CAB HIE Workshop Executive Summary Report

Pacha Chen I UX Researcher, HIE

2017.11.21

OUTLINES

- BACKGROUND
- WORKSHOP PARTICIPANTS
- KEY FINDINGS AND RECOMMENDATIONS

BACKGROUND

OBJECTIVES

1. Understand use cases and requirements better
2. Get some design inspiration from users
3. **Receive early feedback on new SMS UI for new features planned for 2018**
   - Profile Tuning via SMS (Filter reviewing/tuning + performance tuning)
     - eVR: Include IPS performance data in profile tuning, automatic retrieval of vuln scans, extract more context from vuln scans (OS, host priority, installed apps,etc…)
     - Malware in the wild: Tuning based on active malware campaigns / attacks

METHODOLOGY: CO-DESIGN WORKSHOP

Engage real world users in design activities in order to uncover new ideas, priorities, and flows

- Co-design methods provide a concrete way for innovation teams to **collaborate with end users** to understand opportunities and develop new products and services.

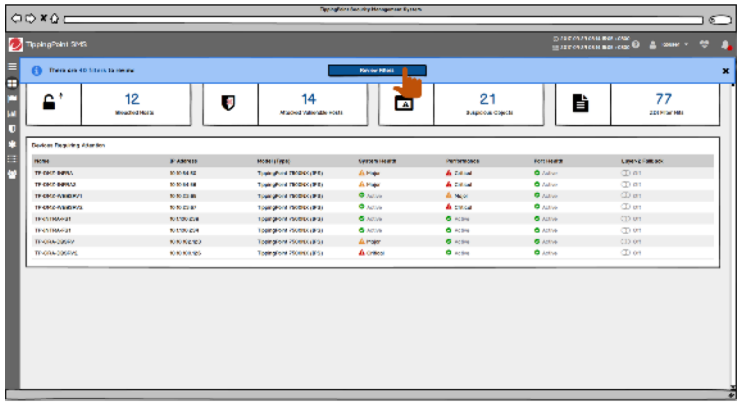
- It **allows users to become an active part of the creative development of a product** by interacting directly with design and research teams.
  - It is grounded in the belief that all people are creative and that users, as experts of their own experiences, bring different points of view that inform design and innovation direction.

AGENDA

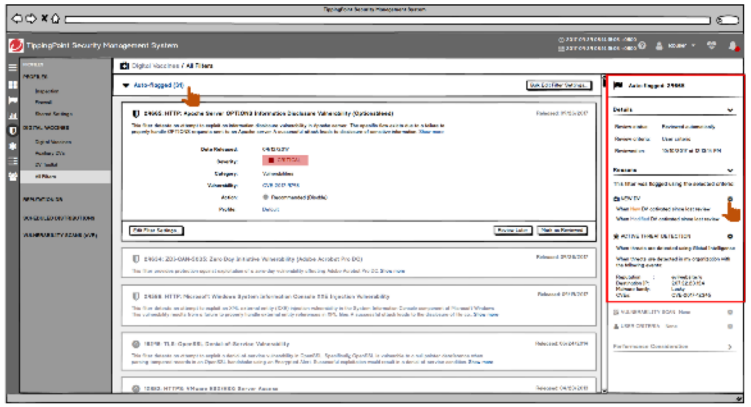
Time	Activity	Purpose
12:00pm-12:10pm	Opening	
12:10pm-12:55pm	**Warm-up: Create Your Own Avatar**	Ice-breaking, identify top 3 problems with SMS.
12:55pm-01:40pm	**Avatar Story - Security Tuning**	Understand users' typical scenario of security tuning. (Do-Think-Pain)
01:40pm-02:00pm	Tea Break	
02:00pm-02:40pm	**Design Concept Overview**	Explain the design concepts through storyboard: 1. Filter reviewing/tuning 2. Performance tuning
02:40pm-04:45pm	**Design Concept Evaluation & Ideation**	Let users review the concept and generate more ideas.
~~04:45pm-05:00pm~~	~~Closing Event - Web UI Concept Sharing~~	~~Give users a high level idea about web UI concept. (This activity was dropped due to the time constraint.)~~

