paloalto TECHDOCS

Security Lifecycle Review (SLR)

Getting Started Guide

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2018-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 4, 2023

Table of Contents

Getting Started With Security Lifecycle Review (SLR)..... 5

About Security Lifecycle Review (SLR)..... 6

Security Lifecycle Review (SLR)—What's in the Report?..... 7

Activate the Security Lifecycle Review (SLR) App..... 12

Create a New Security Lifecycle Review (SLR) Report..... 14

Customize Security Lifecycle Review (SLR) Reports..... 18

Security Lifecycle Review (SLR) Support Requirements..... 20

Security Lifecycle Review (SLR) Updates..... 21

What's New..... 21

Known Issues..... 24

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Getting Started With Security Lifecycle Review (SLR)

Security Lifecycle Review (SLR) is a cloud-based application that summarizes the risks your organization faces. SLR is free with a Palo Alto Networks Strata Logging Service subscription, and you can find the SLR app on the Palo Alto Networks hub.

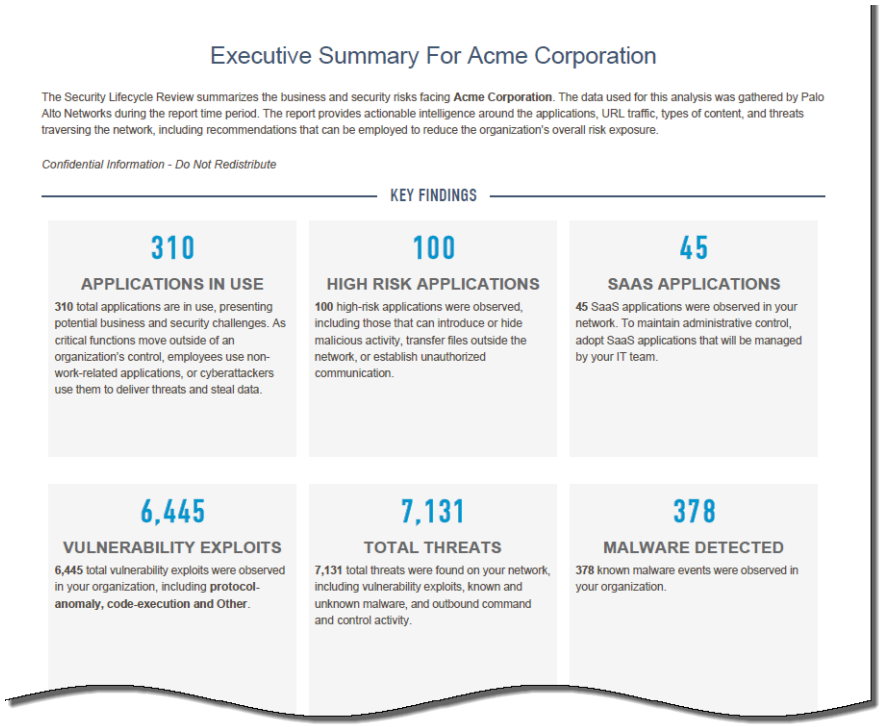
Here's what you need to get started with SLR:

- About Security Lifecycle Review (SLR)
- Security Lifecycle Review (SLR)—What's in the Report?
- Activate the Security Lifecycle Review (SLR) App
- Create a New Security Lifecycle Review (SLR) Report
- Customize Security Lifecycle Review (SLR) Reports
- Security Lifecycle Review (SLR) Support Requirements
- Security Lifecycle Review (SLR) Updates

About Security Lifecycle Review (SLR)

Security Lifecycle Review (SLR) is a cloud-based application that summarizes the security risks that your organization faces. The SLR app is available in the Palo Alto Networks hub, and uses the logs that firewalls forward to Strata Logging Service to gain visibility into your network (SLR is free with a Strata Logging Service subscription).

SLR reports—which you can generate at any time and save as a PDF—can be used as part of an initial product evaluation, or during regular security check-ups to assess threat exposure. These reports provide a high-level view of the applications in use on your network (including SaaS applications), the websites that your users are accessing, and the types of files they're sharing. SLR reports also outline the vulnerabilities, malware, and command-and-control (C2) infections found on your network and helps you to contextualize these findings against industry peers.



Executive Summary For Acme Corporation

The Security Lifecycle Review summarizes the business and security risks facing **Acme Corporation**. The data used for this analysis was gathered by Palo Alto Networks during the report time period. The report provides actionable intelligence around the applications, URL traffic, types of content, and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk exposure.

Confidential Information - Do Not Redistribute

KEY FINDINGS

310
APPLICATIONS IN USE
310 total applications are in use, presenting potential business and security challenges. As critical functions move outside of an organization's control, employees use non-work-related applications, or cyberattackers use them to deliver threats and steal data.

100
HIGH RISK APPLICATIONS
100 high-risk applications were observed, including those that can introduce or hide malicious activity, transfer files outside the network, or establish unauthorized communication.

45
SAAS APPLICATIONS
45 SaaS applications were observed in your network. To maintain administrative control, adopt SaaS applications that will be managed by your IT team.

6,445
VULNERABILITY EXPLOITS
6,445 total vulnerability exploits were observed in your organization, including **protocol-anomaly, code-execution and Other**.

7,131
TOTAL THREATS
7,131 total threats were found on your network, including vulnerability exploits, known and unknown malware, and outbound command and control activity.

378
MALWARE DETECTED
378 known malware events were observed in your organization.

SLR reports are customizable—you can choose to include only the information that is most important to you, and make summaries, findings, and recommendations more targeted.

