Designing Active Threat Defense Workflows

Michael Lang, UI designer, HIE Design Team

Design

Design

Customers

PMs

UX

Devs

Customers

PMs

UX

Devs

- User needs
- User stories
- Feature ideation

Customers

PMs

UX

Devs

- User needs
- User stories
- Feature ideation

- API
- Wireframes
- Prototypes

Customers

PMs

UX

Devs

- User needs
- User stories
- Feature ideation

- API
- Wireframes
- Prototypes

- Development
- User testing
- L10N/Docs

Customers

PMs

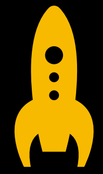
UX

Devs

- User needs
- User stories
- Feature ideation

- API
- Wireframes
- Prototypes

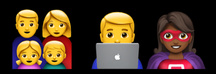
- Development
- User testing
- L10N/Docs



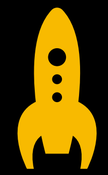
PRODUCT

- User needs
- User stories
- Feature ideation

- API
- Wireframes
- Prototypes

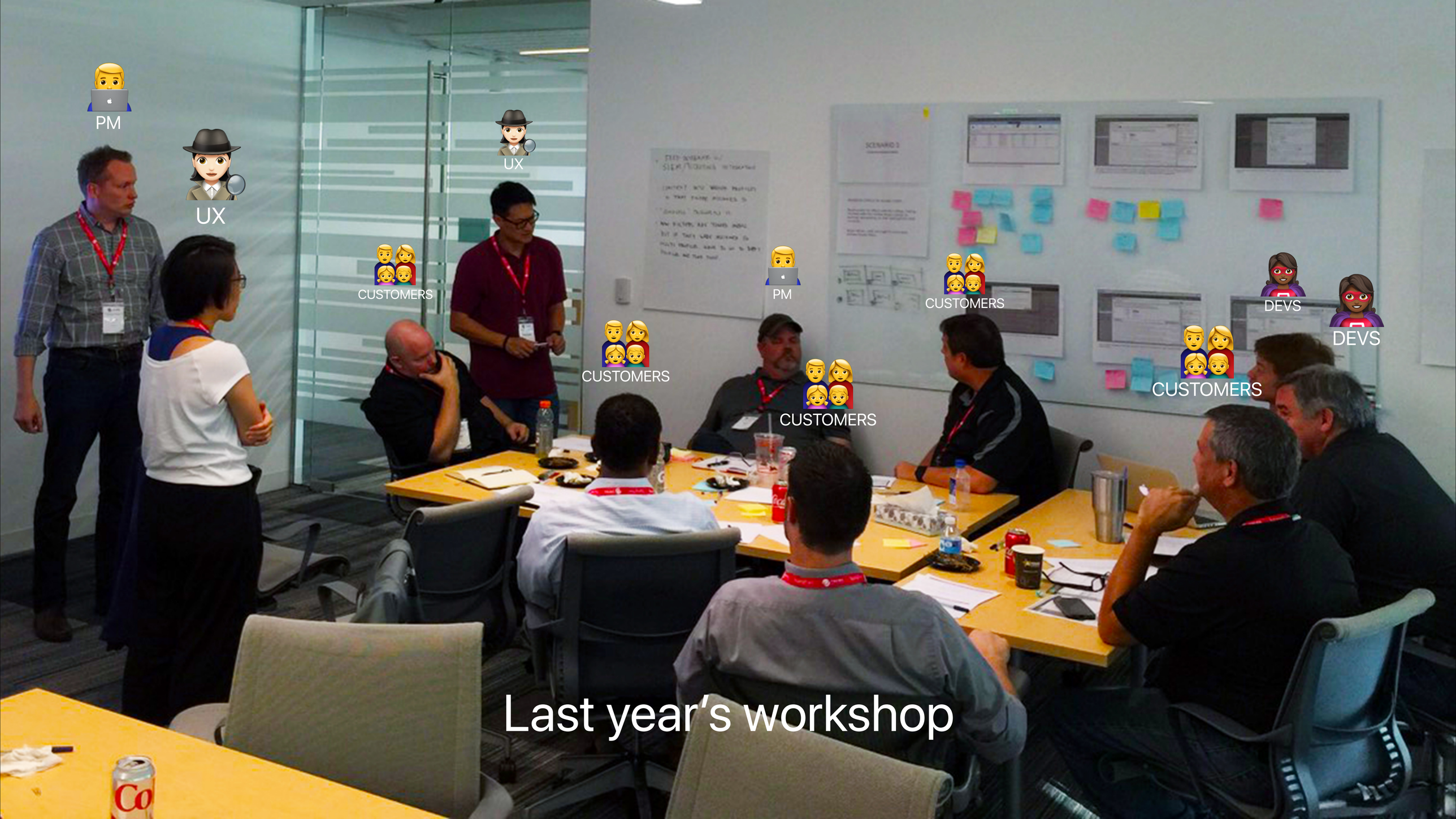


- Development
- User testing
- L10N/Docs

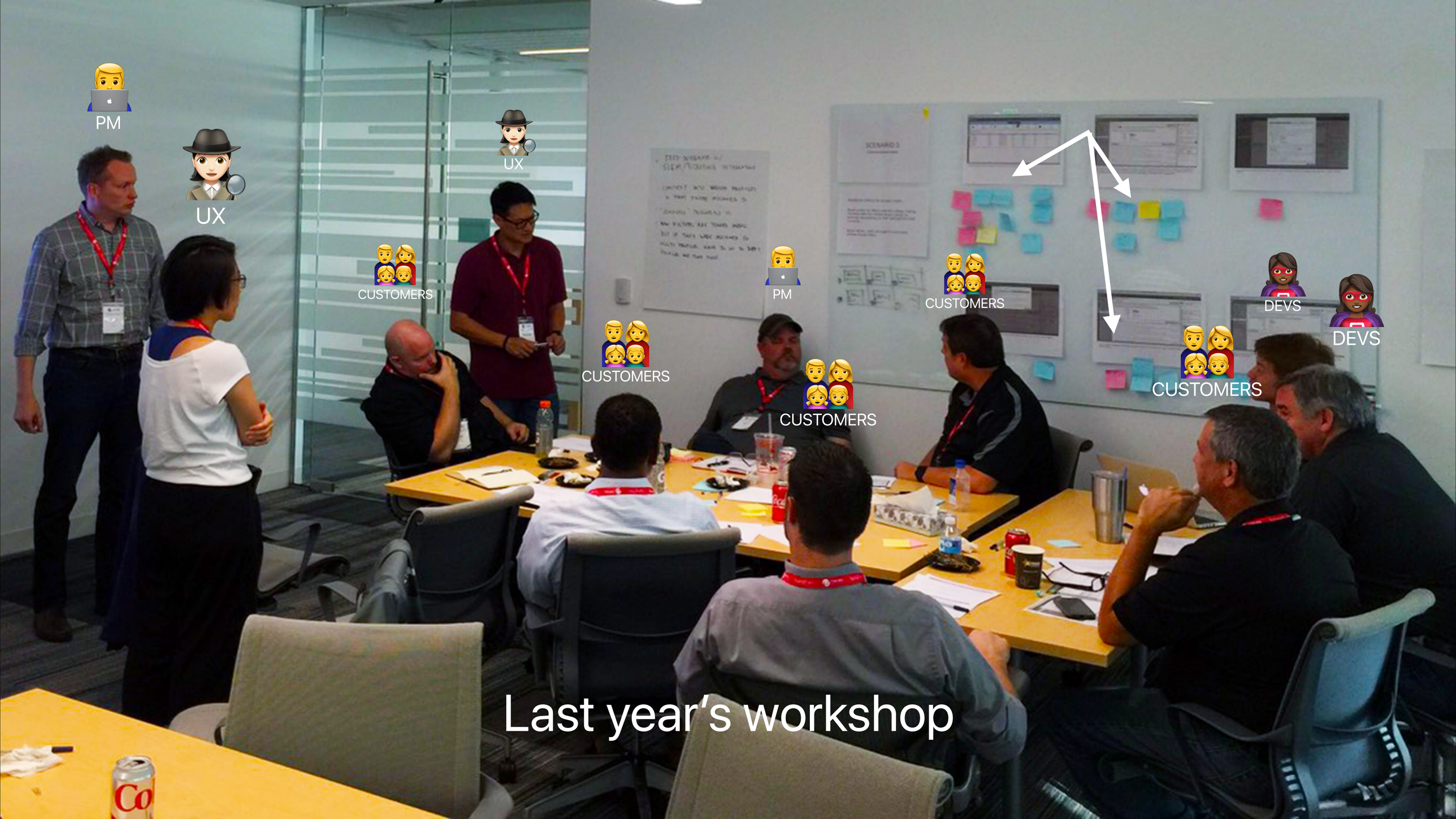


PRODUCT

✅ UX Workshop ✅ Prototype ❌ Implementation



Last year’s workshop



Last year’s workshop

Filters tuning

Performance management

SCENARIO 1

FILTER REVIEWING/TUNING

Brad enters his office with his coffee. Taking his time with his coffee, Brad notices a banner appearing on the TippingPoint SMS console.

Brad: Hmm.. well, let's get to work and review those filters.

SCENARIO 2

PERFORMANCE MANAGEMENT

Brad just got back from lunch and has decided to take a nap but notices another banner, this time in red.

Brad (offscreen): Uh oh! No time for a nap. I better look into this...

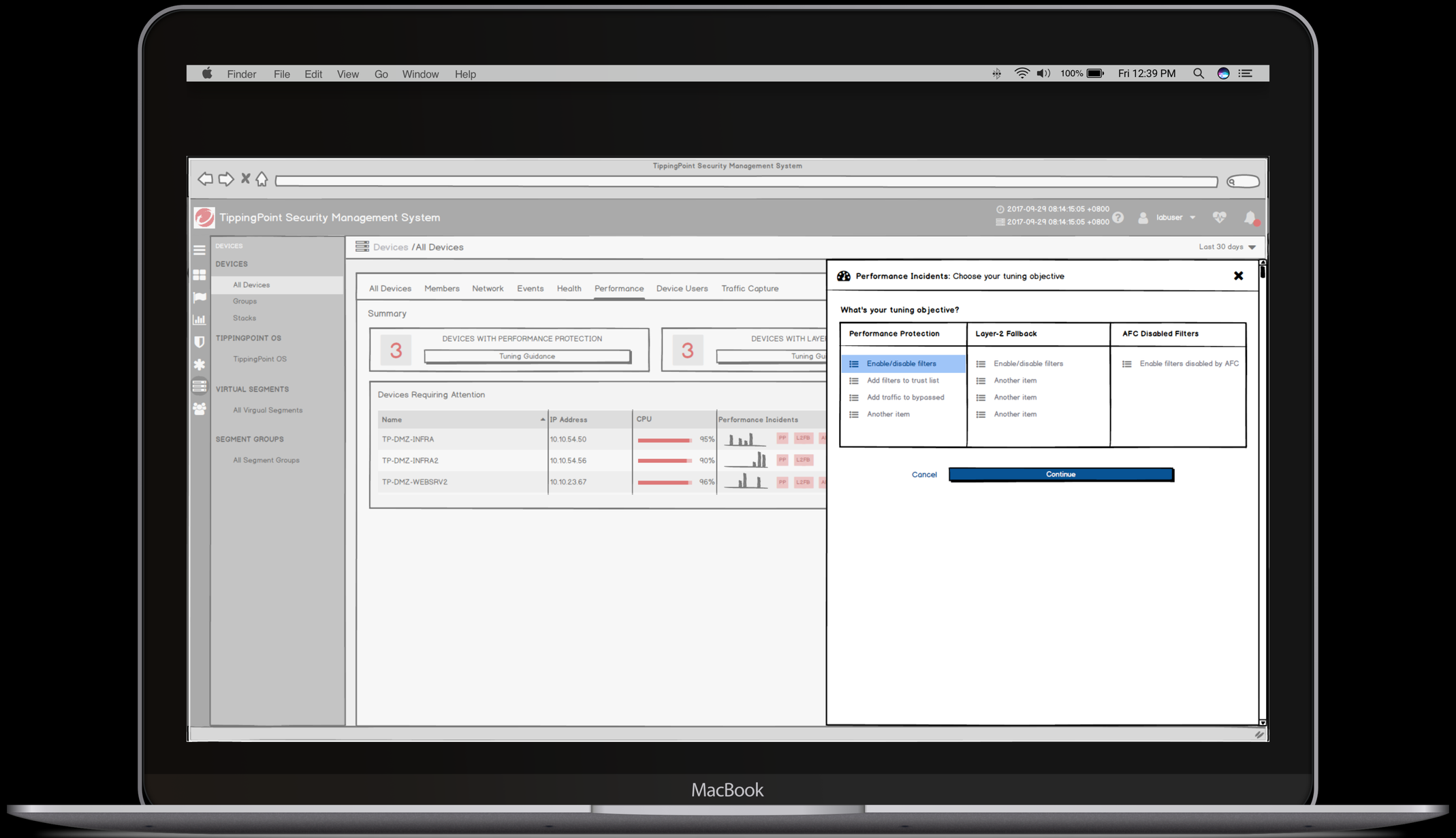
Issues

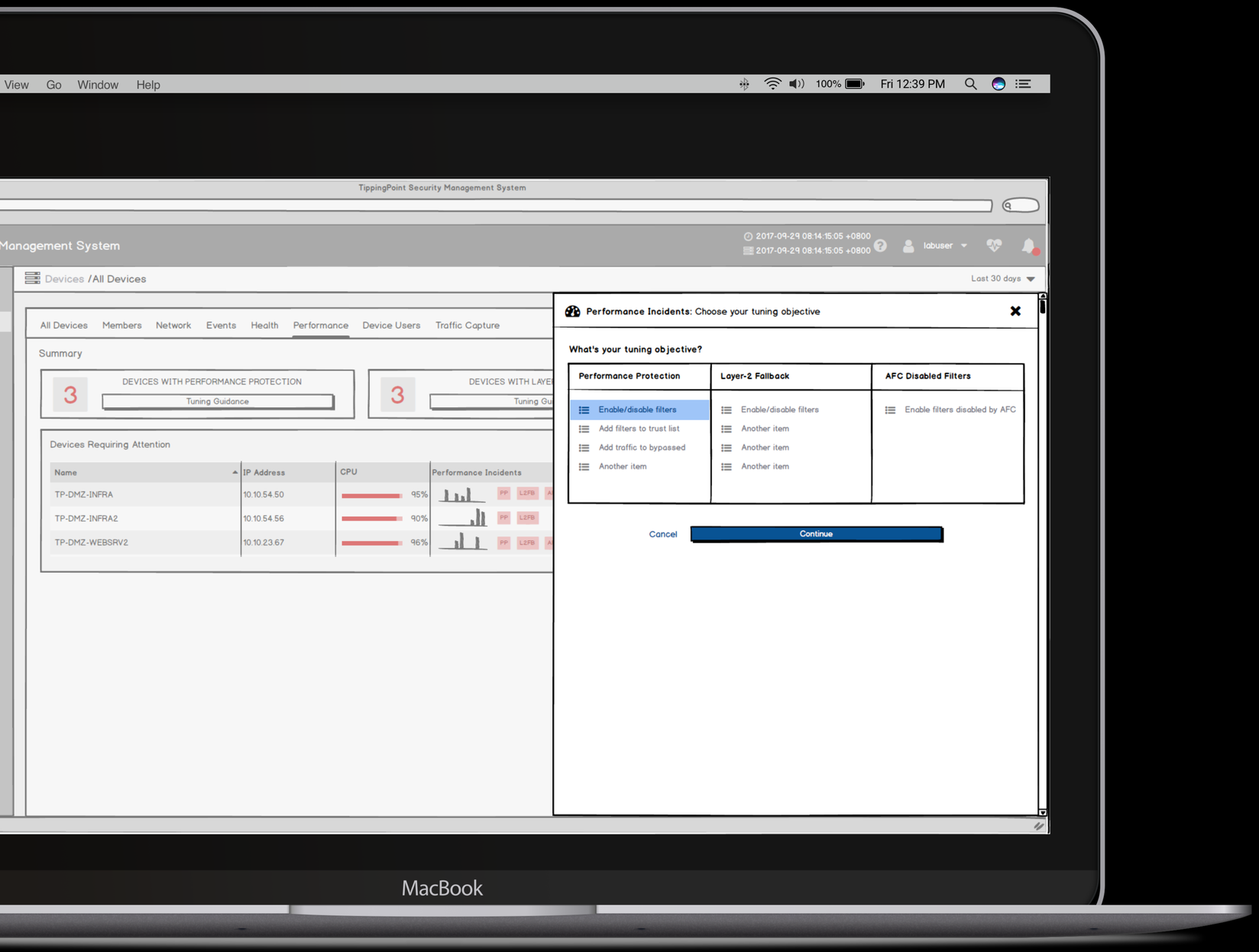
Useful

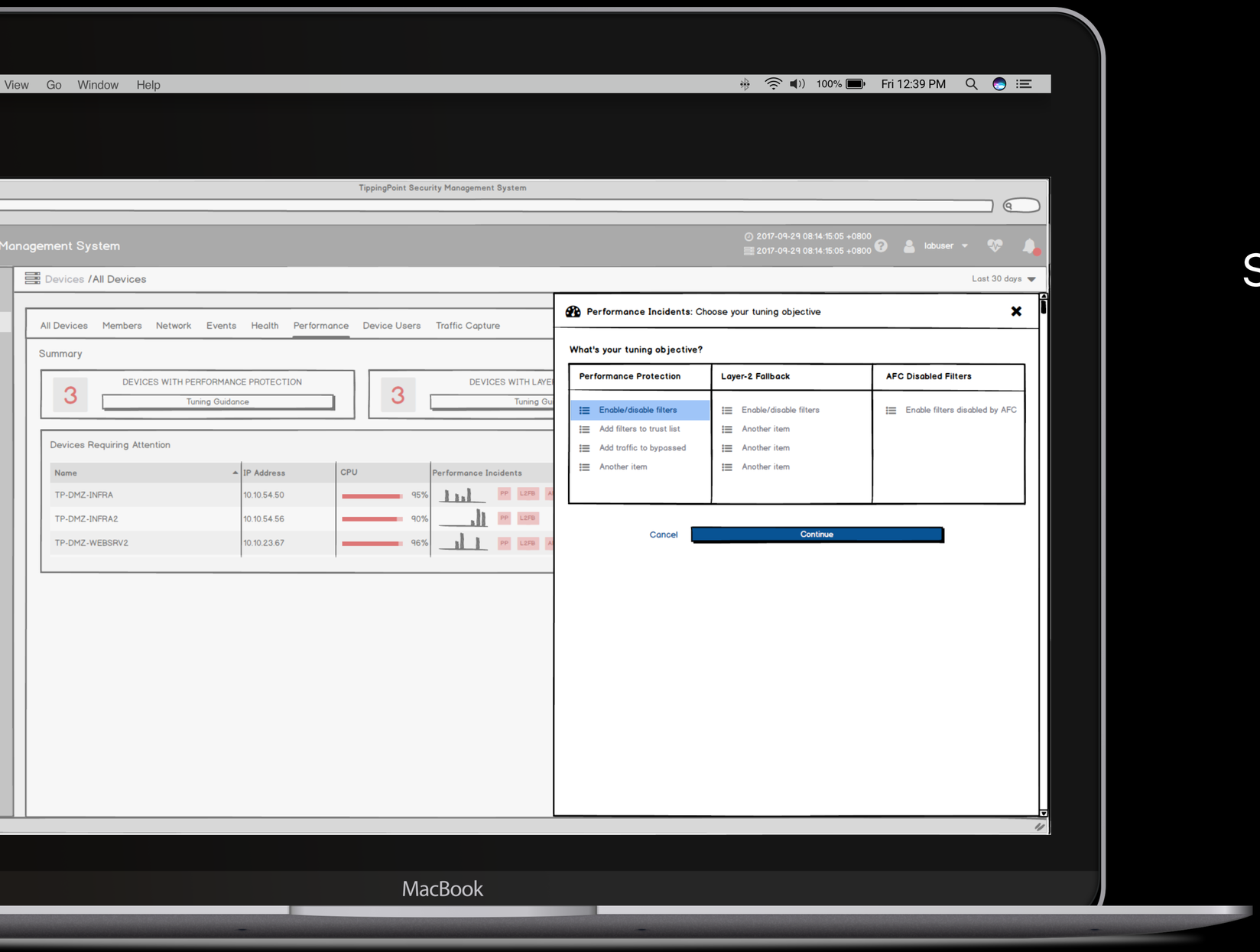
Suggestions

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.

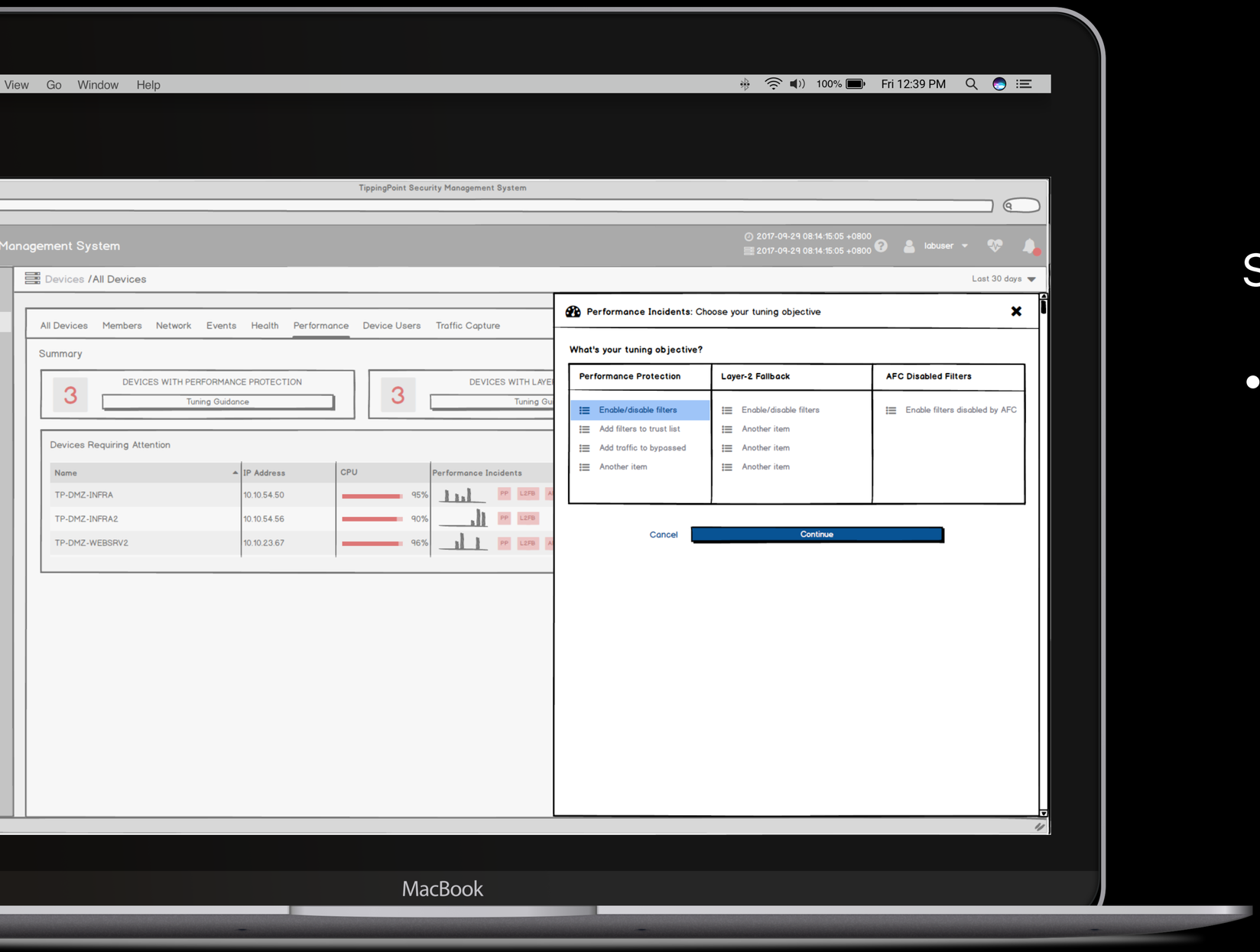
Central Performance Management


Finder File Edit View Go Window Help
100% Fri 12:39 PM
TippingPoint Security Management System
TippingPoint Security Management System
2017-09-29 08:14:15.05 +0800
2017-09-29 08:14:15.05 +0800
labuser
DEVICES
DEVICES
All Devices
Groups
Stacks
TIPPINGPOINT OS
TippingPoint OS
VIRTUAL SEGMENTS
All Virgual Segments
SEGMENT GROUPS
All Segment Groups
Devices /All Devices
Last 30 days
All Devices Members Network Events Health Performance Device Users Traffic Capture
Summary
3
DEVICES WITH PERFORMANCE PROTECTION
Tuning Guidance
3
Devices Requiring Attention
Name
IP Address
CPU
Performance Incidents
TP-DMZ-INFRA
10.10.54.50
95%
TP-DMZ-INFRA2
10.10.54.56
90%
TP-DMZ-WEBSRV2
10.10.23.67
96%
Performance Incidents: Choose your tuning objective
What's your tuning objective?
Performance Protection
Enable/disable filters
Add filters to trust list
Add traffic to bypassed
Another item
Layer-2 Fallback
Enable/disable filters
Another item
Another item
Another item
AFC Disabled Filters
Enable filters disabled by AFC
Cancel
Continue
MacBook


View Go Window Help
100% Fri 12:39 PM
TippingPoint Security Management System
Management System
2017-09-29 08:14:15:05 +0800
2017-09-29 08:14:15:05 +0800
labuser
Devices /All Devices
Last 30 days
All Devices Members Network Events Health Performance Device Users Traffic Capture
Summary
3
DEVICES WITH PERFORMANCE PROTECTION
Tuning Guidance
3
Devices Requiring Attention
Name
IP Address
CPU
Performance Incidents
TP-DMZ-INFRA
10.10.54.50
95%
TP-DMZ-INFRA2
10.10.54.56
90%
TP-DMZ-WEBSRV2
10.10.23.67
96%
Performance Incidents: Choose your tuning objective
What's your tuning objective?
Performance Protection
Enable/disable filters
Add filters to trust list
Add traffic to bypassed
Another item
Layer-2 Fallback
Enable/disable filters
Another item
Another item
Another item
AFC Disabled Filters
Enable filters disabled by AFC
Cancel
Continue
MacBook