SCENARIO 1 - FILTER REVIEWING/TUNING

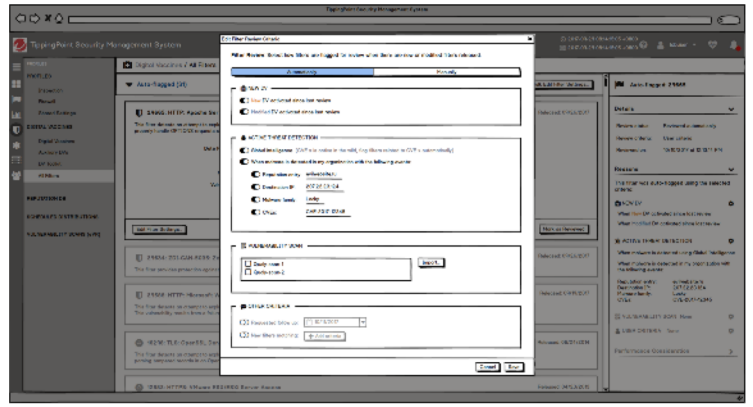
Actively auto-flagged filters for users to review based on users' contextual information, such as active threat detection (identify filters that are related to exploits identified in users' environment.)



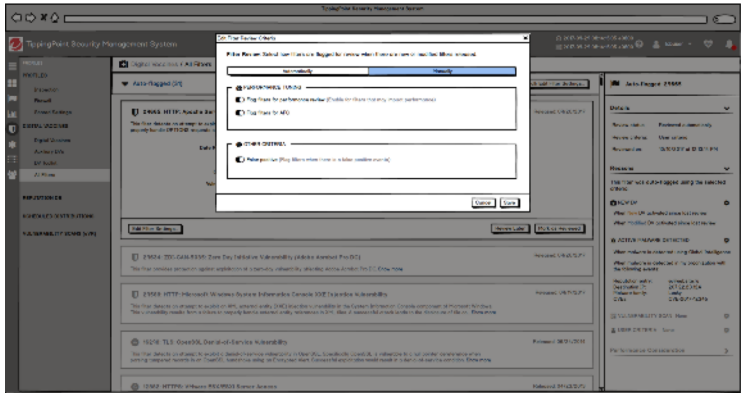
Brad sees there are 40 filters to review, so he clicks 'Review Filters' to see the details.



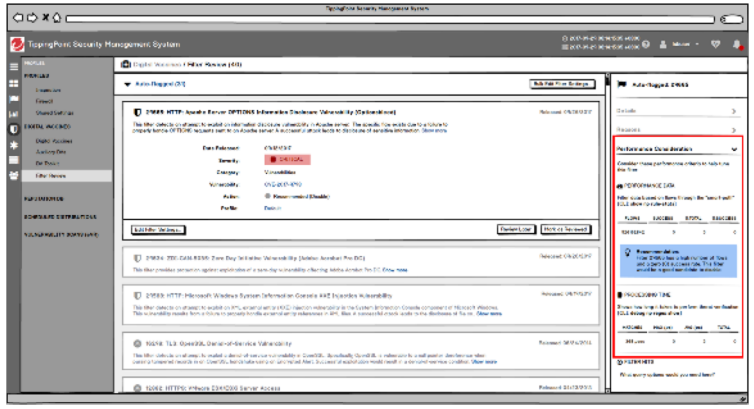
Brad notices some filters were auto-flagged by the SMS, so one-by-one, he drills down to the details to understand the reasons that were flagged. After checking one of the filters, Brad looks at the right panel, which indicates it is not only a new DV, but that there are also detected threats that were actively trying to take advantage of a CVE exploit within his organization.



