



Release Notes

Version

5.2

June 2020

1 CONTENTS

- 2 Introduction 2
- 3 Version 5.2 Update Summary 2
 - 3.1 User Interface Enhancements 2
 - 3.1.1 Form Factor Expansion 2
 - 3.1.2 DNS and DHCP Landing Pages..... 3
 - 3.1.3 New Managed Services Portal Pages..... 3
 - 3.1.4 Scan Surveillance..... 4
 - 3.1.5 Upgrade of Controls 5
 - 3.1.6 New Menu Layout 5
 - 3.1.7 Version 4.22 Portal Page Decommissions- Removal of Alert and Threat Centers in 4.22.... 8
 - 3.2 Reporting Enhancements 8
 - 3.2.1 CSV Reporting Enhancements..... 8
 - 3.2.2 Log & Alert Summary Reporting..... 8
 - 3.3 Third Party Integrations..... 9
 - 3.3.1 Incapsula Web Application Firewall Support 9
 - 3.3.2 Cisco DUO 2 Factor Integration Support..... 9
 - 3.4 Platform Enhancements 9
 - 3.4.1 User and Asset Behavior Enhancements 9
 - 3.4.2 DHCP Advanced Correlation – Host name mapping of DHCP logs..... 9
 - 3.4.3 Device Inactivity Notification Enhancement (Hourly) 10
- 4 Questions & Support..... 10

2 INTRODUCTION

Version 5.2 is a major upgrade of the ThreatWatch® cyber-security platform that powers SOD’s Advanced Threat & Log Analysis Service. New improvements to the service provide Clients with rich user interface enhancements, added reporting functionality, additional integrations, and platform/threat detection enhancements.

This document provides further information on the new version, capabilities and limitation notes on the new version 5.2 solution of Advanced Threat & Log Analysis Service (ATLAS) and ThreatWatch® Log Analysis Service.

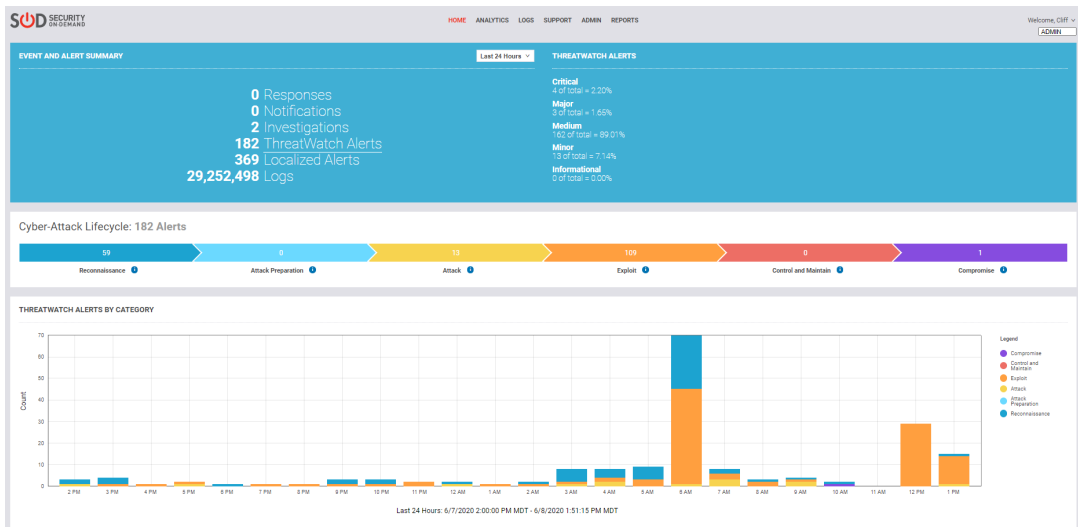
This upgrade will be provided automatically for all clients, effective from the date notified. Version 5.2 is fully backwards compatible with previous versions and all current popular browsers. Along with the upgrade, the version 5.2 portal has replaced many of the pages and functionality from the v.4.22 portal and those pages will be decommissioned on the date of the release. The previous version 4.2.2 is still available from the version 5.2 portal menu for any functions or pages not yet ported over.

