Security Lifecycle Review (SLR)

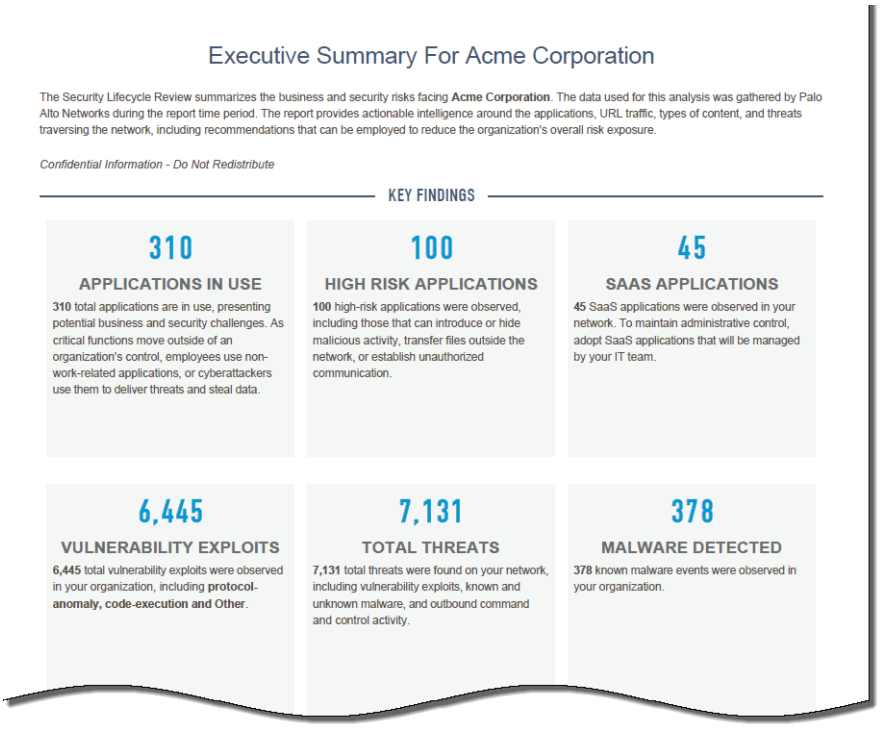
Getting Started Guide

techDOCS

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 Cortex hub, and uses the logs that firewalls forward to Cortex Data Lake to gain visibility into your network (SLR is free with a Cortex Data Lake 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.

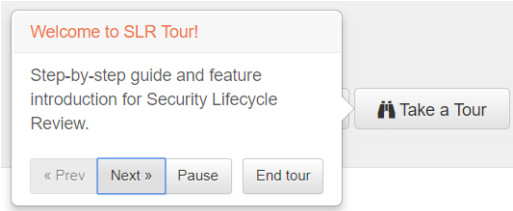
SLR reports are customizable—you can choose to include only the information that is most important to you, and make summaries, findings, and recommendations more targeted.

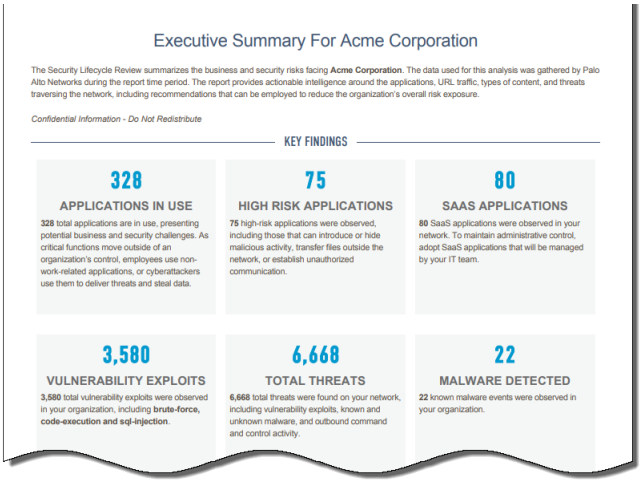
Importantly, SLR contains only summarized, statistical data and not individual identifiers, such as IP addresses or usernames (read the SLR privacy datasheet for details on how SLR captures, processes, and stores information).

