypes of the proposed solutions and tested them with users to validate effectiveness.

Solution Exploration

- 1. Improved Grouping Visualization:
- Enhanced the visual cues to clearly indicate that alerts are grouped.
- Made the grouping criteria more transparent.
- 2. Aggregate Alert Details:
- Redesigned the group right rail to show an aggregate view of data across the group rather than sample data from one alert.
- 3. Clear Group Size Indication:
 - Added a clear indicator of the number of alerts in each group within the initial grouped table view.
- 4. Informative Labeling:
- Replaced generic labels with more informative ones that help users understand the list represents groups of alerts.

More than half the participants easily completed the task



ew

										Aug Aug	
	vm o	Carbor	Black Clo	ud					Noticeires -	140 - U	ar hana (purlorg (r)
		LENS								(New C	tiget bet
		0									
	- 11	Antonatio	a site tights she	-						Graphy Mount	~ 00
	6		S* 194748	0	njetim	O	CART MART -	Oreast	100	O weeks an	ACTIONS
No.		•	10 10 10 10 10 10 10 10 10 10 10 10 10 1	- 8	Rectified Process such was provided by the region Vinsings Disorders - Subsets in Endow (# 2 weighted)	00.0020 pectr.0020	10.10.00 (ar.27.00)		Ourisee Descenarie	(*************************************	100.000 m
contract of the second	E I	0	1	- 8	O Andelas Bacta surangelar surange of Santa Santa Sa	062120 (ex17.302	66.6536 3/#-27.2523		2 decises		man ·)
lado ha dia number af In dia dia kanta fia India agai	D		2	- 8	streed via The application is deal for attempted to particle a incident exceeding a strength of the dealerst for the strength of the strength	47.4536 (11.27.262)	60.63 (477.20)		i deba	(* mm)	10.000 x)
-	8				(un) boson is formation action and copilati						
diskuster in a specific a the fideway fit	R	0	* *******	- 1	Readers Protected of the set of a fair set Training Insurance Subscription in Station (III)	00.00.20 [00.27.2022	97.9638 (44.77,701)) devices	(1997) (1997)	100.000 ·)
when one group											
en na dimet. Ograng en na bing verse dett var for samt ogen en forstererererere tantorerererererere	8										
2000											
energy mentals and to inform users and a symmetry from the per-											
			0.00	a text					Interior II	W MARKE	

Action Menu Update

e#**	New - Grouped All Options (1 device)	New - Grouped All Options (2+ devices)	CB Analytics	Watchlist	USB Device	HBFW	K8s
•	Close all				Oreal Opend	Cond Send	Concell Concell
~	Marcali e prograe Nativariae Matay	Markall is progress Neethuniers Procey Prince (1)	Wash of Puppers NetRotourneary Treat O	Nethal is progress Nethation Neory	Markali manageen Nachtation Neury Throad ID	Rohal inprogram Rohalow/Holay Train 0	Makati e program Nochations Antoniy Abt to bealthe
•	CapyBreak D View publicitum Can	Cappelinear ED Vine auto-close nate	Tage Procedb View and - does not	Capy West ID Viter Astrodise LaW	Capy Invasi D Vine autoritize rule	Dag Treat D The address of the	Ogg Thrat D Ogg Thrat D Year water date twit
•	FEETRE Deale device and the "searching same" Dealer CO. "NOO"	Disable den fra den	Add reaching approach (inc. Add reaching approach (inc. Add reaching approach (inc. Respect optimal) Friend and add	Duals alms for works "watches rune" Duals alms for works "watches rune" Duals ages "reput rune" Duals OC NOC"	Construction of a second (implementation of a second) Construction Construction Construction	Currentine of a same (Anguer and a same) Query same	
•	Althout is approached. Althout is approached. Althout is beined to: Beined included.	Although to approach the Although to approach the Although the approach the Research active	Outer application	Survive of Haseb (Incurrence of Hased) Survivants	Year of UK decisi Approx 125 decis" tane*		
	final to the field Dense againstine (service service) Endek lippens (Dentik lippens)	Our ways of the second state					
	Guardene and (begunnering and) Guardene Golden URI Strategie West of Strategie	Very Keller Very					