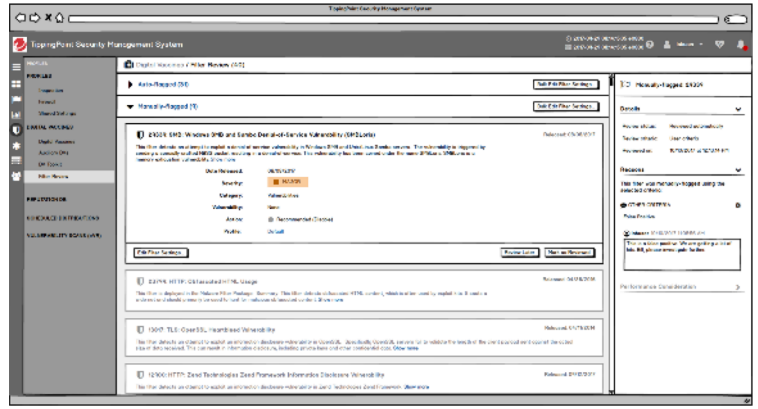
Brad looks at the 'Edit Filter Review Criteria' screen to see if he needs to make any changes to the automatic or manual flagging criteria.



Brad looks at the 'Edit Filter Review Criteria' screen to see if he needs to make any changes to the automatic or manual flagging criteria.



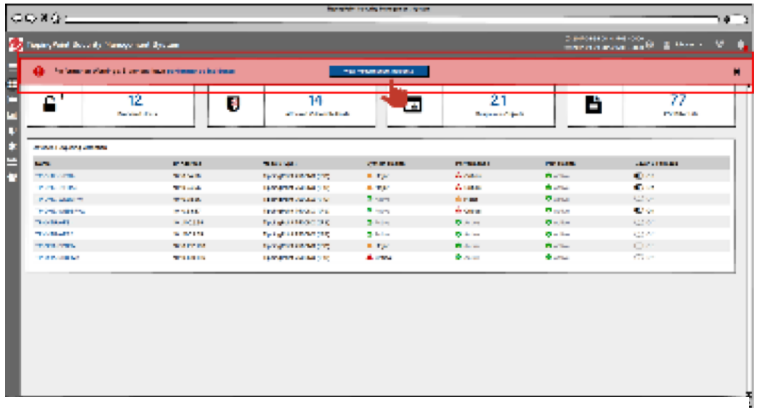
After reviewing the flagging settings, Brad continues to check the performance of this filter in order to decide whether to disable or enable the filter.



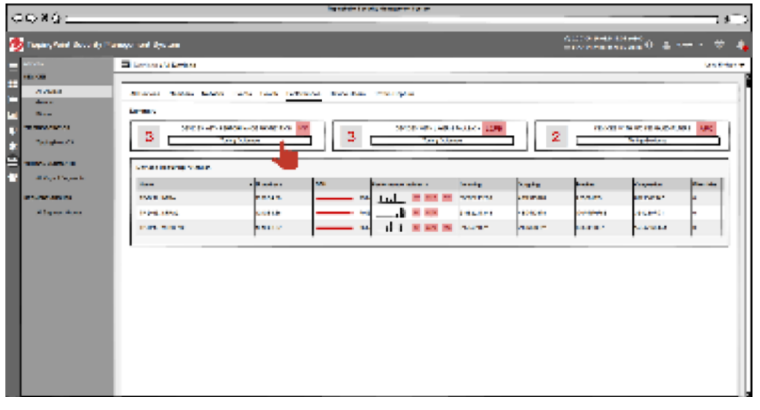
After reviewing all of auto-flagged filters, Brad continues to review all the manually-flagged filters. He notices that his colleague left a comment on this filter.

SCENARIO 2 – PERFORMANCE MANAGEMENT

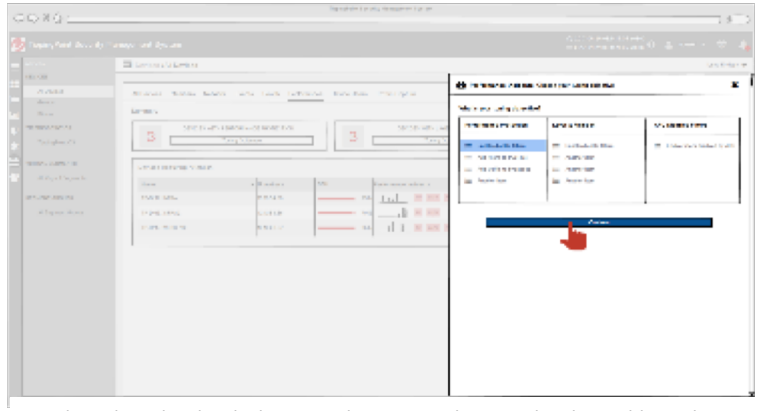
Actively notify users about performance issues along with performance statistics data on SMS console. Then, provide tuning guidance to users for step-by-step troubleshooting.