3 VERSION 5.2 UPDATE SUMMARY

3.1 USER INTERFACE ENHANCEMENTS

3.1.1 Form Factor Expansion

Improved browser compatibility on the portal with an expanded use of display real estate to fit more data on the display screen without the need for scrolling. The new interface fits more columns and rows on the pages when displaying reports and grids to allow you to filter and sort with increased data visibility.



3.1.2 DNS and DHCP Landing Pages

New portal pages display the alert data generated from the DNS Advanced Use Case and the DHCP Advanced Use Case. These pages offer the ability to drill into information that is pre-grouped and summarized. Additional filtering, detailed drill downs, and data export to CSV format is also included.

The dedicated page for DNS is available under the Analytics/Alerts Menu:

The dedicated page for DHCP is available under the Logs Menu:

3.1.3 New Managed Services Portal Pages

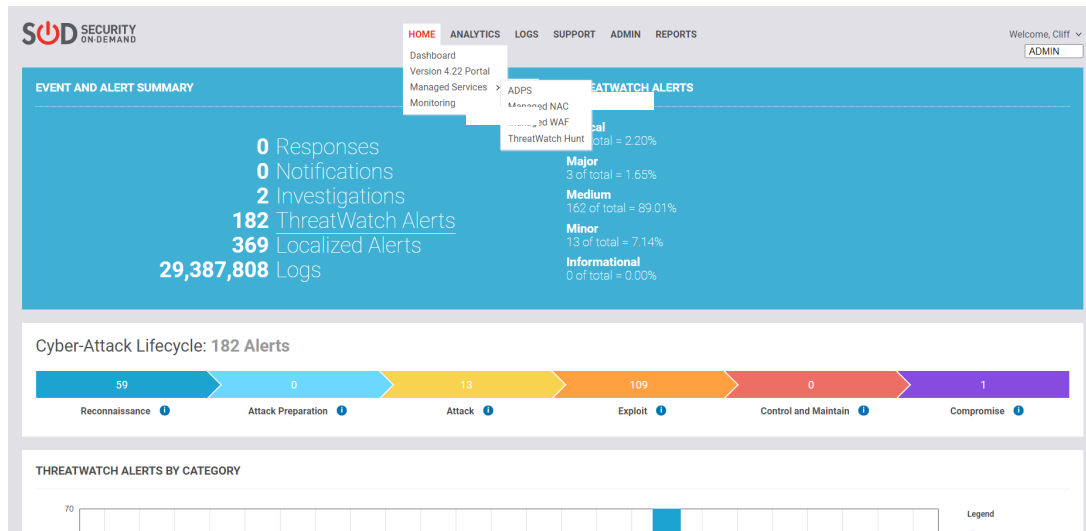
New portal pages display alert and log data for specified managed security services, if included as a part of the services. Each service page offers the ability to drill into information that is pre-grouped and summarized to provide an overview of log and alert activity from the service.

Additional filtering, detailed drill downs, and data export to CSV format are also included. Corresponding pages in 4.22 are now removed since the new managed service portal pages have been created.

Dedicated portal pages have been created for:

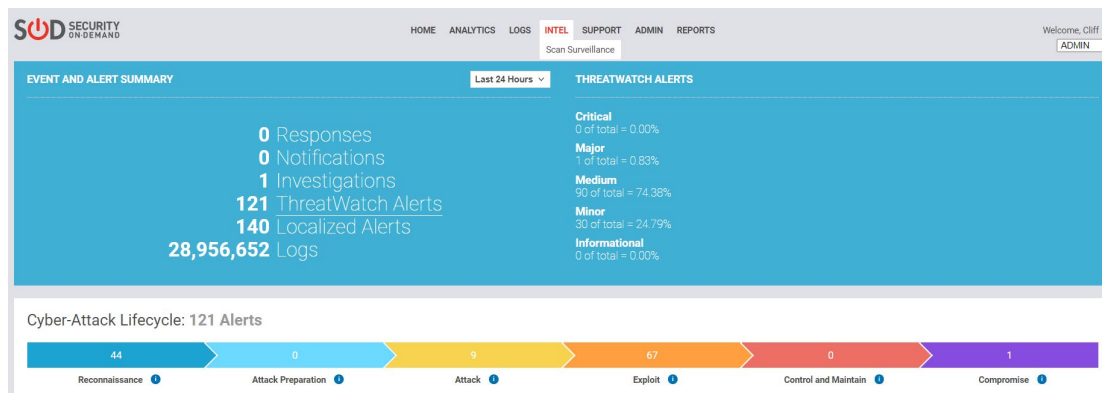
- Managed Web Application Firewalls
- ThreatWatch Hunt
- Managed NAC

These pages are available under the Home/Managed Services Menu



3.1.4 Scan Surveillance

Scan Surveillance is being re-enabled in the V5 platform across our customer base over the course of the next quarter. Once available to your organization it will be accessed from a new Intel Menu:



This page provides a view of progressive external and internal scan activity against your organization with visual chart views as well as the ability to generate a details table.

SOD SECURITY ON-DEMAND
HOME ANALYTICS LOGS INTEL SUPPORT ADMIN REPORTS
Welcome, Haley ADMIN

Scan Surveillance

Total Scans: 1,069 Scans Basic Filter Last 7 Days

Scan Category +
Source IP +
Source Country +
IP/Port Scan +
Scan Type +

Filters Add filters using the controls above to refine the data returned below.

[RESET FILTERS](#)

Scan Summary: Last 7 Days

Legend

- External Active Scan
- External Discovery Scan
- Internal Active Scan
- Internal Discovery Scan

APPLY FILTERS

Include Active Scans

Last 7 Days: 6/18/2020 12:00:00 AM PDT - 6/24/2020 10:29:16 AM PDT

Scan Events: 1,069 Scans

VIEW WHITELIST
VIEW SCAN DETAILS
SELECT COLUMNS
EXPORT CSV

Last 7 Days: 6/18/2020 12:00:00 AM PDT - 6/24/2020 10:29:16 AM PDT

Drag here to set row groups.

VIEW	ADD TO WHITELIST	SCAN CATEGORY	SOURCE IP	SOURCE COUNTRY	FIRST SEEN (PDT)	LAST SEEN (PDT)	SCAN COUNT	HISTORICAL COUNT	ALLOWED	IP/PORT SCAN	ESCALATION DATE	SCAN TYPE
+	+	External Active Scan	92.53.65.188		6/17/2020 10:22:56 PM	6/18/2020 12:05:22 AM	13	44	15.38% (2 / 13)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	87.251.74.48		6/17/2020 11:39:23 PM	6/18/2020 12:05:47 AM	14	54	14.29% (2 / 14)	N/A	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	103.145.12.145		6/18/2020 12:13:43 AM	6/18/2020 12:16:44 AM	28	14	28.57% (8 / 28)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	94.102.51.58		6/17/2020 9:34:35 PM	6/18/2020 10:32:43 AM	37	47	8.11% (3 / 37)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	141.98.60.204		6/17/2020 10:12:39 PM	6/18/2020 12:25:36 AM	23	202	8.70% (2 / 23)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	185.175.93.14		6/17/2020 9:33:51 PM	6/18/2020 12:28:17 AM	48	179	4.17% (2 / 48)	N/A	6/18/2020 2:00:14 AM	External
+	+	External Discovery Scan	94.102.56.231		6/18/2020 12:23:28 AM	6/18/2020 12:48:21 AM	10	22	0.00% (0 / 10)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Discovery Scan	51.161.12.231		6/17/2020 10:05:07 PM	6/18/2020 12:49:49 AM	14	149	0.00% (0 / 14)	IP	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	185.136.225.45		6/17/2020 4:54:02 PM	6/18/2020 12:53:20 AM	60	144	3.33% (2 / 60)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Active Scan	45.34.44.234		6/17/2020 9:04:03 PM	6/18/2020 12:54:40 AM	29	16	20.69% (6 / 29)	IP & Port	6/18/2020 2:00:14 AM	External
+	+	External Discovery Scan	213.248.168.236		6/17/2020 11:57:16 PM	6/18/2020 1:04:40 AM	20	1	0.00% (0 / 20)	N/A	6/18/2020 3:00:17 AM	External
+	+	External Active Scan	146.88.240.4		6/17/2020 5:04:52 PM	6/18/2020 1:10:28 AM	116	218	29.31% (94 / 116)	IP & Port	6/18/2020 3:00:12 AM	External
+	+	External Active Scan	185.39.10.45		6/17/2020 10:25:45 PM	6/18/2020 1:24:19 AM	17	58	5.88% (1 / 17)	Port	6/18/2020 3:00:12 AM	External

