# Designing IPS Policy Workflow

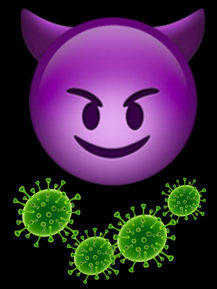
Michael Lang, UI Designer, HIE

# Design

# Design

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

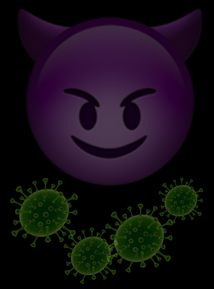
*–Russ Meyers*



Threats in The Wild

Filters Tuning

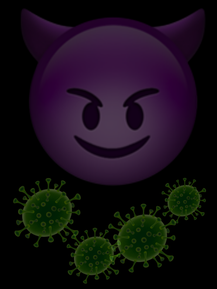
Performance Management



Threats in The Wild

Filters Tuning

Performance Management

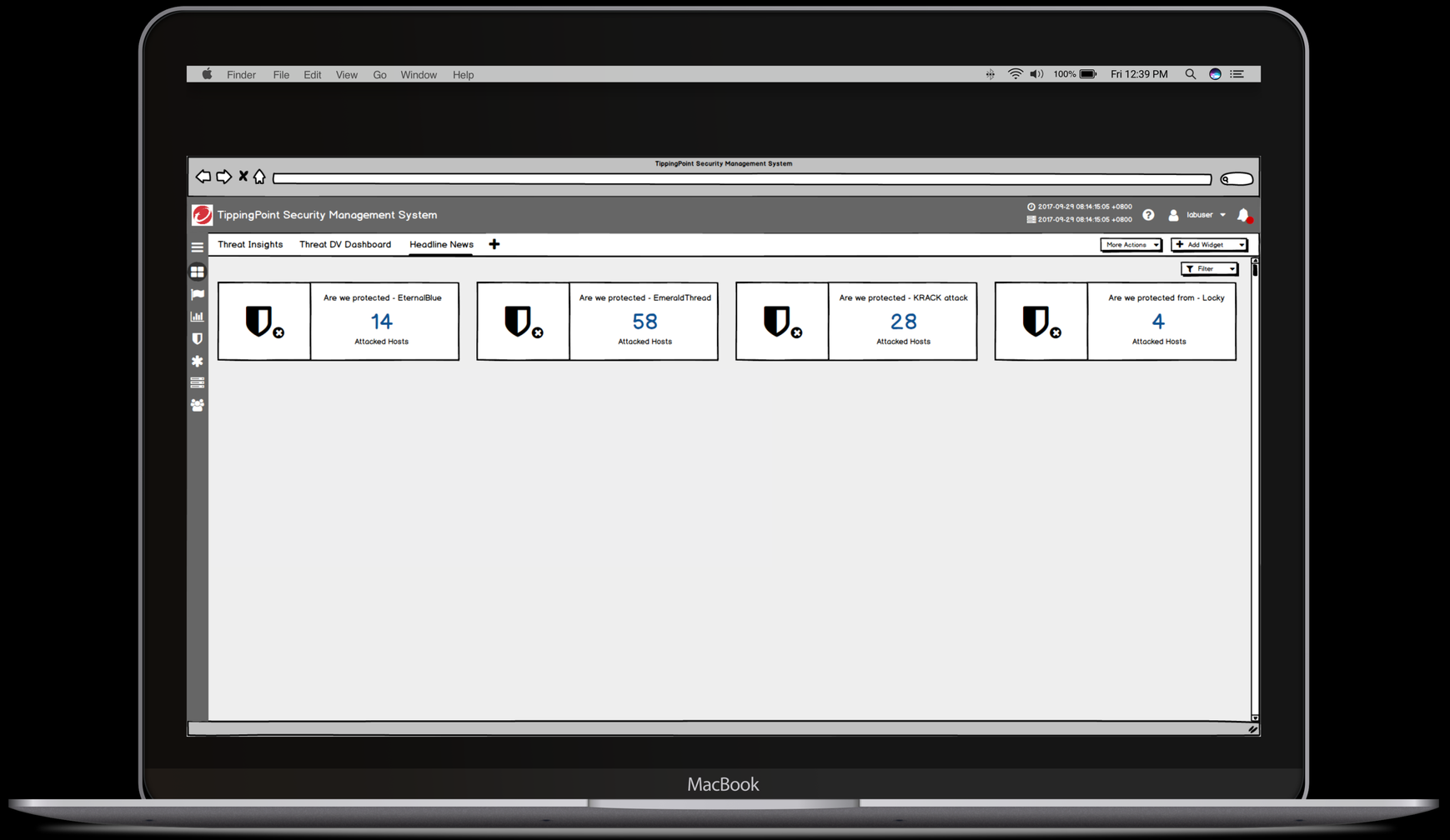


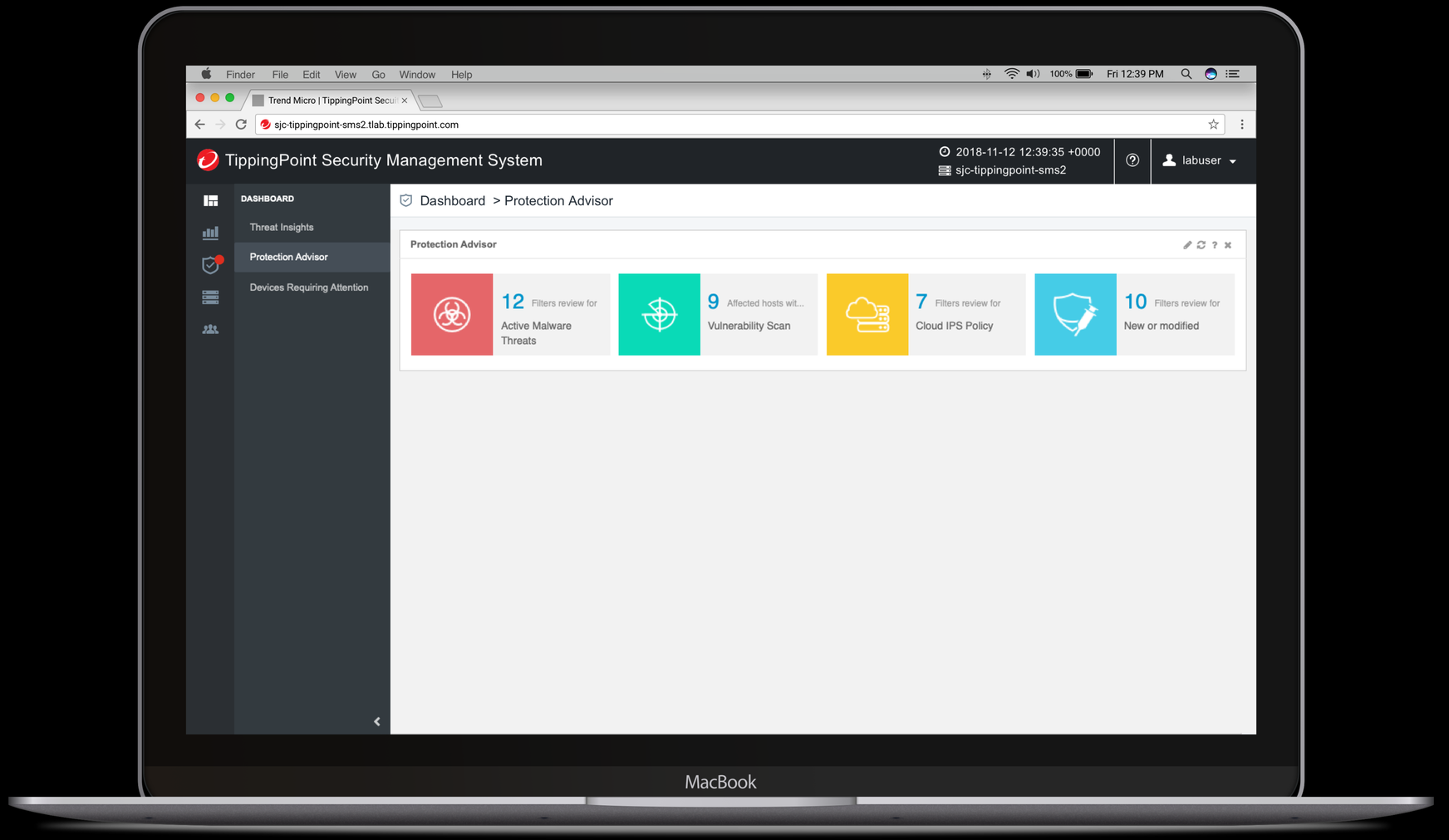
Threats in The Wild

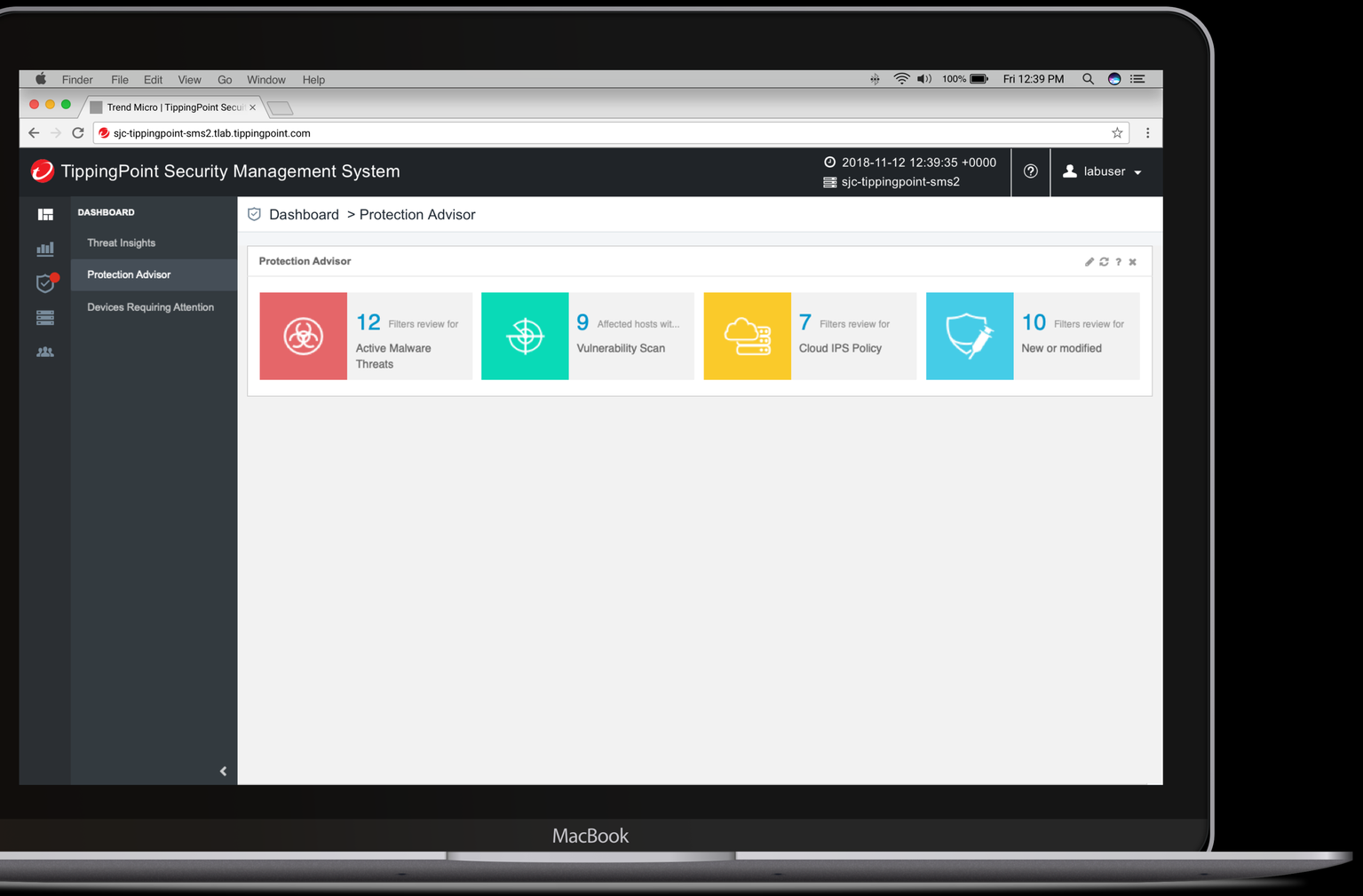
Filters Tuning

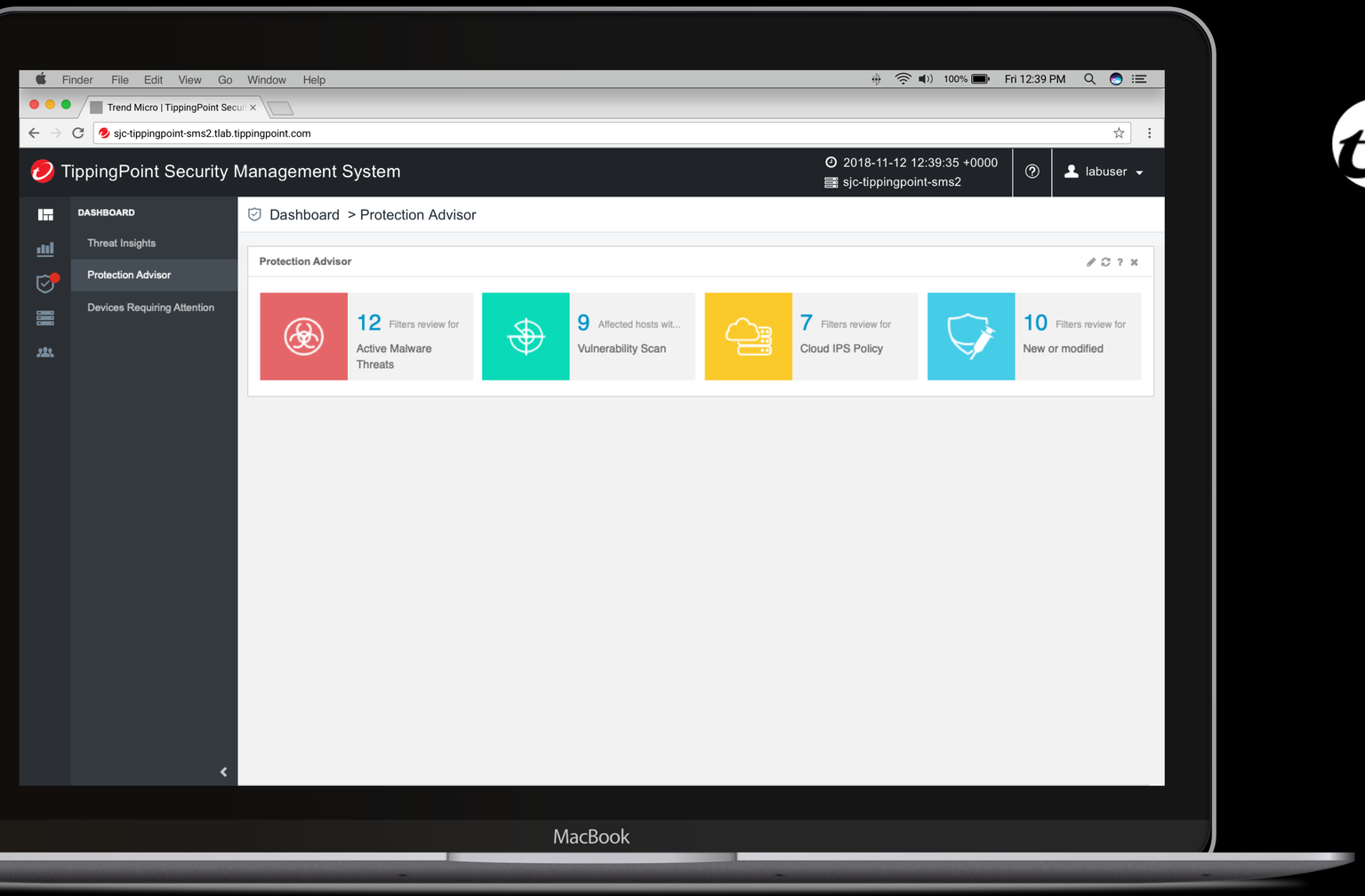
Performance Management