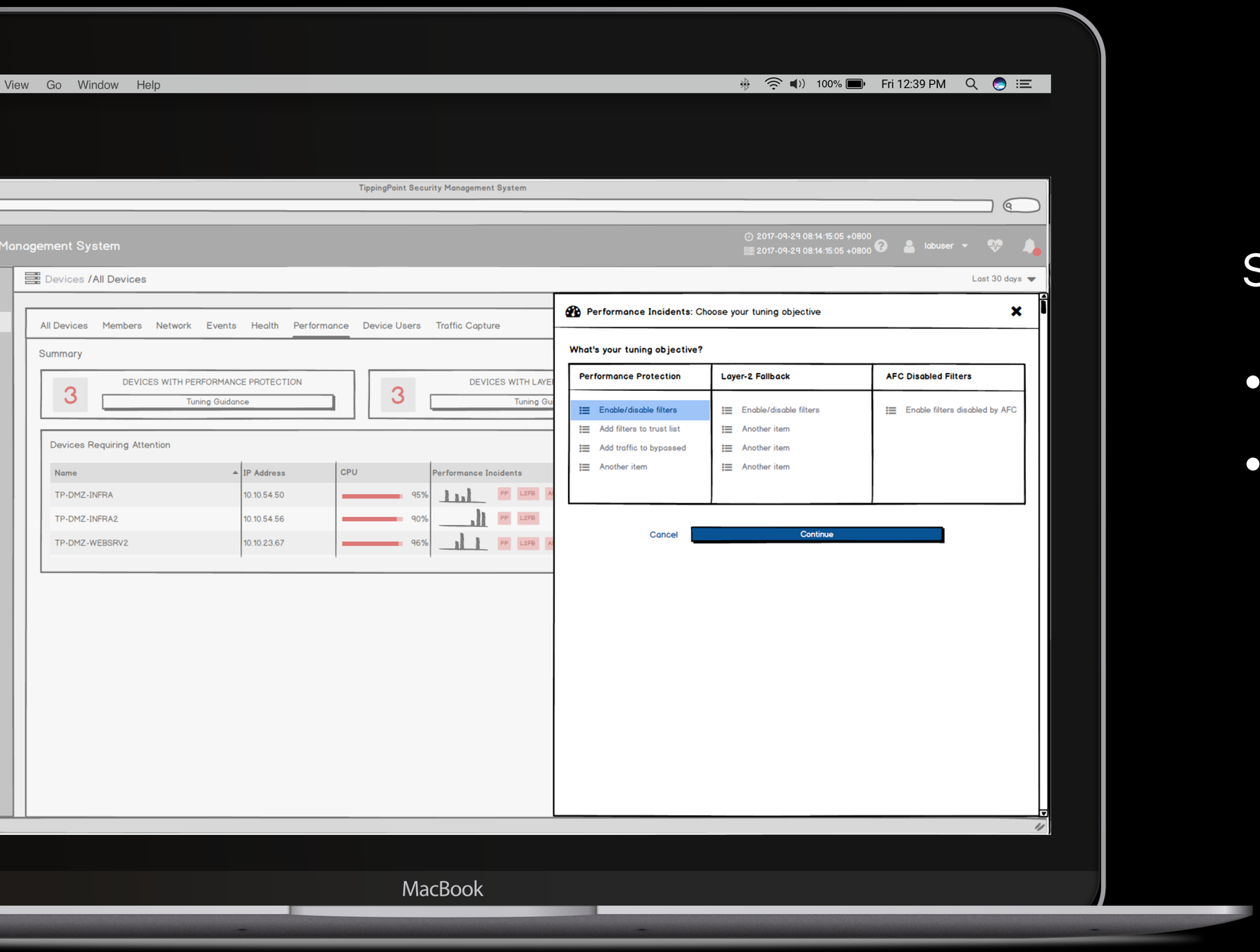


Sketch focused on:



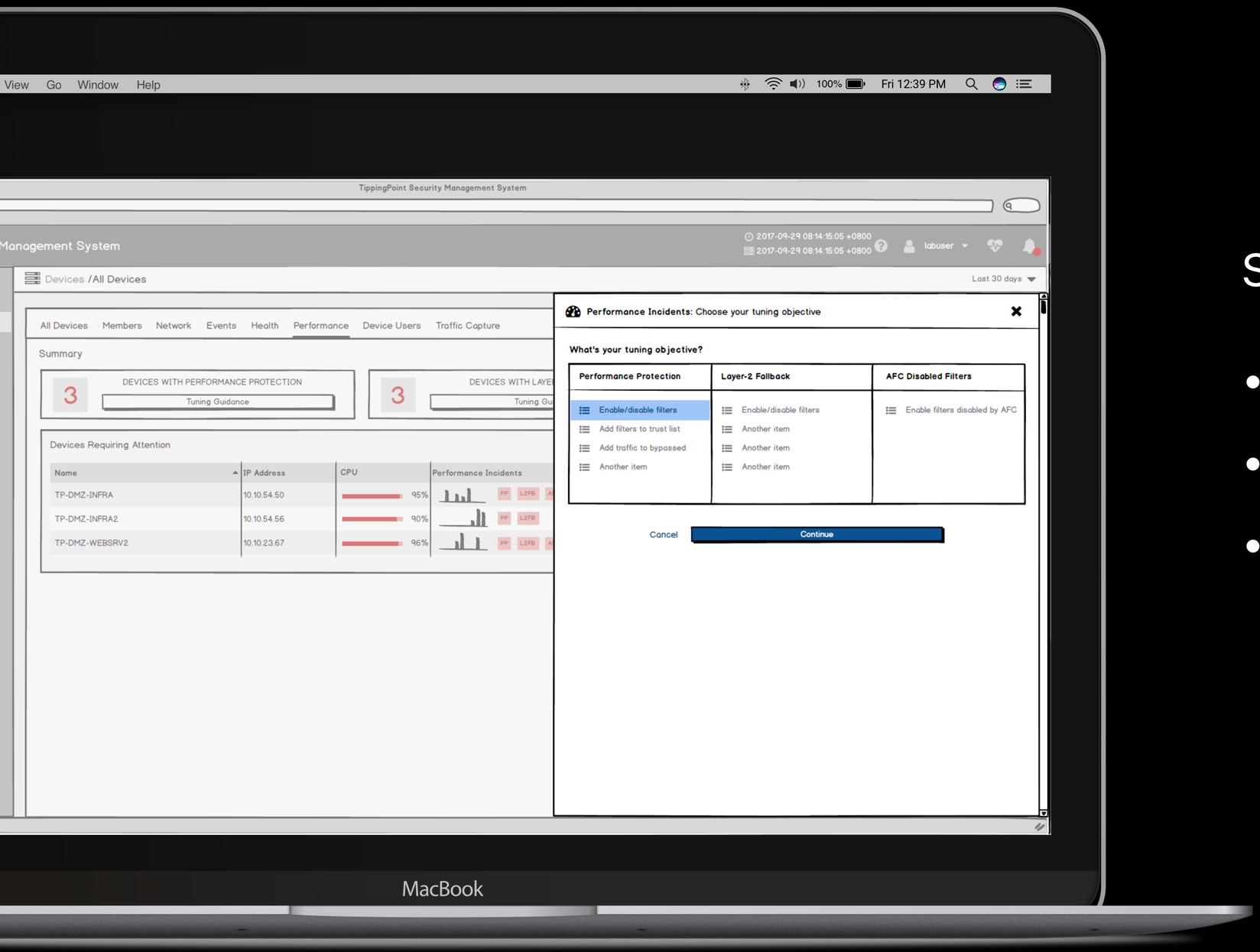
Sketch focused on:

- Devices with performance protection



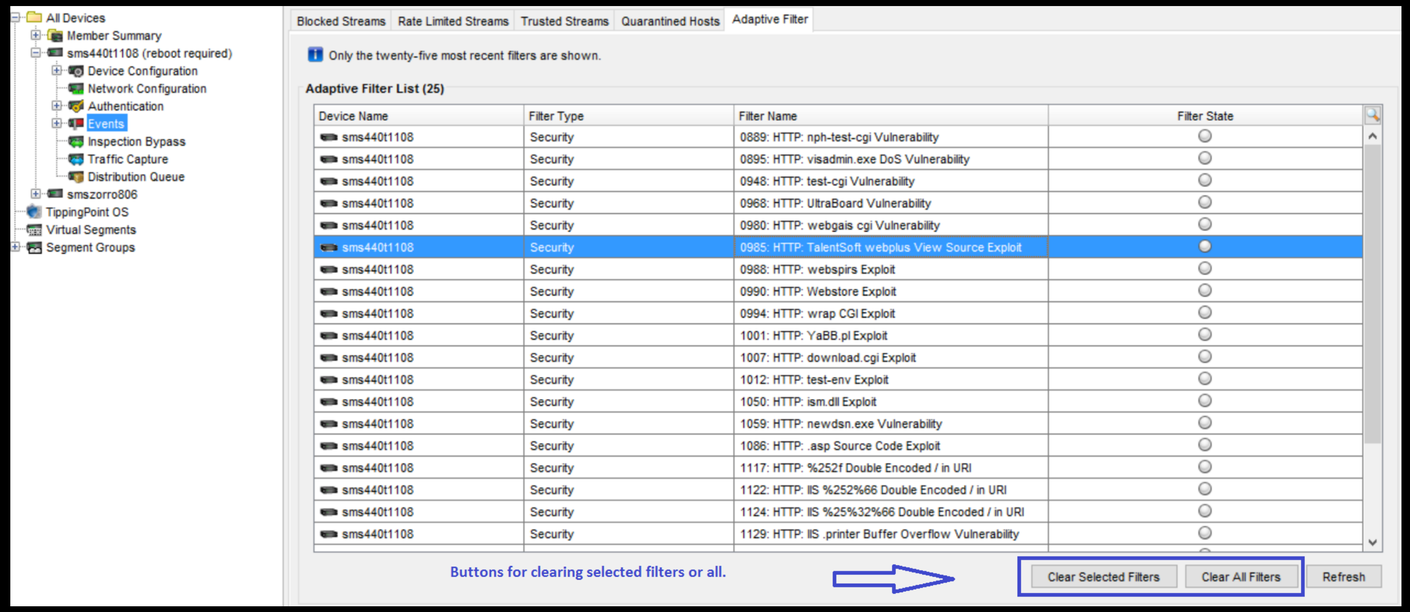
Sketch focused on:

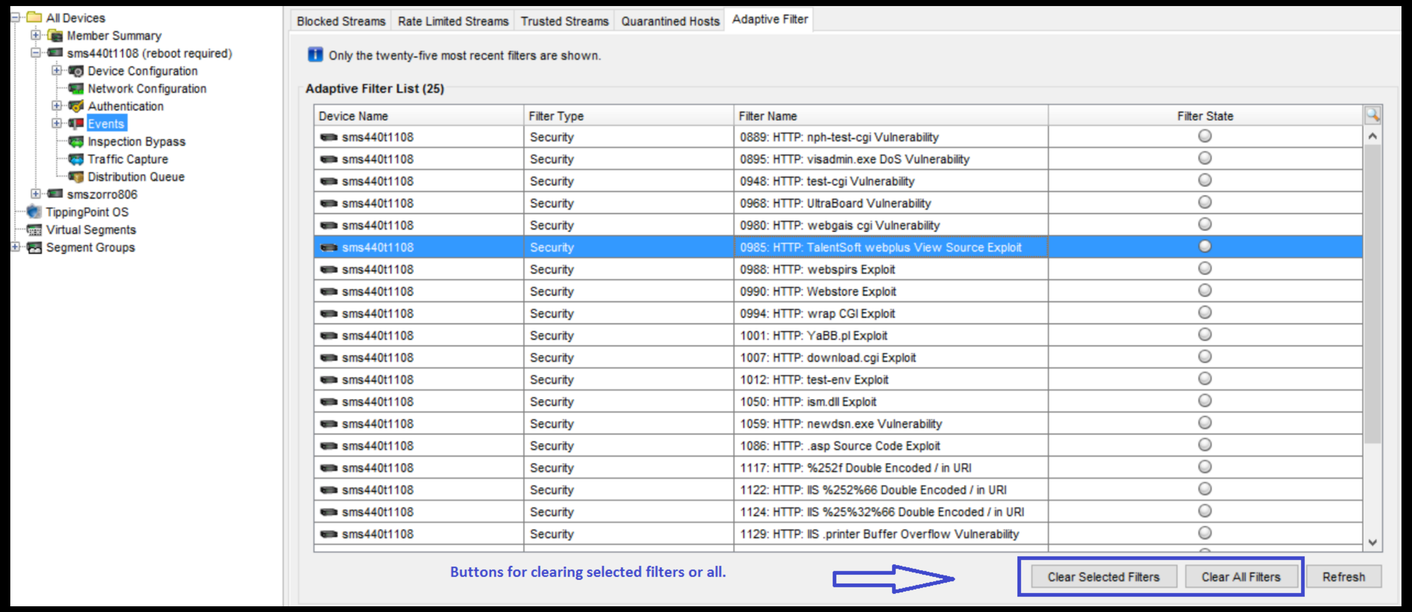
- Devices with performance protection
- Devices with L2FB disabled filters



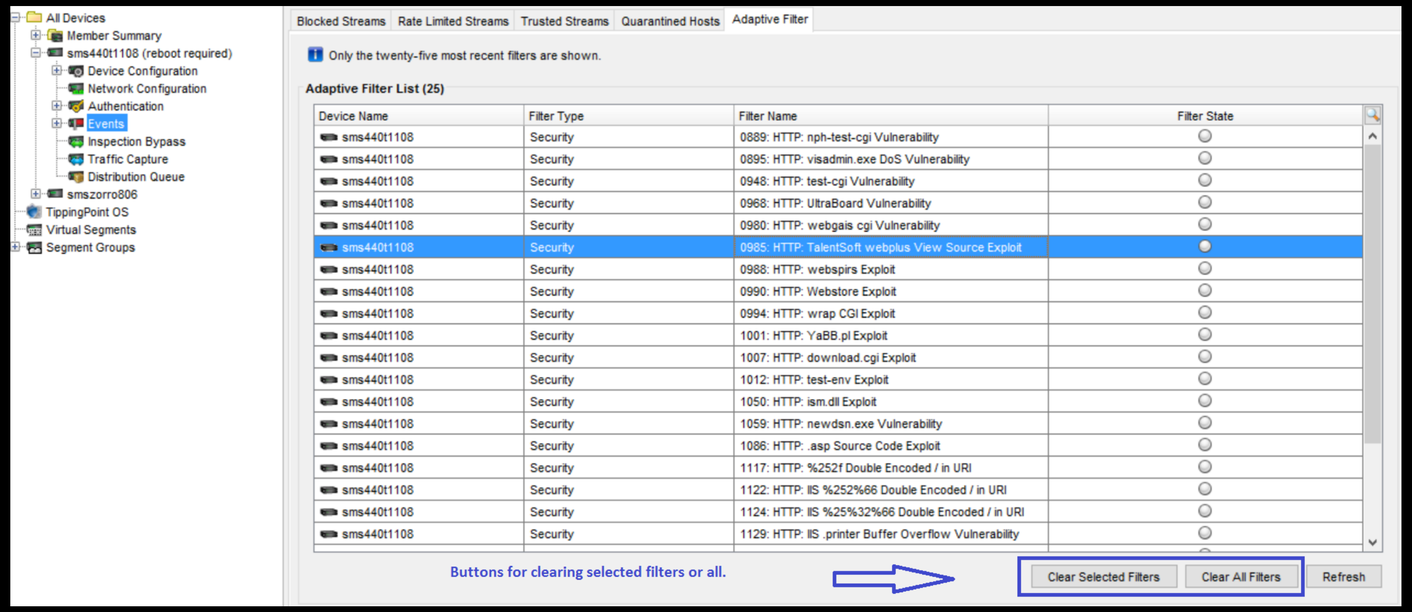
Sketch focused on:

- Devices with performance protection
- Devices with L2FB disabled filters
- Devices with AFC disabled filters


All Devices
Member Summary
sms440t1108 (reboot required)
Device Configuration
Network Configuration
Authentication
Events
Inspection Bypass
Traffic Capture
Distribution Queue
smszorro806
TippingPoint OS
Virtual Segments
Segment Groups
Blocked Streams
Rate Limited Streams
Trusted Streams
Quarantined Hosts
Adaptive Filter
Only the twenty-five most recent filters are shown.
Adaptive Filter List (25)
Device Name
Filter Type
Filter Name
Filter State
sms440t1108 Security 0889: HTTP: nph-test-cgi Vulnerability
sms440t1108 Security 0895: HTTP: visadmin.exe DoS Vulnerability
sms440t1108 Security 0948: HTTP: test-cgi Vulnerability
sms440t1108 Security 0968: HTTP: UltraBoard Vulnerability
sms440t1108 Security 0980: HTTP: webgais cgi Vulnerability
sms440t1108 Security 0985: HTTP: TalentSoft webplus View Source Exploit
sms440t1108 Security 0988: HTTP: webspirs Exploit
sms440t1108 Security 0990: HTTP: Webstore Exploit
sms440t1108 Security 0994: HTTP: wrap CGI Exploit
sms440t1108 Security 1001: HTTP: YaBB.pl Exploit
sms440t1108 Security 1007: HTTP: download.cgi Exploit
sms440t1108 Security 1012: HTTP: test-env Exploit
sms440t1108 Security 1050: HTTP: ism.dll Exploit
sms440t1108 Security 1059: HTTP: newdsn.exe Vulnerability
sms440t1108 Security 1086: HTTP: .asp Source Code Exploit
sms440t1108 Security 1117: HTTP: %252f Double Encoded / in URI
sms440t1108 Security 1122: HTTP: IIS %252%66 Double Encoded / in URI
sms440t1108 Security 1124: HTTP: IIS %25%32%66 Double Encoded / in URI
sms440t1108 Security 1129: HTTP: IIS .printer Buffer Overflow Vulnerability
Buttons for clearing selected filters or all.
Clear Selected Filters
Clear All Filters
Refresh

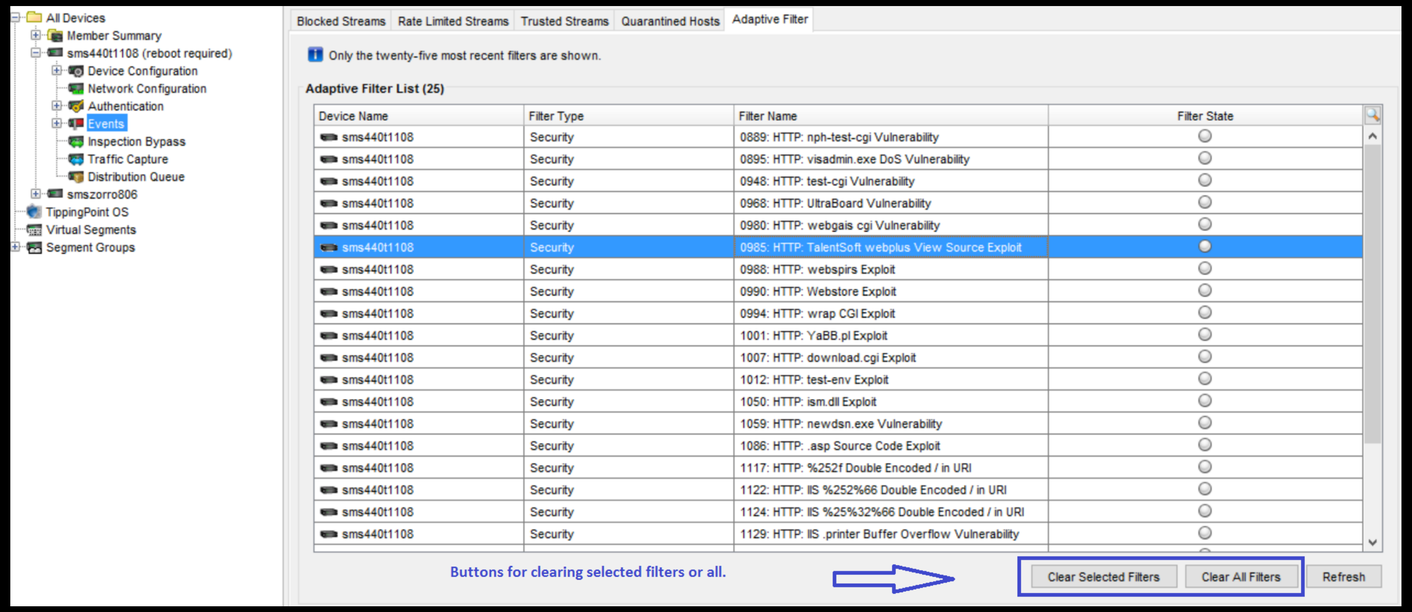

All Devices
Member Summary
sms440t1108 (reboot required)
Device Configuration
Network Configuration
Authentication
Events
Inspection Bypass
Traffic Capture
Distribution Queue
smszorro806
TippingPoint OS
Virtual Segments
Segment Groups
Blocked Streams
Rate Limited Streams
Trusted Streams
Quarantined Hosts
Adaptive Filter
Only the twenty-five most recent filters are shown.
Adaptive Filter List (25)
Device Name
Filter Type
Filter Name
Filter State
sms440t1108 Security 0889: HTTP: nph-test-cgi Vulnerability
sms440t1108 Security 0895: HTTP: visadmin.exe DoS Vulnerability
sms440t1108 Security 0948: HTTP: test-cgi Vulnerability
sms440t1108 Security 0968: HTTP: UltraBoard Vulnerability
sms440t1108 Security 0980: HTTP: webgais cgi Vulnerability
sms440t1108 Security 0985: HTTP: TalentSoft webplus View Source Exploit
sms440t1108 Security 0988: HTTP: webspirs Exploit
sms440t1108 Security 0990: HTTP: Webstore Exploit
sms440t1108 Security 0994: HTTP: wrap CGI Exploit
sms440t1108 Security 1001: HTTP: YaBB.pl Exploit
sms440t1108 Security 1007: HTTP: download.cgi Exploit
sms440t1108 Security 1012: HTTP: test-env Exploit
sms440t1108 Security 1050: HTTP: ism.dll Exploit
sms440t1108 Security 1059: HTTP: newdsn.exe Vulnerability
sms440t1108 Security 1086: HTTP: .asp Source Code Exploit
sms440t1108 Security 1117: HTTP: %252f Double Encoded / in URI
sms440t1108 Security 1122: HTTP: IIS %252%66 Double Encoded / in URI
sms440t1108 Security 1124: HTTP: IIS %25%32%66 Double Encoded / in URI
sms440t1108 Security 1129: HTTP: IIS .printer Buffer Overflow Vulnerability
Buttons for clearing selected filters or all.
Clear Selected Filters
Clear All Filters
Refresh