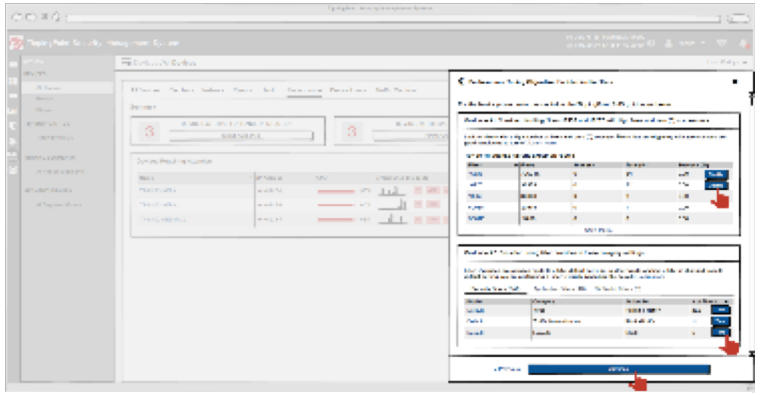
On the screen, the banner on the top displays, "Performance Warnings: 3 devices have performance incidents." Brad quickly clicks the 'View Performance Incidents' button to check the performance incident details, and tries to resolve them.



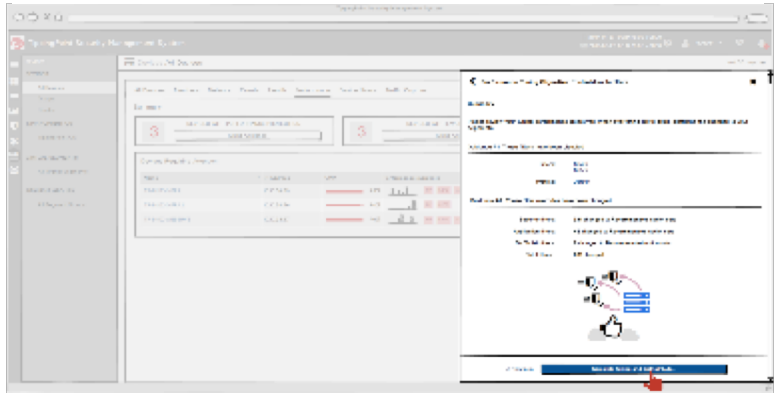
On the performance details page, Brad sees a summary of devices that have performance issues, device details, and other statistical data. After reviewing the performance incident details, Brad confirms that this incident needs to be resolved immediately. So, Brad clicks the 'Tuning Guidance' button to see what actions he can take to resolve the problem.



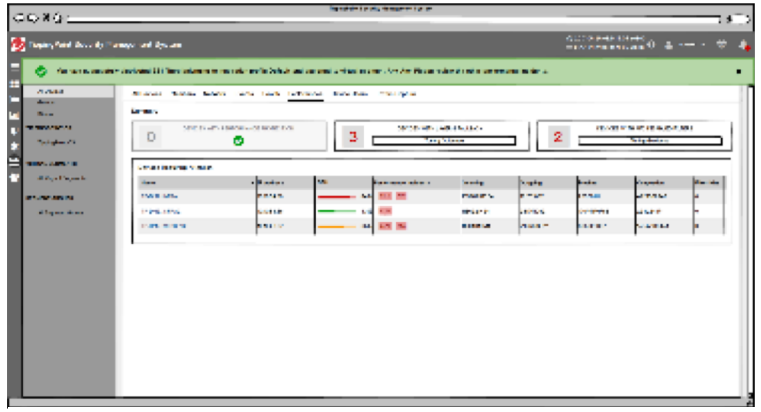
Brad needs to decide which tuning objective can best resolve the problem. Then, he continues on to the next step.