Outcome

 Nanopalan kar A dask helfer i biskel v for od or disk samplete grade til.
 Or disk helfer i od beset d for dask helfer i od beset d for dask helfer i od beset biskel disk helfer på biskel disk helfer for dask helfer i od beset ment disk helfer for dask helfer i od beset ment disk helfer i od beset biskel disk helfer for dask helfer i od beset ment disk helfer i od beset ment disk helfer i od beset ment disk helfer for dask helfer for

The new design provides a clearer and more intuitive grouping of alerts by Threat ID, reducing user confusion and enhancing the overall user experience. These improvements have been positively received in user testing, with users reporting reduced alert fatigue and a better understanding of the grouped alerts.

Threat ID > Group Alert List

vm	Car	Don Blace	(Clou				Notifications -		
	ALC								-
		-							
	ž	10 alerta h	n Dreet I	CONTRACTOR AND ADD ADD TO ADD.				Starting Terror B	0
0	10	status.	-	TOURADOW	ORANG.	DOVER -	POLICY	NONLIN	80
	•	Victory registed		Works Process sale and descriptify the sport "Prolognitociation: Solvers at Under a 2 workloss.	36.5038 34-31-363	teriorane teriorane	Record Lane		4 0
	0	0 m		WeedBel The Tal spring for excade clustering under dealers (1988) dealers on a let WeedB.	1019108 (m.17.391)	Operative Device Later	20000		4
I	0	0 m		Workfeld The appropriate excitations attemption to perform a painting execution rate a second that Activation efforts (Act hypers: A harmout action was applied.	22.403 (e-21.303	Decorume Decorume	2000		4
l		 Autoprogeties 		Wanchiel Process on Associate and Antonio Up the sport Win-Aspectacianses. Subsect in Contrast of Association	10,0024 (m-31,362	Comana Declarame	Report of the	(1997)	40
	D	011		WARTER Process may update as any descentify the space "Reconcest Intelligence of Experime forms' Meaning 'In samiful' Garlier Back Advanced Pressy'	1000 July 200	terrare become	Report Anna		40
	•	0 m		QR margins. The contraction contract another application (cell cont) & Decay Netry Astron was applied.	153.MJ (#35.MJ	Contarte Descenarte			40
l	•	Antisy suggested		Wardfell Robertschot ann een printed by the report two op?" if welchiel feel was aprend	18/21/28 149-25 262	Devianaria Devianaria	Report raine	(com)	40
l	0	0 100 cm		VM Kenas General Prozenskelli zar an ameriki iyine nyon Yahmer Sasan, ali sari am Genera Andre Anazoni, Generalaki Generaliyi	10.000 (0.000	instance Instance	24	(1997)	40
I	0	· Antopogetied		(E Augen) The agriculture encoder present and empired to perform summary behavior. Alternatives and associated	3723.46 (4-76.767	Unitatia Decisione	Russ Review		40

Threat ID > Group Alert List > Right Rail

Q									- 0
	10-10-10-10-10-10-10-10-10-10-10-10-10-1						<	C Province (News	000
C a.+ mme	Radon	- 000		84.6	-	A/108	ALANT DOTAGE		
C C C C C C C C C C C C C C C C C C C	O Analysis Se aphone schones atemped topologies pringe content as some the Aspect Ortel Strategies. A Science action are apped	11-0-36 Jac 24, 26D	Design rame	Public Harry			Ture CRAwlyrin Harrith Mar Nuch Anno Annum Mercanitation Sectored Administration	a charte frank, and and an industry and an application of the process and an application	
	CR Analysisa The application such assume attempted to perform a prologo musclehom dir a treasm liner Account Central LINC Approx. A "seminateraction non applied	10406 (#15.90)	Bears take	Pulsy Netwo	-	<0.	tin minter timest		
	O Analysis The approximation of the energy of the performance prompt assume the transmission of the energy of the performance of the energy of the energy of the performance of the energy of the energy of the energy of the other energy of the energy of th	11.40 M (# 15.300	Desce tarte	Pulsy Name	(town)	<	Process and an Pharma republican Annual Espanian	ownet accent	8.
C C C C C C C C C C C C C C C C C C C	Ch Analysiss The sublicities surface the standard is perform a printige exception of a tasket then declarit Control DHC logics: A "strength action on approx.	11.00 M H H	Beauty name	Public Name	(1999)	= 0 + >	Preside Oracide United		а.
	O Analysis The application surfacement attempted to perform a prologic modeling do a traver time model's Control SINC oppose A ferroheat action and applied	12-408 (#-28-262	para tetta	maky tarne	(1.000)	<0•)	Platini sporden in Detent Sporten Sebrigan	ica, a.dw o intent house Vinten	
	Octoangless The application inclusions attempted to perform a printiple exclusion due to beam that we perform that papers. A formation action was applied	11-00 H (an 24, 260)	Desize tarta	Policy Name	((1100)	40 ·)		(and a constant)	
C C C C C C C C C C C C C C C C C C C	Of Analysiss. The application rank waterward to perform a printing monotonic dra tensor line recourt General DHCs legres. A formula action was appreci-	34.97 MIN 104630	Beauty name	Publy Serve	(1198)	e 0 • >	partitus partitus	(Wynastawiy)	
Departure and	Testers Test			(1)				a series and a series of the s	