# Threats in The Wild

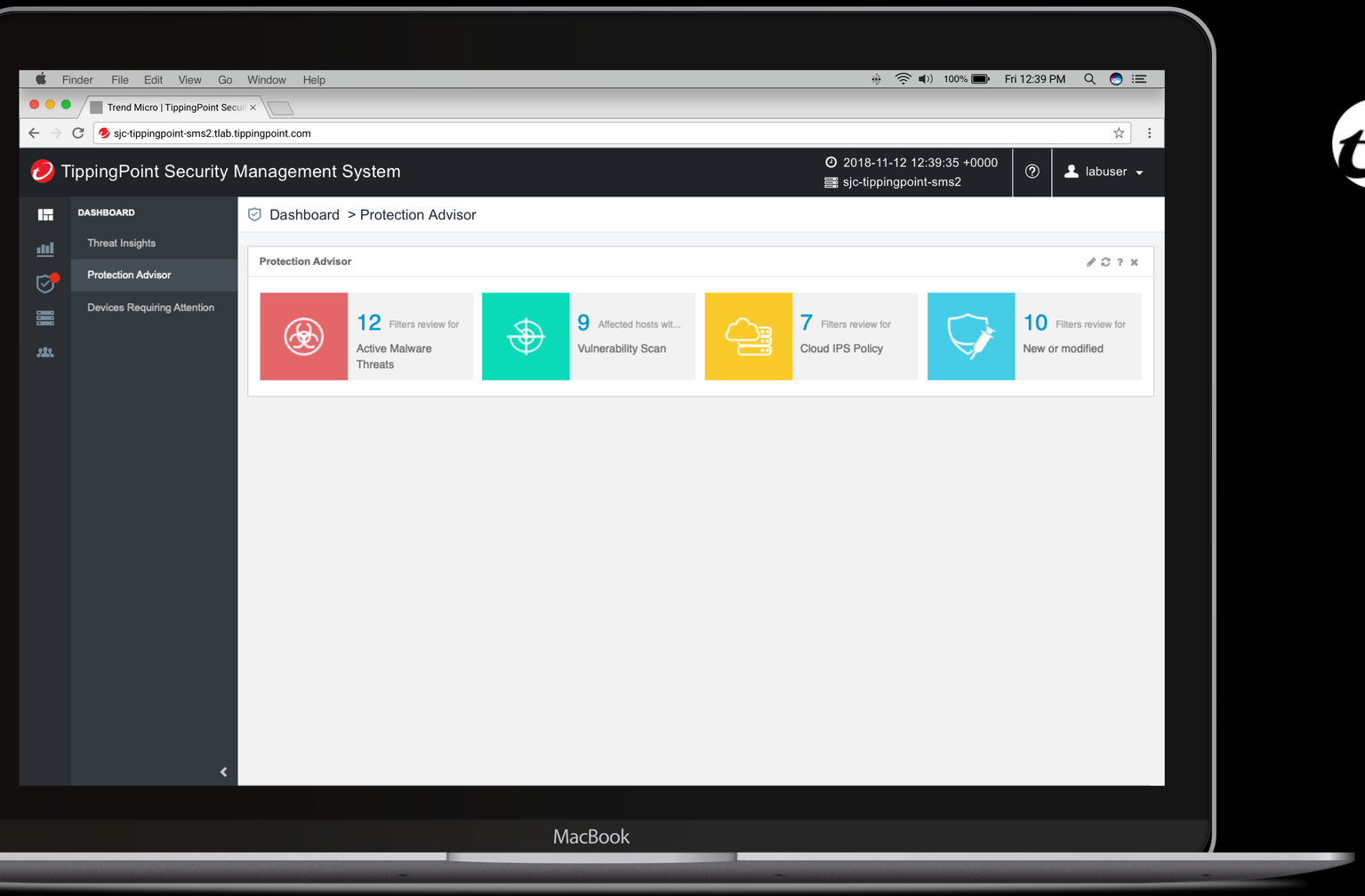

Finder File Edit View Go Window Help
100% Fri 12:39 PM
TippingPoint Security Management System
TippingPoint Security Management System
2017-04-24 08:14:15:05 +0800
2017-04-24 08:14:15:05 +0800
labuser
Threat Insights
Threat DV Dashboard
Headline News
More Actions
Add Widget
Filter
Are we protected - 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


Finder File Edit View Go Window Help
100% Fri 12:39 PM
Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0000
sjc-tippingpoint-sms2
labuser
DASHBOARD
Threat Insights
Protection Advisor
Devices Requiring Attention
Dashboard > Protection Advisor
Protection Advisor
12 Filters review for
Active Malware Threats
9 Affected hosts wit...
Vulnerability Scan
7 Filters review for
Cloud IPS Policy
10 Filters review for
New or modified
MacBook


Finder File Edit View Go Window Help
100% Fri 12:39 PM
Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0000
sjc-tippingpoint-sms2
labuser
DASHBOARD
Threat Insights
Protection Advisor
Devices Requiring Attention
Dashboard > Protection Advisor
Protection Advisor
12 Filters review for
Active Malware Threats
9 Affected hosts wit...
Vulnerability Scan
7 Filters review for
Cloud IPS Policy
10 Filters review for
New or modified
MacBook