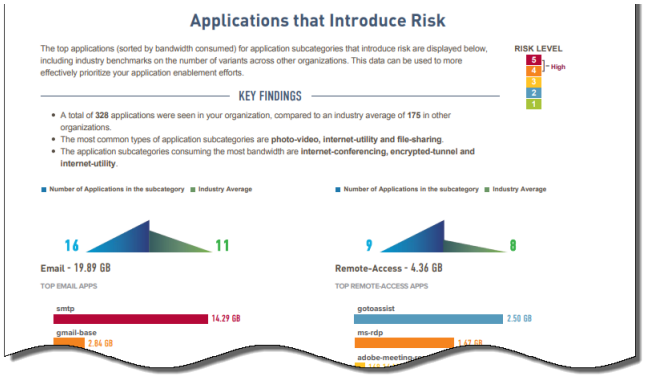
Security Lifecycle Review (SLR)—What's in the Report?

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.

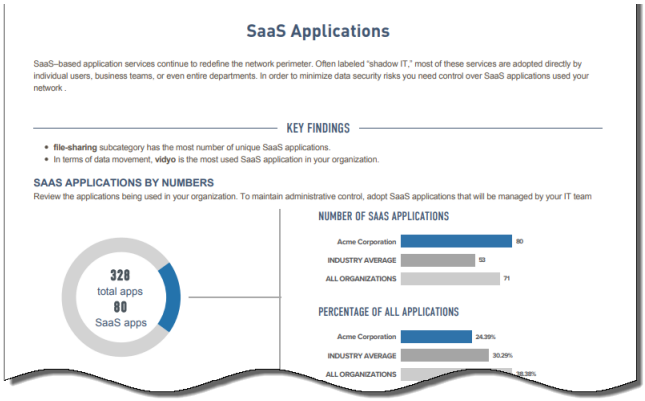


Executive Summary	Provides a bird's-eye view of the state of your network. Statements on the total number threats detected on your network and the number of applications in use (including high-risk and SaaS applications) allow you to quickly assess how exposed you are to risk and focus areas for more 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 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.