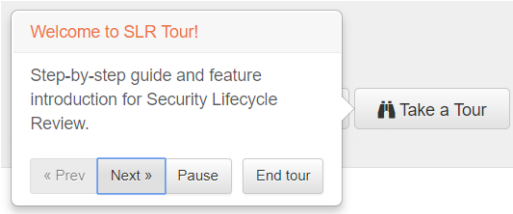
Importantly, SLR contains only summarized, statistical data and not individual identifiers, such as IP addresses or usernames (read the SLR privacy datasheet for details on how SLR captures, processes, and stores information).

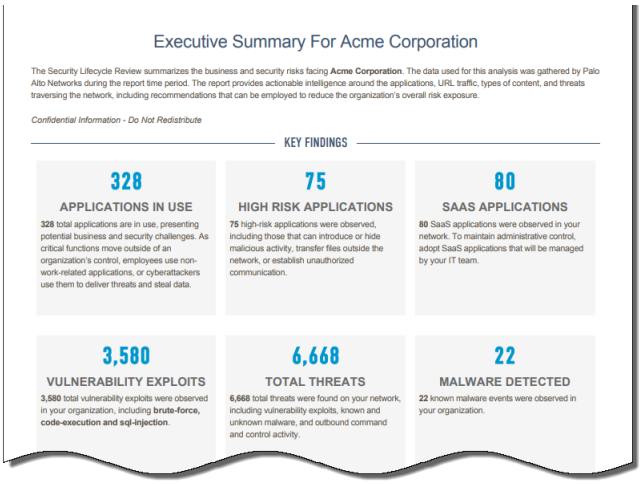
 ©2024 Palo Alto Networks, Inc.

Security Lifecycle Review (SLR)—What's in the Report?

Security Lifecycle Review (SLR) reports summarize the security and operational risks your organization faces, and breaks this data down so that you can quickly and easily identify how to reduce your attack surface. Each section of the SLR report focuses on different types network activity—application usage, web-browsing, data transfer, and threat prevalence—and surfaces the greatest risks in each area. SLR reports display your organization's statistics alongside the averages for your industry peers, so you can best understand your results in context.

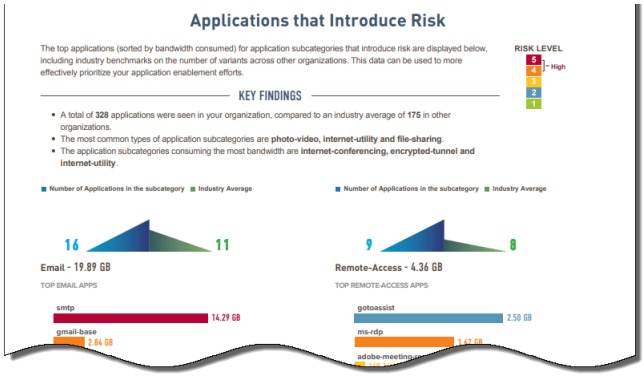
After you generate an SLR report, or open an existing SLR report, there is an option to **Take a Tour** of the report. Select this option to walk through and learn about each section of an SLR report.



Executive Summary	Provides a bird's-eye view of the state of your network. Statements on the total number threats detected on your network and the number of applications in use (including high-risk and SaaS applications) allow you to quickly assess how exposed you are to risk and focus areas for more strict or granular security policy control. 
Applications	Gives you a view into the applications traversing your network, especially highlighting applications that are commonly non-compliant and/or can introduce operational or security risks. Application findings also include total and application-level bandwidth consumption and the applications in use according to type (like media or collaboration). This application visibility allows you to weigh the business value of applications in use on your network, against the risk applications can

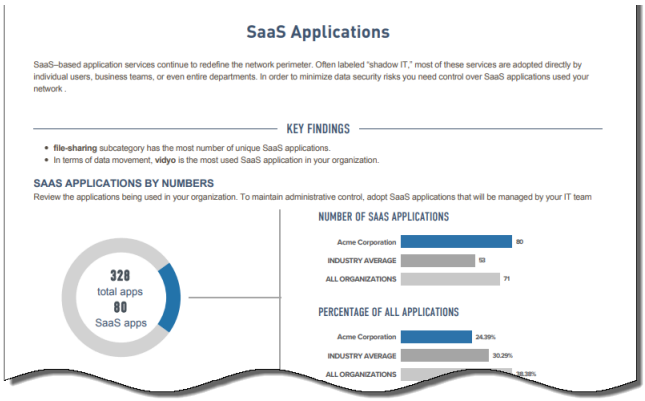
 ©2024 Palo Alto Networks, Inc.

introduce (such as malware delivery, data exfiltration, or excessive bandwidth consumption).



SaaS Applications

Highlights the SaaS applications in use on your network, including the SaaS apps that are transferring the most data and those that have risky hosting characteristics (frequent data breaches, poor terms of service, etc.). Understanding the presence of SaaS apps on your network can help you work towards safely enabling the apps that are critical to your business, while providing threat protection and preventing data leaks.