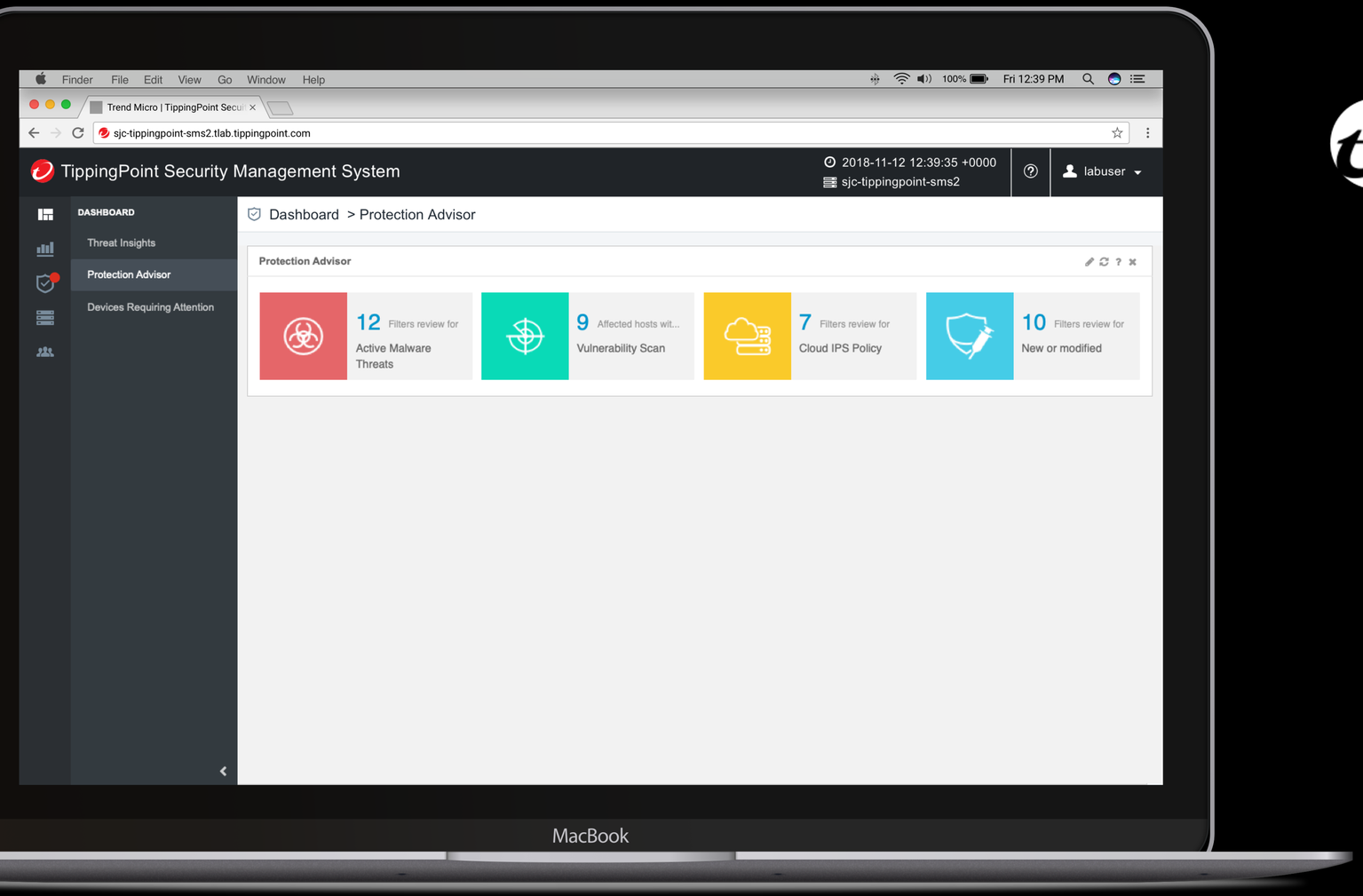

Finder File Edit View Go Window Help
100% Fri 12:39 PM
Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0000
sjc-tippingpoint-sms2
labuser
DASHBOARD
Threat Insights
Protection Advisor
Devices Requiring Attention
Dashboard > Protection Advisor
Protection Advisor
12 Filters review for
Active Malware Threats