CPM



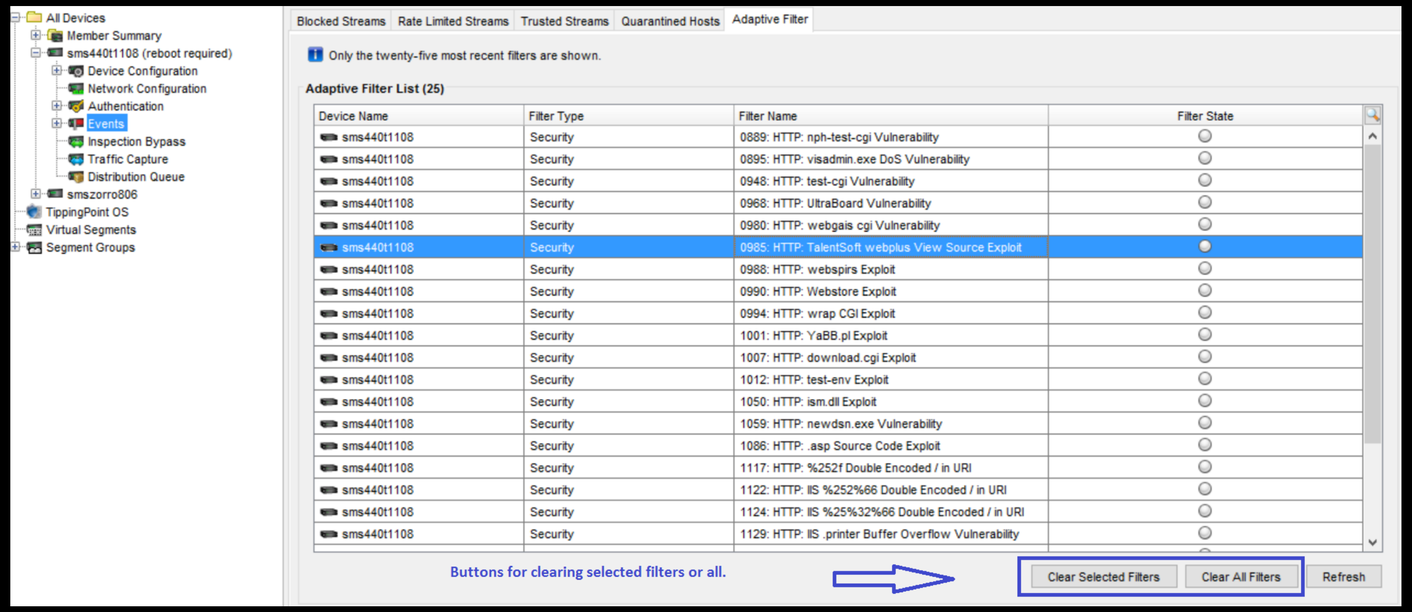
CPM

- Incident reports



CPM

- Incident reports
- Stats for IPS/TPS devices



CPM

- Incident reports
- Stats for IPS/TPS devices
- Downloadable datasets

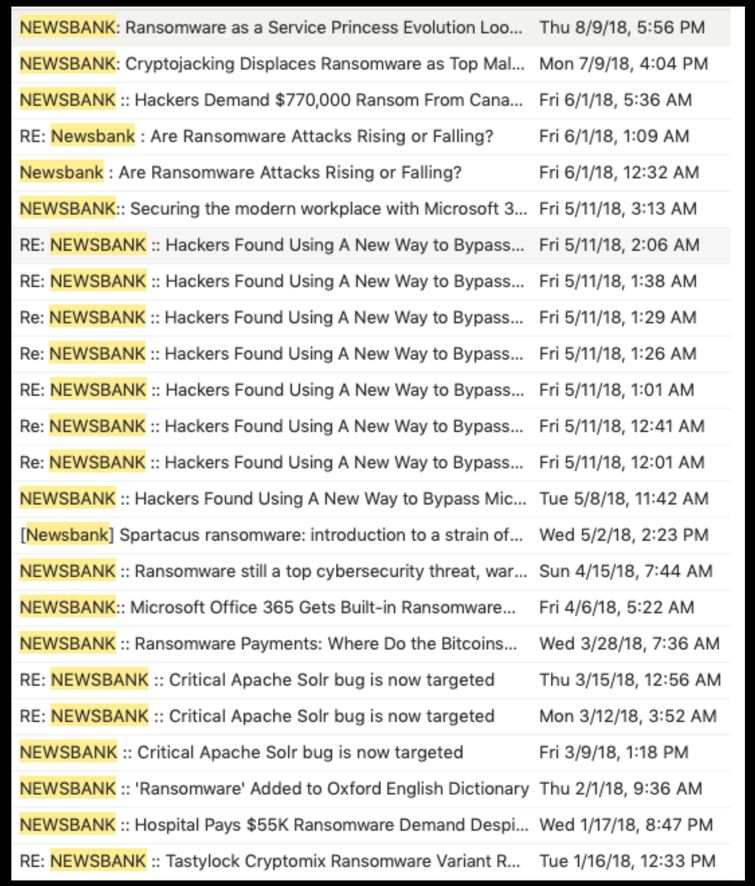

PERFORMANCE


Debriefing

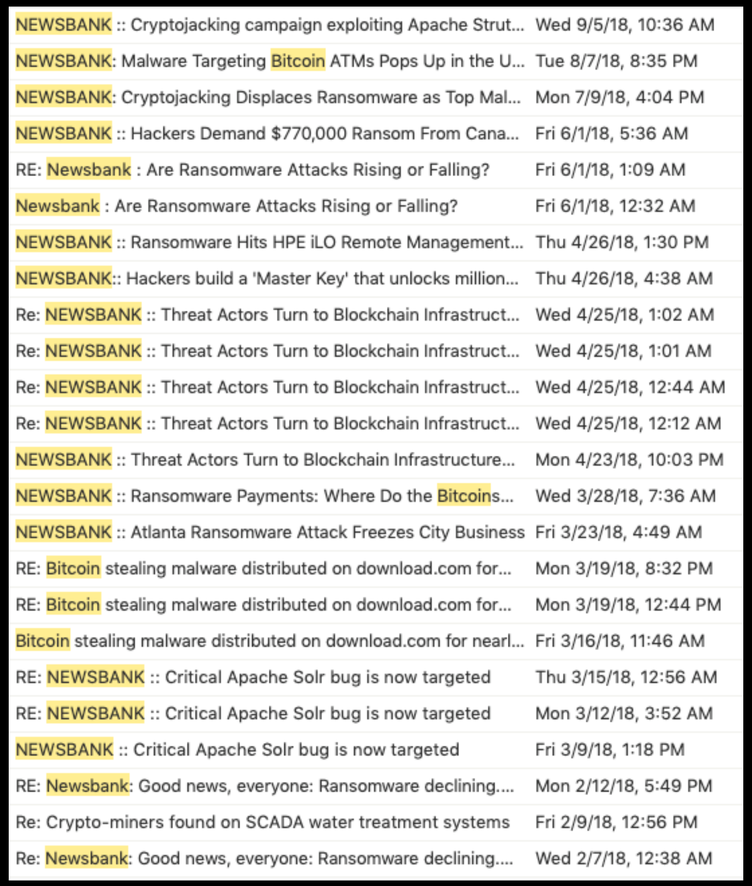
NEWSBANK: Ransomware as a Service Princess Evolution Loo...	Thu 8/9/18, 5:56 PM
NEWSBANK: Cryptojacking Displaces Ransomware as Top Mal...	Mon 7/9/18, 4:04 PM
NEWSBANK :: Hackers Demand $770,000 Ransom From Cana...	Fri 6/1/18, 5:36 AM
RE: Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 1:09 AM
Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 12:32 AM
NEWSBANK:: Securing the modern workplace with Microsoft 3...	Fri 5/11/18, 3:13 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 2:06 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:38 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:29 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:26 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:01 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 12:41 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 12:01 AM
NEWSBANK :: Hackers Found Using A New Way to Bypass Mic...	Tue 5/8/18, 11:42 AM
[Newsbank] Spartacus ransomware: introduction to a strain of...	Wed 5/2/18, 2:23 PM
NEWSBANK :: Ransomware still a top cybersecurity threat, war...	Sun 4/15/18, 7:44 AM
NEWSBANK:: Microsoft Office 365 Gets Built-in Ransomware...	Fri 4/6/18, 5:22 AM
NEWSBANK :: Ransomware Payments: Where Do the Bitcoins...	Wed 3/28/18, 7:36 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Thu 3/15/18, 12:56 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Mon 3/12/18, 3:52 AM
NEWSBANK :: Critical Apache Solr bug is now targeted	Fri 3/9/18, 1:18 PM
NEWSBANK :: 'Ransomware' Added to Oxford English Dictionary	Thu 2/1/18, 9:36 AM
NEWSBANK :: Hospital Pays $55K Ransomware Demand Despi...	Wed 1/17/18, 8:47 PM
RE: NEWSBANK :: Tastylock Cryptomix Ransomware Variant R...	Tue 1/16/18, 12:33 PM

NEWSBANK :: Cryptojacking campaign exploiting Apache Strut...	Wed 9/5/18, 10:36 AM
NEWSBANK: Malware Targeting Bitcoin ATMs Pops Up in the U...	Tue 8/7/18, 8:35 PM
NEWSBANK: Cryptojacking Displaces Ransomware as Top Mal...	Mon 7/9/18, 4:04 PM
NEWSBANK :: Hackers Demand $770,000 Ransom From Cana...	Fri 6/1/18, 5:36 AM
RE: Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 1:09 AM
Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 12:32 AM
NEWSBANK :: Ransomware Hits HPE iLO Remote Management...	Thu 4/26/18, 1:30 PM
NEWSBANK:: Hackers build a 'Master Key' that unlocks million...	Thu 4/26/18, 4:38 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 1:02 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 1:01 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 12:44 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 12:12 AM
NEWSBANK :: Threat Actors Turn to Blockchain Infrastructure...	Mon 4/23/18, 10:03 PM
NEWSBANK :: Ransomware Payments: Where Do the Bitcoins...	Wed 3/28/18, 7:36 AM
NEWSBANK :: Atlanta Ransomware Attack Freezes City Business	Fri 3/23/18, 4:49 AM
RE: Bitcoin stealing malware distributed on download.com for...	Mon 3/19/18, 8:32 PM
RE: Bitcoin stealing malware distributed on download.com for...	Mon 3/19/18, 12:44 PM
Bitcoin stealing malware distributed on download.com for nearl...	Fri 3/16/18, 11:46 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Thu 3/15/18, 12:56 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Mon 3/12/18, 3:52 AM
NEWSBANK :: Critical Apache Solr bug is now targeted	Fri 3/9/18, 1:18 PM
RE: Newsbank: Good news, everyone: Ransomware declining....	Mon 2/12/18, 5:49 PM
Re: Crypto-miners found on SCADA water treatment systems	Fri 2/9/18, 12:56 PM
Re: Newsbank: Good news, everyone: Ransomware declining....	Wed 2/7/18, 12:38 AM

Re: NEWSBANK :: Optionsbleed bug makes Apache HTTP Ser...	Fri 9/22/17, 8:52 AM
Cyber Digest September 22nd 2017	Fri 9/22/17, 12:49 AM
NEWSBANK :: Equifax's disastrous Struts patching blunder: TH...	Thu 9/21/17, 5:43 AM
NEWSBANK :: Optionsbleed bug makes Apache HTTP Server l...	Thu 9/21/17, 5:26 AM
NEWSBANK :: Equifax Shares More Details About Breach	Mon 9/18/17, 3:19 AM
NEWSBANK :: Equifax CIO, CSO Step Down	Fri 9/15/17, 7:59 PM
NEWSBANK:: FLASH MC-000086-MW TLP: AMBER, Apache...	Fri 9/15/17, 2:49 PM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Thu 9/14/17, 2:55 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Wed 9/13/17, 7:13 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Wed 9/13/17, 3:33 AM
NEWSBANK :: Organizations are uncovering a cloud security p...	Wed 9/13/17, 3:27 AM
NEWSBANK :: Apache Struts Flaw Increasingly Exploited to Ha...	Tue 9/12/17, 3:33 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Mon 9/11/17, 3:12 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 2:50 PM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 6:09 AM
RE: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 12:29 AM
RE: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 4:15 PM
Re: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:46 AM
RE: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:38 AM
Re: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:37 AM
NEWSBANK :: Hackers Exploit Recently Patched Apache Strut...	Fri 9/8/17, 10:31 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Fri 9/8/17, 10:05 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Wed 9/6/17, 10:29 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Wed 9/6/17, 5:42 AM



NEWSBANK: Ransomware as a Service Princess Evolution Loo...	Thu 8/9/18, 5:56 PM
NEWSBANK: Cryptojacking Displaces Ransomware as Top Mal...	Mon 7/9/18, 4:04 PM
NEWSBANK :: Hackers Demand $770,000 Ransom From Cana...	Fri 6/1/18, 5:36 AM
RE: Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 1:09 AM
Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 12:32 AM
NEWSBANK:: Securing the modern workplace with Microsoft 3...	Fri 5/11/18, 3:13 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 2:06 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:38 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:29 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:26 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:01 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 12:41 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 12:01 AM
NEWSBANK :: Hackers Found Using A New Way to Bypass Mic...	Tue 5/8/18, 11:42 AM
[Newsbank] Spartacus ransomware: introduction to a strain of...	Wed 5/2/18, 2:23 PM
NEWSBANK :: Ransomware still a top cybersecurity threat, war...	Sun 4/15/18, 7:44 AM
NEWSBANK:: Microsoft Office 365 Gets Built-in Ransomware...	Fri 4/6/18, 5:22 AM
NEWSBANK :: Ransomware Payments: Where Do the Bitcoins...	Wed 3/28/18, 7:36 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Thu 3/15/18, 12:56 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Mon 3/12/18, 3:52 AM
NEWSBANK :: Critical Apache Solr bug is now targeted	Fri 3/9/18, 1:18 PM
NEWSBANK :: 'Ransomware' Added to Oxford English Dictionary	Thu 2/1/18, 9:36 AM
NEWSBANK :: Hospital Pays $55K Ransomware Demand Despi...	Wed 1/17/18, 8:47 PM
RE: NEWSBANK :: Tastylock Cryptomix Ransomware Variant R...	Tue 1/16/18, 12:33 PM

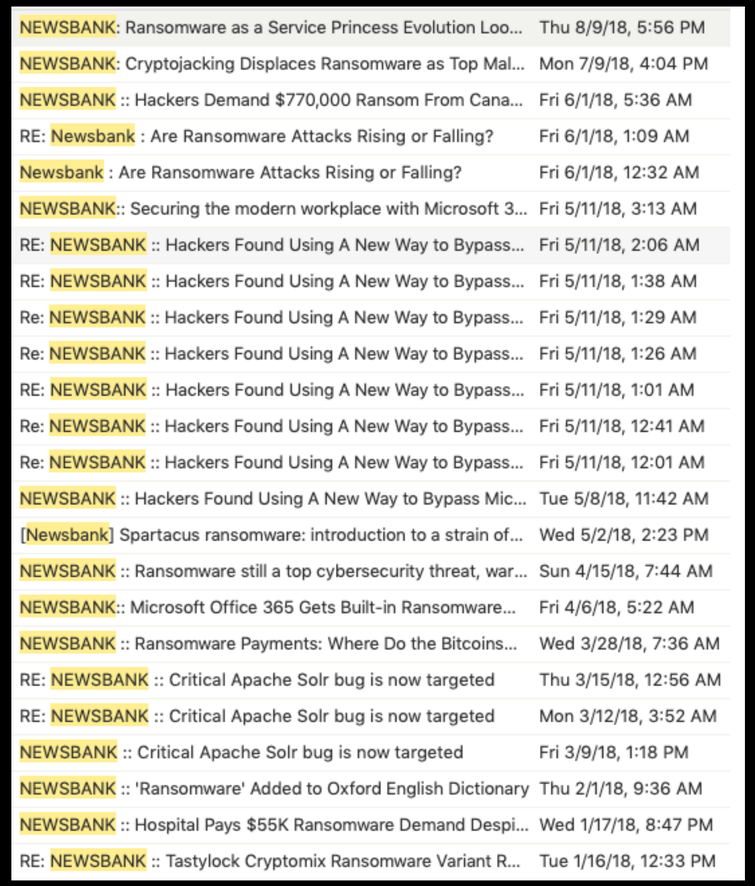


NEWSBANK :: Cryptojacking campaign exploiting Apache Strut...	Wed 9/5/18, 10:36 AM
NEWSBANK: Malware Targeting Bitcoin ATMs Pops Up in the U...	Tue 8/7/18, 8:35 PM
NEWSBANK: Cryptojacking Displaces Ransomware as Top Mal...	Mon 7/9/18, 4:04 PM
NEWSBANK :: Hackers Demand $770,000 Ransom From Cana...	Fri 6/1/18, 5:36 AM
RE: Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 1:09 AM
Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 12:32 AM
NEWSBANK :: Ransomware Hits HPE iLO Remote Management...	Thu 4/26/18, 1:30 PM
NEWSBANK:: Hackers build a 'Master Key' that unlocks million...	Thu 4/26/18, 4:38 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 1:02 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 1:01 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 12:44 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 12:12 AM
NEWSBANK :: Threat Actors Turn to Blockchain Infrastructure...	Mon 4/23/18, 10:03 PM
NEWSBANK :: Ransomware Payments: Where Do the Bitcoins...	Wed 3/28/18, 7:36 AM
NEWSBANK :: Atlanta Ransomware Attack Freezes City Business	Fri 3/23/18, 4:49 AM
RE: Bitcoin stealing malware distributed on download.com for...	Mon 3/19/18, 8:32 PM
RE: Bitcoin stealing malware distributed on download.com for...	Mon 3/19/18, 12:44 PM
Bitcoin stealing malware distributed on download.com for nearl...	Fri 3/16/18, 11:46 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Thu 3/15/18, 12:56 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Mon 3/12/18, 3:52 AM
NEWSBANK :: Critical Apache Solr bug is now targeted	Fri 3/9/18, 1:18 PM
RE: Newsbank: Good news, everyone: Ransomware declining....	Mon 2/12/18, 5:49 PM
Re: Crypto-miners found on SCADA water treatment systems	Fri 2/9/18, 12:56 PM
Re: Newsbank: Good news, everyone: Ransomware declining....	Wed 2/7/18, 12:38 AM

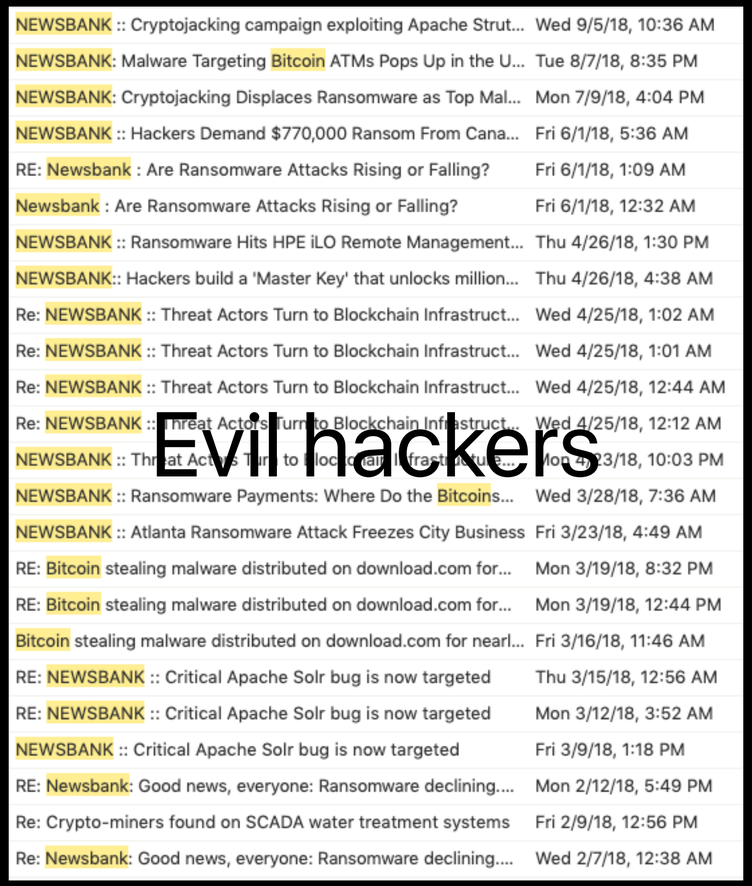
Re: NEWSBANK :: Optionsbleed bug makes Apache HTTP Ser...	Fri 9/22/17, 8:52 AM
Cyber Digest September 22nd 2017	Fri 9/22/17, 12:49 AM
NEWSBANK :: Equifax's disastrous Struts patching blunder: TH...	Thu 9/21/17, 5:43 AM
NEWSBANK :: Optionsbleed bug makes Apache HTTP Server l...	Thu 9/21/17, 5:26 AM
NEWSBANK :: Equifax Shares More Details About Breach	Mon 9/18/17, 3:19 AM
NEWSBANK :: Equifax CIO, CSO Step Down	Fri 9/15/17, 7:59 PM
NEWSBANK:: FLASH MC-000086-MW TLP: AMBER, Apache...	Fri 9/15/17, 2:49 PM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Thu 9/14/17, 2:55 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Wed 9/13/17, 7:13 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Wed 9/13/17, 3:33 AM
NEWSBANK :: Organizations are uncovering a cloud security p...	Wed 9/13/17, 3:27 AM
NEWSBANK :: Apache Struts Flaw Increasingly Exploited to Ha...	Tue 9/12/17, 3:33 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Mon 9/11/17, 3:12 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 2:50 PM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 6:09 AM
RE: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 12:29 AM
RE: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 4:15 PM
Re: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:46 AM
RE: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:38 AM
Re: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:37 AM
NEWSBANK :: Hackers Exploit Recently Patched Apache Strut...	Fri 9/8/17, 10:31 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Fri 9/8/17, 10:05 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Wed 9/6/17, 10:29 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Wed 9/6/17, 5:42 AM

"Securing the world from **evil hackers** by making it **easier to tune** your IPS policy."

–Russ



NEWSBANK: Ransomware as a Service Princess Evolution Loo...	Thu 8/9/18, 5:56 PM
NEWSBANK: Cryptojacking Displaces Ransomware as Top Mal...	Mon 7/9/18, 4:04 PM
NEWSBANK :: Hackers Demand $770,000 Ransom From Cana...	Fri 6/1/18, 5:36 AM
RE: Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 1:09 AM
Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 12:32 AM
NEWSBANK:: Securing the modern workplace with Microsoft 3...	Fri 5/11/18, 3:13 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 2:06 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:38 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:29 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:26 AM
RE: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 1:01 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 12:41 AM
Re: NEWSBANK :: Hackers Found Using A New Way to Bypass...	Fri 5/11/18, 12:01 AM
NEWSBANK :: Hackers Found Using A New Way to Bypass Mic...	Tue 5/8/18, 11:42 AM
[Newsbank] Spartacus ransomware: introduction to a strain of...	Wed 5/2/18, 2:23 PM
NEWSBANK :: Ransomware still a top cybersecurity threat, war...	Sun 4/15/18, 7:44 AM
NEWSBANK:: Microsoft Office 365 Gets Built-in Ransomware...	Fri 4/6/18, 5:22 AM
NEWSBANK :: Ransomware Payments: Where Do the Bitcoins...	Wed 3/28/18, 7:36 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Thu 3/15/18, 12:56 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Mon 3/12/18, 3:52 AM
NEWSBANK :: Critical Apache Solr bug is now targeted	Fri 3/9/18, 1:18 PM
NEWSBANK :: 'Ransomware' Added to Oxford English Dictionary	Thu 2/1/18, 9:36 AM
NEWSBANK :: Hospital Pays $55K Ransomware Demand Despi...	Wed 1/17/18, 8:47 PM
RE: NEWSBANK :: Tastylock Cryptomix Ransomware Variant R...	Tue 1/16/18, 12:33 PM



NEWSBANK :: Cryptojacking campaign exploiting Apache Strut...	Wed 9/5/18, 10:36 AM
NEWSBANK: Malware Targeting Bitcoin ATMs Pops Up in the U...	Tue 8/7/18, 8:35 PM
NEWSBANK: Cryptojacking Displaces Ransomware as Top Mal...	Mon 7/9/18, 4:04 PM
NEWSBANK :: Hackers Demand $770,000 Ransom From Cana...	Fri 6/1/18, 5:36 AM
RE: Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 1:09 AM
Newsbank : Are Ransomware Attacks Rising or Falling?	Fri 6/1/18, 12:32 AM
NEWSBANK :: Ransomware Hits HPE iLO Remote Management...	Thu 4/26/18, 1:30 PM
NEWSBANK:: Hackers build a 'Master Key' that unlocks million...	Thu 4/26/18, 4:38 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 1:02 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 1:01 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 12:44 AM
Re: NEWSBANK :: Threat Actors Turn to Blockchain Infrastruct...	Wed 4/25/18, 12:12 AM
NEWSBANK :: Threat Actors Turn to Blockchain Infrastructure...	Mon 4/23/18, 10:03 PM
NEWSBANK :: Ransomware Payments: Where Do the Bitcoins...	Wed 3/28/18, 7:36 AM
NEWSBANK :: Atlanta Ransomware Attack Freezes City Business	Fri 3/23/18, 4:49 AM
RE: Bitcoin stealing malware distributed on download.com for...	Mon 3/19/18, 8:32 PM
RE: Bitcoin stealing malware distributed on download.com for...	Mon 3/19/18, 12:44 PM
Bitcoin stealing malware distributed on download.com for nearl...	Fri 3/16/18, 11:46 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Thu 3/15/18, 12:56 AM
RE: NEWSBANK :: Critical Apache Solr bug is now targeted	Mon 3/12/18, 3:52 AM
NEWSBANK :: Critical Apache Solr bug is now targeted	Fri 3/9/18, 1:18 PM
RE: Newsbank: Good news, everyone: Ransomware declining....	Mon 2/12/18, 5:49 PM
Re: Crypto-miners found on SCADA water treatment systems	Fri 2/9/18, 12:56 PM
Re: Newsbank: Good news, everyone: Ransomware declining....	Wed 2/7/18, 12:38 AM

Evil hackers

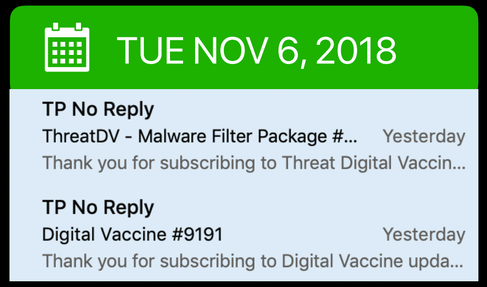
Re: NEWSBANK :: Optionsbleed bug makes Apache HTTP Ser...	Fri 9/22/17, 8:52 AM
Cyber Digest September 22nd 2017	Fri 9/22/17, 12:49 AM
NEWSBANK :: Equifax's disastrous Struts patching blunder: TH...	Thu 9/21/17, 5:43 AM
NEWSBANK :: Optionsbleed bug makes Apache HTTP Server l...	Thu 9/21/17, 5:26 AM
NEWSBANK :: Equifax Shares More Details About Breach	Mon 9/18/17, 3:19 AM
NEWSBANK :: Equifax CIO, CSO Step Down	Fri 9/15/17, 7:59 PM
NEWSBANK:: FLASH MC-000086-MW TLP: AMBER, Apache...	Fri 9/15/17, 2:49 PM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Thu 9/14/17, 2:55 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Wed 9/13/17, 7:13 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Wed 9/13/17, 3:33 AM
NEWSBANK :: Organizations are uncovering a cloud security p...	Wed 9/13/17, 3:27 AM
NEWSBANK :: Apache Struts Flaw Increasingly Exploited to Ha...	Tue 9/12/17, 3:33 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Mon 9/11/17, 3:12 AM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 2:50 PM
Re: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 6:09 AM
RE: NEWSBANK: RE: Giant Equifax data breach: 143 million pe...	Sat 9/9/17, 12:29 AM
RE: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 4:15 PM
Re: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:46 AM
RE: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:38 AM
Re: NEWSBANK :: Hackers Exploit Recently Patched Apache S...	Fri 9/8/17, 10:37 AM
NEWSBANK :: Hackers Exploit Recently Patched Apache Strut...	Fri 9/8/17, 10:31 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Fri 9/8/17, 10:05 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Wed 9/6/17, 10:29 AM
RE: NEWSBANK :: Exploit Available for Critical Apache Struts V...	Wed 9/6/17, 5:42 AM

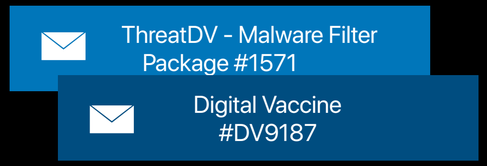
"Securing the world from **evil hackers** by making it **easier to tune** your IPS policy."

–Russ

Current Workflow

Current Workflow





Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes

Search all filters enabled by default

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes

Search all filters enabled by default

Read individual filter descriptions

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes

Search all filters enabled by default

Read individual filter descriptions

Any filters with rec'd settings of Block?

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes

Search all filters enabled by default

Read individual filter descriptions

Any filters with rec'd settings of Block?

Are rec'd settings disruptive to my env?

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab
- Monitor events of the filters

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab
- Monitor events of the filters
- Any suspicious events or not?

- "Note to self": revert changes after "trial"

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab
- Monitor events of the filters
- Any suspicious events or not?

- "Note to self": revert changes after "trial"
- Document changes in spreadsheet

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab
- Monitor events of the filters
- Any suspicious events or not?

- "Note to self": revert changes after "trial"
- Document changes in spreadsheet
- Send out an email with changes

- Decide: Yes or No accept rec'd settings

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab
- Monitor events of the filters
- Any suspicious events or not?

- "Note to self": revert changes after "trial"
- Document changes in spreadsheet
- Send out an email with changes

- Decide: Yes or No accept rec'd settings
- Enable filters put dates/ comment in filter field

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

- Read release notes
- Search all filters enabled by default
- Read individual filter descriptions
- Any filters with rec'd settings of Block?
- Are rec'd settings disruptive to my env?
- Put filters into "trial" mode for x wks?
- Navigate into the Events tab
- Monitor events of the filters
- Any suspicious events or not?

- "Note to self": revert changes after "trial"
- Document changes in spreadsheet
- Send out an email with changes

- Decide: Yes or No accept rec'd settings
- Enable filters put dates/ comment in filter field

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

MON NOV 12, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

MON NOV 12, 2018

Attend UX Workshop
Find my replacement
Hope STG==PROD

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

MON NOV 12, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

MON NOV 12, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

TUE NOV 13, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

MON NOV 12, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

TUE NOV 13, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9191

Current Workflow

TUE NOV 6, 2018

TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday
Thank you for subscribing to Digital Vaccine upda...