Advanced URL Filtering Activity

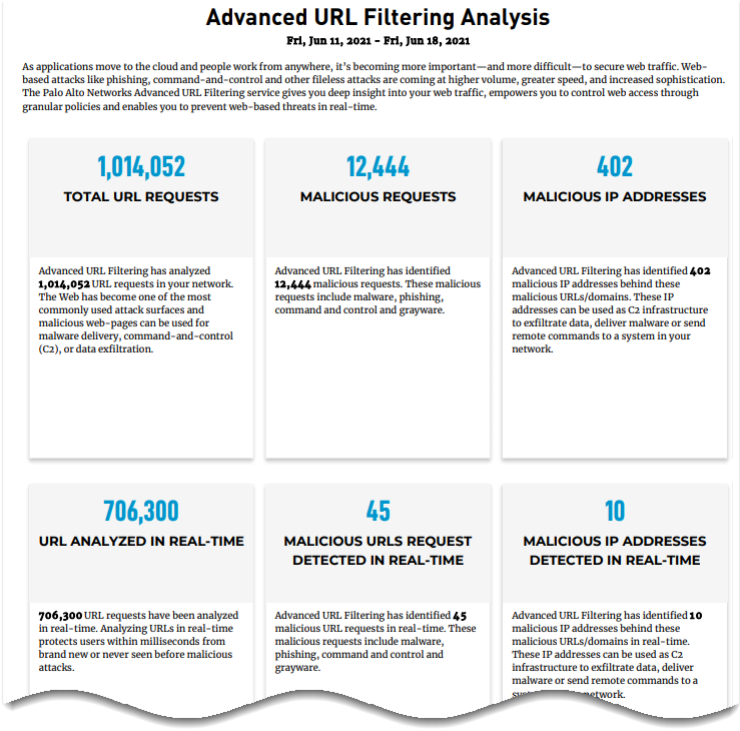
Summarizes the web browsing activity on your network. Uncontrolled web access can result in exposure to malware, phishing attacks, and data loss. The advanced URL filtering activity report is broken down into several sections:

If you are operating PAN-DB, but do not have an advanced URL filtering subscription, only the relevant network activity metrics are displayed.

- **Summary**—The summary provides high level analysis statistics about the URL requests passing through your network, including a categorized breakdown of URL requests, the associated malicious IP addresses, and real-time detection statistics.
- **Traffic Distribution**—Displays key metrics describing the URL requests in your network based on the risk level and categorization.

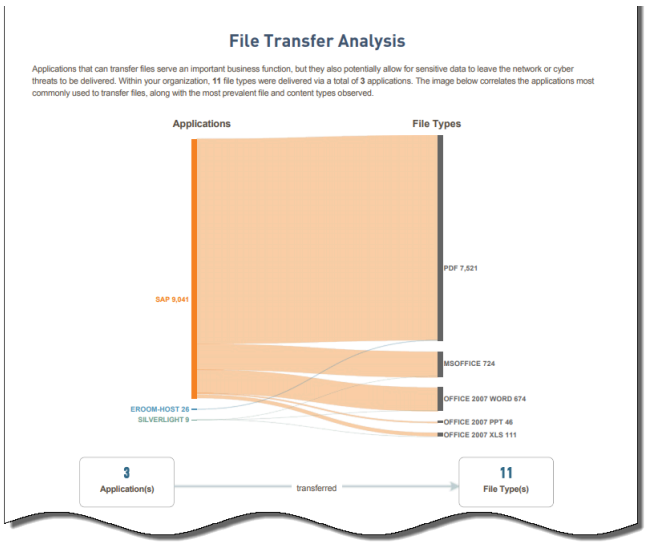
 ©2024 Palo Alto Networks, Inc.

- **Top Categories and Domains Distribution**—Displays a series of charts showing the top visited URL and domain categories.
- **Top Malicious URLs In Real-Time**—Displays the top 10 malicious URLs detected in real-time by the Advanced URL filtering service.

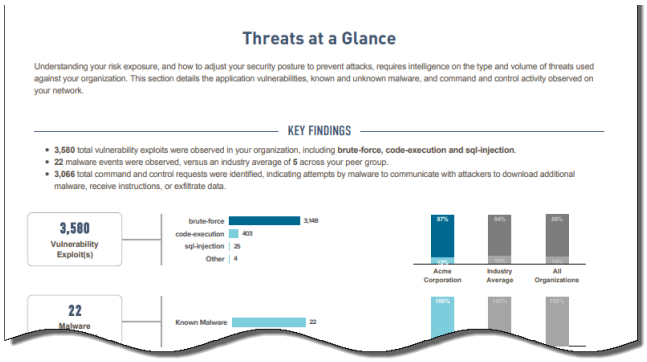


File Transfer

Gives you insight into the most commonly-used file types on your network, and what applications are being used to transfer these files. You can use the analysis provided here to consider more strict controls that prevent sensitive or proprietary data from leaving your network, and the delivery of malicious content into your network.