Two suggestions display for Brad:
1.) Disable certain filters with high flow rates that also have a zero success rate.
2.) Tune the filter overrides in certain category settings.
After Brad performs the tuning, he clicks 'Continue'…



Brad reviews the actions he took earlier to ensure that everything is working as he expected before he distributes the changes to other segments.
Once the review is done, Brad clicks 'Complete tuning and distribute…'.



Brad then checks that the changes have been successfully applied to the appropriate filters.

TREND MICRO

WORKSHOP PARTICIPANTS

- **USER PROFILE**
- **USER SCENARIOS**

Attendees – 19 Customers

Attendee		Role	Company
Yijoon	Park	Security Ops Manager	Hyundai AutoEver America
Russell	Jordan	IT Infrastructure Security Manager	Trustmark
Kevin	Glass	Manager - Network IPS	Regions Bank
Justin	Simmons	Sr. Security Analyst	Mastercard
Bill	LaRiviere	Sr Cyber Security Engineer	Regions Bank
steven	greenberg	Director	Nelnet
Benjamin	Focht	InfoSec Engineer	Nelnet
Christopher	Copeland	Senior Information Security Analyst	The University of Alabama
Randy	Freston	Information Security Engineer	Bank of America
Logan	Zahn	Security Engineer	GoDaddy.com
Imad	Elimam	Senior Analyst	Alabama Power Company
Dale	Gleneck	Security Analyst III	International Paper
Arthur	Jeffords	Enterprise Architect	Covenant Health
Gregg	LeBel	Security Architect	Asurion
Bradford	Hutchins	Associate Director, GSIRT Operations	Sony Corp. of America
Vincent	Koski	Security Engineer	Godaddy.com
Steve	Magers	Manager Cyber Security	Sempra Infrastructure
Sean	Thomas		Embry Riddle
Greg	Gabet		LFG

USER TYPES

SMALLER SECURITY TEAM

TRUST VENDOR

- Although they would like to do security tuning, they currently **adopt default or recommended settings due to resource constraint,** and rely on the solution to function and perform with no issue
- **Push rules immediately**
  - Would like to have a dependable way to insert a test period to new / modified rules to placing them in block mode
- **Any help here would save us significant effort & expand our capabilities**.

LARGER SECURITY TEAM

GET TO THE BOTTOM OF MATTER

- Highly specialized division of labors (Review – Implement – Distribute)
- Write **custom signature** by their threat researcher
- Want to **know the content of signature**
- Want to **know the definition and reasons behind filters** or **recommended actions**
  - *"Why do you suggest enable this filter? Why the recommended action is block?"*

KEY FINDINGS & RECOMMENDATIONS

SCENARIO - NEW DV RELEASE

ULTIMATE GOAL: KNOWING WHICH FILTERS TO TURN ON/OFF TO PROTECT MY ENVIRONMENT EFFECTIVELY.

RESEARCH & REVIEW	TEST	IMPLEMENT/DISTRIBUTE	TRACK
• Knowing new Zero-day notification immediately • Knowing which filters are relevant to my environment	• All applicable rules are set properly. Don't under/over tune • Blocking bad without impacting good	Ease and speed of pushing changes	Have a visibility of why it was done and what were changed
Pain Points	**Pain Points**	**Pain Points**	**Pain Points**
• Resource intensive • Manual process is easy to miss a filter • Insufficient information for making informative decisions	• Difficult to predict potential impact • Difficult to establish a baseline	Time consuming for distributing profiles globally	• Audit issues are frustrating and hard to fix • Manually document any changes in a spreadsheet

SCENARIO - MONITOR & ADJUST

MONITOR

- Watch for issues that affect the business
- Ensure filters work as expected

Pain Points

- Worrying about passing something that we are not paying attention through all the noise
- Visibility of non-communication devices
- Keeping sensors online
- Current performance graphs are very slow to generate & not very scalable