WED NOV 7, 2018

THU NOV 8, 2018

FRI NOV 9, 2018

WEEKEND

MON NOV 12, 2018

Review

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9187

Read release notes	Search all filters enabled by default	Read individual filter descriptions
Any filters with rec'd settings of Block?	Are rec'd settings disruptive to my env?	Put filters into "trial" mode for x wks?
Navigate into the Events tab	Monitor events of the filters	Any suspicious events or not?
"Note to self": revert changes after "trial"	Document changes in spreadsheet	Send out an email with changes
Decide: Yes or No accept rec'd settings	Enable filters put dates/ comment in filter field	Deploy new DV profiles update to Prod

TUE NOV 13, 2018

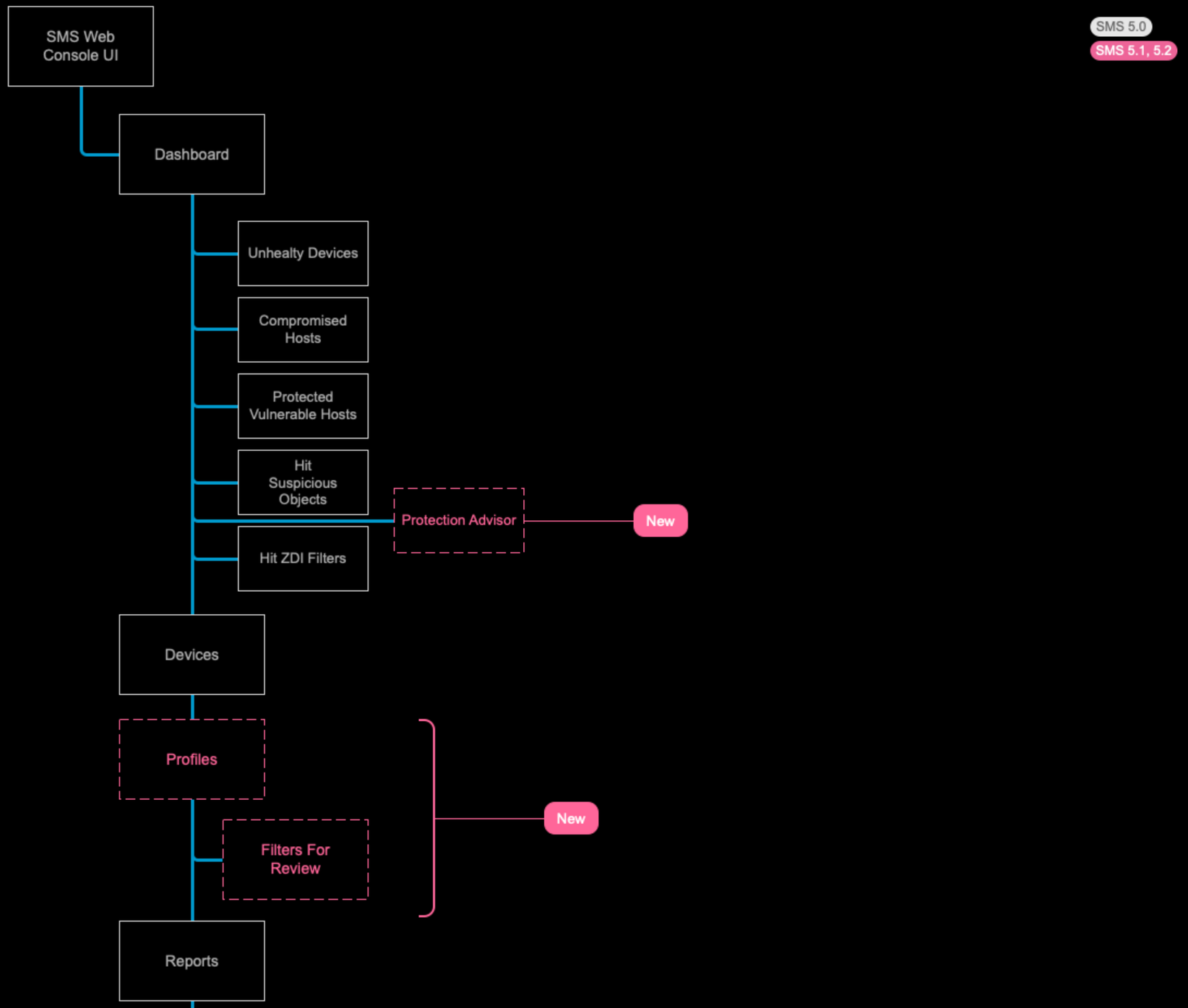
TP No Reply
ThreatDV - Malware Filter Package #... Yesterday
Thank you for subscribing to Threat Digital Vaccin...

TP No Reply
Digital Vaccine #9191 Yesterday

ThreatDV - Malware Filter Package #1571

Digital Vaccine #DV9191

Repeat


SMS 5.0
SMS 5.1, 5.2
SMS Web Console UI
Dashboard
Unhealty Devices
Compromised Hosts
Protected Vulnerable Hosts
Hit Suspicious Objects
Protection Advisor
New
Hit ZDI Filters
Devices
Profiles
Filters For Review
New
Reports

SMS 5.0

SMS 5.1, 5.2

SMS Web Console UI

Dashboard

Unhealty Devices

Compromised Hosts

Protected Vulnerable Hosts

Hit Suspicious Objects

Protection Advisor

New

Hit ZDI Filters

Threat Protection Advisor

Devices

Profiles

Filters For Review

New

Reports

SMS 5.0

SMS 5.1, 5.2

SMS Web Console UI

Dashboard

Unhealty Devices

Compromised Hosts

Protected Vulnerable Hosts

Hit Suspicious Objects

Protection Advisor

New

Threat Protection Advisor

Hit ZDI Filters

Devices

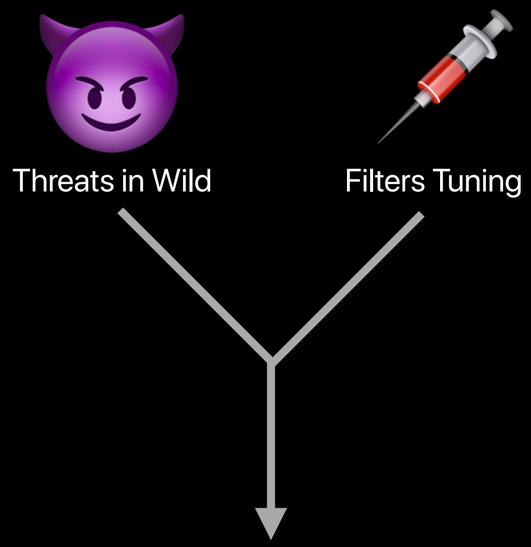
Profiles

Filters For Review

New

Filters for Review

Reports



Active Threat Defense

New

Looking for _____?

Looking for _____?

Optionsbleed HTTP Vulnerability

Looking for _____?

Optionsbleed HTTP Vulnerability

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

WannaCry

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

WannaCry

Coinminer

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

WannaCry

Coinminer

Mirai Botnet

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

WannaCry

Coinminer

Mirai Botnet

BadRabbit

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

WannaCry

Coinminer

Mirai Botnet

BadRabbit

/ Zero-day Vulnerabilities

Looking for _____?

Optionsbleed HTTP Vulnerability

Apache Struts (Equifax data breach)

Heartbleed Open SSL

WannaCry

Coinminer

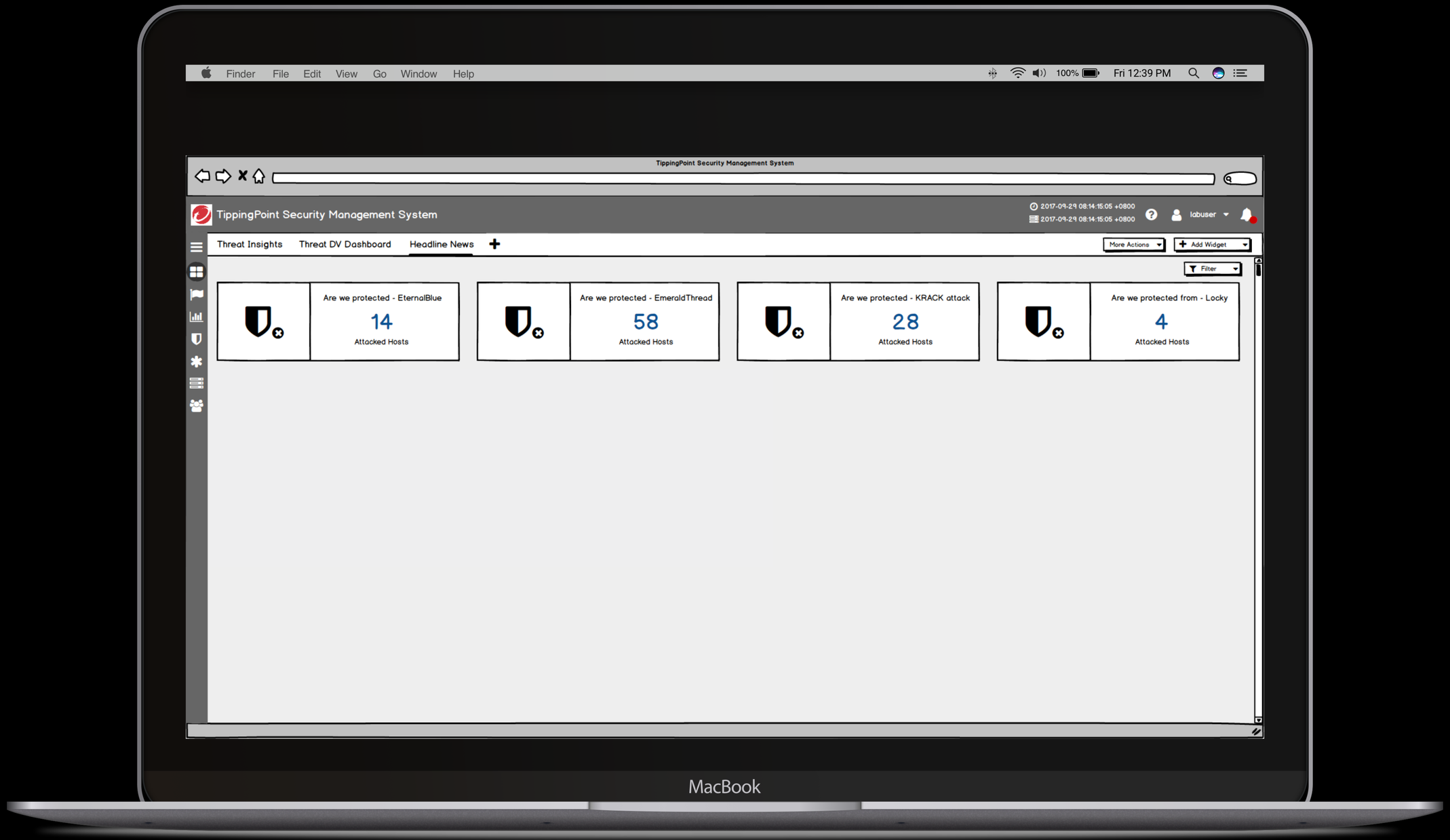
Mirai Botnet

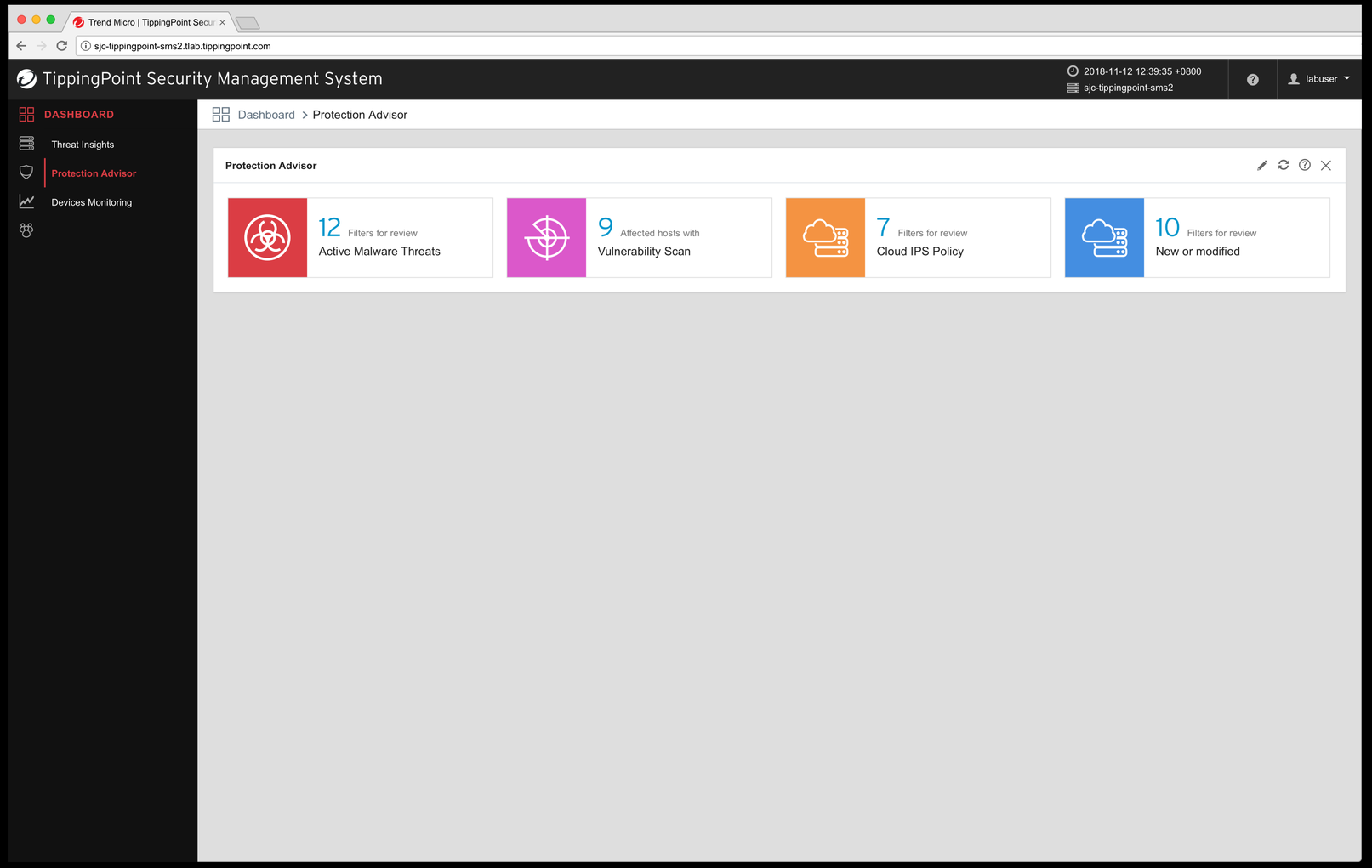
BadRabbit

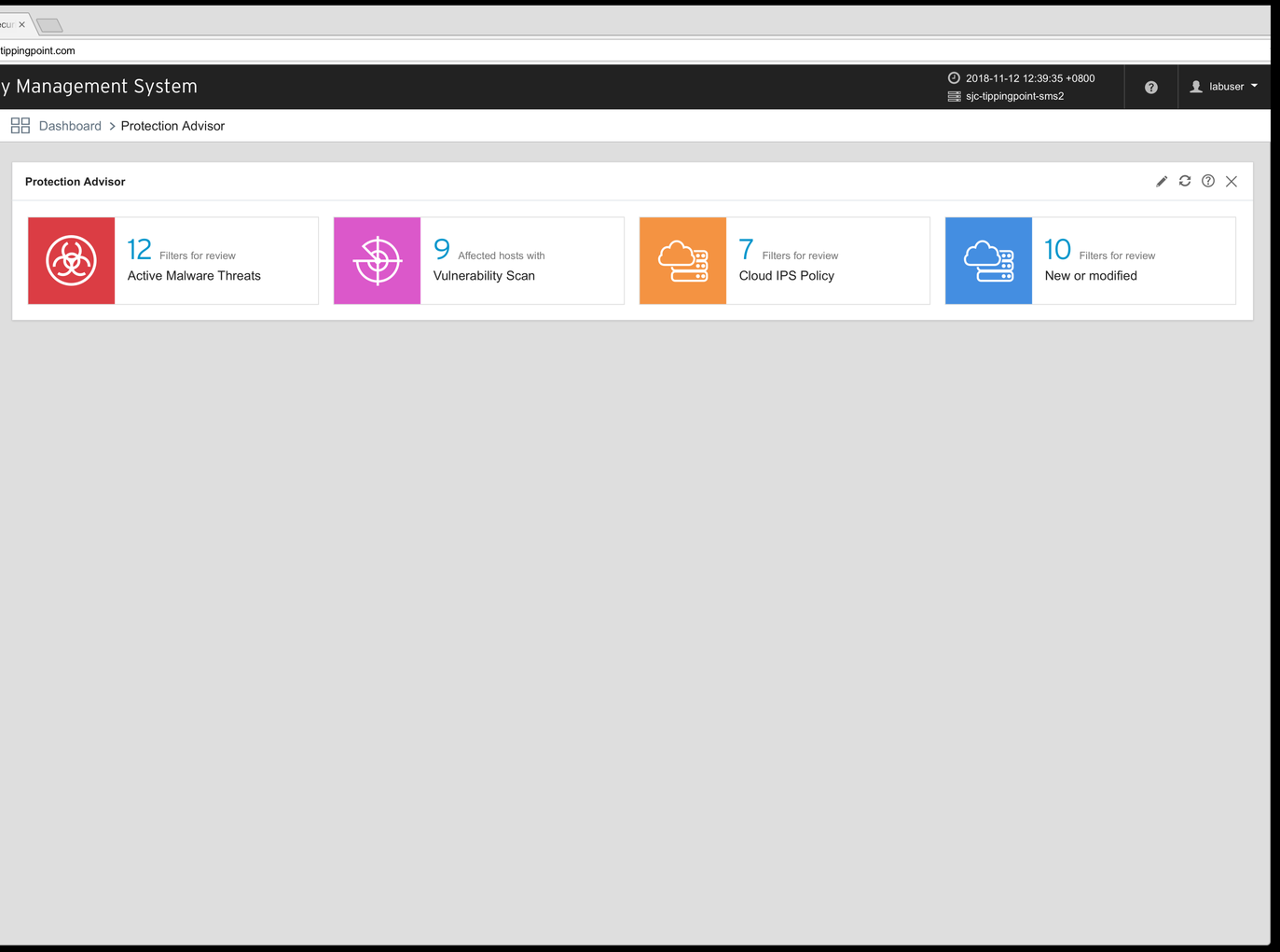
/ Zero-day Vulnerabilities

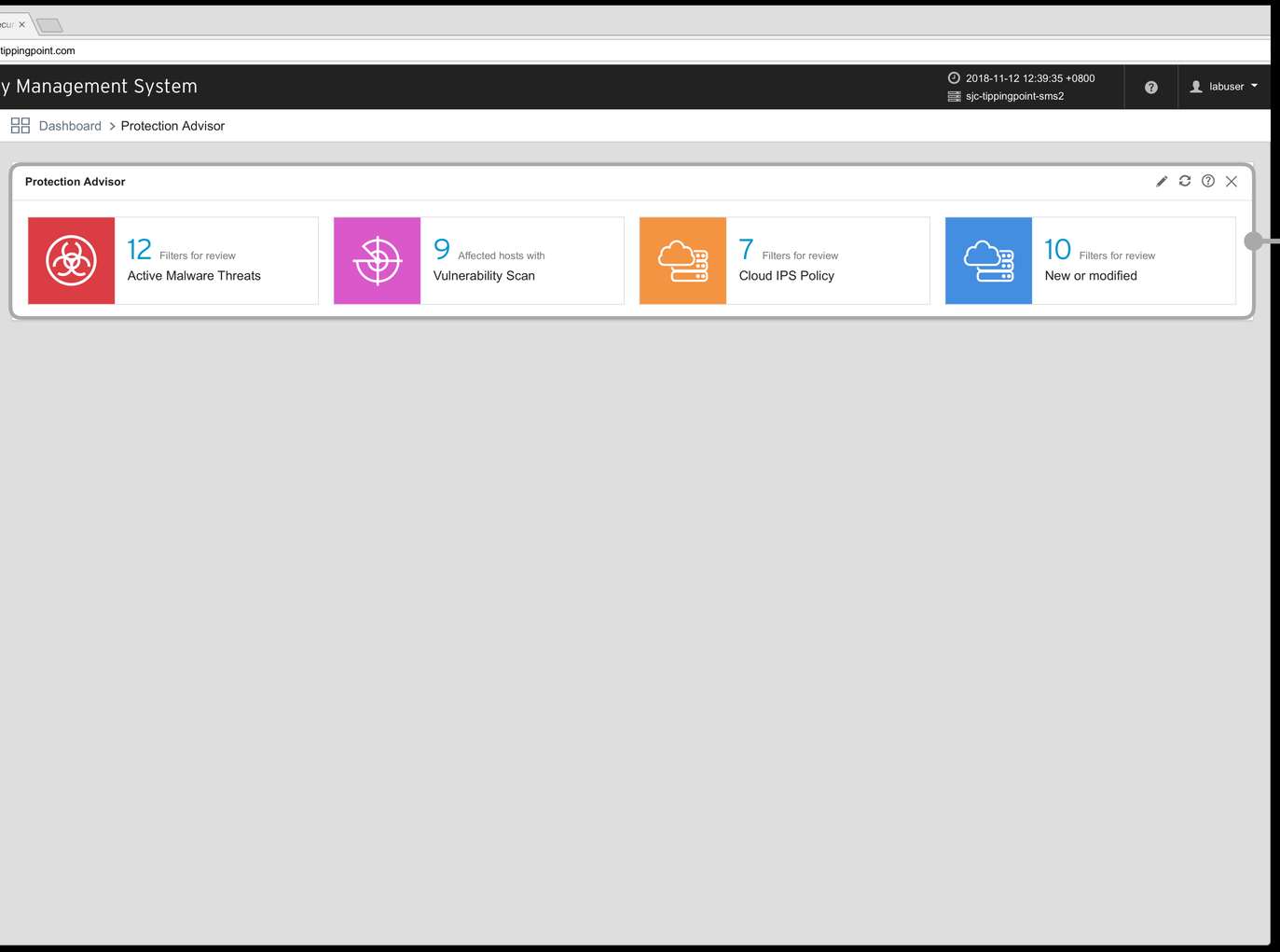
TREND MICRO SMART Protection Network™

Allow tuning recommendations from vulnerability and active malware using filter(s) _____

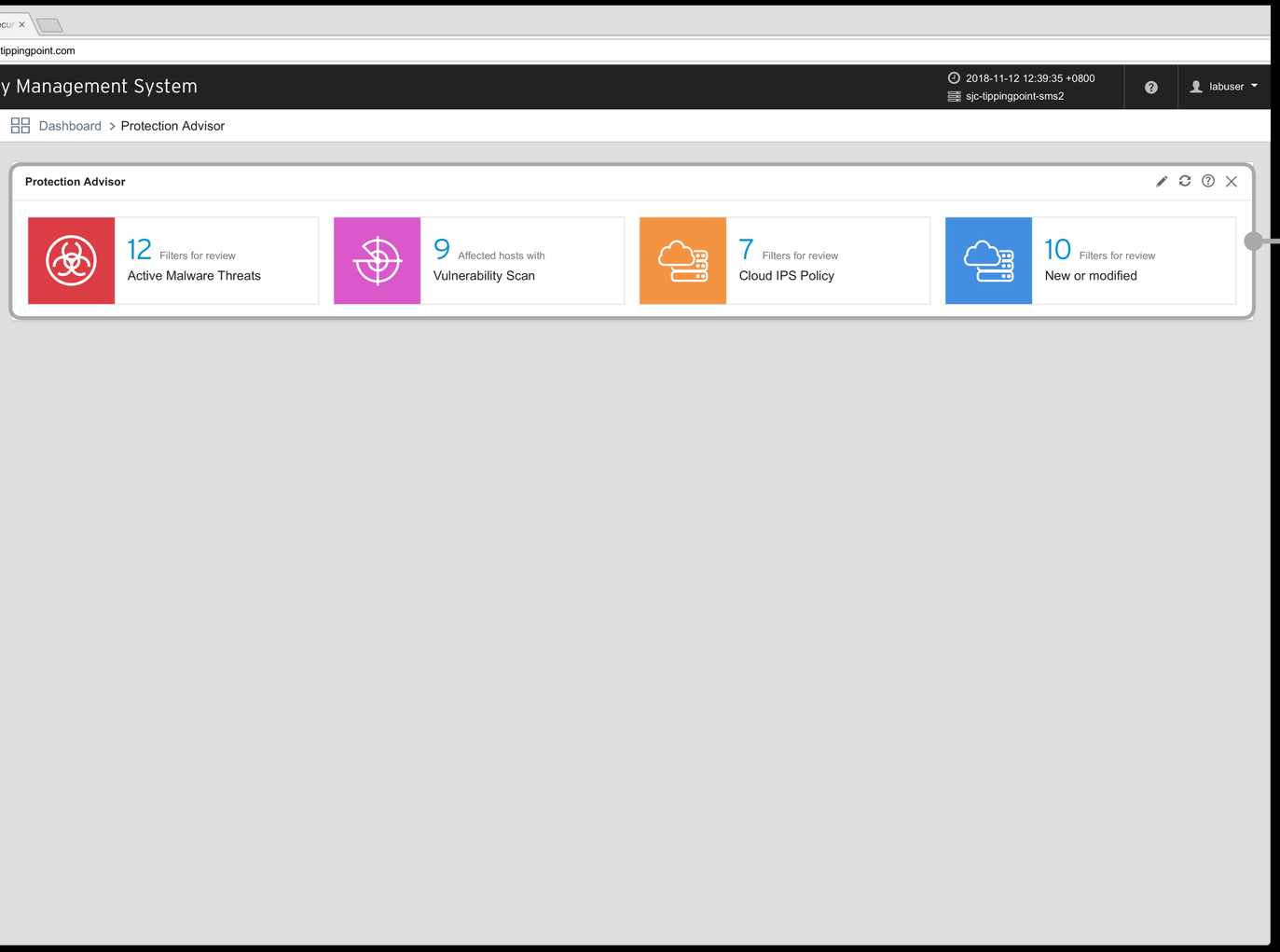

Finder File Edit View Go Window Help
100% Fri 12:39 PM
TippingPoint Security Management System
TippingPoint Security Management System
2017-09-29 08:14:15:05 +0800
2017-09-29 08:14:15:05 +0800
labuser
Threat Insights
Threat DV Dashboard
Headline News
More Actions
Add Widget
Filter
Are we protected - EternalBlue
14
Attacked Hosts
Are we protected - EmeraldThread
58
Attacked Hosts
Are we protected - KRACK attack
28
Attacked Hosts
Are we protected from - Locky
4
Attacked Hosts
MacBook