9 Affected hosts wit...
Vulnerability Scan
7 Filters review for
Cloud IPS Policy
10 Filters review for
New or modified
MacBook

# Design



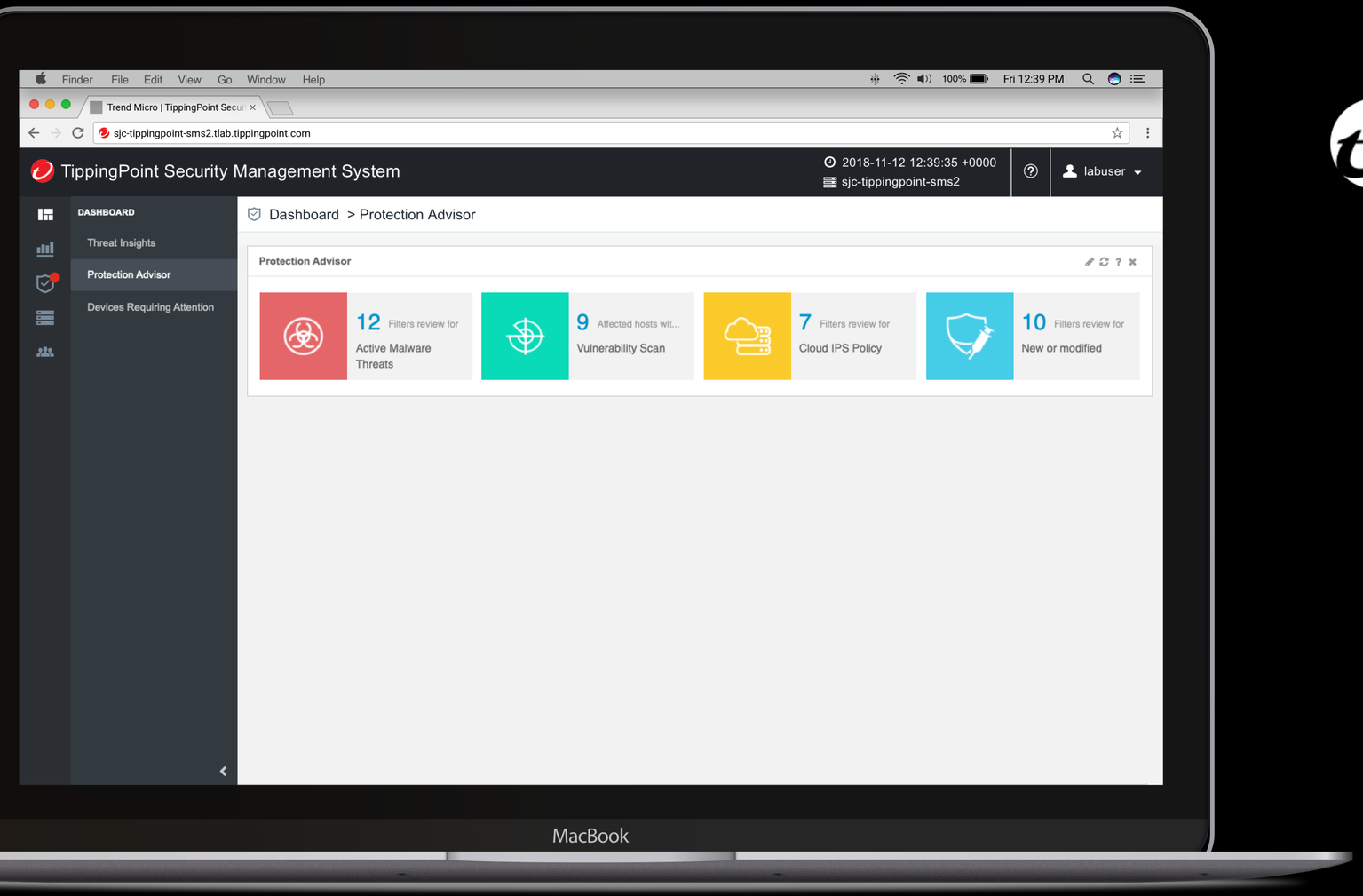

# Design

- Auto-categorize filters




# Design

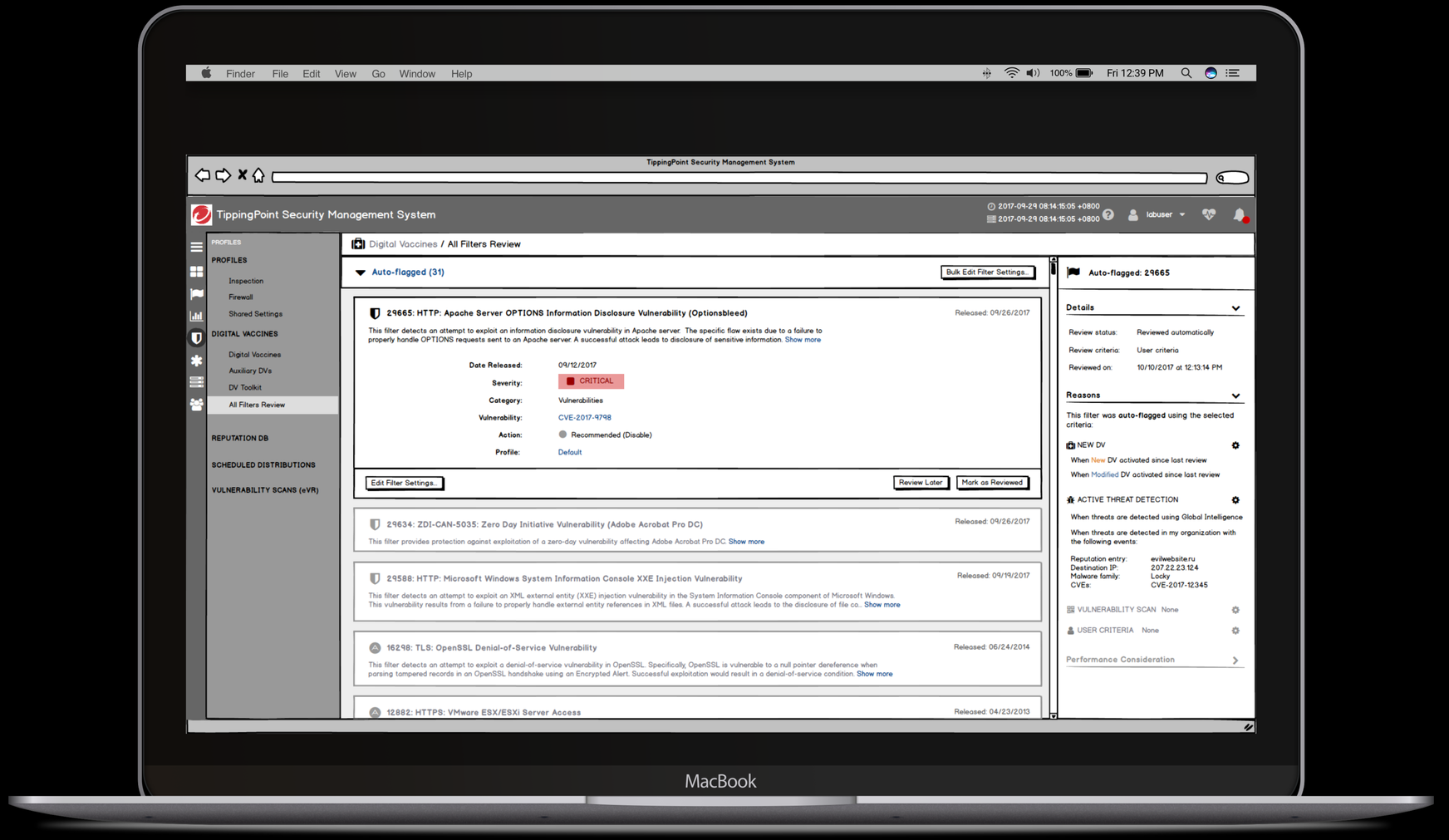
- Auto-categorize filters
- Threat Intelligence: SPN top threats