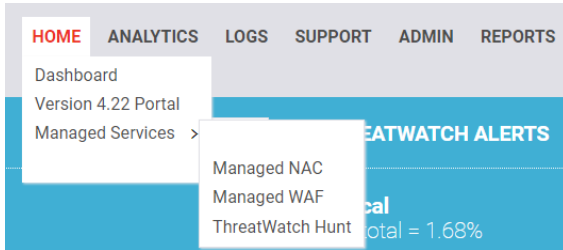
3.1.5 Upgrade of Controls

The standardized and upgraded look and feel across the different input screens create a consistent look across the platform.

3.1.6 New Menu Layout

In addition to the updated look and feel to our version 5.2 release, the platform includes an updated menu layout with upgraded functionality.

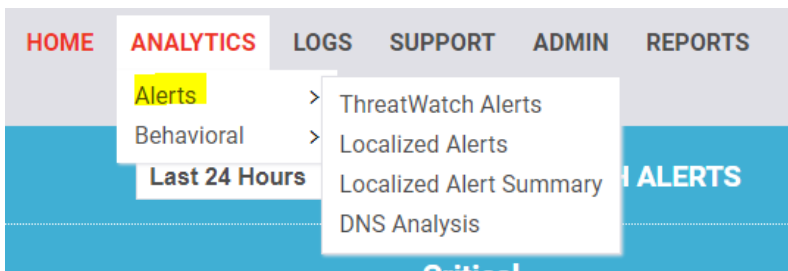
Home Menu Page:



Navigation to:

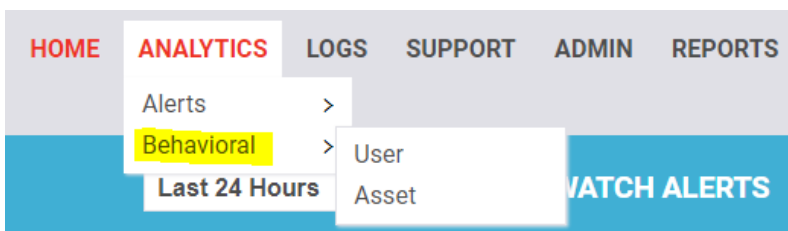
- Dashboard (the first landing page a user sees when logging into the portal)
- Navigation to V4.22 (will open a 2nd browser window next to the existing window)
- Managed Service Pages (for Clients that are contracted for any of these Managed Services)

Analytics Menu Page:



Alerts provide a nested set of pages for

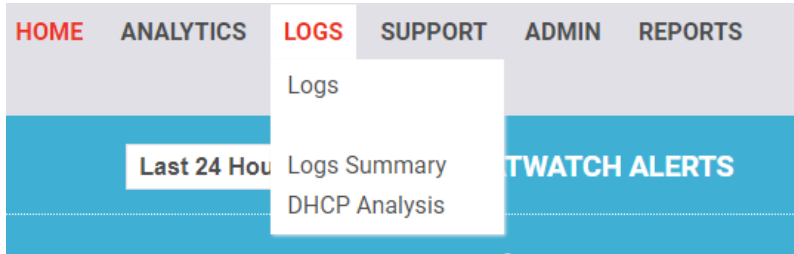
- ThreatWatch Alerts
- Localized Alerts
- Localized Alert Summary
- DNS Analysis (For Clients that have purchased the DNS Advanced Correlation Source)



Behavioral provides a nested set of pages (for clients that have added User and or Asset Behavioral Analysis to their service)

- User Behavior
- Asset Behavior

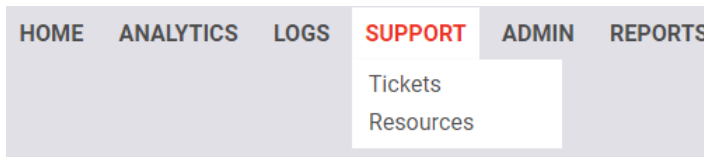
Logs Menu Page:



This page provides access to:

- Logs
- Log Summary
- DHCP Analysis (For Clients that have purchased the DHCP Advanced Correlation Source)

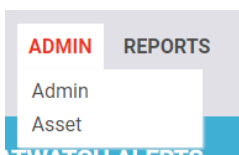
Support Menu Page:



Support provides access to:

- 4.2 Tickets page (will open a 2nd browser window next to the existing window)
- Resources page providing access to:
 - Training videos
 - User guides
 - Release notes

Admin Menu Page:



Admin provides access to:

- 4.2 Admin page
- 4.2 Managed Assets page

Reports Menu Page:



Reports provides access to:

- Reports- V5
- Templates- V5 Report Templates that can be added for scheduling/running
- Reports 4.22- V4.22 Reporting

3.1.7 Version 4.22 Portal Page Decommissions- Removal of Alert and Threat Centers in 4.22

As we've been transitioning from our version 4.2 portal to our new version 5.2 updated portal, we're deprecating old functionality. This means that Threat Center and Alert Center (v.4.2) will no longer be supported or available in the previous version.