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
DASHBOARD
Threat Insights
Protection Advisor
Devices Monitoring
Dashboard > Protection Advisor
Protection Advisor
12 Filters for review
Active Malware Threats
9 Affected hosts with
Vulnerability Scan
7 Filters for review
Cloud IPS Policy
10 Filters for review
New or modified


tippingpoint.com
y Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
Dashboard > Protection Advisor
Protection Advisor
12 Filters for review
Active Malware Threats
9 Affected hosts with
Vulnerability Scan
7 Filters for review
Cloud IPS Policy
10 Filters for review
New or modified

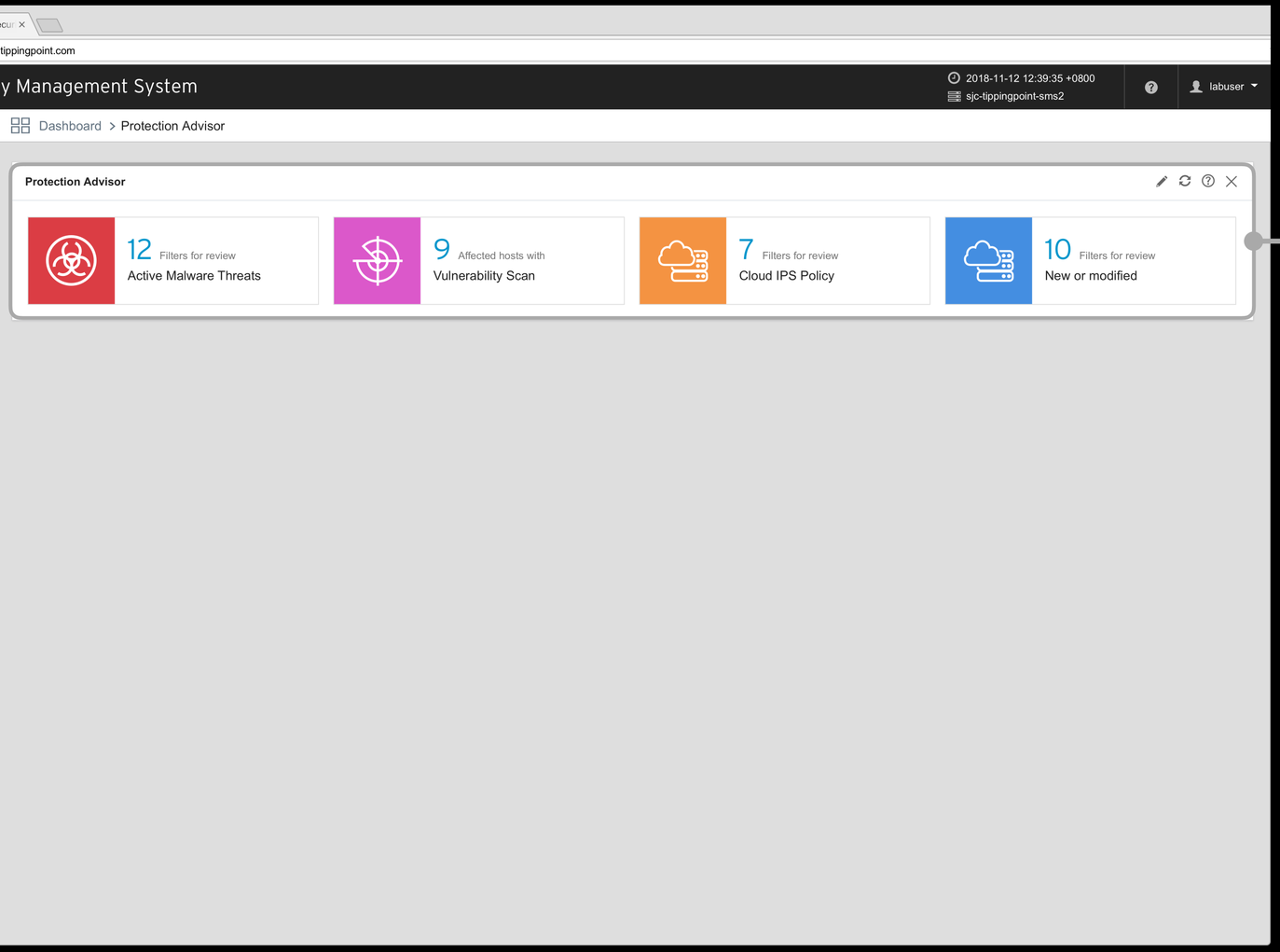


Active Threat Defense



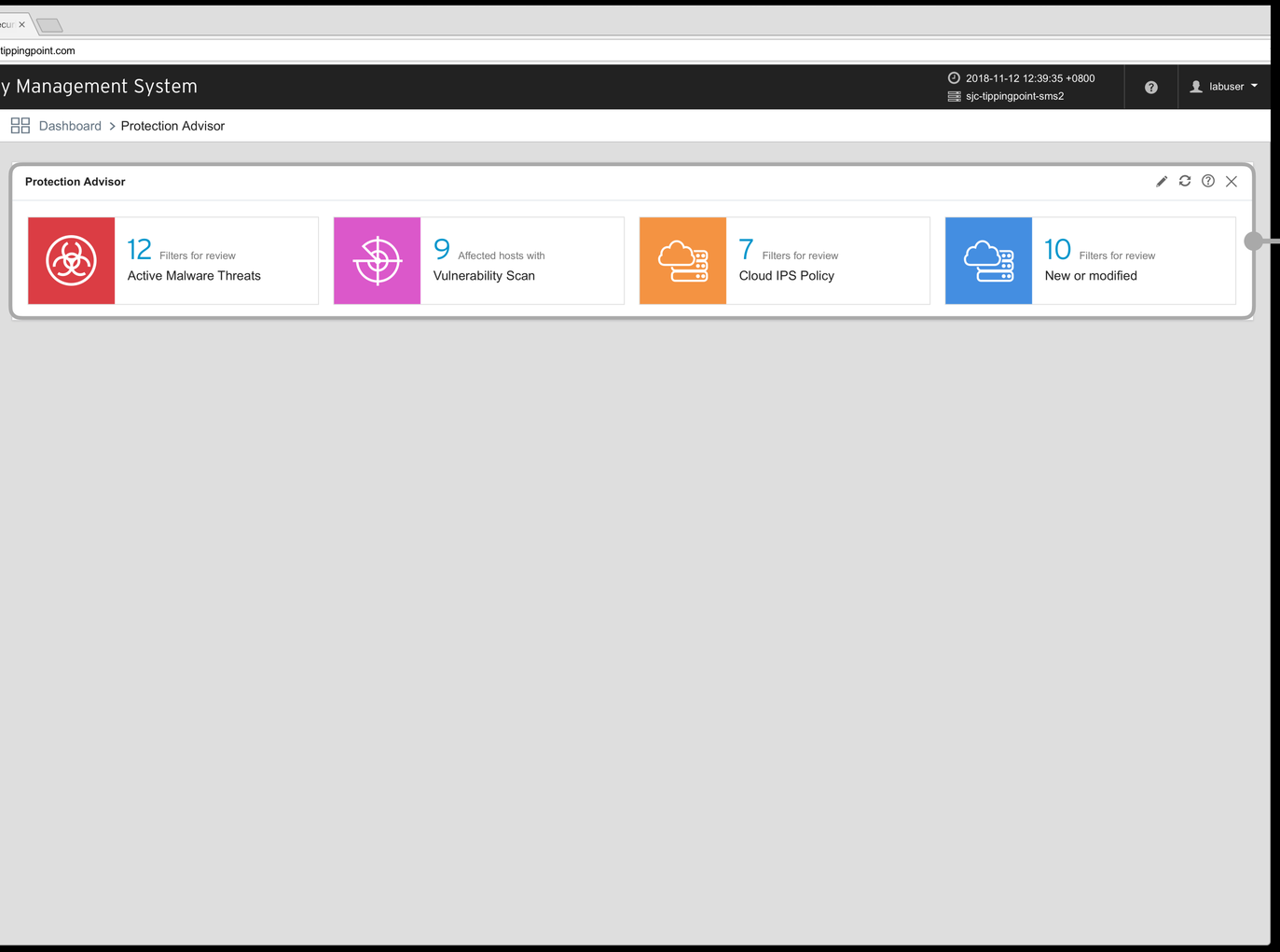
Active Threat Defense

- Made available through an elegant Web UI



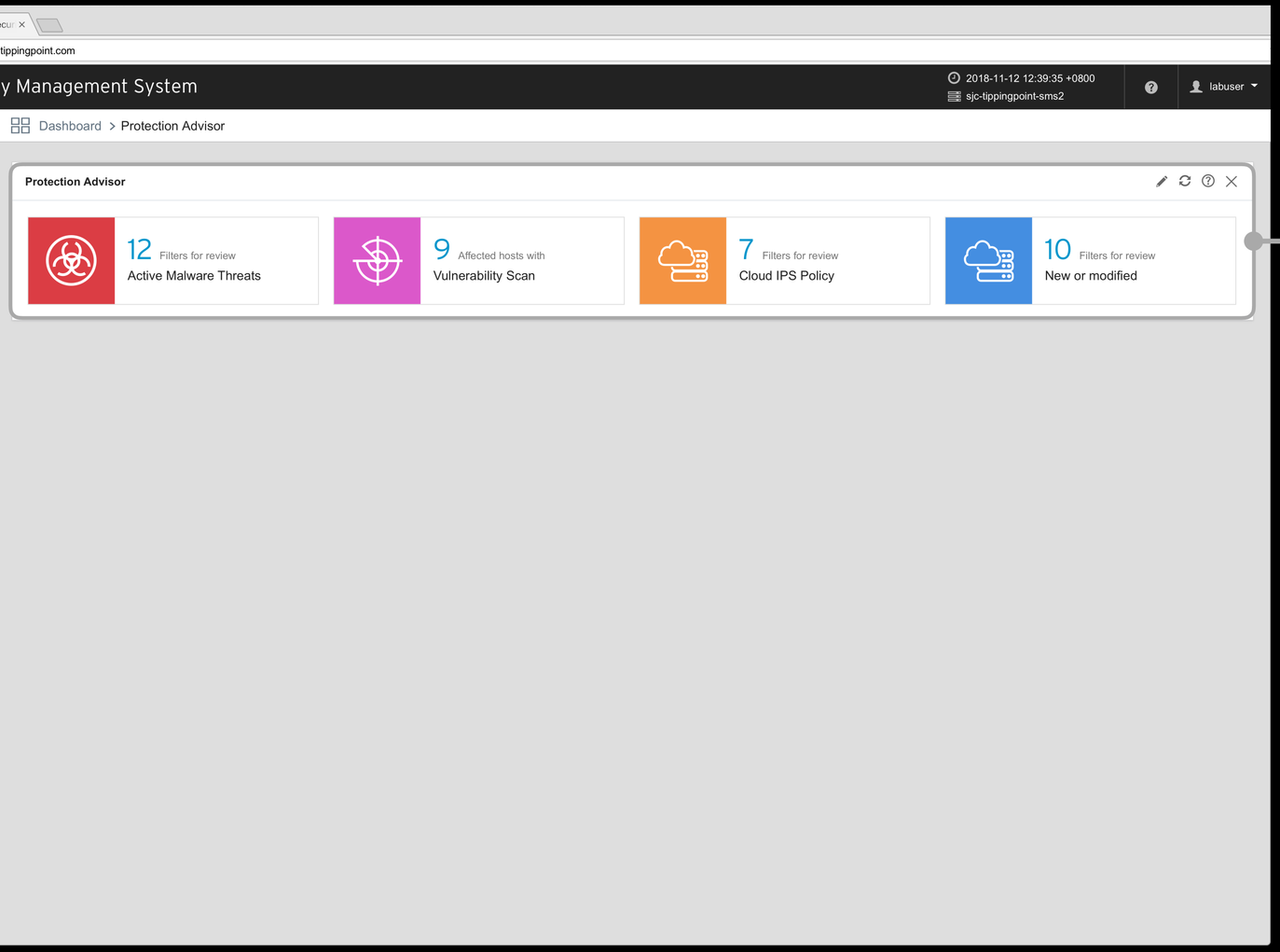
Active Threat Defense

- Made available through an elegant Web UI
- Happy path to defend against vulns and malwares



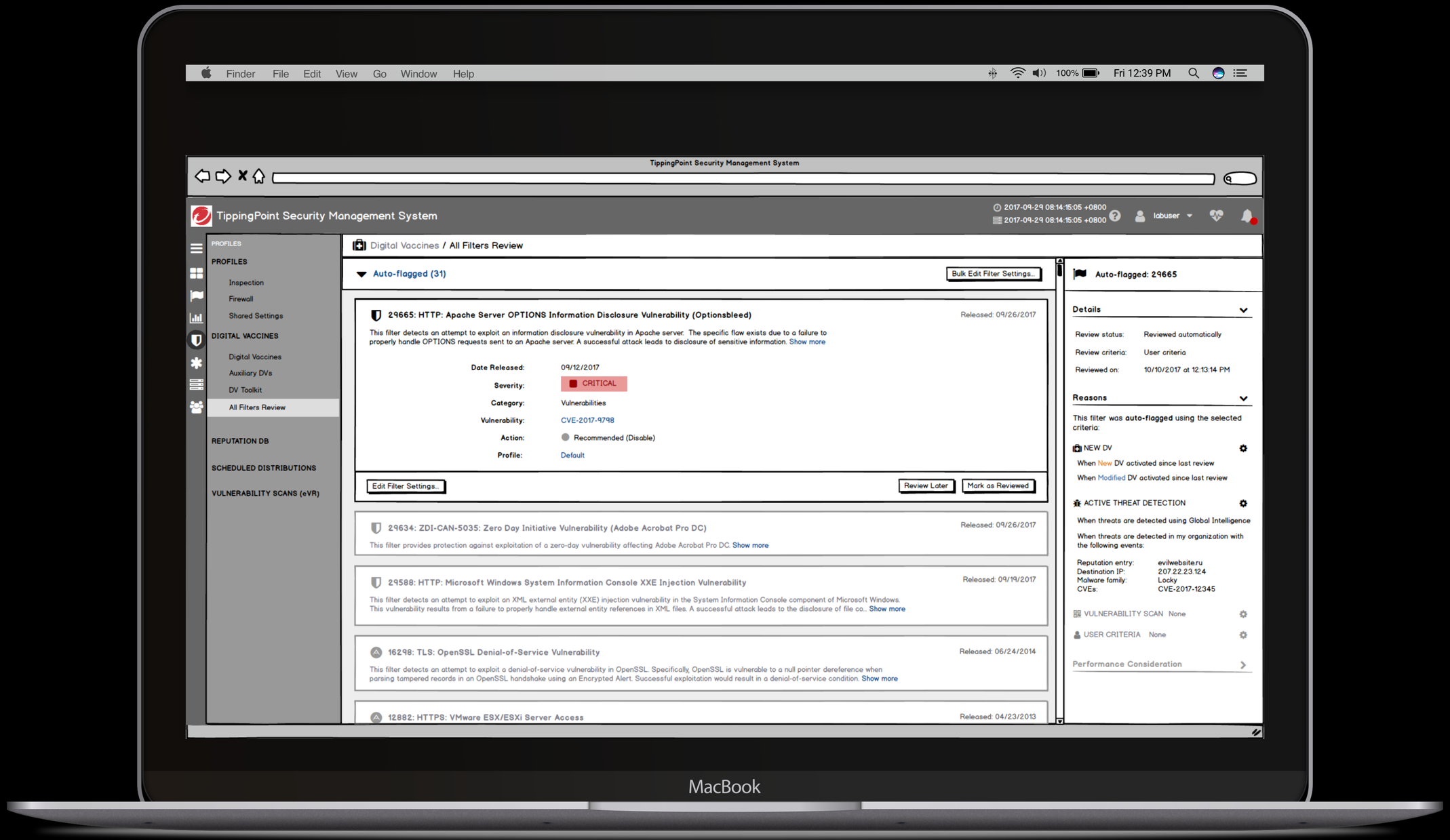
Active Threat Defense

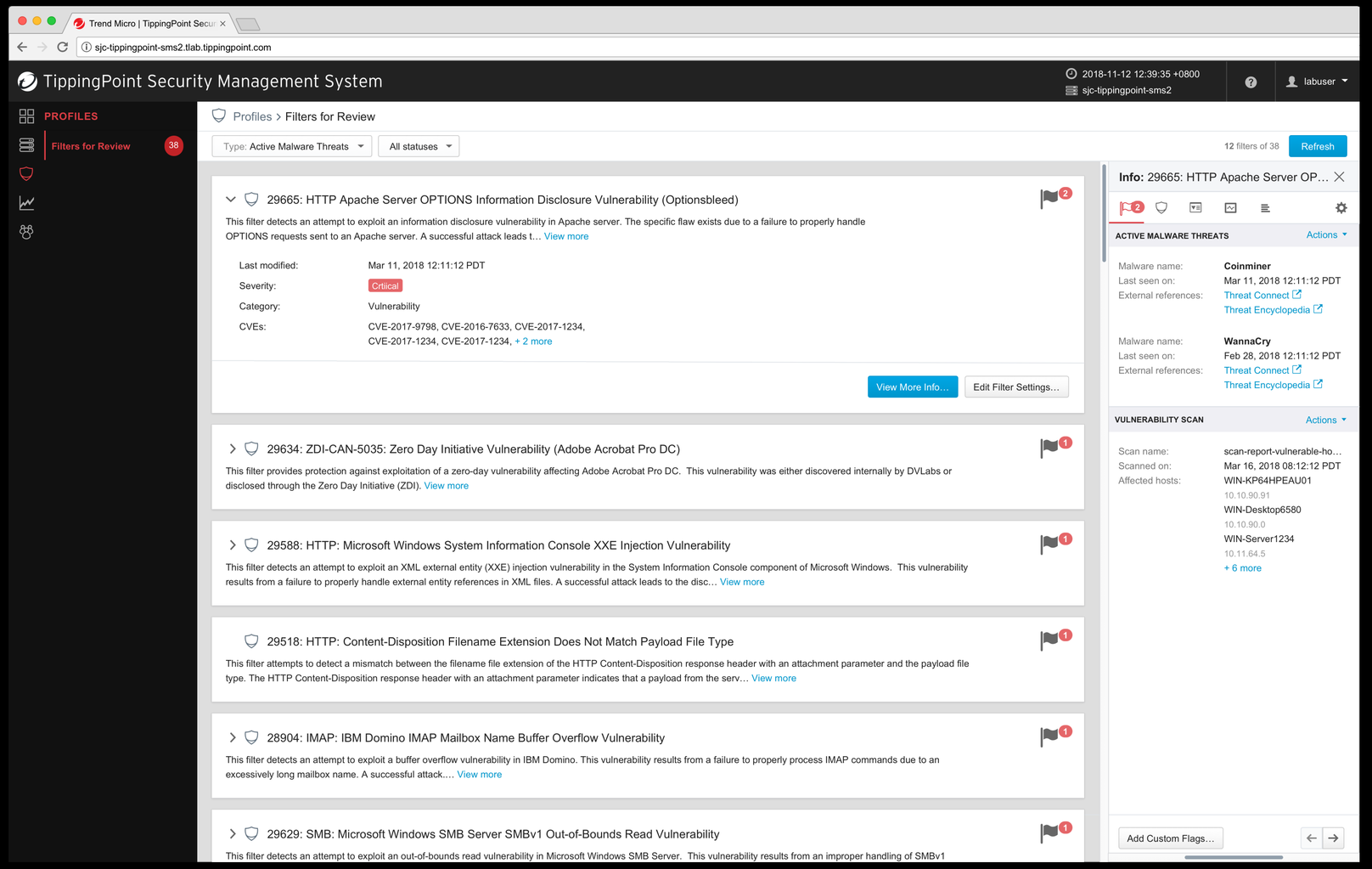
- Made available through an elegant Web UI
- Happy path to defend against vulns and malwares
- Pulls latest threat intelligence updates from SPN

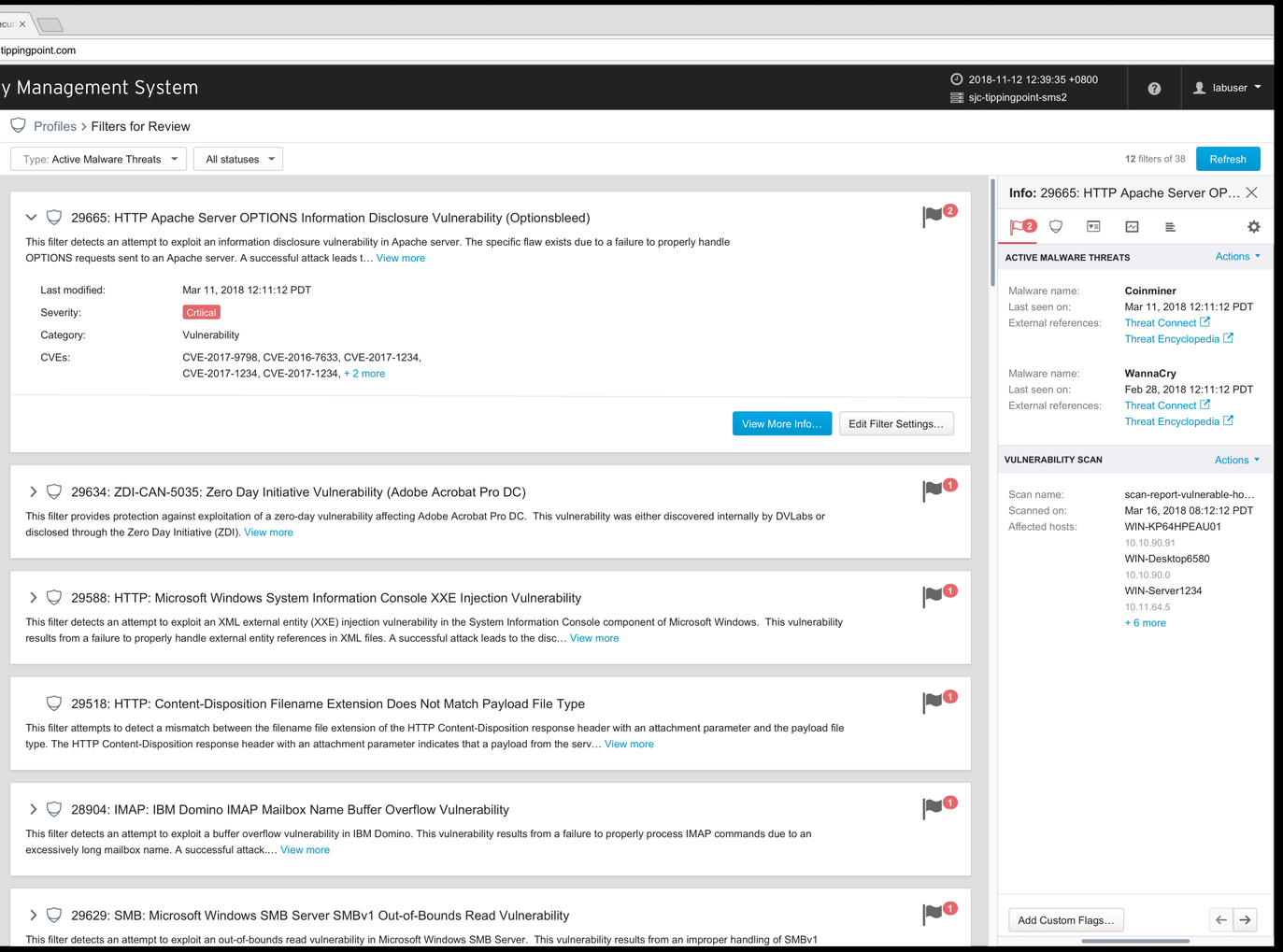


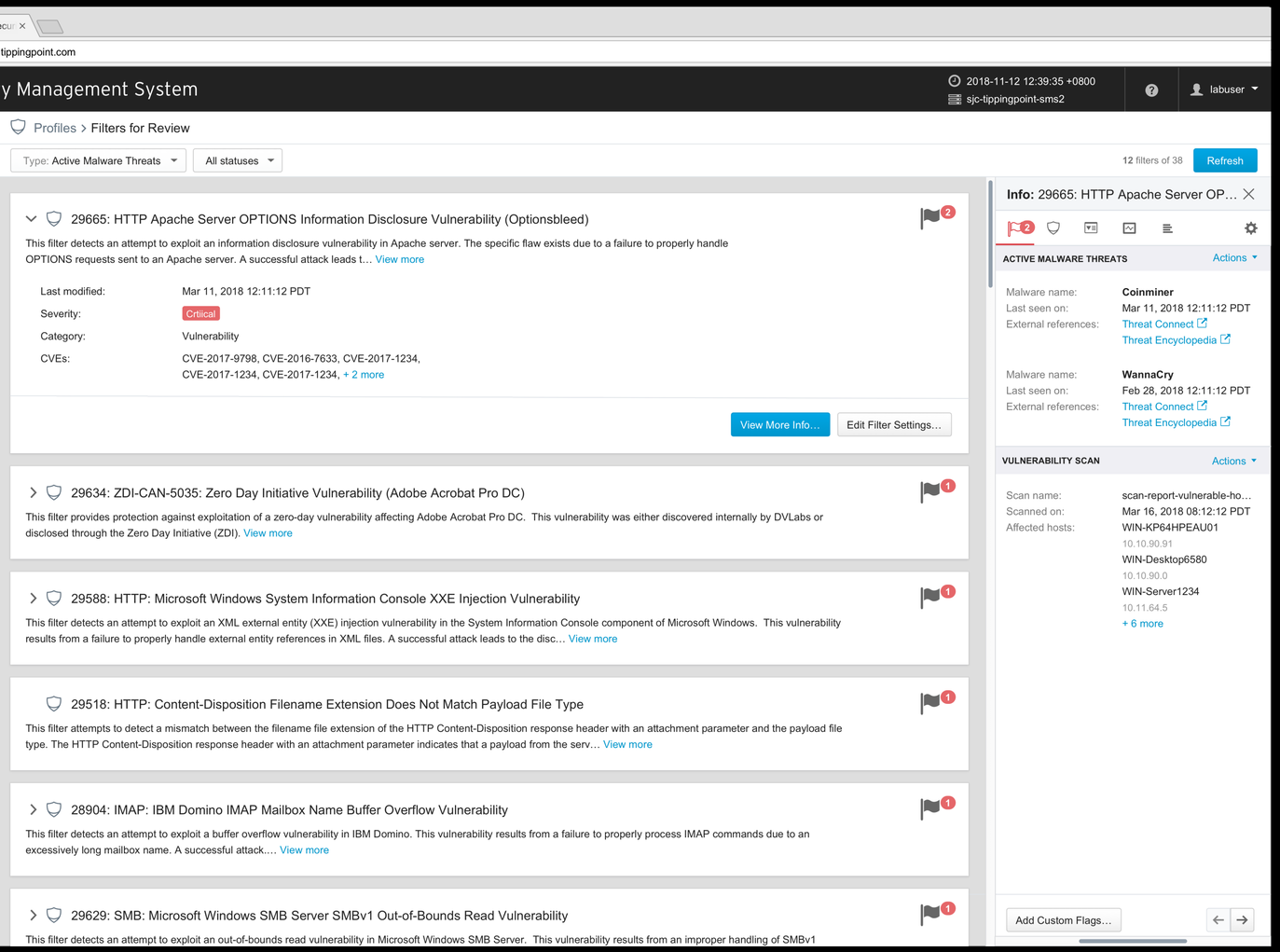
Active Threat Defense

- Made available through an elegant Web UI
- Happy path to defend against vulns and malwares
- Pulls latest threat intelligence updates from SPN
- Visibility into network and cloud IPS policy settings based IPS policy settings