Threat ID	Summarv
TH Cat ID	Sammary





Alert Detail in a Group

Design Specification Wireframes

Threat ID List View

EPIC 3: Alert Detail Page

User Stories, Design Requirements

User Story

As a SOC or Security Analyst, I want a holistic alert details view that shows me relevant alert information so I can perform the majority of alert investigation and relevant actions for the selected alert without **pivoting** to other page

To add richer experience we anabled the user to view right rail alert information in a full page view to ease data digestion and collation. The new navigation through this detail view to the top of the alert list giving a context of alert data.

User Goal:

Reviewing a specific alert, determining True Positive/False Positive, beginning investigation

Expanded view of Alert Details with summary header An expanded view of the Alert details gives analysts a full view of the alert in one screen.

The alert summary header (maintained from the expanded details view) gives users a sense of "place" while triaging an alert. Users can navigate here from the alert list page to quickly reference individual alert information. Affordances like open in a new tab allow users to easily leverage multiple monitors.

Design and Usability Validation UXR

<complex-block></complex-block>	<section-header><list-item><list-item><list-item><list-item><list-item><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></list-item></list-item></list-item></list-item></list-item></section-header>	xpanded View ¹ can get a prefit good view of eventifying and it seems really say just break though inst read it lends like a short prefit issue here are developed inst of who really has ownering the issue here are dwhol can collaborate with and all and if the fit stuff. Eventfitting's in one easy to see screen where I could just click through it." -Participant 1 "Open that the with all the information. I like that, I will not lie. I much prefer bils view without having to scroll so much." -Participant 4
	Rating Ease of Use and Requirement Expand View	ts Met
	Meets Requirements	Ease of Use
	Ti's a lot of the same data that I'm already seeing from that si jump to and do right away because it's just showing us the same quality of the improvements, be able to do more from this pay before, I hink they would be a lot higher in that ranking." -Participant 5 "I would say eight because I didn't know I wanted It. But yes, a -Participant 1	Abba: So expanding It is probably not something they're going to data in a slightly different way. So if you can bring me some e, than just view the same data that I already had access to seven, a seven's good.*
il Page Navigation and Alert Brow	se	