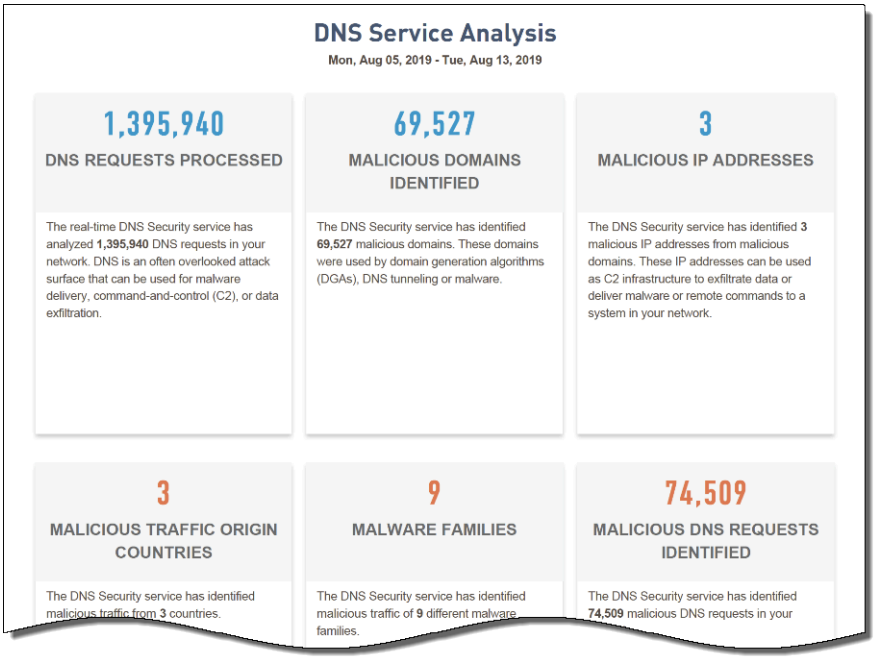


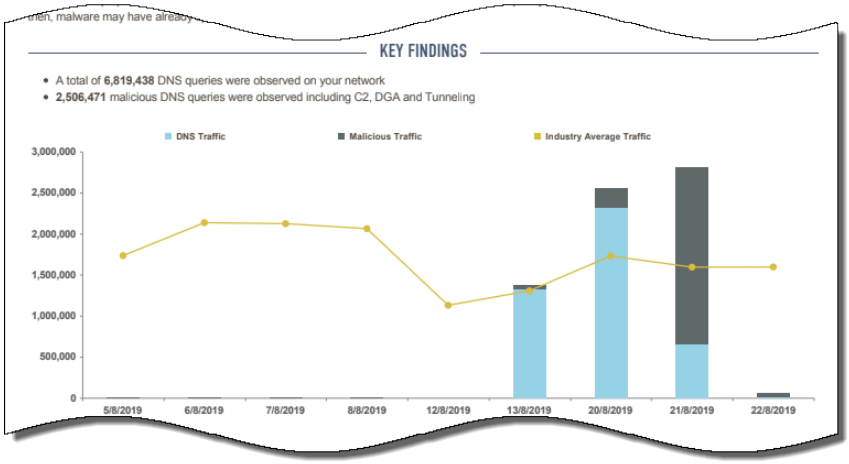
 ©2024 Palo Alto Networks, Inc.

Threats	Summarizes your organization's risk exposure by breaking down the attacks detected in your network: • Detected viruses and malware. • System flaws that an attacker might attempt to exploit. • Command-and-control (C2) activity, where spyware is collecting data and/or communicating with a remote attacker. • Vulnerable, unpatched applications that attackers can leverage to gain access to or further infiltrate your network. Your Threat summary also breaks down the high risk file types detected on your network, and the file types found to have delivered malware that was unknown until WildFire detection. Examine this data to best assess where you can immediately start to reduce your attack surface. New threat data *is now included in your report:* • *Threats first found on the endpoint.* • *Threats associated with targeted campaigns or malicious actors.* • *The geographic locations most targeted by threats found in your network.* 
DNS Security Analysis	Summarizes your exposure to threats hidden within DNS traffic. DNS is an often overlooked attack vector. Advanced attackers in particular use DNS-based techniques like DNS tunneling and DGAs (domain generation algorithms) to exfiltrate data and to set up command-and-control (C2) channels, respectively. To give you a view into malicious DNS activity on your network, the DNS Security Analysis section also reveals: • How much of your DNS traffic is malicious, and then categorizes the malicious DNS traffic as C2, DGA, or DNS tunneling. • The domains and destination IP addresses that are most requested from within your network. • The top malicious domains accessed from your network, and the countries hosting most of these malicious domains.

 ©2024 Palo Alto Networks, Inc.

- The malware families most associated with the malicious domains being accessed from inside your network.





Summary	The final summary provides recommendations that you can consider to safely enable the applications you need to do business, while reducing the organization's overall threat exposure.

 ©2024 Palo Alto Networks, Inc.

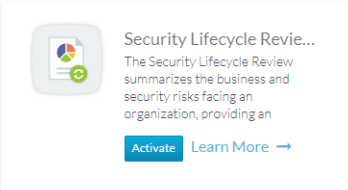
Activate the Security Lifecycle Review (SLR) App

Security Lifecycle Review (SLR) is a free Palo Alto Networks app that requires Strata Logging Service.

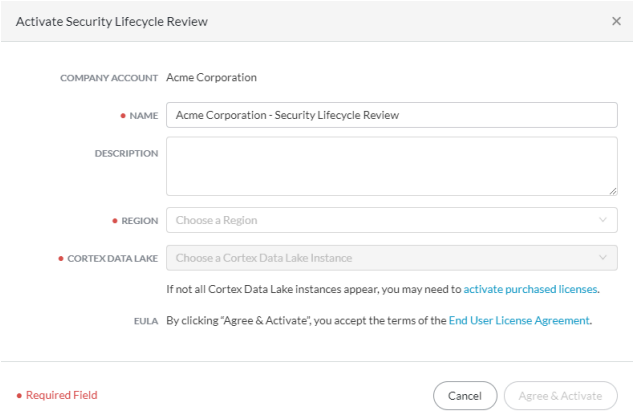
SLR examines the network data in Strata Logging Service to provide an overview of your security posture. To use SLR for the first time, you must activate the SLR app on the hub. When you first activate SLR, you are creating a single SLR app *instance*, and each SLR instance must be paired with aStrata Logging Service instance. You can create as many instances of the SLR app as you like; for example, you might create different SLR instances to generate reports for specific regions or audiences.

STEP 1 | Log in to the hub and find the Security Lifecycle Review (SLR) app listed under **More Available Palo Alto Networks Apps**.