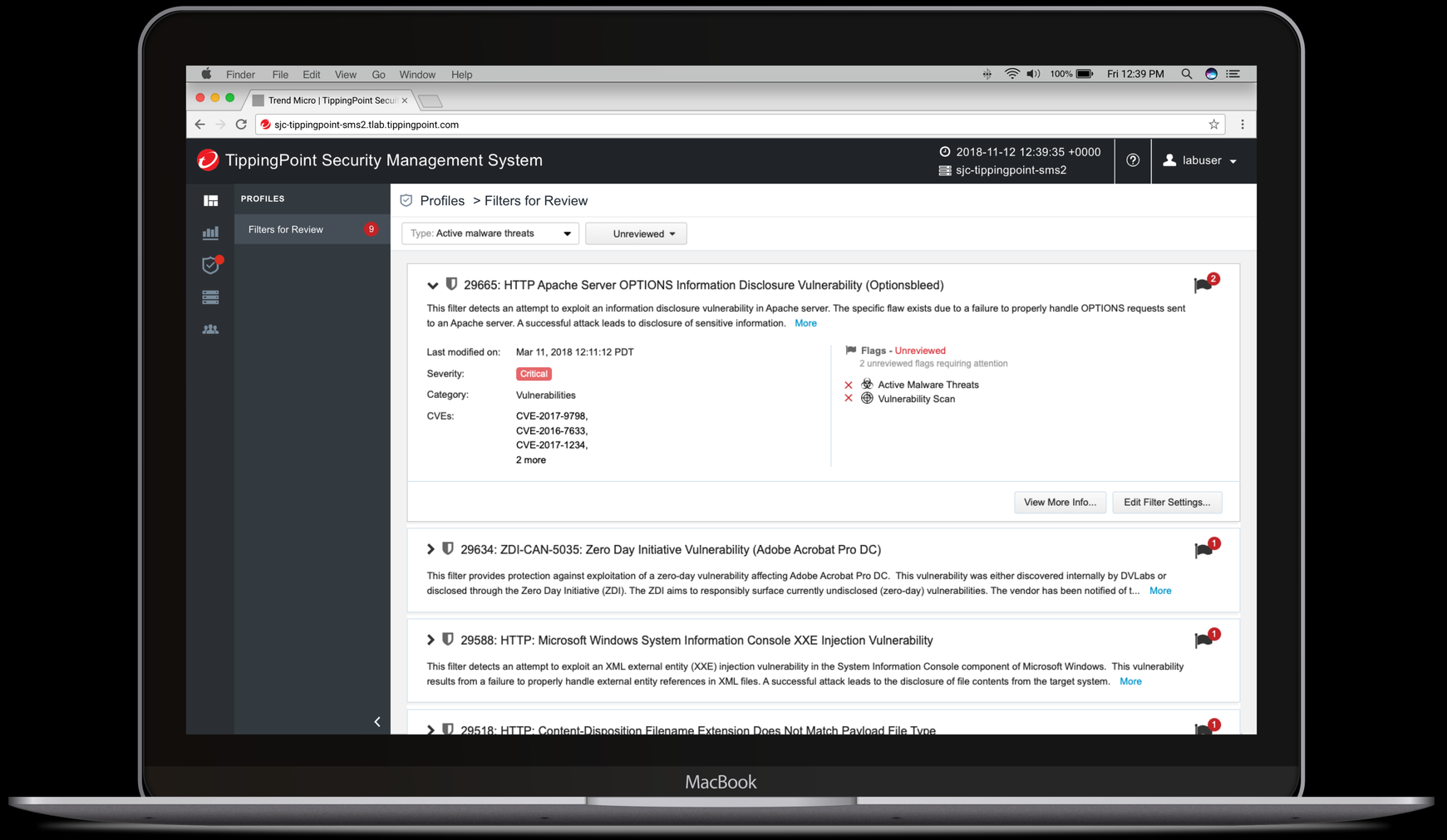


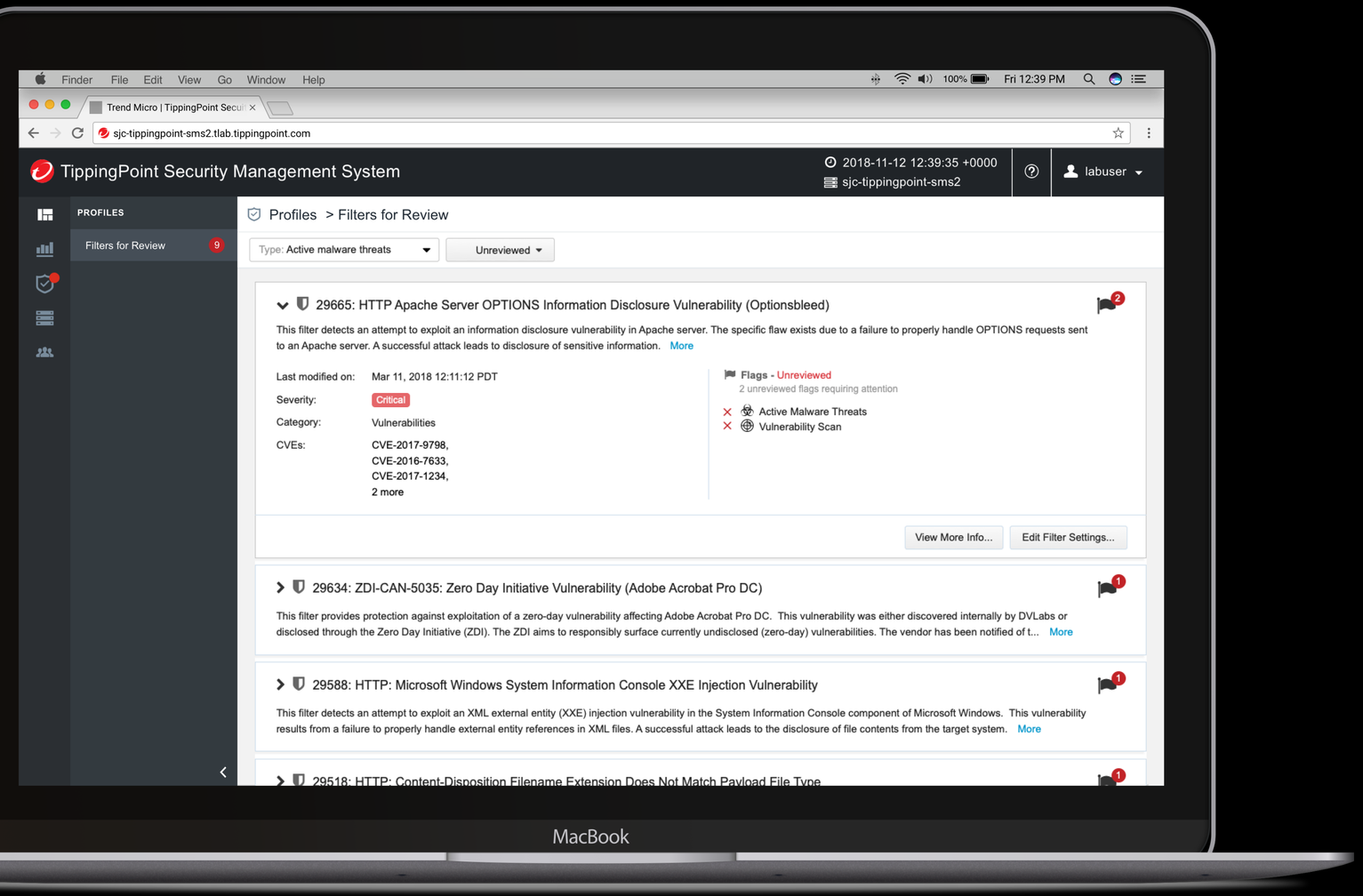

# Design

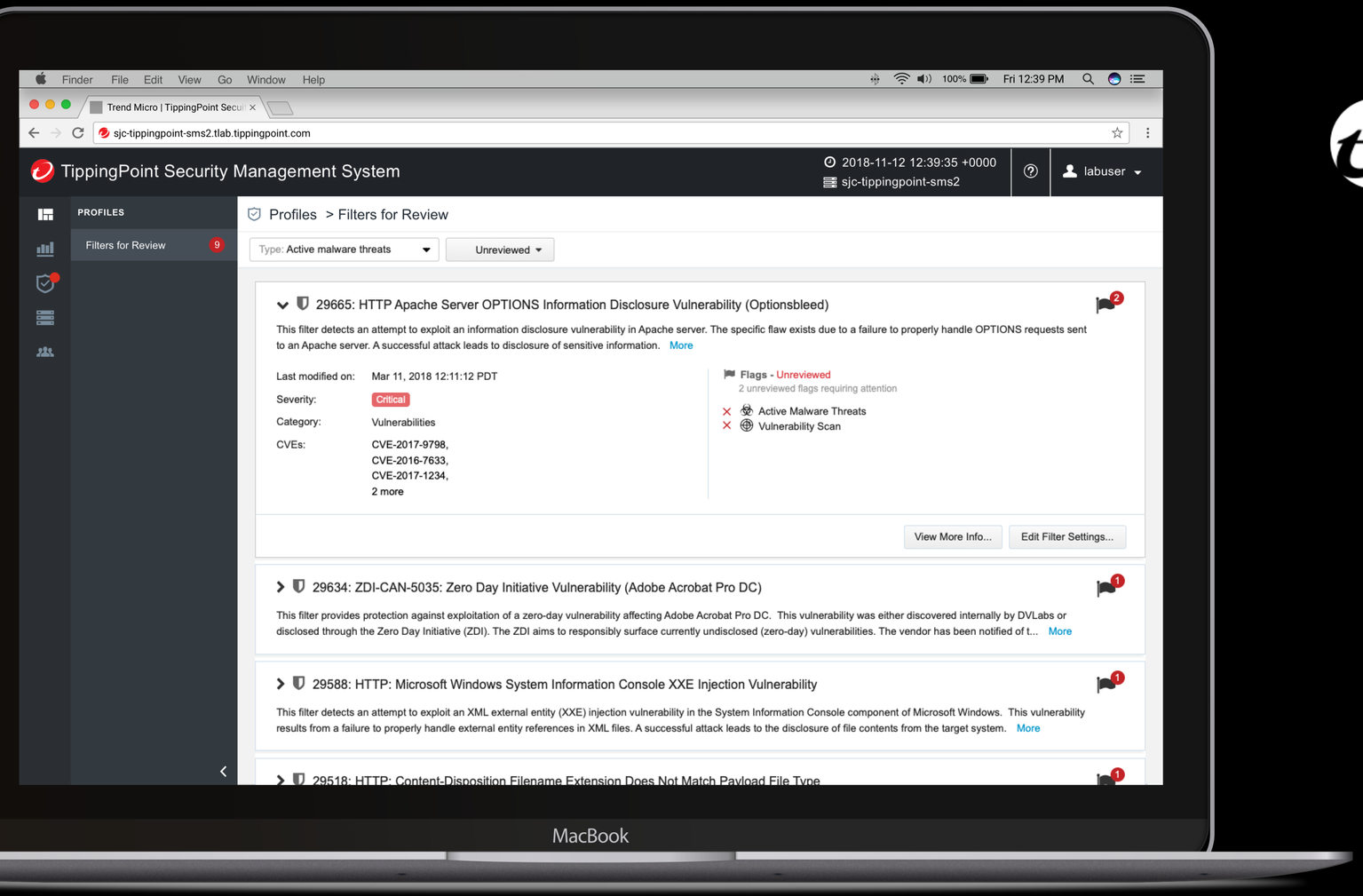
- Auto-categorize filters
- Threat Intelligence: SPN top threats
- Leads to filters tuning workflows