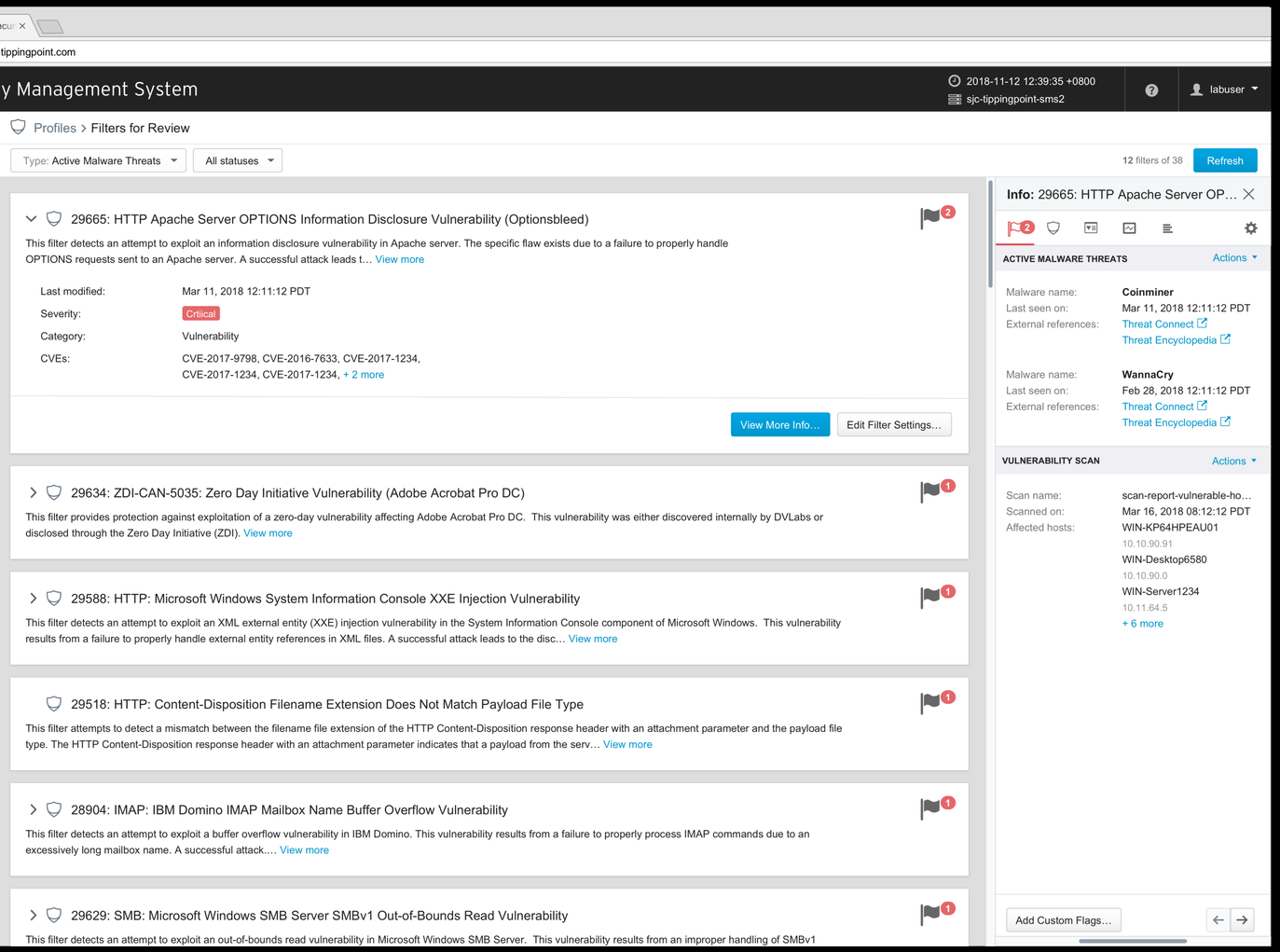

Finder File Edit View Go Window Help
100% Fri 12:39 PM
TippingPoint Security Management System
TippingPoint Security Management System
2017-09-29 08:14:15:05 +0800
2017-09-29 08:14:15:05 +0800
labuser
PROFILES
PROFILES
Inspection
Firewall
Shared Settings
DIGITAL VACCINES
Digital Vaccines
Auxiliary DVs
DV Toolkit
All Filters Review
REPUTATION DB
SCHEDULED DISTRIBUTIONS
VULNERABILITY SCANS (eVR)
Digital Vaccines / All Filters Review
Auto-flagged (31)
Bulk Edit Filter Settings...
29665: HTTP: Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
Released: 09/26/2017
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads to disclosure of sensitive information. Show more
Date Released: 09/12/2017
Severity: CRITICAL
Category: Vulnerabilities
Vulnerability: CVE-2017-9798
Action: Recommended (Disable)
Profile: Default
Edit Filter Settings...
Review Later
Mark as Reviewed
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
Released: 09/26/2017
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. Show more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
Released: 09/19/2017
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disclosure of file co... Show more
16298: TLS: OpenSSL Denial-of-Service Vulnerability
Released: 06/24/2014
This filter detects an attempt to exploit a denial-of-service vulnerability in OpenSSL. Specifically, OpenSSL is vulnerable to a null pointer dereference when parsing tampered records in an OpenSSL handshake using an Encrypted Alert. Successful exploitation would result in a denial-of-service condition. Show more
12882: HTTPS: VMware ESX/ESXi Server Access
Released: 04/23/2013
Auto-flagged: 29665
Details
Review status: Reviewed automatically
Review criteria: User criteria
Reviewed on: 10/10/2017 at 12:13:14 PM
Reasons
This filter was auto-flagged using the selected criteria:
NEW DV
When New DV activated since last review
When Modified DV activated since last review
ACTIVE THREAT DETECTION
When threats are detected using Global Intelligence
When threats are detected in my organization with the following events:
Reputation entry: evilwebsite.ru
Destination IP: 207.22.23.124
Malware family: Locky
CVEs: CVE-2017-12345
VULNERABILITY SCAN None
USER CRITERIA None
Performance Consideration
MacBook


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Crtiical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disc… View more
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.… View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Info: 29665: HTTP Apache Server OP…
ACTIVE MALWARE THREATS
Actions
Malware name: Coinminer
Last seen on: Mar 11, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
Malware name: WannaCry
Last seen on: Feb 28, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
VULNERABILITY SCAN
Actions
Scan name: scan-report-vulnerable-ho…
Scanned on: Mar 16, 2018 08:12:12 PDT
Affected hosts: WIN-KP64HPEAU01
10.10.90.91
WIN-Desktop6580
10.10.90.0
WIN-Server1234
10.11.64.5
+ 6 more
Add Custom Flags…


tippingpoint.com
y Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
Profiles › Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Crtiical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disc… View more
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.… View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Info: 29665: HTTP Apache Server OP…
ACTIVE MALWARE THREATS
Actions
Malware name: Coinminer
Last seen on: Mar 11, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
Malware name: WannaCry
Last seen on: Feb 28, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
VULNERABILITY SCAN
Actions
Scan name: scan-report-vulnerable-ho…
Scanned on: Mar 16, 2018 08:12:12 PDT
Affected hosts: WIN-KP64HPEAU01
10.10.90.91
WIN-Desktop6580
10.10.90.0
WIN-Server1234
10.11.64.5
+ 6 more
Add Custom Flags…

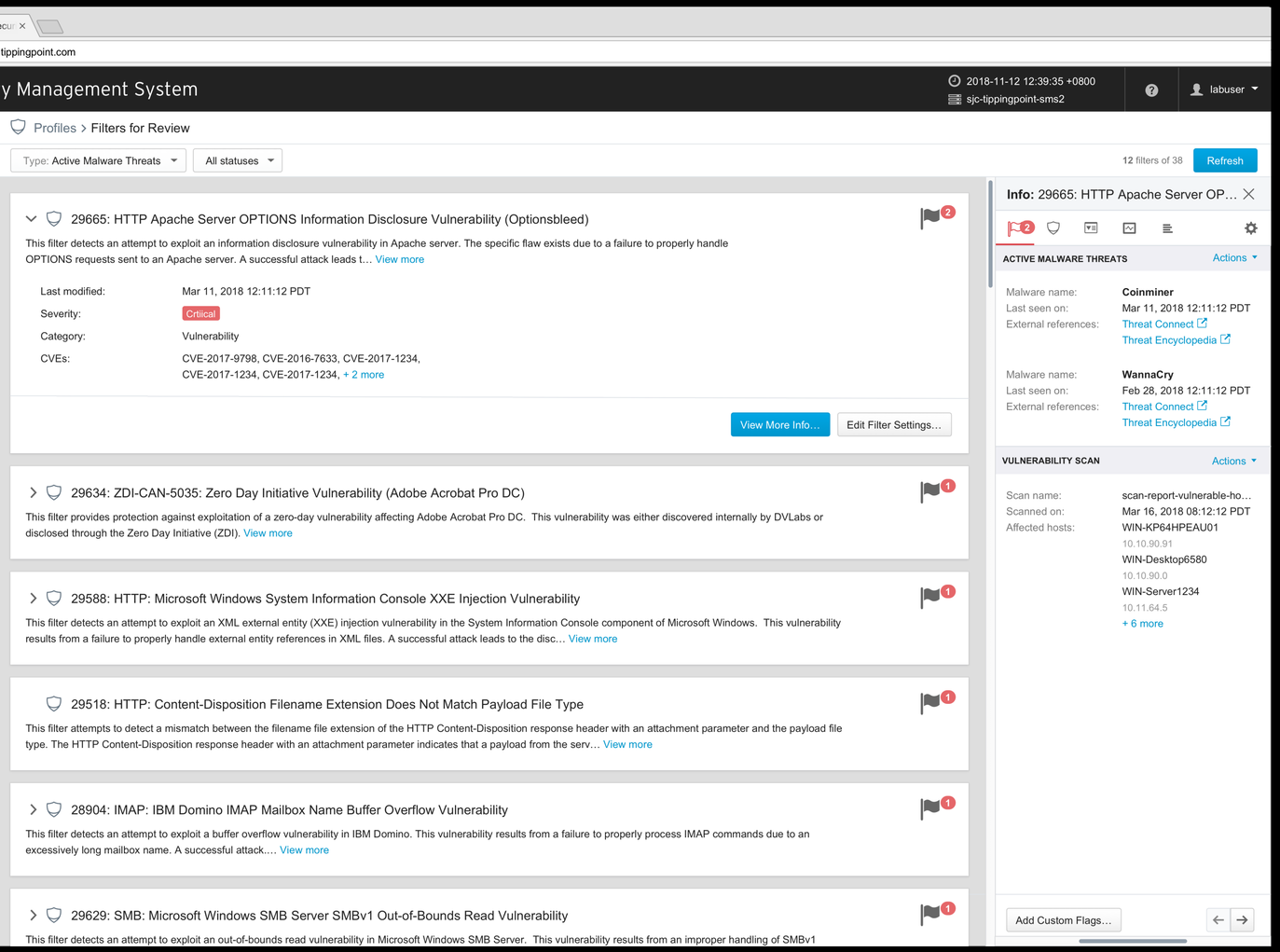


Filters Tuning Workflow - Simplified



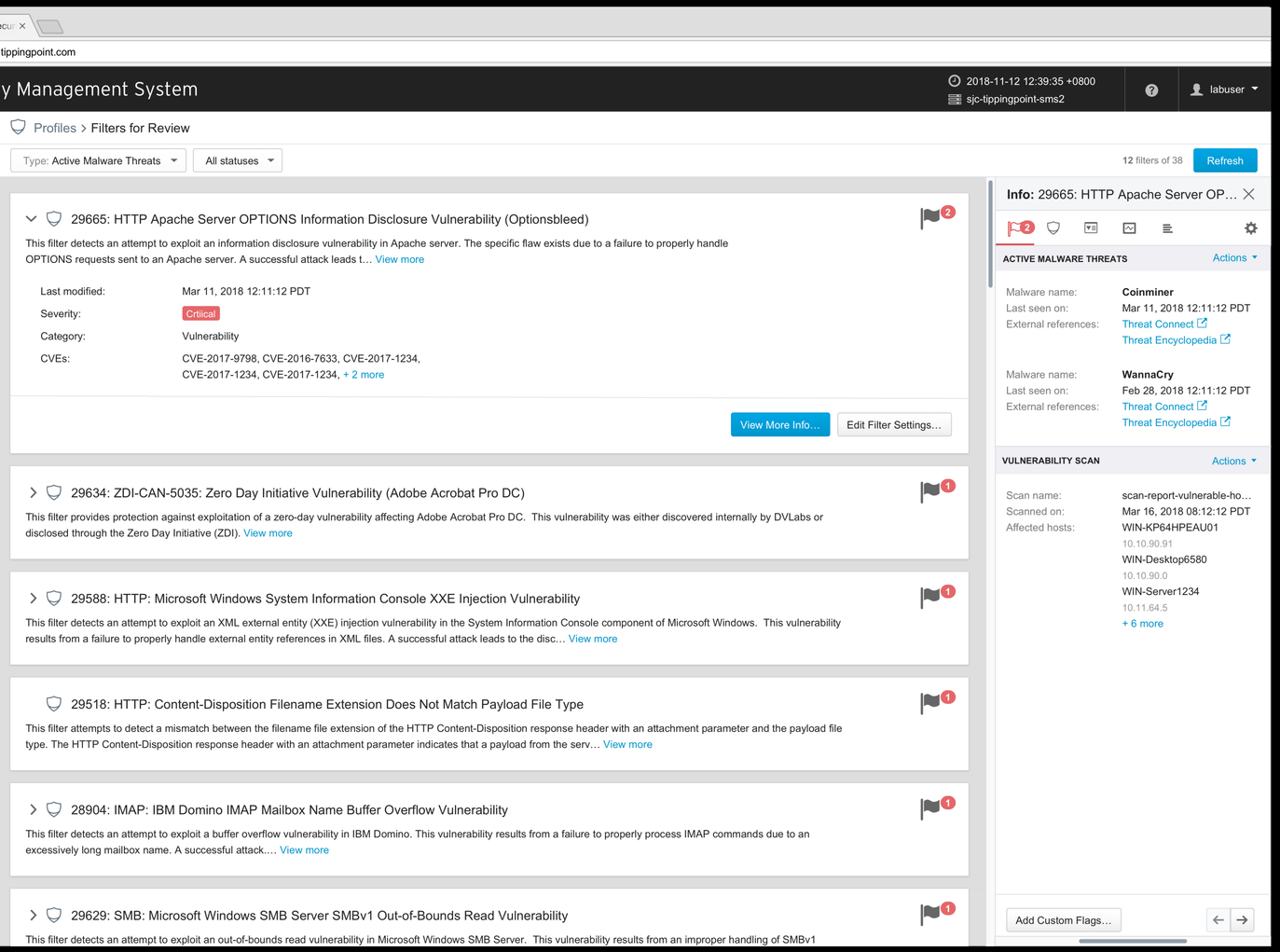
Filters Tuning Workflow - Simplified

- Apache Struts (flagged vulnerable & malware active)



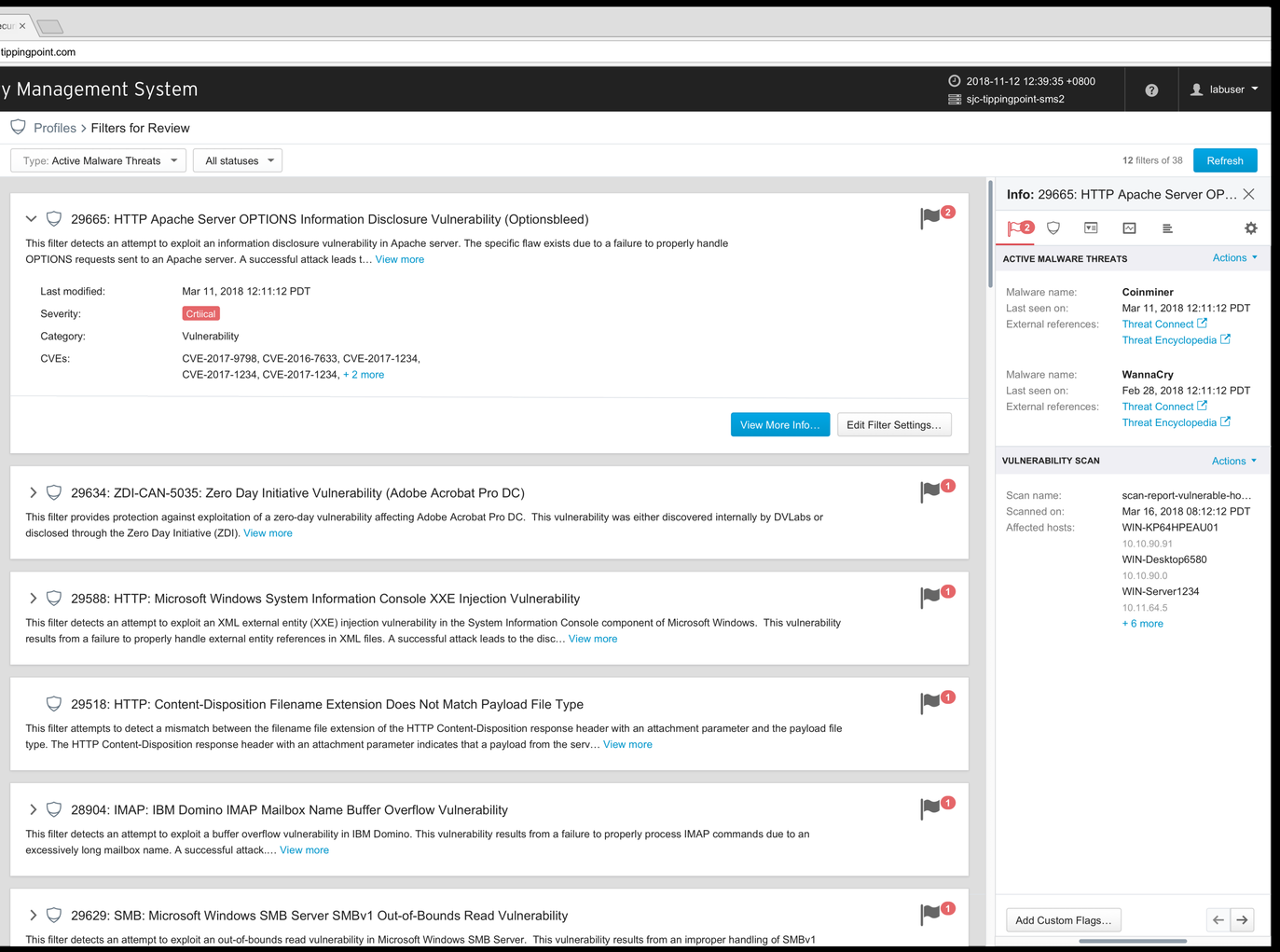
Filters Tuning Workflow - Simplified

- Apache Struts (flagged vulnerable & malware active)
- Context specific to your environment



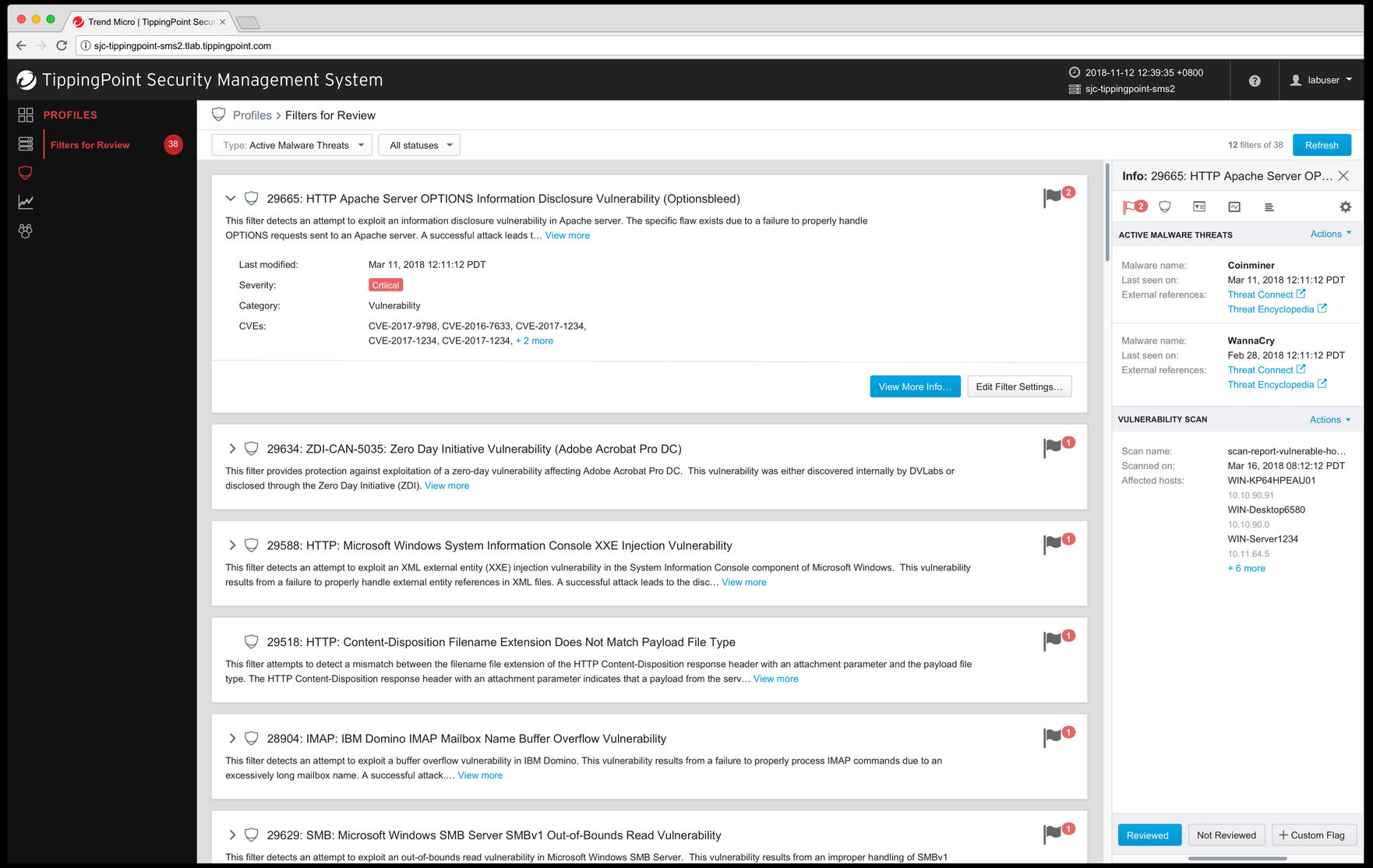
Filters Tuning Workflow – Simplified

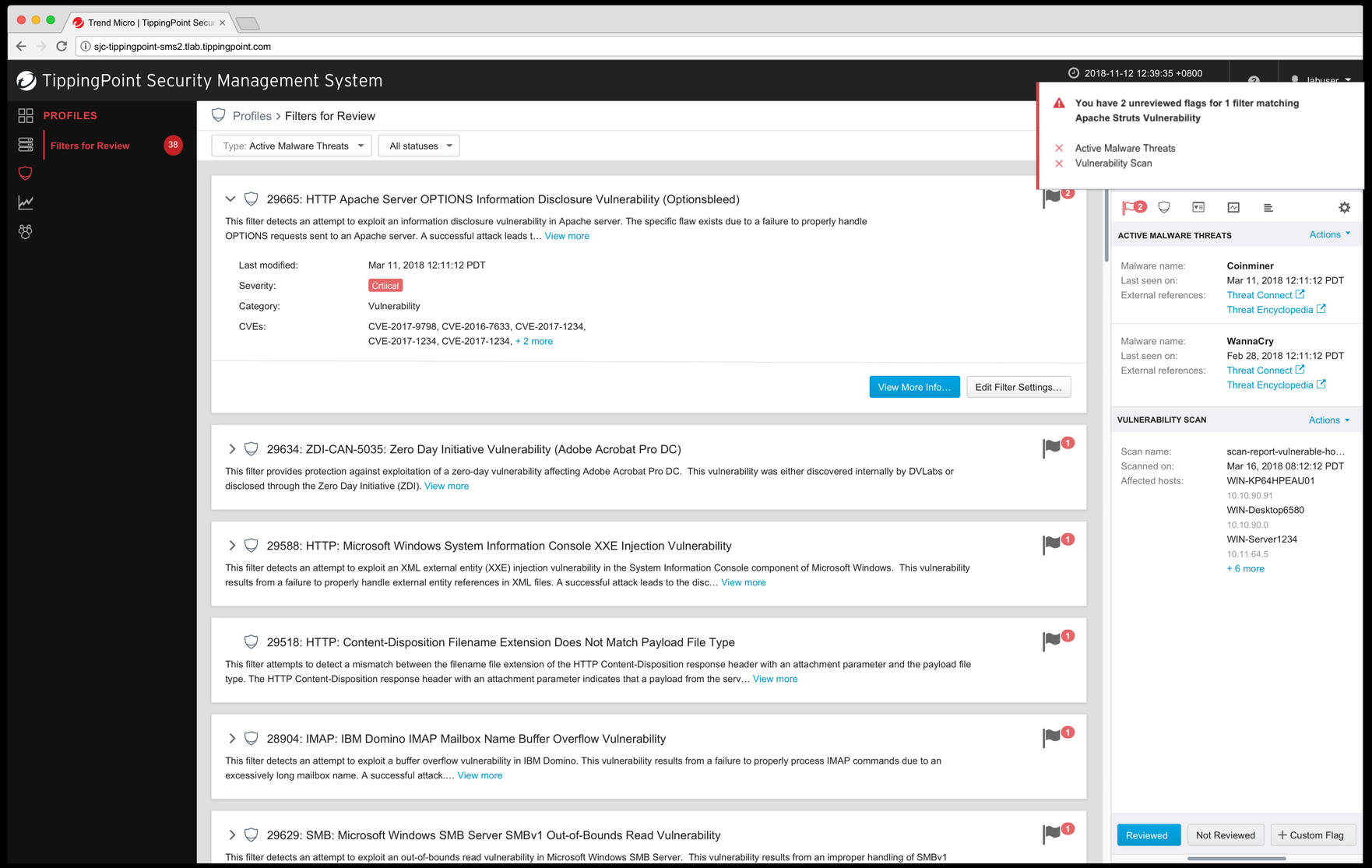
- Apache Struts (flagged vulnerable & malware active)
- Context specific to your environment
- Optimized for operational ease of use