STEP 2 | **Activate** the SLR app.



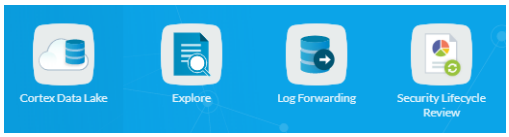
STEP 3 | Continue to pair this instance of the SLR app with a Strata Logging Service instance. SLR findings are based on the data stored in the Strata Logging Service instance you choose.



1. Enter a descriptive **Name** for this SLR app instance.
2. Select the **Region** in which Palo Alto Networks has deployed your Strata Logging Service infrastructure (SLR and Strata Logging Service must be deployed in the same region).
3. Select the **Strata Logging Service** instance to pair with SLR. SLR report data is based off the logs forwarded to this Strata Logging Service instance.
4. **Agree and Activate** SLR.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | You'll now see SLR displayed as one of your apps on the hub.



 ©2024 Palo Alto Networks, Inc.

Create a New Security Lifecycle Review (SLR) Report

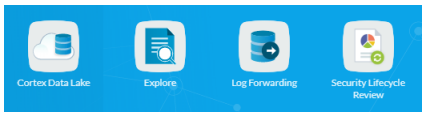
You can generate any number of SLR reports, at any time. An SLR report summarizes up to 90 days of network activity, for any date and time range of your choosing. Past reports are saved on the SLR homepage and list additional details, including the report creator and the creation date.

You can generate an SLR report in the following languages:

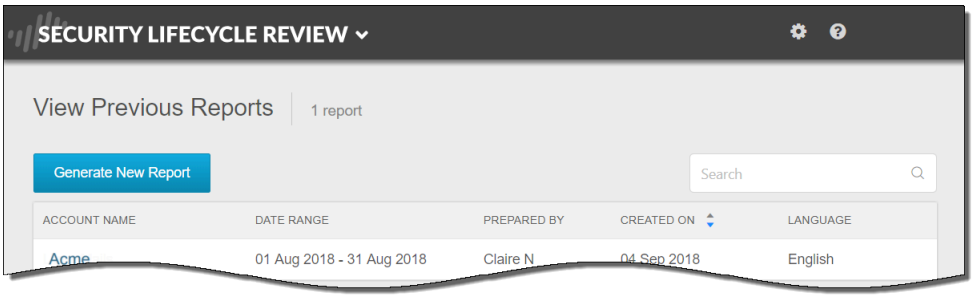
- Chinese (both simplified and traditional)
- English (US and UK)
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish

After you've generated an SLR report, you can customize the report to include only the information that is most important to you, and to make summaries and recommendations that are targeted to your organization.

STEP 1 | Log in to the Palo Alto Networks hub and open the Security Lifecycle Review (SLR) app.



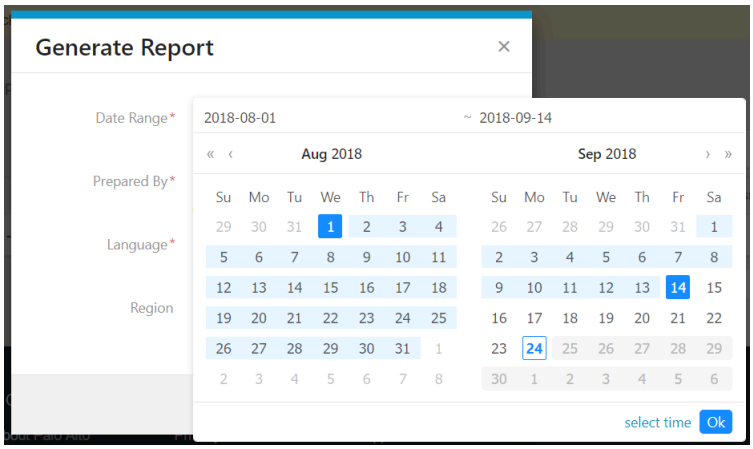
STEP 2 | Select **Generate New Report**.



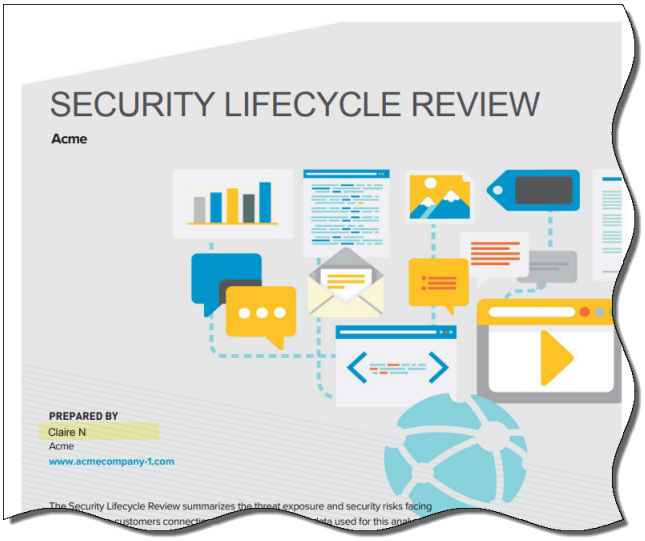
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Define the scope of the report you want to generate:

- **Date Range**—Enter the date range for which you would like SLR to summarize your network activity and threat exposure. You can select a date range up to 90 days, and for the first and last days of the date range, you can select the time of day.



- **Prepared By**—Enter the name of the individual or organization preparing this report. The name you enter here will appear on the report title page.