# Filters Tuning

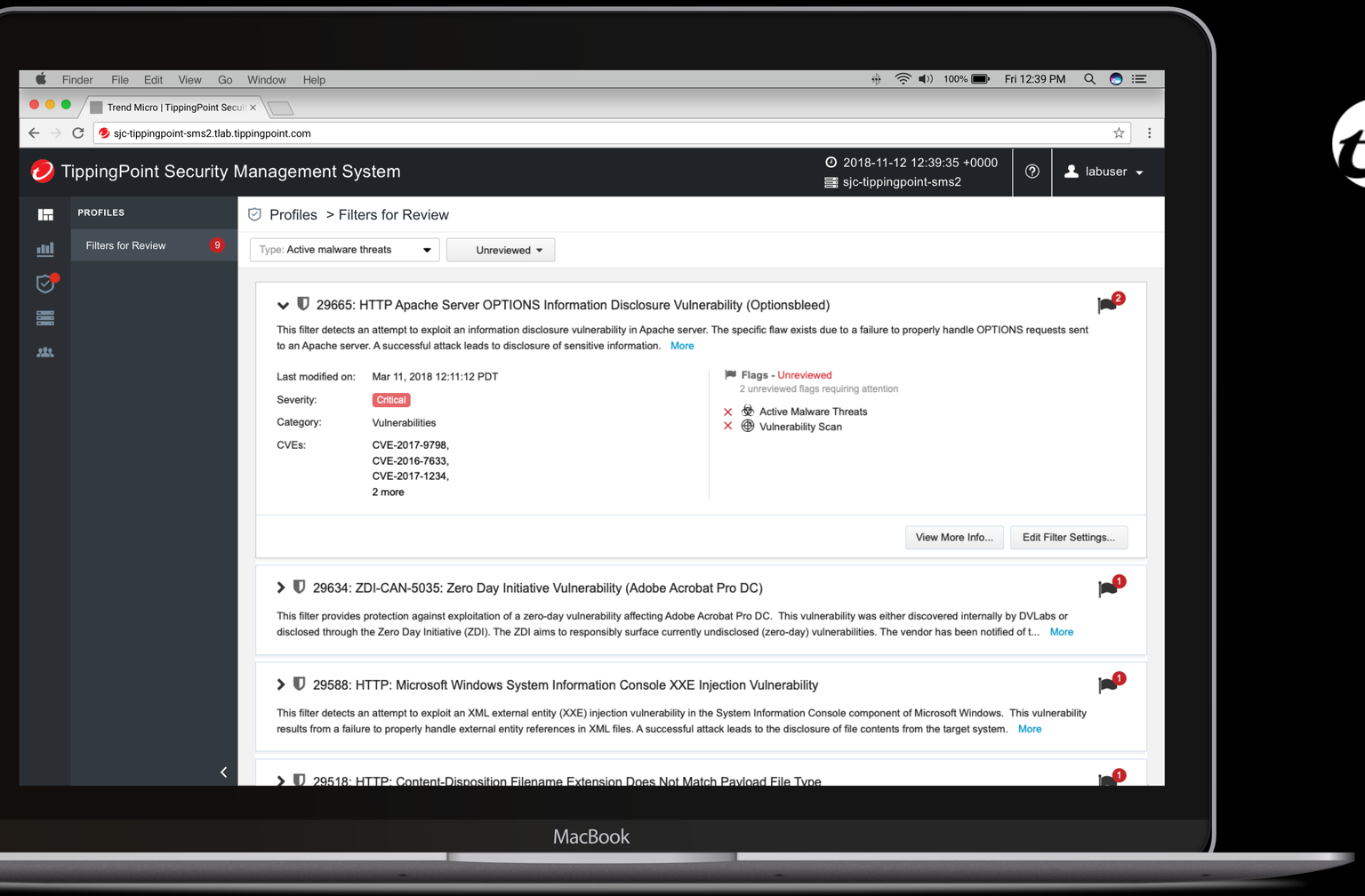

Finder File Edit View Go Window Help
100% Fri 12:39 PM
TippingPoint Security Management System
TippingPoint Security Management System
2017-09-29 08:14:15:05 +0800
2017-09-29 08:14:15:05 +0800
labuser
PROFILES
PROFILES
Inspection
Firewall
Shared Settings
DIGITAL VACCINES
Digital Vaccines
Auxiliary DVs
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


Finder File Edit View Go Window Help
100% Fri 12:39 PM
Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0000
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review 9
Profiles > Filters for Review
Type: Active malware threats
Unreviewed
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 to disclosure of sensitive information. More
Last modified on: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerabilities
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, 2 more
Flags - Unreviewed
2 unreviewed flags requiring attention
Active Malware Threats
Vulnerability Scan
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). The ZDI aims to responsibly surface currently undisclosed (zero-day) vulnerabilities. The vendor has been notified of t... 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 disclosure of file contents from the target system. More
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
MacBook


Finder File Edit View Go Window Help
100% Fri 12:39 PM
Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0000
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review 9
Profiles > Filters for Review
Type: Active malware threats
Unreviewed
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 to disclosure of sensitive information. More
Last modified on: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerabilities
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, 2 more
Flags - Unreviewed
2 unreviewed flags requiring attention
Active Malware Threats
Vulnerability Scan
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). The ZDI aims to responsibly surface currently undisclosed (zero-day) vulnerabilities. The vendor has been notified of t... 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 disclosure of file contents from the target system. More
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
MacBook

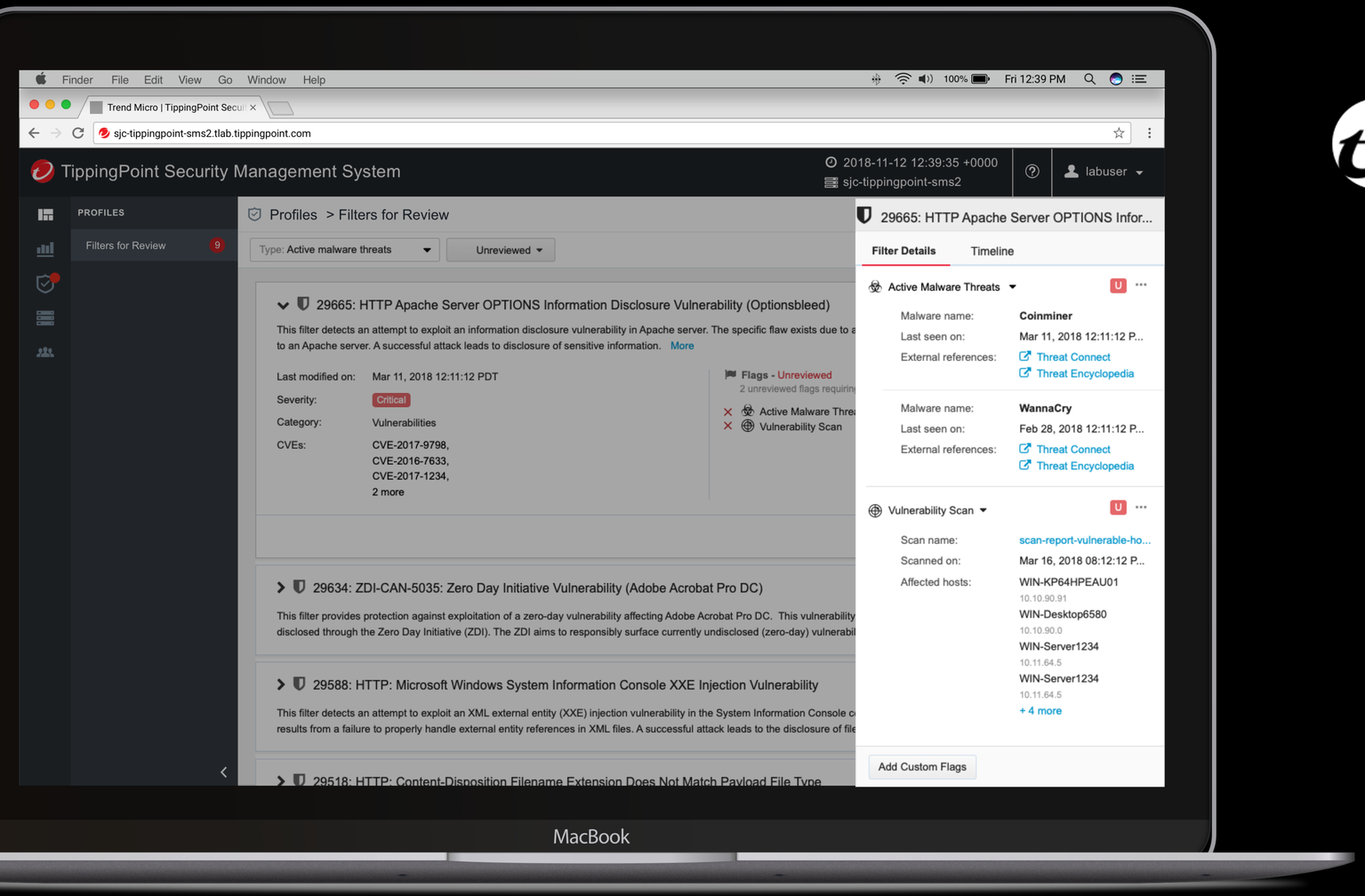

Finder File Edit View Go Window Help
100% Fri 12:39 PM
Trend Micro | TippingPoint Secu
sjc-tippingpoint-sms2.tlab.tippingpoint.com
TippingPoint Security Management System
2018-11-12 12:39:35 +0000
sjc-tippingpoint-sms2
labuser
PROFILES
Filters for Review 9
Profiles > Filters for Review
Type: Active malware threats
Unreviewed
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 to disclosure of sensitive information. More
Last modified on: Mar 11, 2018 12:11:12 PDT
Severity: Critical
Category: Vulnerabilities
CVEs: CVE-2017-9798, CVE-2016-7633, CVE-2017-1234, 2 more
Flags - Unreviewed
2 unreviewed flags requiring attention
Active Malware Threats
Vulnerability Scan
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). The ZDI aims to responsibly surface currently undisclosed (zero-day) vulnerabilities. The vendor has been notified of t... 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 disclosure of file contents from the target system. More
29518: HTTP: Content-Disposition Filename Extension Does Not Match Payload File Type
MacBook