3.2 REPORTING ENHANCEMENTS

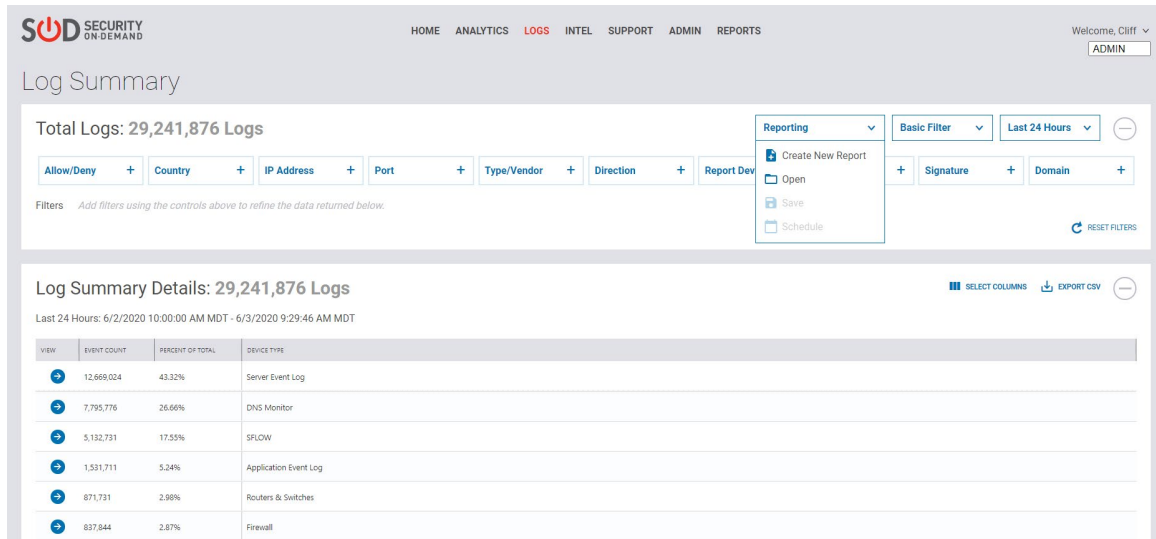
3.2.1 CSV Reporting Enhancements

There are numerous enhancements to CSV-based reporting, which include improved document handling, stability fixes, and formatting improvements.

3.2.2 Log & Alert Summary Reporting

Log Summary and Localized Alert Summary portal pages now feature saved views and scheduled reports. Summary reports can be saved in CSV format as well as displayed on screen. PDF support for these reports will be implemented in the next maintenance release (v.5.2.1), coming soon within the next few months.

Once a user configures filters on the pages and determines that is a view they would like to recreate regularly, they can simply select "Save" from the reporting drop-down menu. When navigating back to the page the user can select "Open" from the reporting drop-down menu to view saved reports that can load the page with previously configured filters and then schedule a report.



VIEW	EVENT COUNT	PERCENT OF TOTAL	SERVICE TYPE
	12,669,024	43.32%	Server Event Log
	7,795,776	26.66%	DNS Monitor
	5,132,731	17.55%	SFLOW
	1,531,711	5.24%	Application Event Log
	871,731	2.98%	Routers & Switches
	897,844	2.87%	Firewall

3.3 THIRD PARTY INTEGRATIONS

3.3.1 Incapsula Web Application Firewall Support

Imperva's WAF service (Incapsula) is now a fully supported integration, which is an optional add-on service.

3.3.2 Cisco DUO 2 Factor Integration Support

Support for Clients that currently leverage DUO multi-factor authentication services. If you own or use the DUO solution, SOD can allow you to utilize this service to provide multi-factor authentication to the Portal at no additional cost. The DUO licenses are not part of the solution.

3.4 PLATFORM ENHANCEMENTS

3.4.1 User and Asset Behavior Enhancements

Clients that have added User/Asset Behavior and leverage the DHCP Advanced correlation source will see additional Events of Interest ("EOI"), which have been added to improve the timeline visualizations and help add more context to understanding threat sequences within the UBA and ABA Client Portal pages.

- DHCP Assign- event was captured notating a new DHCP assignment
- DHCP Renew- event was captured notating a new DHCP renewal

3.4.2 DHCP Advanced Correlation – Host name mapping of DHCP logs

Hostnames are now fully displayed in relation to the source and destination fields. This data is now fully parsed and available in the client portal. Another improvement is that hostname information (assets) are correlated within the ABCD Risk Scoring System.

SORAD notifications from the SOC will now contain hostname information (if included in the device log), which will reduce the time needed for the client to research the IP address and associate it with the corresponding host name.

3.4.3 Device Inactivity Notification Enhancement (Hourly)

Our complimentary Device Inactivity notifications are provided as part of the ATLAS service. The automated notifications are designed to alert the client and our SOC in case a device stops sending logs.

Previously, the default was to notify 24 to 48 hours after the logs stopped flowing, which then auto-generated a ticket and notifications. This is the standard configuration and should work acceptably for most organizations. In certain cases, there are critical devices where the notification interval is too long and is desired to notify in a shorter time frame after logs have not been received. The enhanced service capability now allows the client to change the default setting to a shorter time period determined by them (as measured in hours). Access to these settings is available through the Asset Center in the Client Portal.

4 QUESTIONS & SUPPORT

Please contact us at info@securityondemand.com if you would like to setup a demonstration or have further questions about how these solutions help to enhance your service.