TROUBLESHOOT & REFINE

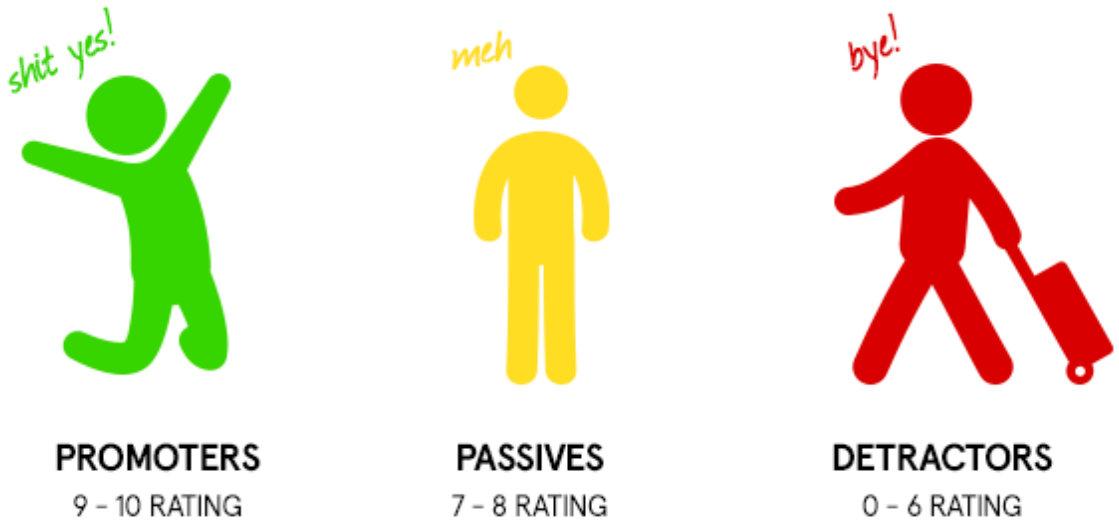
- Analyze block events
- Performance impact investigation
- Adjust filters as needed.

Pain Points

- Difficult to troubleshoot for block events as lacking the cause of block.
  - Have to do L2FB to confirms block location
- Reaction time needs to be much shorter with less manual process
- Logging into each appliance to run metrics, even with relatively few boxes, is cumbersome.

NPS (NET PROMOTER SCORE)

Having looked at this concept today, on a scale of one to ten, how likely is that you would recommend this feature to your colleagues or manager? (0 not at all likely – 10 extremely likely)



- **Promoters** are loyal, enthusiastic fans. They sing the company's praises to friends and colleagues. **They are far more likely than others to remain customers and to increase their purchases over time.**
- **Passives** we call this group "passively satisfied" because this group is **satisfied—for now**.
- **Detractors** are **unhappy customers**. Some may appear profitable from an accounting standpoint, but their criticisms and bad attitudes diminish a company's reputation, discourage new customers and demotivate employees.

OVERALL COMMENTS – FILTER REVIEWING/TUNING

11

PROMOTERS
9 - 10 RATING

- **Anything that helps the admin** - improve the quality of the performance
- **Looking the active threat page starts a hunt.**
- **Efficiency and quality of life**.
- Because **Java client is painful to learn/use**
- Very helpful looking which **provides more detail about scenarios on IPS**
- **Better audit tracking for filter changes** to show which users gave the recommendation for the filter.
- This is **helpful for managing at filter level**, **like to see more of a macro level management of filters** to help reduce support and solution costs.

5

PASSIVES
7 - 8 RATING

- Currently we are **blindly accepting recommended states, which actually bites us, due to time constraints**. **As long as this can be a quick efficient workflow**, **I foresee us scrapping our current approach for reviewing new rules.**
- Review of new filters is already a manual process, but this will make it easier.

1 N/A

DETRACTORS
0 - 6 RATING

OVERALL COMMENTS – PERFORMANCE TUNING

11

PROMOTERS
9 - 10 RATING

- Performance management hits home with me. **Bringing visibility to the SMS is very helpful**.
- **Something needed for a long time**
- Looks to streamline the rule review workflow
- Very much needed to do more intelligence, well informed tuning
- **This takes out much of the standard pain associated with TippingPoint**
- Helps to **avoid admin pain keeps IPS inline and healthy** while not impacting business
- **Having an actual defined review process is a big win**. This will immediately **help new users** as well.

5

PASSIVES
7 - 8 RATING

- I like what I saw in the scenario. However, I would like to know **how this fleshes out L2FB, and AFC are all huge**, but are these guides going to vary? If not, this seems like a wizard for standard tuning.
- Very useful. More is needed to **see which is affected.**
- This functionality is most useful to myself and the SOC. Most only cares about the overall metrics not the day-to-day tuning like this.