Alert Detail New Full Page Layout

well nerte op wiedlice weit i ner	IELIK YNEW PEOLONIES IN PO COROLES					
vm Carbo	on Black Cloud					User Name (your0org-01)
5 Policy applied Ran S Ran 7	Type CB Analytics Alert ID 28100e63-e2d-4432-8e00-0 Reason The file opening for execute me.exe is not allowed.	a06352b5433 🗂 c:users\bspeaker\desktop\20968\bi	User Asset (Value) OS version Sensor version	Username Assetname (Low) Windows 10 x54 build 1909 3.7.0.9999	Policy Policyname Rule Rule name Werkflow In Progress Determin_ Twee trap poster / see poster	• () 2-
PROCESS indicate Ifficture reputation Deleted Signature Techniques Show all 2 Efficience Reputation Debieted Signature Techniques Show all 2	ADAPTIPE ALLOW, LIST Nai seleted Microsoft Windows UKCANALOW Microsoft Mindows Korceoft Mindows	PARADIATION PARADIATION PARADIA NIGUT PARADIA NIG	TEPS musers' devices assets umere on network to miligate risk wwestigation on usstato ecs6e8240272656k1366558ic7 inpu d int d ust 202726790556k1366558ic7 inpu 202726790556k1366558ic7 inpu	Deitee Network Isolata Go Live Virus Total Kation as not husted Add Later investigation	ALERT ID HISTORY ACT Created Act Area Act	Sort 12
INVOLVED PROCESSES aw protectionizent power (minerates processo) (minerates processo) (minerates processo) (minerates processo) (minerates processo) (minerates processo) (minerates processo)	shallooctubar eee ana gatam, ago wr) (antaoant, ggo) write, 11057, process, discovery) nater, 11057, grocess, discovery) rapl_mare)	IF HASH IS TRUSTE Add hash to appro Specify d43ec5884 Add cert to approv Specify Microsoft W Tune policy Update rules in Poli	D ved list EG272575 reputation as trusted red list Indows Publisher as trusted cy name to reduce false positives	Add Add	The second	3
ASSET Device Name User OS version Sensor version Policy Show all >	User Name Windows 10 x64 build 1909 3.7.0.9999 Policy name					

CBC-18548 (DAC Stand-alone Alert Detail CBC Analytic Alerts Detail in Right Rail e Alert Detail Watchlis

Alert List to Alert Detail

EPIC 4: Auto Close Enhancements

Addressing Auto-Closed Alert Rule Management for CB Customers

Background

CB customers have consistently complained about the disappearance of auto-closed alert rules into an inaccessible black box. These rules, created during alert closure, cannot be accessed or managed, leading to significant user frustration. Despite being a known issue, the product team faced challenges implementing the necessary enhancements.

Problem

The UX team questioned whether auto-closing alerts was the optimal solution. It was suggested that this feature might be better addressed at the organizational alert policy level, rather than through the current implementation.

Approach

To address this tension, I organized two design workshops aimed at resolving the conflict between these priorities.

Research

I meticulously reviewed existing research highlighting customer pain points related to alert fatigue and multi-alert management. Key data was presented in design workshops to UX leadership to emphasize the urgency of resolving these issues, especially considering potential dependencies on platform architecture that was not yet ready for implementation.

Solution Exploration

We debated whether to enhance the existing auto-dismissal functionality or design an independent solution to be implemented at the policy level later. Through story mapping and deep dives into potential workflows, we discovered the need for a rule manager for accessing and managing auto-closure rules.

Design Process

During the UX team and alert group meetings, we discussed how customers would access this rule manager and other critical questions. We agreed on a solution that allows users to create auto-close rules during alert closure and access a rule manager to audit and edit these rules. This solution also enables users to filter auto-closed alerts and audit their auto-close triggering rules, providing a safety net and building a trust.

Testing and Validation

This limited experience was tested and validated, demonstrating relief from customer pain. Participants delighted in the new visibility and control over alert auto-close rule.

Outcome

The design process revealed the necessity of a rule manager, where all auto-close rules can be accessed and managed (edit rule endpoints, or delete rule) effectively. Users expected to find rule manager under Enforce section where policy is created.



Design Validation, User stories, Design requirements

UXR Research Goals

- 1. Validate Auto Closure Workflow:
- Do users know how to auto-close alerts?
- Do users understand how auto-closed alerts are defined?
- 2. Validate Understandability of Rules Manager - Where do users go to access the Rules Manager? - What information are they looking for in the Rules Manager?

User Story Requirements

Auto Closure Rule Viewing and Management:

- Users can easily understand and see what auto closure rules are applied to any alert.
- Users can view all auto closure rules applied across their entire environment. •
- Users can see details about each auto closure rule, including: - Rule name
 - Threat/ThreatID
 - Scope (all devices or select devices)
 - Rule duration/expiration
- Users can delete auto closure rules currently in place for the alert or other auto closure rules in their environment.



https://jira.carbonblack.local/browse/CBCUI-4901

User can edit rule in the Rule Manager



https://jira.carbonblack.local/browse/CBCUI-4899

User can preview rule devices in the Rule Manager



Testing > Research Prototyping



3,890