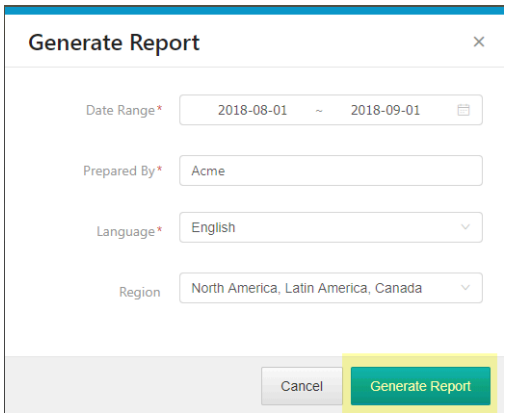


Select the gear on the top menu bar to update the company name and URL displayed on the title page (learn more about how to Customize Security Lifecycle Review (SLR) Reports*).*

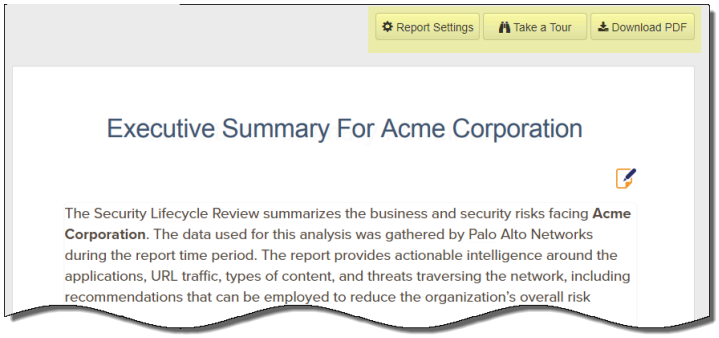
- **Language**—Choose the report language.
- **Region**—Select the region where the Strata Logging Service stores the logs that SLR examine to generate the report.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Select **Generate Report**.



STEP 5 | When report generation is complete, the new report is displayed for your review.



You can now choose to:

- Customize the sections the report includes, or go directly to a specific section (**Report Settings**).

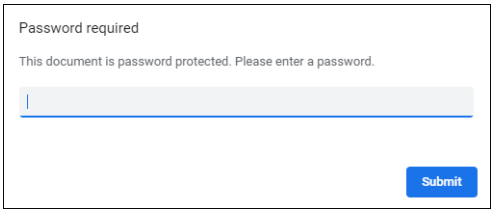
  Go directly to a specific section of the report, or add and remove
- Walk through the report, to learn about the type of information provided in each section (**Take a Tour**).
- Download the report in PDF format, for easy sharing (**Download PDF**).

Continue to Customize Security Lifecycle Review (SLR) Reports, for details on how you can tailor SLR reports to the needs of your organization.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | You will also receive a password-protected copy of the PDF report at the email address associated with your account, along with a separate email containing the password.

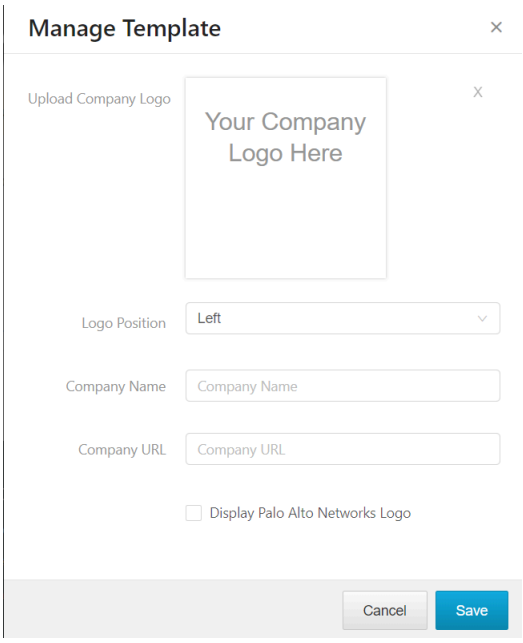
1. In an initial email from the SLR team, you'll receive the password you can use to access the report PDF.
2. You'll then receive a second email with the password-protected PDF.
3. Use the password from the first email to unlock the PDF you receive in the second email:



 ©2024 Palo Alto Networks, Inc.

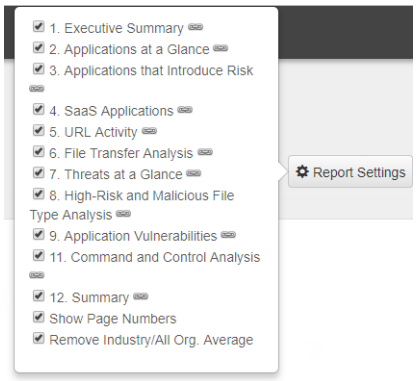
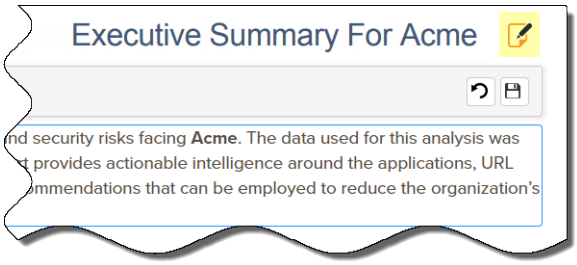
Customize Security Lifecycle Review (SLR) Reports

A Security Lifecycle Reviews (SLR) is a highly customizable report. Beyond the basics—which include options to add a company logo, name, and URL to the report title page—you can choose what type of information is included in the report, and tailor report content to so that it most relevant for your audience.