0

DETRACTORS
0 - 6 RATING

THE MOST USEFUL PART TO THEM

- Help make informative decisions:
  - The additional context around filter activity is very helpful allow us to make informative decisions.
  - Pull in vulnerability data in to make decision
  - detailed information on a filter easily seen
- Single pane of glasses/visibility:
  - Better visibility into important issues
  - Device stats on SMS. We need to squeeze all performance
  - Provide active threat information which gives another monitoring into someone is in.
- Auto-flagged filters
  - Configurable filter review criteria
  - Tagging rules for review historically we have used docs to keep track of these
- User comments to show better audit tracking

THE MOST USEFUL PART TO THEM

- The ability to have lower level techs make a change
- Fix performance issues faster
- The performance data on filters is something I need to program a script to do
  - No need for CLI
  - It is very much useful to see more performance info at the SMS and to dig to the filter level.
- The explanation of why the sensor is having issues and giving recommendations of potential fixes
- The performance tuning objective

USE A WORD TO DESCRIBE YOUR FEELING OF THE CONCEPT

- **Excellent!** This is the direction things need to go.
- **Helpful** - busy admins need help.
- **Great!** Feels much better, good flow and modern design.
- **Improvement**. Increase ease of use.
- **Potential.** I see this being a huge leap forward in product and my own SOC's monitoring.
- **Happy**. We have in-house scripts to help with performance due to almost complete lack of performance data actually on the SMS.
- **High level.** This seems like a good idea and framework. Keep going! Consider options to automate steps, maybe based on time, maybe in response to traffic spikes or other temporary issues.
- **Useful.** Use as training for inexperience analyst.

FEEDBACK AND SUGGESTIONS FROM USERS - 1

- "Don't want to only have a single place where a feature is implemented, want to do whatever we can in both Web and JAVA UI clients. **If we have to switch between interfaces to do a single job, then we are not doing it right**."
- The workflow needs to support for folks who separate reviews and pushes, or having multiple administrators review filters together
  - Role-based control
  - Filter review audit (by user)
  - They would like to know the domain account to know who login to SMS
- Auto flagged criteria could consider including the followings:
  - DVT filters
  - User defined or other internal source/IOC
  - ThreatLinQ/Threat Insights website
  - Host IPS Data

FEEDBACK AND SUGGESTIONS FROM USERS - 2

- More contextual information are expected by users to help them make informative decisions, such as:
  - **Profiles** that filter is assigned to
  - Shows number of **events** associated with flagged filters
  - **History of filters**: Has this filter been on before, when?
  - What are **other companies doing** with this filter info?
  - An indicator of confidence (green/red)
  - Pull the value of the CVE (# that 1-10) that's associated with CVE (CVSS)
  - Add Geo location
  - Filter explanation as well as the reasons of recommended action

FEEDBACK AND SUGGESTIONS FROM USERS - 3

- Actively advise filters to enable/disable:
  - Call out specifically active threats and give recommendation on what related filters to enable
  - If vulnerability scan shows the vulnerability patched, then advise users disable filter
  - Vuln scan results from URL - warn if disabling indicates exposure
- Include more performance metrics
  - sh np rule-stats, sh np tier-stats, debug np regex show; display XLR A/B/C balance; show L threads
- Change management: Any attempts to change filter action that has been reviewed should raise an alert.
  - Add (Profile and Filter) comments like blog (for history/audit)
- Have a mechanism to control overrides (allow/prevent tuned filters from being enabled/disabled)

Recommendations

- Conduct **task analysis** to scrub through currently filter reviewing and performance tuning tasks on JAVA console (As-Is user flow).
  - A diagram explaining the steps that a user must take in order to complete a goal.
  - Laid all the steps out, you will then be in a position to see where additional user support is required (for example, you might wish to automate some actions that the user currently undertakes), or eliminate unnecessary steps, in order to minimize the number of actions that a user has to undertake, unassisted.
- Conduct **gap analysis** between As-Is and To-Be flow
- Iterative user validations

Thank you.