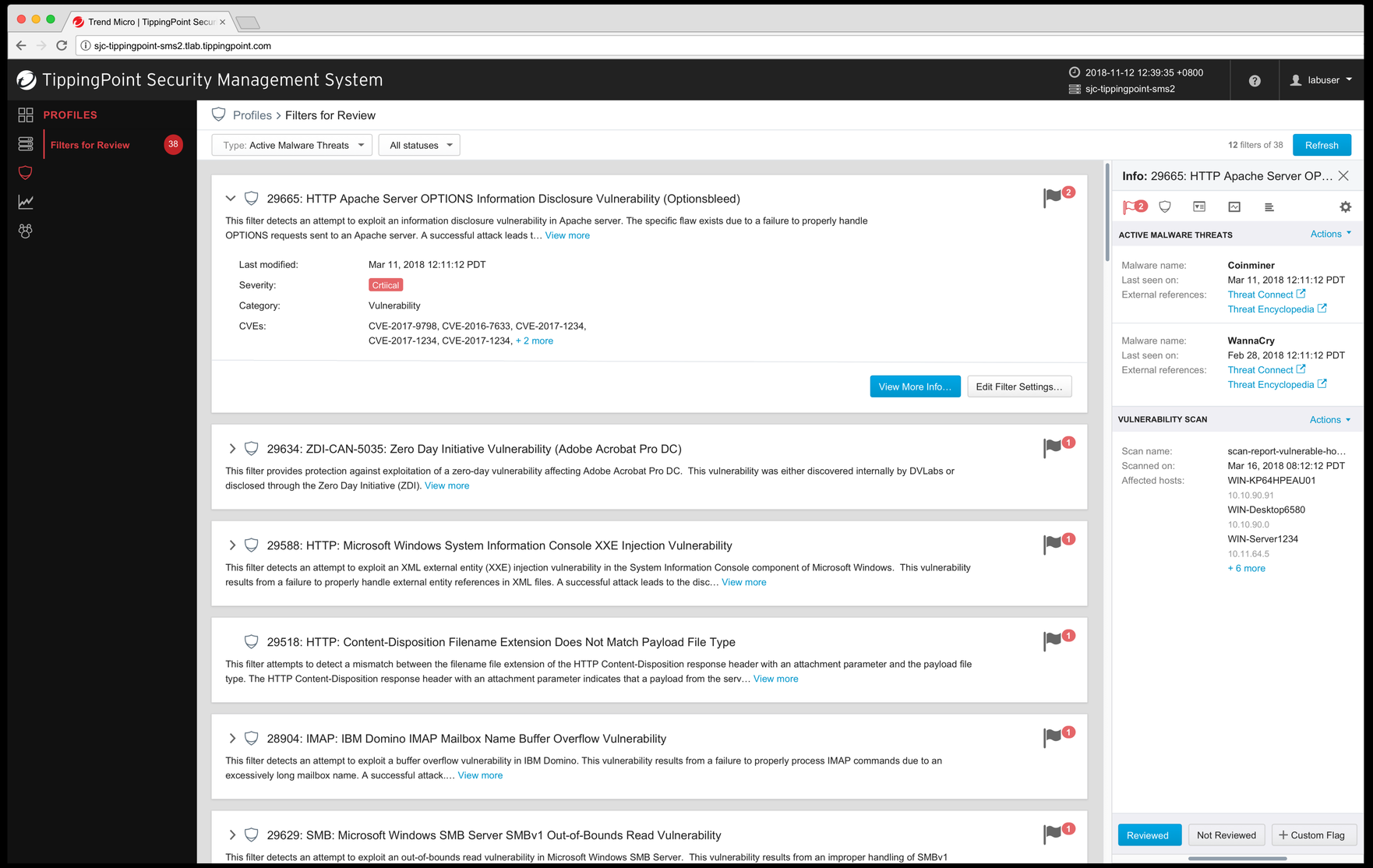


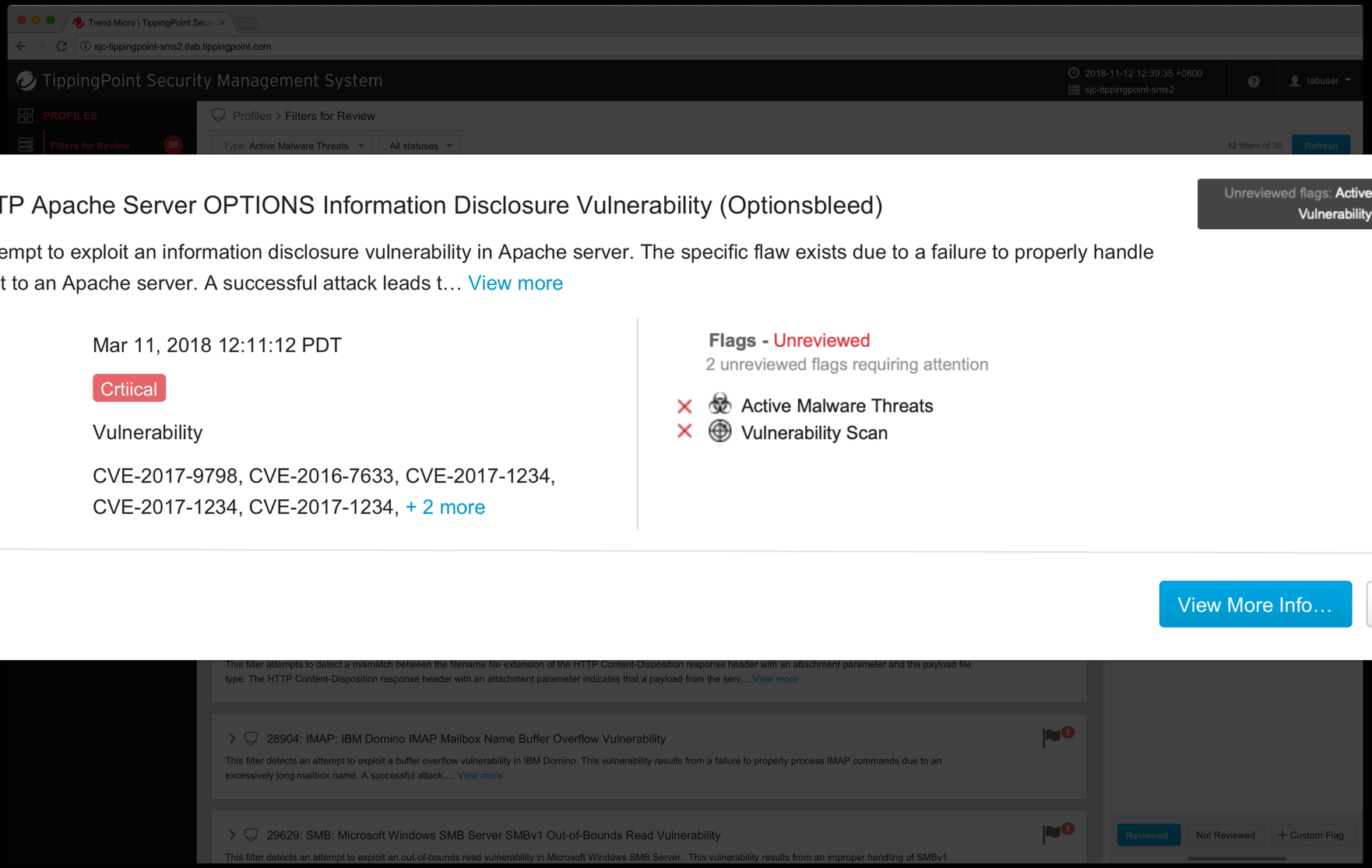
Filters Tuning Workflow – Simplified

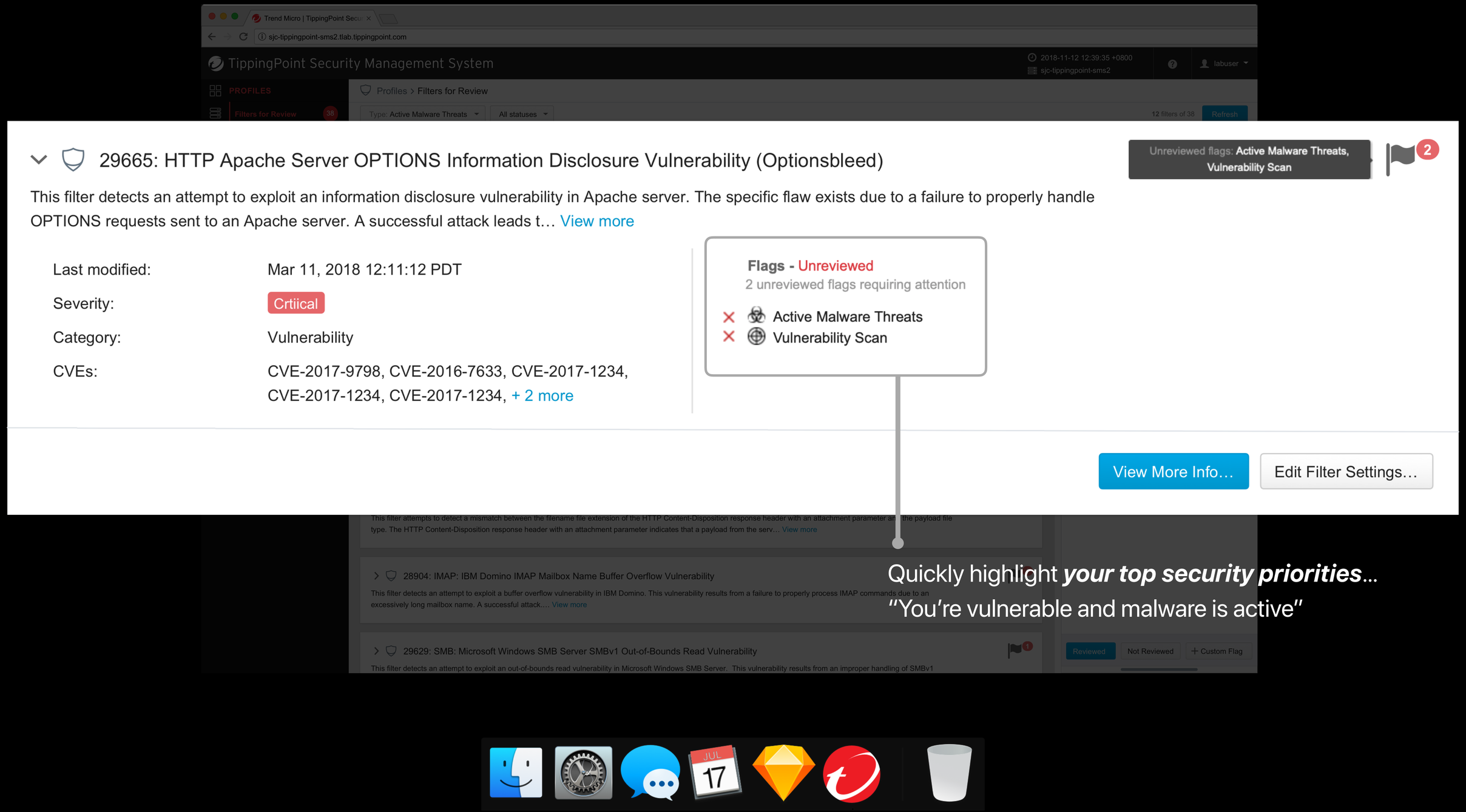
- Apache Struts (flagged vulnerable & malware active)
- Context specific to your environment
- Optimized for operational ease of use
- Recent events related the Apache Struts attack


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disc… View more
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.… View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Info: 29665: HTTP Apache Server OP…
ACTIVE MALWARE THREATS
Actions
Malware name: Coinminer
Last seen on: Mar 11, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
Malware name: WannaCry
Last seen on: Feb 28, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
VULNERABILITY SCAN
Actions
Scan name: scan-report-vulnerable-ho…
Scanned on: Mar 16, 2018 08:12:12 PDT
Affected hosts: WIN-KP64HPEAU01
10.10.90.91
WIN-Desktop6580
10.10.90.0
WIN-Server1234
10.11.64.5
+ 6 more
Reviewed
Not Reviewed
+ Custom Flag


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
You have 2 unreviewed flags for 1 filter matching Apache Struts Vulnerability
Active Malware Threats
Vulnerability Scan
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disc… View more
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.… View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
ACTIVE MALWARE THREATS
Actions
Malware name: Coinminer
Last seen on: Mar 11, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
Malware name: WannaCry
Last seen on: Feb 28, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
VULNERABILITY SCAN
Actions
Scan name: scan-report-vulnerable-ho…
Scanned on: Mar 16, 2018 08:12:12 PDT
Affected hosts: WIN-KP64HPEAU01
10.10.90.91
WIN-Desktop6580
10.10.90.0
WIN-Server1234
10.11.64.5
+ 6 more
Reviewed
Not Reviewed
+ Custom Flag


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disc… View more
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.… View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Info: 29665: HTTP Apache Server OP…
ACTIVE MALWARE THREATS
Actions
Malware name: Coinminer
Last seen on: Mar 11, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
Malware name: WannaCry
Last seen on: Feb 28, 2018 12:11:12 PDT
External references: Threat Connect
Threat Encyclopedia
VULNERABILITY SCAN
Actions
Scan name: scan-report-vulnerable-ho…
Scanned on: Mar 16, 2018 08:12:12 PDT
Affected hosts: WIN-KP64HPEAU01
10.10.90.91
WIN-Desktop6580
10.10.90.0
WIN-Server1234
10.11.64.5
+ 6 more
Reviewed
Not Reviewed
+ Custom Flag


Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
Unreviewed flags: Active Malware Threats, Vulnerability Scan
2
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified:
Mar 11, 2018 12:11:12 PDT
Severity:
Crtiical
Category:
Vulnerability
CVEs:
CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
Flags - Unreviewed
2 unreviewed flags requiring attention
Active Malware Threats
Vulnerability Scan
View More Info…
Edit Filter Settings…
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.... View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Reviewed
Not Reviewed
+ Custom Flag
JUL
17



Quickly highlight ***your top security priorities***…
"You're vulnerable and malware is active"

Info: 29665: HTTP Apache Server OP…

ACTIVE MALWARE THREATS Unreviewed Actions

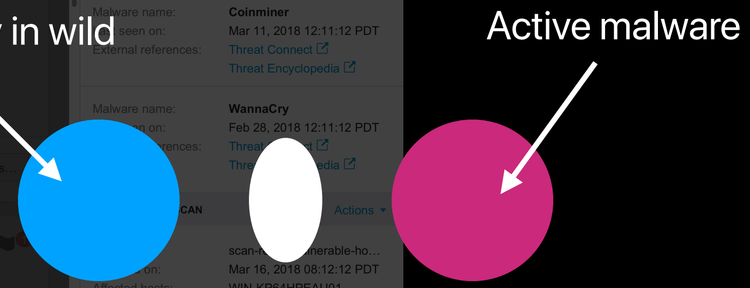
Malware name:	**Coinminer**
Last seen on:	Mar 11, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

Malware name:	**WannaCry**
Last seen on:	Feb 28, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

VULNERABILITY SCAN Unreviewed Actions

Scan name:	scan-report-vulnerable-ho…
Scanned on:	Mar 16, 2018 08:12:12 PDT
Affected hosts:	WIN-KP64HPEAU01 10.10.90.91 WIN-Desktop6580 10.10.90.0 WIN-Server1234 10.11.64.5 + 6 more

Reviewed | Not Reviewed | + Custom Flag



Info: 29665: HTTP Apache Server OP…

ACTIVE MALWARE THREATS Unreviewed Actions

Malware name:	**Coinminer**
Last seen on:	Mar 11, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

Malware name:	**WannaCry**
Last seen on:	Feb 28, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

VULNERABILITY SCAN Unreviewed Actions

Scan name:	scan-report-vulnerable-ho…
Scanned on:	Mar 16, 2018 08:12:12 PDT
Affected hosts:	WIN-KP64HPEAU01 10.10.90.91 WIN-Desktop6580 10.10.90.0 WIN-Server1234 10.11.64.5 + 6 more

Reviewed | Not Reviewed | + Custom Flag

Info: 29665: HTTP Apache Server OP…

ACTIVE MALWARE THREATS Unreviewed Actions

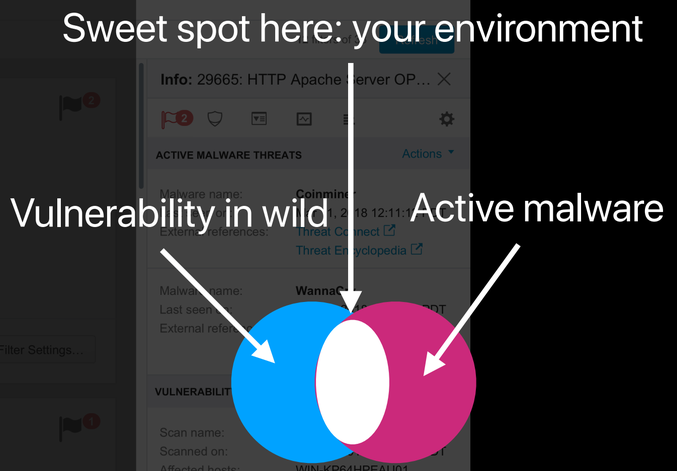
Malware name:	**Coinminer**
Last seen on:	Mar 11, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

Malware name:	**WannaCry**
Last seen on:	Feb 28, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

VULNERABILITY SCAN Unreviewed Actions

Scan name:	scan-report-vulnerable-ho…
Scanned on:	Mar 16, 2018 08:12:12 PDT
Affected hosts:	WIN-KP64HPEAU01 10.10.90.91 WIN-Desktop6580 10.10.90.0 WIN-Server1234 10.11.64.5 + 6 more

Reviewed | Not Reviewed | + Custom Flag



Info: 29665: HTTP Apache Server OP…

ACTIVE MALWARE THREATS Unreviewed Actions

Malware name:	**Coinminer**
Last seen on:	Mar 11, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

Malware name:	**WannaCry**
Last seen on:	Feb 28, 2018 12:11:12 PDT
External references:	Threat Connect Threat Encyclopedia

VULNERABILITY SCAN Unreviewed Actions

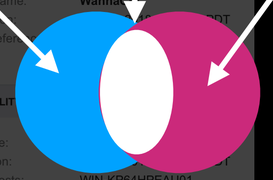
Scan name:	scan-report-vulnerable-ho…
Scanned on:	Mar 16, 2018 08:12:12 PDT
Affected hosts:	WIN-KP64HPEAU01 10.10.90.91 WIN-Desktop6580 10.10.90.0 WIN-Server1234 10.11.64.5 + 6 more