Before Report Generation (New Reports Only)	
❑ Customize the report title page	To display your company information on the title page of SLR reports, select the gear on the menu bar (top right) and choose to **Manage Template**. Add your company logo, name, and URL to the report title page.  Choosing to **Display Palo Alto Networks Logo** add the logo to the top right corner of each page of the report:

After Report Generation (New and Existing Reports)	
❑ Choose what sections and data appears in the report	A new SLR report includes all available sections of the report; however, you can decide to remove certain sections from the report, or to remove comparison data to industry peers. Open any existing report and select **Report Settings**.

 ©2024 Palo Alto Networks, Inc.

	
❑ Edit report highlights and recommendations	Open any existing report to edit the report content. You can update report summaries, highlights, and recommendations to make them more relevant or specific based on business needs or the SLR review audience. 

 ©2024 Palo Alto Networks, Inc.

Security Lifecycle Review (SLR) Support Requirements

- SLR requires (and is free) with Strata Logging Service.
- SLR works with a wide range of browsers—the most recent stable versions of Apple Safari and Google Chrome are supported.

 ©2024 Palo Alto Networks, Inc.

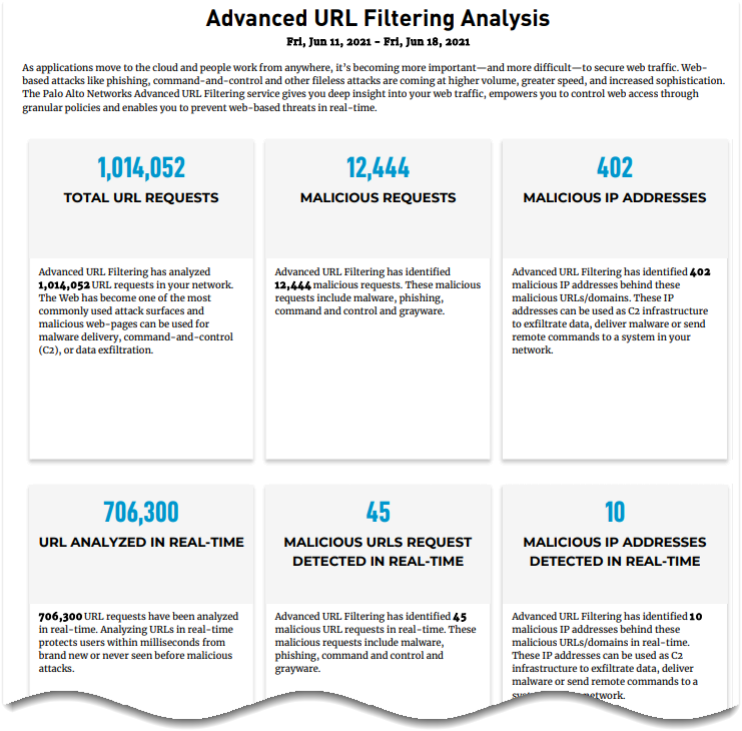
Security Lifecycle Review (SLR) Updates

Here's what's new in Security Lifecycle Review (SLR), and the issues we're working on to make your reports even better.

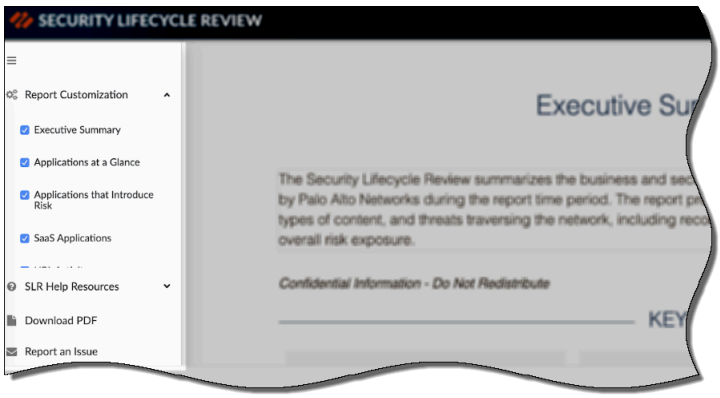
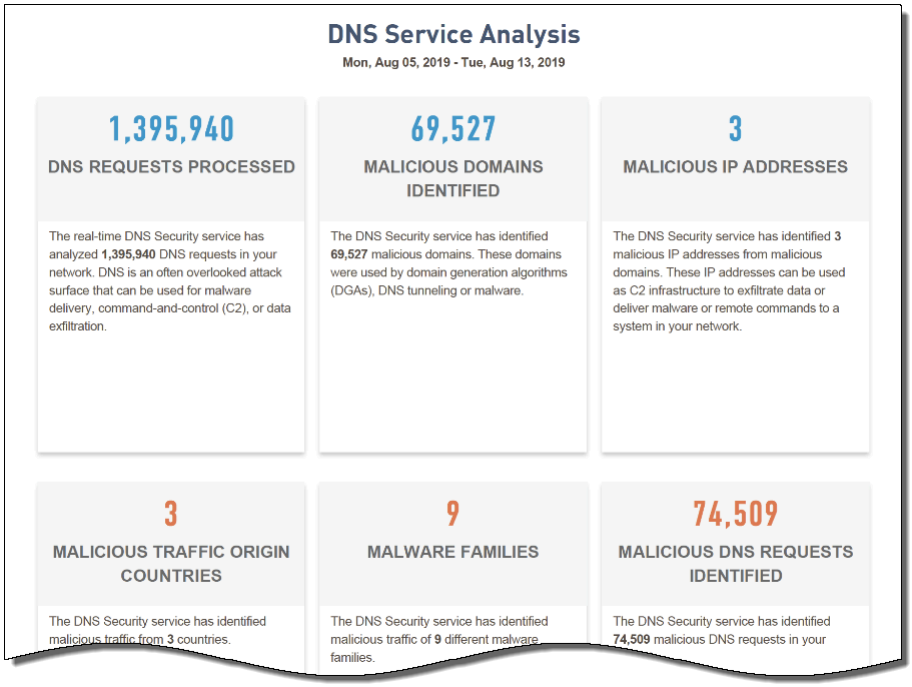
- What's New
- Known Issues

What's New

Learn about new SLR features, and how they can give you a view into your organization's risk exposure.