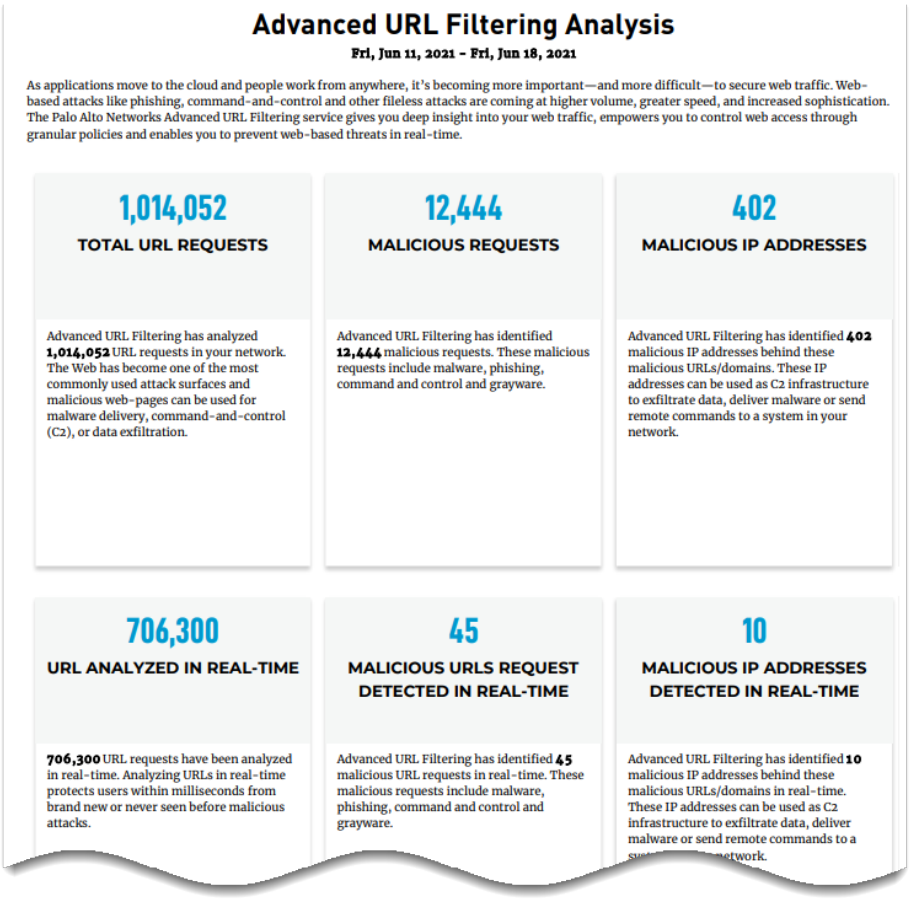


Advanced URL Filtering Activity

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.
- **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.



Advanced URL Filtering Analysis

Fri, Jun 11, 2021 - Fri, Jun 18, 2021

As applications move to the cloud and people work from anywhere, it's becoming more important—and more difficult—to secure web traffic. Web-based attacks like phishing, command-and-control and other fileless attacks are coming at higher volume, greater speed, and increased sophistication. The Palo Alto Networks Advanced URL Filtering service gives you deep insight into your web traffic, empowers you to control web access through granular policies and enables you to prevent web-based threats in real-time.

1,014,052
TOTAL URL REQUESTS

Advanced URL Filtering has analyzed **1,014,052** URL requests in your network. The Web has become one of the most commonly used attack surfaces and malicious web-pages can be used for malware delivery, command-and-control (C2), or data exfiltration.

12,444
MALICIOUS REQUESTS

Advanced URL Filtering has identified **12,444** malicious requests. These malicious requests include malware, phishing, command and control and grayware.

402
MALICIOUS IP ADDRESSES

Advanced URL Filtering has identified **402** malicious IP addresses behind these malicious URLs/domains. These IP addresses can be used as C2 infrastructure to exfiltrate data, deliver malware or send remote commands to a system in your network.

706,300
URL ANALYZED IN REAL-TIME

706,300 URL requests have been analyzed in real-time. Analyzing URLs in real-time protects users within milliseconds from brand new or never seen before malicious attacks.

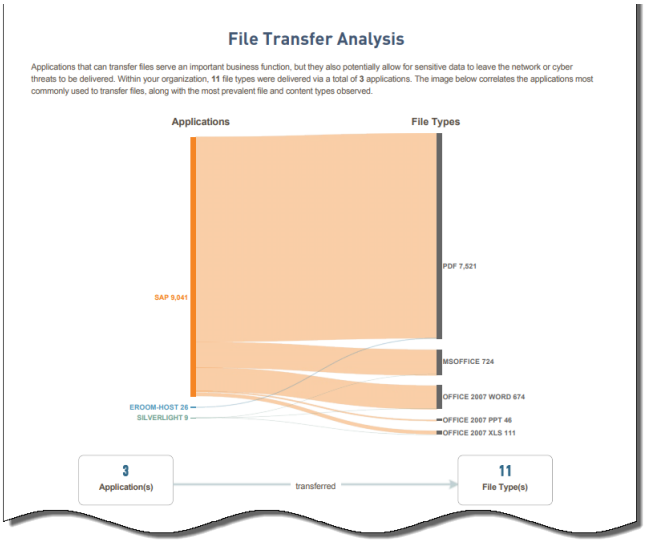
45
MALICIOUS URLS REQUEST DETECTED IN REAL-TIME

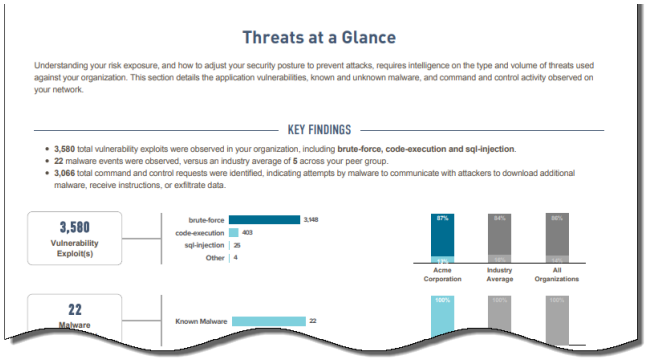
Advanced URL Filtering has identified **45** malicious URL requests in real-time. These malicious requests include malware, phishing, command and control and grayware.