Reviewed | Not Reviewed | + Custom Flag

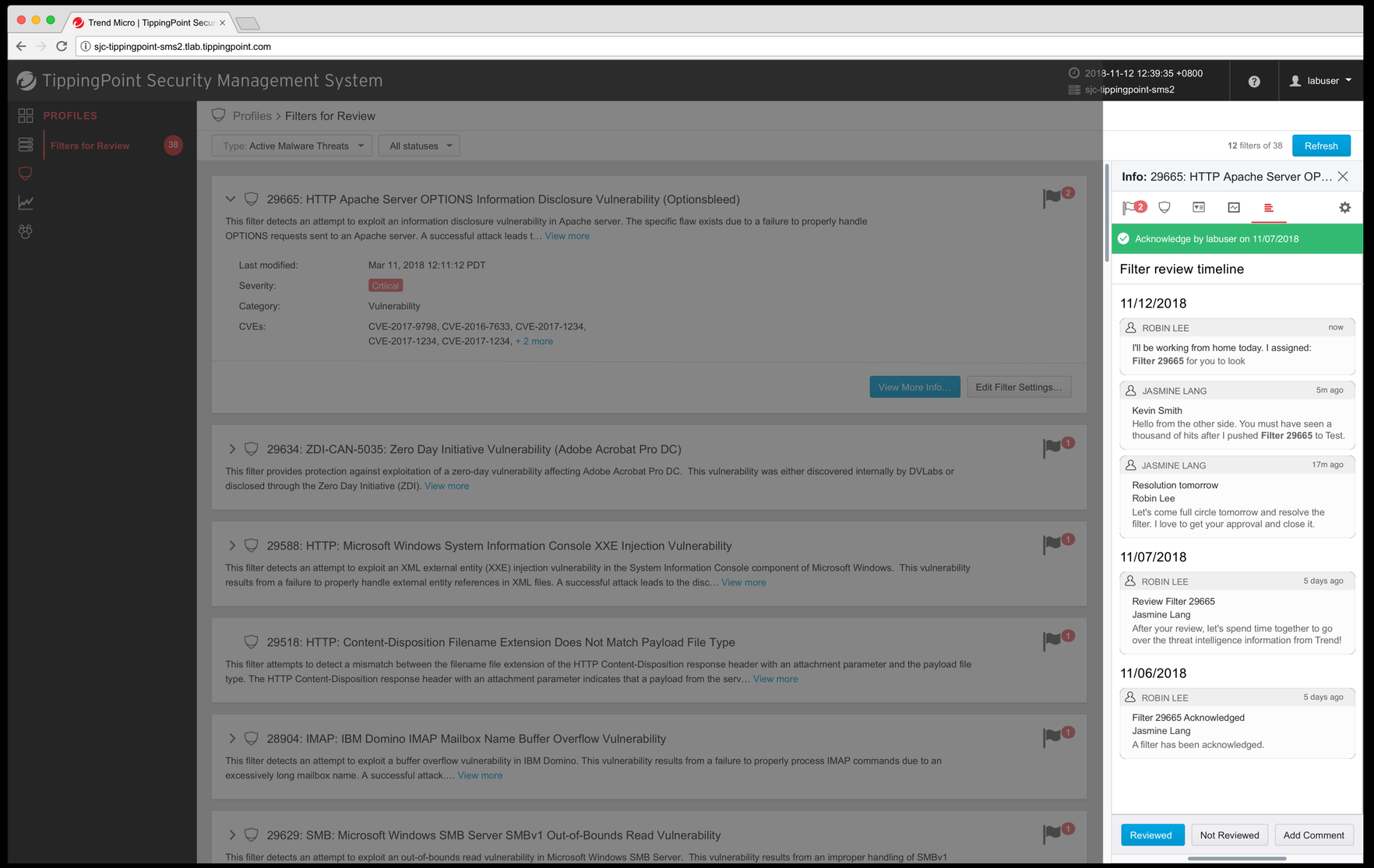
Sweet spot here: your environment

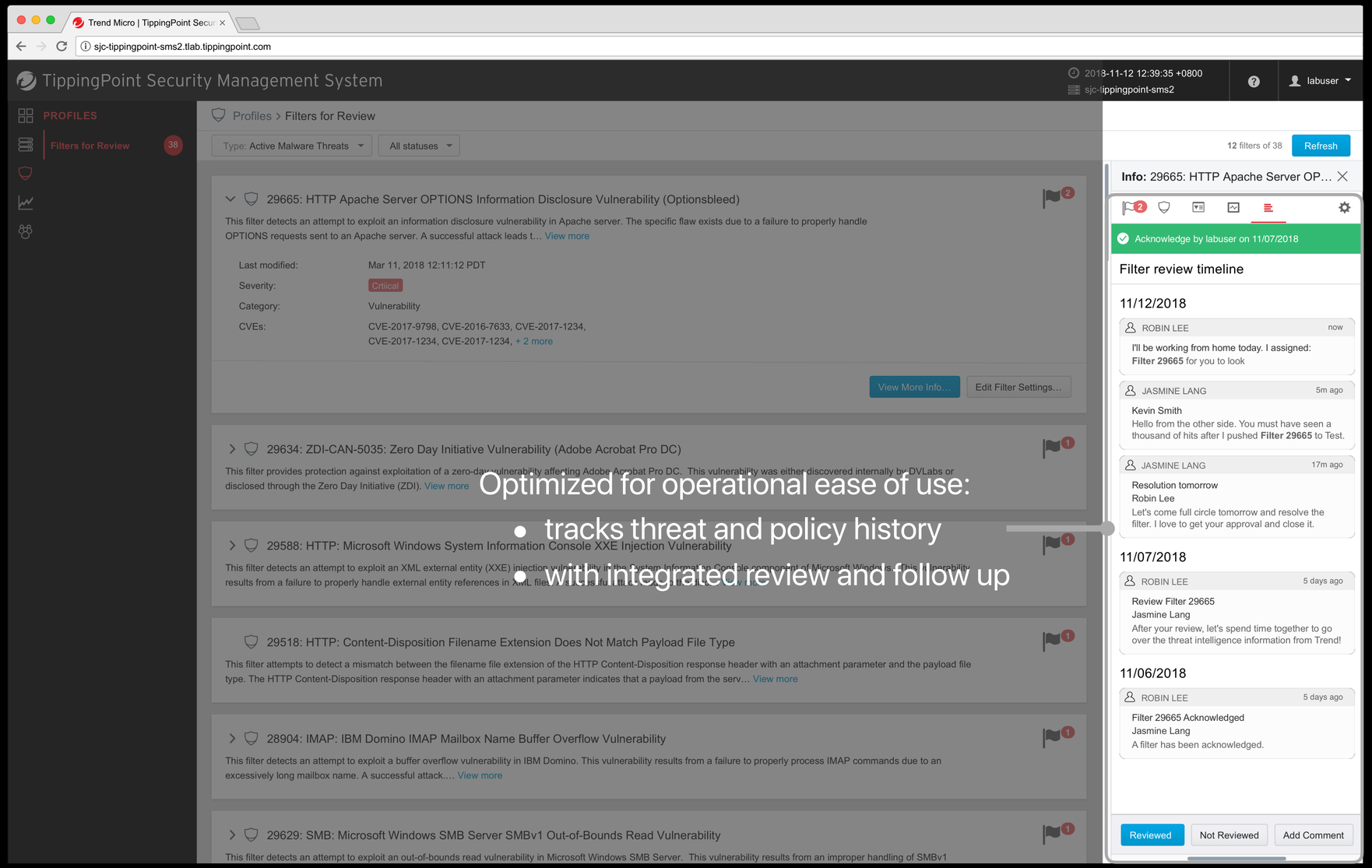
Vulnerability in wild

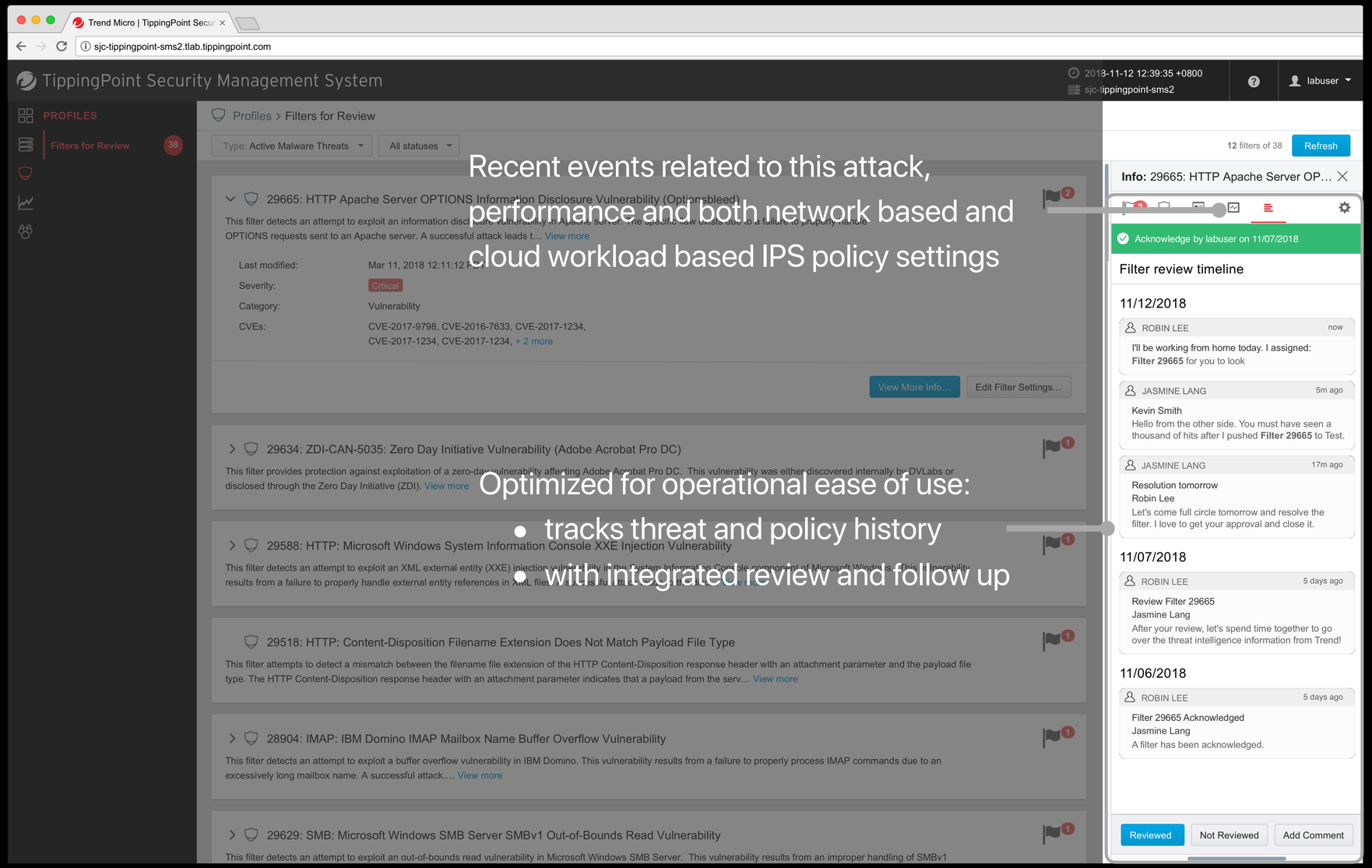
Active malware



Context specific to ***your*** environment including vulnerability assessments


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2013-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files. A successful attack leads to the disc… View more
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.... View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Info: 29665: HTTP Apache Server OP…
Acknowledge by labuser on 11/07/2018
Filter review timeline
11/12/2018
ROBIN LEE now
I'll be working from home today. I assigned: Filter 29665 for you to look
JASMINE LANG 5m ago
Kevin Smith
Hello from the other side. You must have seen a thousand of hits after I pushed Filter 29665 to Test.
JASMINE LANG 17m ago
Resolution tomorrow
Robin Lee
Let's come full circle tomorrow and resolve the filter. I love to get your approval and close it.
11/07/2018
ROBIN LEE 5 days ago
Review Filter 29665
Jasmine Lang
After your review, let's spend time together to go over the threat intelligence information from Trend!
11/06/2018
ROBIN LEE 5 days ago
Filter 29665 Acknowledged
Jasmine Lang
A filter has been acknowledged.
Reviewed
Not Reviewed
Add Comment

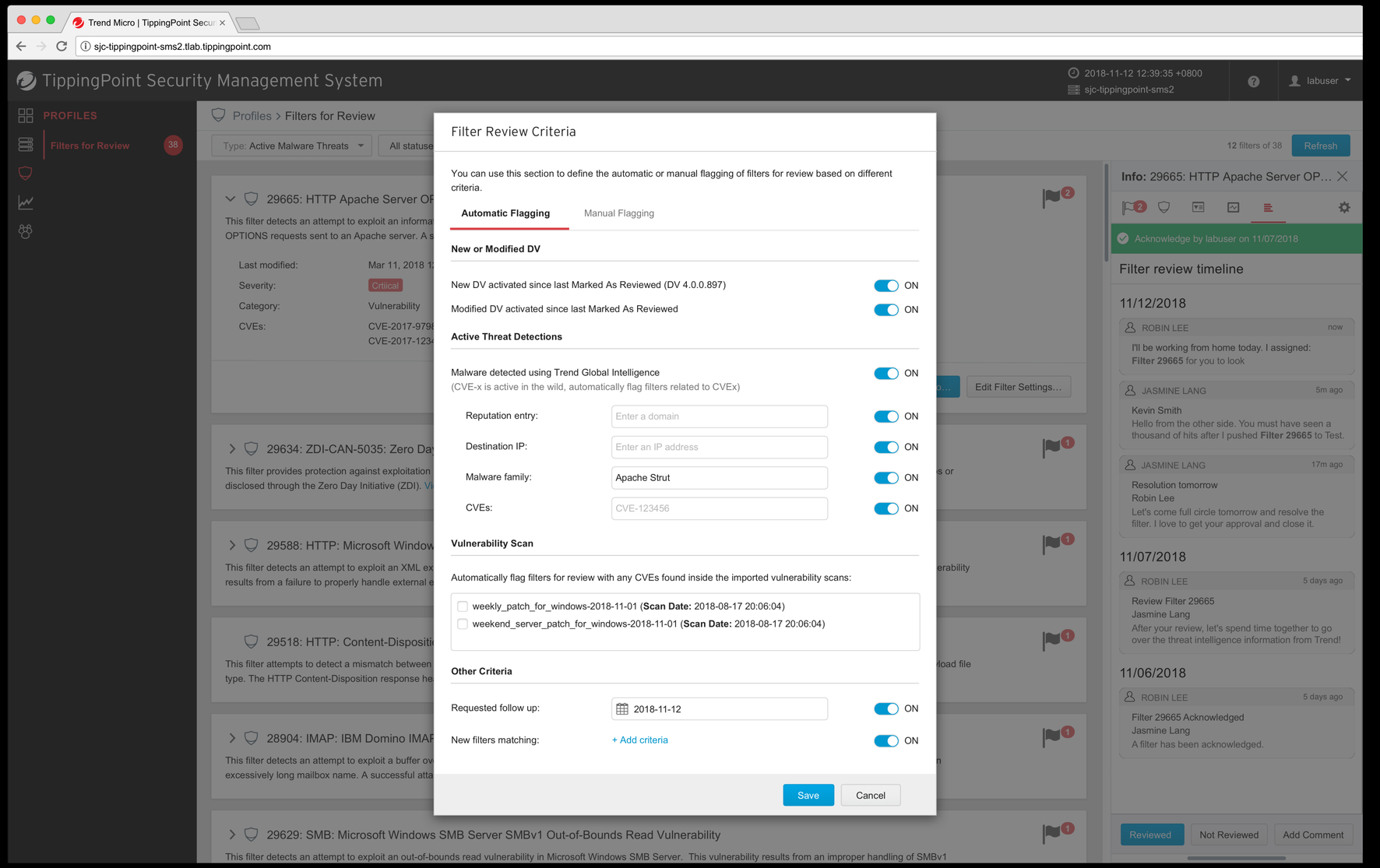

Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2013-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OPTIONS Information Disclosure Vulnerability (Optionsbleed)
This filter detects an attempt to exploit an information disclosure vulnerability in Apache server. The specific flaw exists due to a failure to properly handle OPTIONS requests sent to an Apache server. A successful attack leads t… View more
Last modified: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerability
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, CVE-2017-1234, CVE-2017-1234, + 2 more
View More Info…
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Day Initiative Vulnerability (Adobe Acrobat Pro DC)
This filter provides protection against exploitation of a zero-day vulnerability affecting Adobe Acrobat Pro DC. This vulnerability was either discovered internally by DVLabs or disclosed through the Zero Day Initiative (ZDI). View more
29588: HTTP: Microsoft Windows System Information Console XXE Injection Vulnerability
This filter detects an attempt to exploit an XML external entity (XXE) injection vulnerability in the System Information Console component of Microsoft Windows. This vulnerability results from a failure to properly handle external entity references in XML files
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
This filter attempts to detect a mismatch between the filename file extension of the HTTP Content-Disposition response header with an attachment parameter and the payload file type. The HTTP Content-Disposition response header with an attachment parameter indicates that a payload from the serv… View more
28904: IMAP: IBM Domino IMAP Mailbox Name Buffer Overflow Vulnerability
This filter detects an attempt to exploit a buffer overflow vulnerability in IBM Domino. This vulnerability results from a failure to properly process IMAP commands due to an excessively long mailbox name. A successful attack.... View more
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Info: 29665: HTTP Apache Server OP…
Acknowledge by labuser on 11/07/2018
Filter review timeline
11/12/2018
ROBIN LEE now
I'll be working from home today. I assigned: Filter 29665 for you to look
JASMINE LANG 5m ago
Kevin Smith
Hello from the other side. You must have seen a thousand of hits after I pushed Filter 29665 to Test.
JASMINE LANG 17m ago
Resolution tomorrow
Robin Lee
Let's come full circle tomorrow and resolve the filter. I love to get your approval and close it.
11/07/2018
ROBIN LEE 5 days ago
Review Filter 29665
Jasmine Lang
After your review, let's spend time together to go over the threat intelligence information from Trend!
11/06/2018
ROBIN LEE 5 days ago
Filter 29665 Acknowledged
Jasmine Lang
A filter has been acknowledged.
Reviewed
Not Reviewed
Add Comment
Optimized for operational ease of use:
tracks threat and policy history
with integrated review and follow up

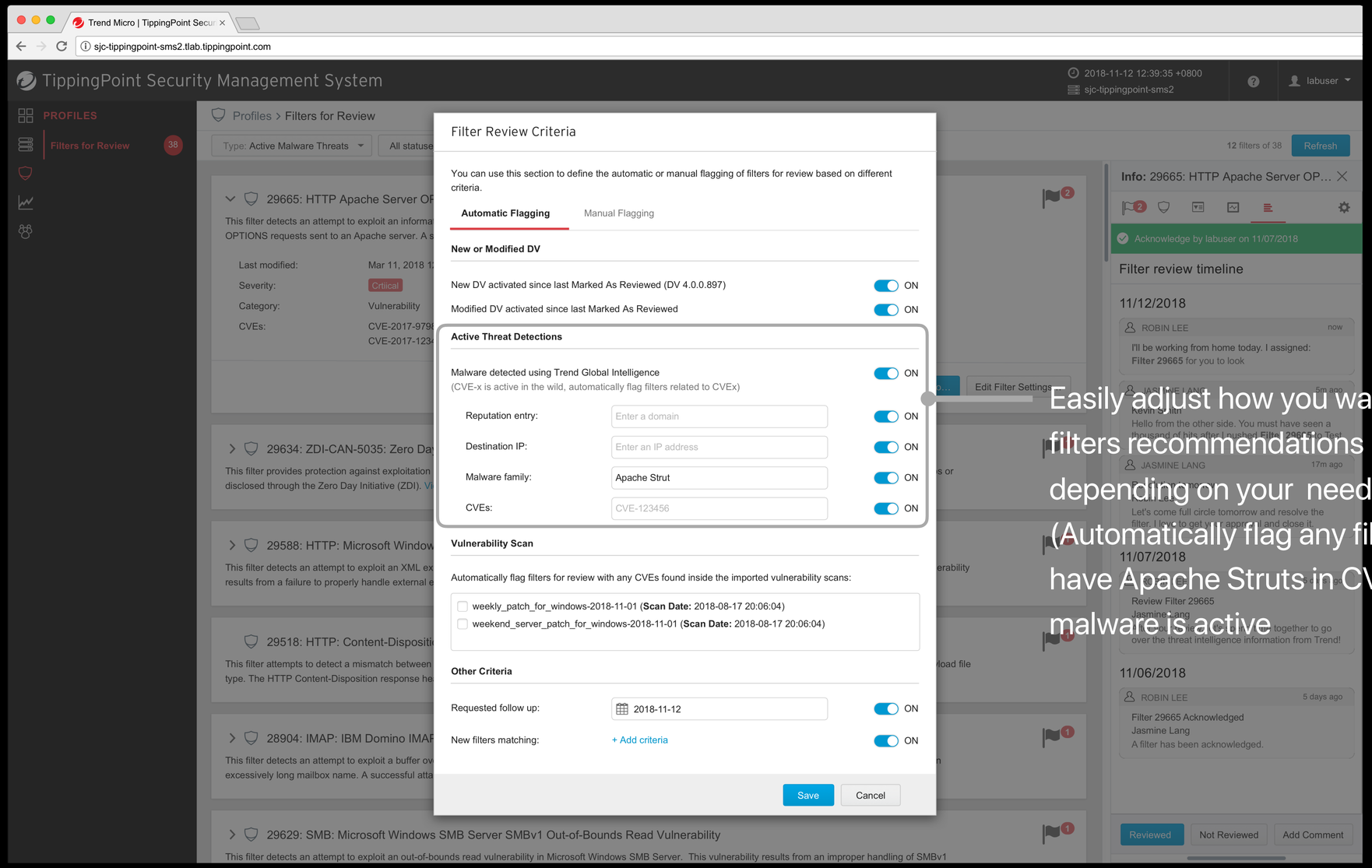


Recent events related to this attack, performance and both network based and cloud workload based IPS policy settings

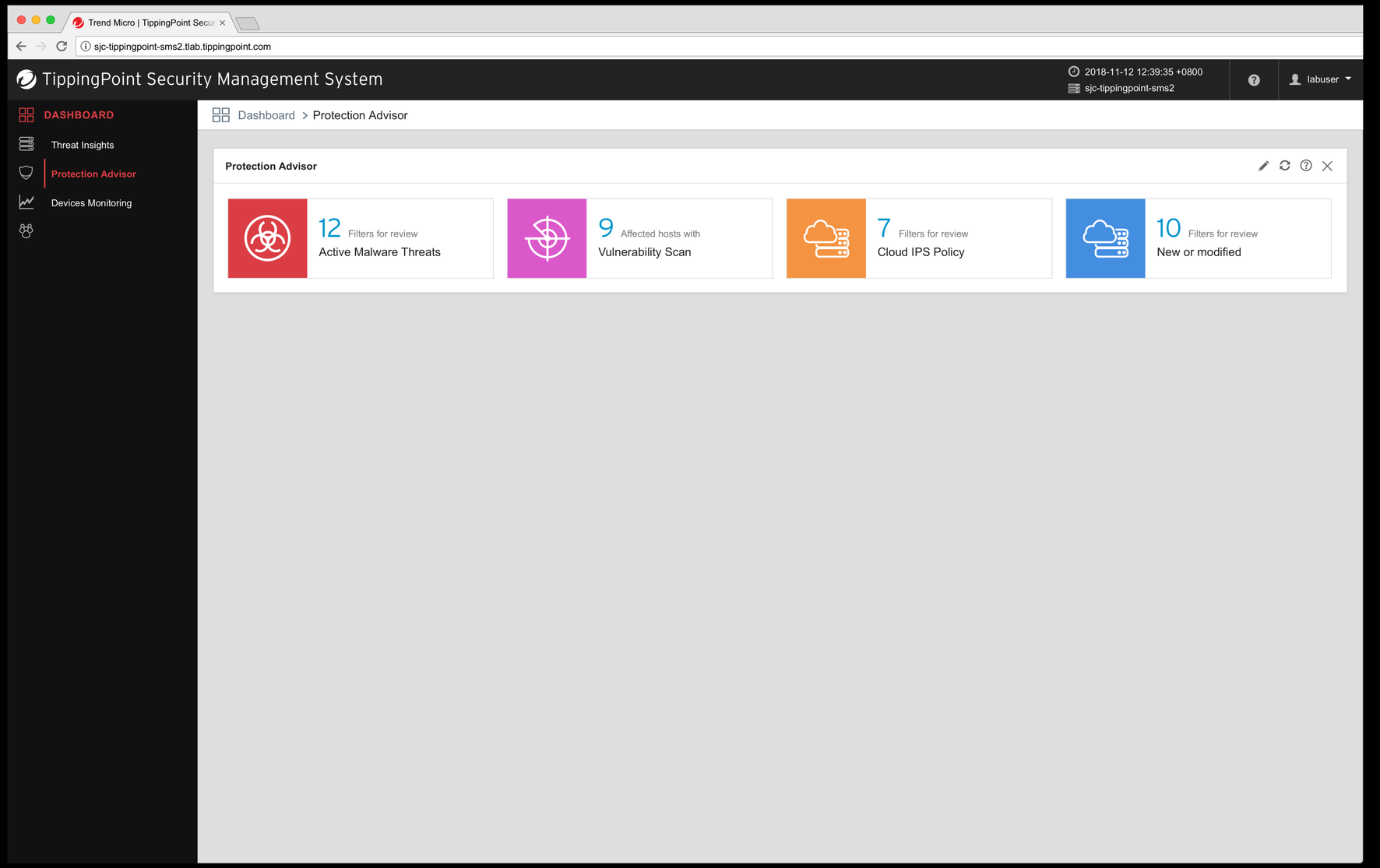
Optimized for operational ease of use:

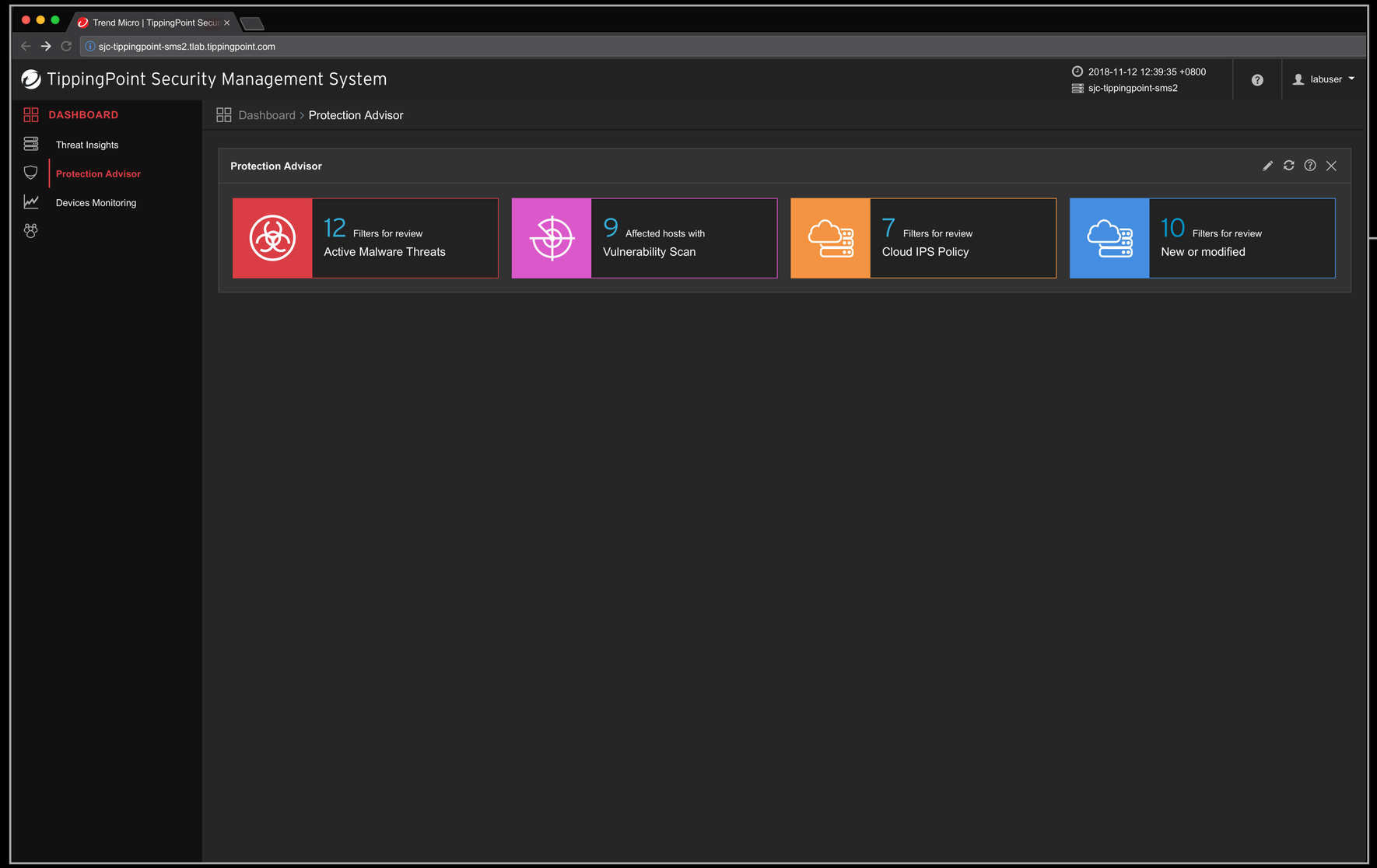
- tracks threat and policy history
- with integrated review and follow up


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review
38
Profiles > Filters for Review
Type: Active Malware Threats
All statuses
12 filters of 38
Refresh
29665: HTTP Apache Server OP
This filter detects an attempt to exploit an informa
OPTIONS requests sent to an Apache server. A s
Last modified:
Mar 11, 2018 1
Severity:
Critical
Category:
Vulnerability
CVEs:
CVE-2017-979
CVE-2017-123
Edit Filter Settings…
29634: ZDI-CAN-5035: Zero Da
This filter provides protection against exploitation
disclosed through the Zero Day Initiative (ZDI).
29588: HTTP: Microsoft Windo
This filter detects an attempt to exploit an XML ex
results from a failure to properly handle external e
29518: HTTP: Content-Dispositi
This filter attempts to detect a mismatch between
type. The HTTP Content-Disposition response he
28904: IMAP: IBM Domino IMAP
This filter detects an attempt to exploit a buffer ov
excessively long mailbox name. A successful atta
29629: SMB: Microsoft Windows SMB Server SMBv1 Out-of-Bounds Read Vulnerability
This filter detects an attempt to exploit an out-of-bounds read vulnerability in Microsoft Windows SMB Server. This vulnerability results from an improper handling of SMBv1
Filter Review Criteria
You can use this section to define the automatic or manual flagging of filters for review based on different criteria.
Automatic Flagging
Manual Flagging
New or Modified DV
New DV activated since last Marked As Reviewed (DV 4.0.0.897)
ON
Modified DV activated since last Marked As Reviewed
ON
Active Threat Detections
Malware detected using Trend Global Intelligence
(CVE-x is active in the wild, automatically flag filters related to CVEx)
ON
Reputation entry:
Enter a domain
ON
Destination IP:
Enter an IP address
ON
Malware family:
Apache Strut
ON
CVEs:
CVE-123456
ON
Vulnerability Scan
Automatically flag filters for review with any CVEs found inside the imported vulnerability scans:
weekly_patch_for_windows-2018-11-01 (Scan Date: 2018-08-17 20:06:04)
weekend_server_patch_for_windows-2018-11-01 (Scan Date: 2018-08-17 20:06:04)
Other Criteria
Requested follow up:
2018-11-12
ON
New filters matching:
+ Add criteria
ON
Save
Cancel
Info: 29665: HTTP Apache Server OP…
Acknowledge by labuser on 11/07/2018
Filter review timeline
11/12/2018
ROBIN LEE
now
I'll be working from home today. I assigned: Filter 29665 for you to look
JASMINE LANG
5m ago
Kevin Smith
Hello from the other side. You must have seen a thousand of hits after I pushed Filter 29665 to Test.
JASMINE LANG
17m ago
Resolution tomorrow
Robin Lee
Let's come full circle tomorrow and resolve the filter. I love to get your approval and close it.
11/07/2018
ROBIN LEE
5 days ago
Review Filter 29665
Jasmine Lang
After your review, let's spend time together to go over the threat intelligence information from Trend!
11/06/2018
ROBIN LEE
5 days ago
Filter 29665 Acknowledged
Jasmine Lang
A filter has been acknowledged.
Reviewed
Not Reviewed
Add Comment



Easily adjust how you want filters recommendations depending on your needs (Automatically flag any filters that have Apache Struts in CVEs or malware is active


Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
DASHBOARD
Threat Insights
Protection Advisor
Devices Monitoring
Dashboard > Protection Advisor
Protection Advisor
12 Filters for review
Active Malware Threats
9 Affected hosts with
Vulnerability Scan
7 Filters for review
Cloud IPS Policy
10 Filters for review
New or modified

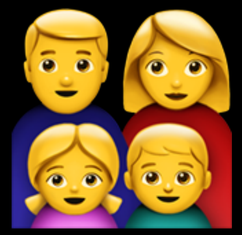

Trend Micro | TippingPoint Secur
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0800
sjc-tippingpoint-sms2
labuser
DASHBOARD
Threat Insights
Protection Advisor
Devices Monitoring
Dashboard > Protection Advisor
Protection Advisor
12 Filters for review
Active Malware Threats
9 Affected hosts with
Vulnerability Scan
7 Filters for review
Cloud IPS Policy
10 Filters for review
New or modified

Dark Theme

DEMO

UXSW2018

https://8az3pp.axshare.com (password: ~~SXSW2018~~)



Please give us feedback on the new Active Threat Defense experience:

- Active malware/vulnerabilities
- Filters tuning workflow


Thank you