Release	New Features
June 2021	The section of the report that was previously designated as URL Activity has been relabeled as Advanced URL Filtering Analysis to reflect statistics data from the new real-time URL analysis security service, and now includes additional network activity metrics and threat trends. The updated section provides more details and a centralized view of your URL and domain statistics to help you assess the attack surface and specific attack vectors that make your organization vulnerable to web threats. 
May 2020	A new navigation bar gives you easy access to SLR report features and customization options:

 ©2024 Palo Alto Networks, Inc.

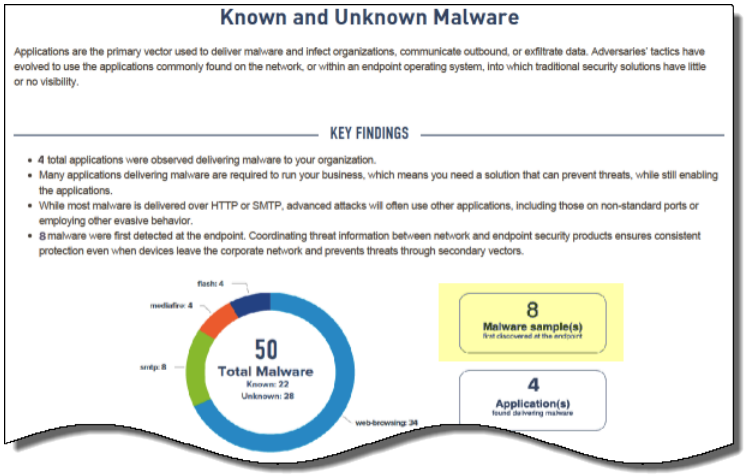
Release	New Features
	• **SLR Help Resources**—Launch the guided report tour, or access the Security Lifecycle Review Quick Start Guide. • **Pagination**—Add or remove pages or page numbers, or skip to a specific page in the report. • **PDF Report**—Download the report in PDF format. • **Send Feedback**—Report issues directly from the app. 
August 2019	We've added a new section to the SLR report! DNS is an often overlooked attack vector—advanced attackers in particular use DNS-based techniques like DNS tunneling and domain generation algorithms (DGAs) to exfiltrate data and set up command-and-control (C2) communication channels. The new DNS Security Analysis section gives you visibility in to threats hidden within DNS traffic. Learn more about what's in an SLR report or create a new SLR report now. 

 ©2024 Palo Alto Networks, Inc.

Release	New Features
April 2019 *New Threat Data*	The Threats section of an SLR report summarizes your organization's risk exposure by breaking down the attacks detected in your network. Threat data now shows you: ☐ Malware First Detected on the Endpoint ☐ Real-World Context for Threats ☐ The Countries that Threats Are Targeting Keep reading to learn more about each of these features...

Malware That Was First Detected at the Endpoint

Get visibility into the malware on your network that was first found on an endpoint. This shows you malware that might go undetected without an endpoint security solution in place, or without a solution that works consistently with your network security policy.

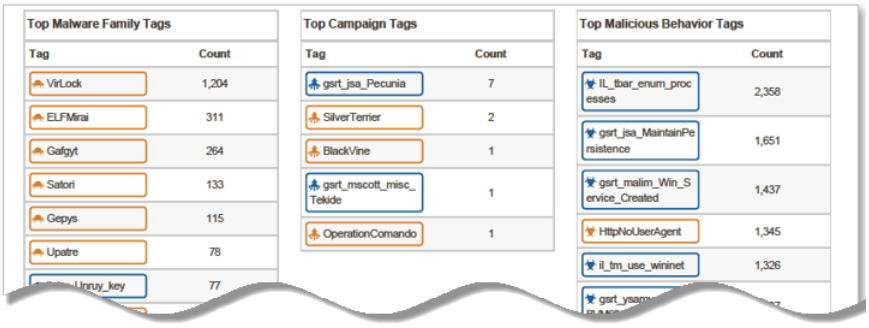


The availability of information on malware detected on the endpoint is based on the products deployed and the malware found in the network.

Real-World Context for Threats

AutoFocus tags show you when malware indicates a larger threat—like a targeted campaign or the activity of a specific malicious actor. AutoFocus tags in your SLR report give you context for the malicious activity on your network, and can help you to think about where to focus both prevention and remediation efforts.

 ©2024 Palo Alto Networks, Inc.

Release	New Features
	 **The Countries Threats Are Targeting** Now you can see the geographic locations that are most targeted by the malware found on your network.

Known Issues

We’re working on the following open issues to improve your SLR experience:

Issue	Description
FIXED on March 5, 2019	SLR does not include summary details for unknown malware detected by WildFire. *As of March 5, 2019, SLR reports include summary details for malware that was unknown before WildFire detection. See the Threats section in an SLR report for details on unknown malware found in your network.*

 ©2024 Palo Alto Networks, Inc.