# Design



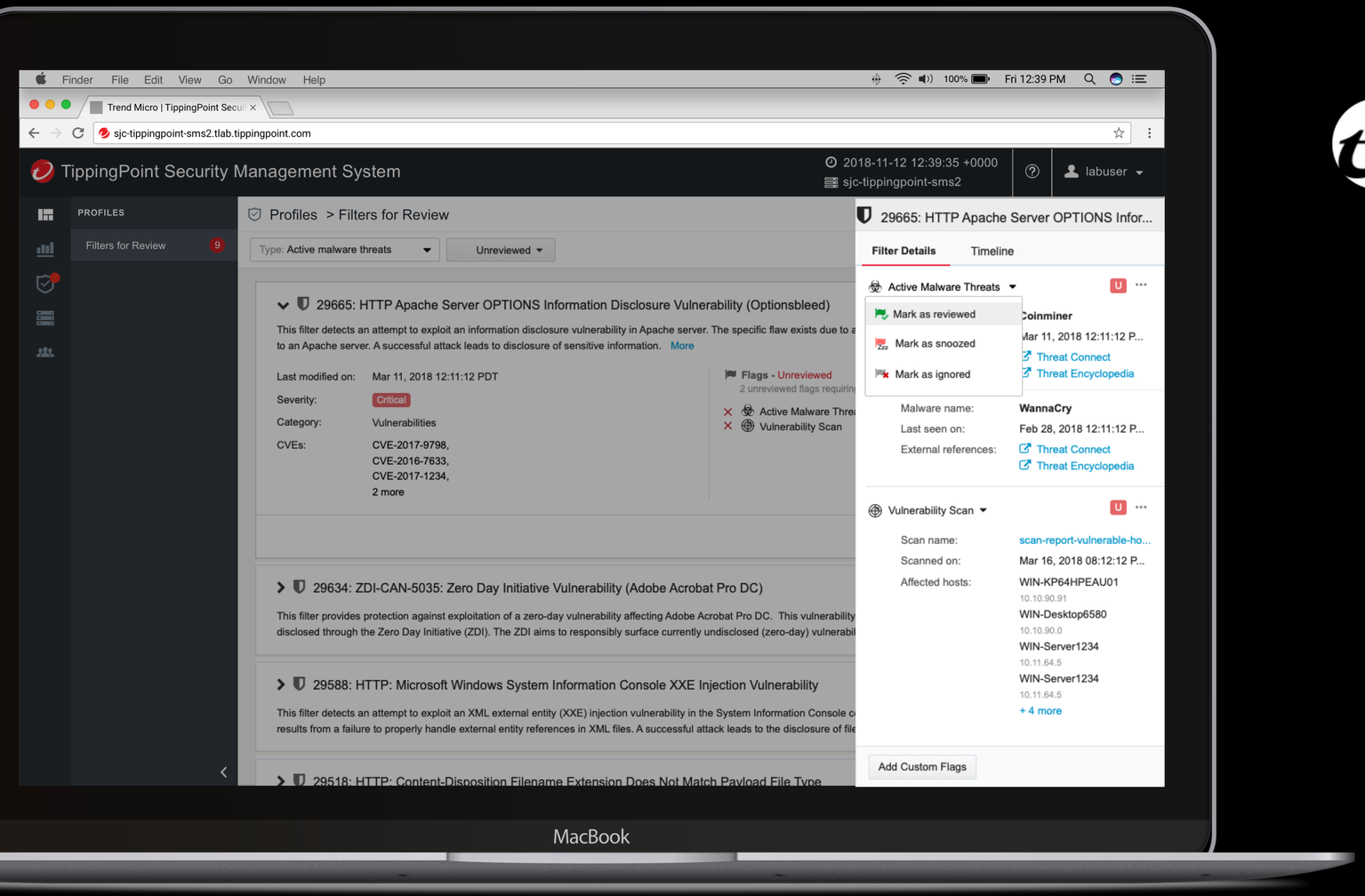

# Design

- Contextual filter information



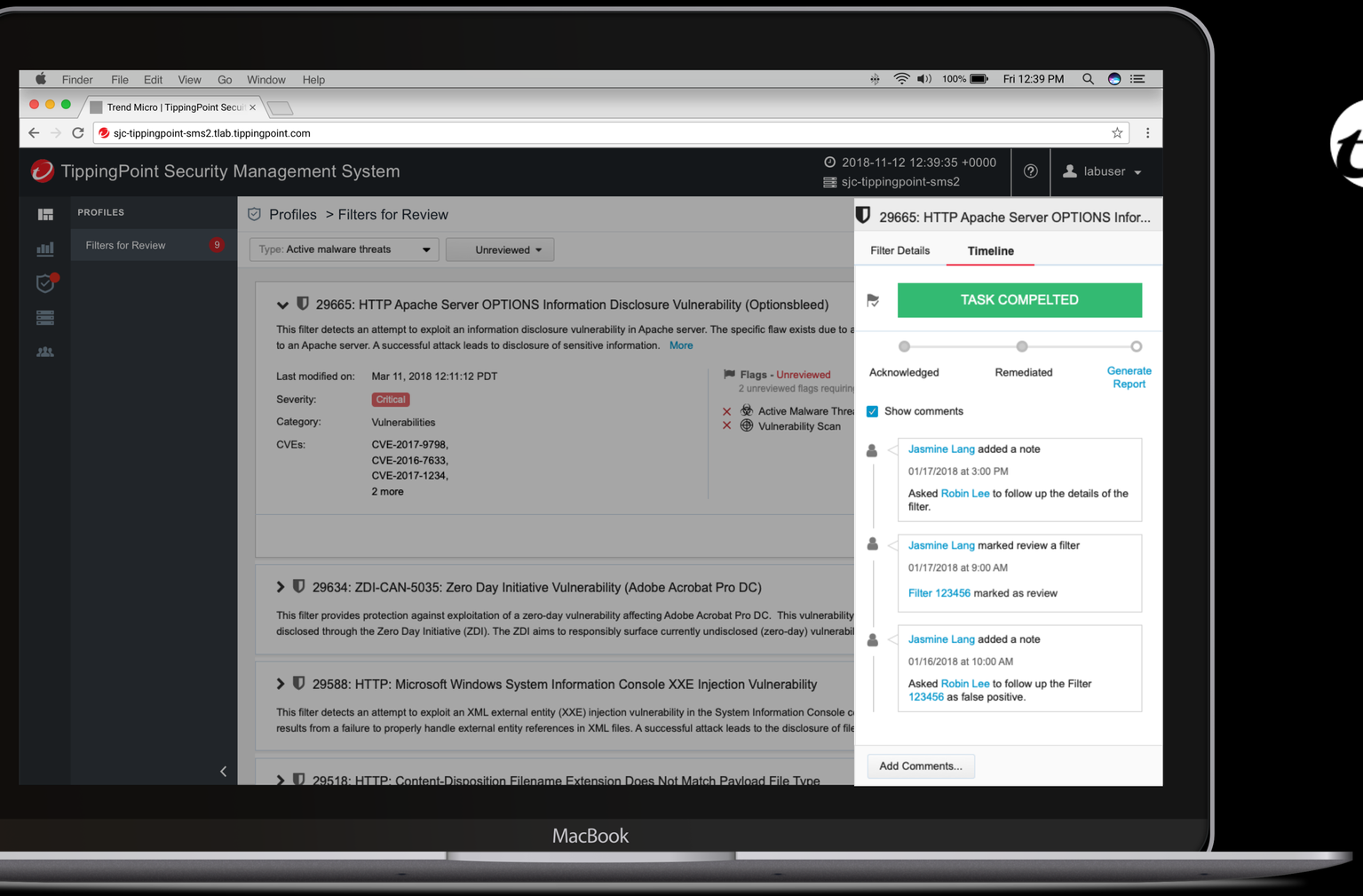

# Design

- Contextual filter information
- Filters tuning workflow




# Design

- Contextual filter information
- Filters tuning workflow




# Design

- Contextual filter information
- Filters tuning workflow
- Timeline of changes

# Prototype

https://8az3pp.axshare.com (password: SMS2018)


Thank you