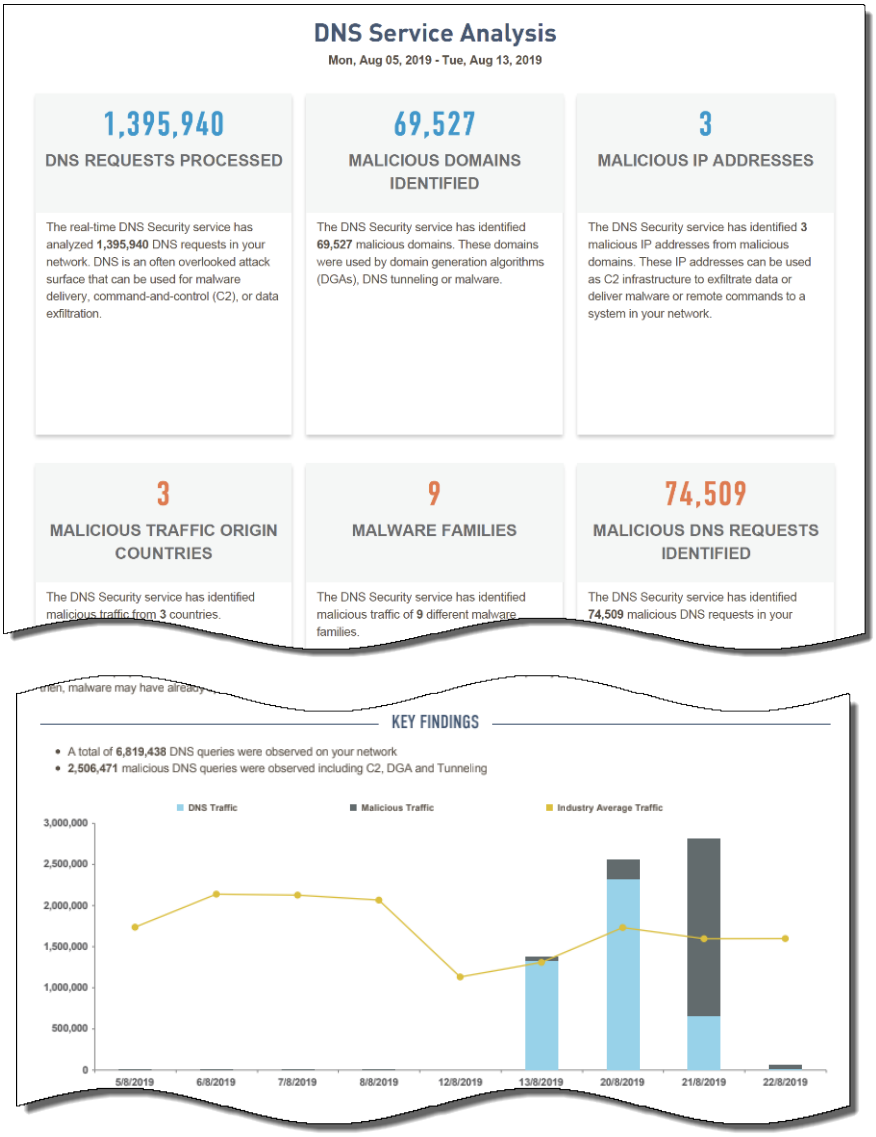
10
MALICIOUS IP ADDRESSES DETECTED IN REAL-TIME

Advanced URL Filtering has identified **10** malicious IP addresses behind these malicious URLs/domains in real-time. These IP addresses can be used as C2 infrastructure to exfiltrate data, deliver malware or send remote commands to a

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.



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. • 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.