Security Lifecycle Review

Do you really know what's on your network? Most companies lack full visibility into activity and devices on their networks, leaving them in the dark about security risks. A Security Lifecycle Review (SLR) provides a customized security assessment of the applications, internet of things (IoT) devices, vulnerabilities, threats, and risks in your environment. Once you know where the biggest risks are, you can determine where to focus, develop an action plan, and improve your security posture.

Benefits of an SLR

- **Complete visibility:** See how adversaries are trying to breach your defenses, all applications in use, and all devices on your network.
- **Quantified risk:** Confidently make data-driven decisions, prioritize, and take the right policy or technology actions based on what you learn.
- **Time saved:** A single report summarizes key risks and recommendations so your security teams can focus on the top priorities.

What Is an SLR?

A focused, free security risk assessment, the SLR produces a report that summarizes the volume and types of threat exposures and vulnerabilities identified on your network over a specified time period. It also includes recommendations on how to reduce your overall risk exposure and improve your security posture.

IoT Device Visibility and Risks	SaaS and Other Application Risks	DNS Security Analysis	URL Activity Analysis	Threats by Destination Country
Application Vulnerabilities	Threat Analysis	File Transfer Analysis	Malware Analysis	Bandwidth Consumed

Figure 1: Found in your SLR report[1]

An SLR can be done during an initial evaluation or as part of a regular security checkup. Findings are based on data collected during the review period (typically seven days) and is non-intrusive.

Why Run an SLR?

To effectively manage network security and have a robust intrusion prevention system (IPS), you need deep visibility into your organization's environment. All threats should be regularly assessed to have their relative risk assigned. Then, you can effectively manage priorities and resources to address these risks, develop the strongest security posture, and prevent business interruptions and attacks.

An SLR is a quick and easy way to view applications, threats, and vulnerabilities on your network. The report provides details on software-as-a-service (SaaS) and other applications, URL traffic, content types, IoT devices (see figure 3), and known and unknown threats traversing your network (see figure 4), along with recommendations on the highest risks and priority areas to focus on (see figure 5).

Figure 2: SLR Executive Summary page

The Executive Summary page provides a high-level digest of the applications and threats observed on your network.

1. Note prerequisite subscriptions.

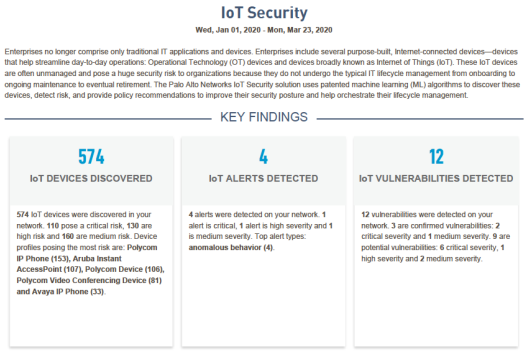

Figure 3: IoT Security section

The IoT Security section provides industry-leading visibility and risk prioritization of IoT devices so you can better manage IoT security throughout the device lifecycle.

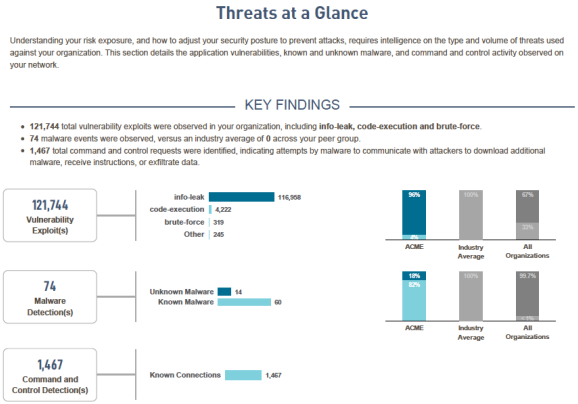

Figure 4: Threats at a Glance section

The Threats at a Glance section shows the type and volume of threats used against your organization, including known and unknown malware, command-and-control activity, and application vulnerabilities.

Figure 5: Recommendations section

The final section of the SLR report summarizes key findings and provides recommendations on how your organization can address the highest risks identified.

Frequently Asked Questions

How do I run an SLR?

You can access a self-service SLR from the Customer Support Portal. If you need help, please contact your sales representative.

The SLR is also available as a cloud-delivered application.

I'm not a Palo Alto Networks customer. Can I run an SLR?

Yes! Please contact your local sales representative or request an SLR online.

To conduct an SLR for your organization, we can run an SLR in your environment. This process is non-intrusive. An SLR can be run for a virtual or physical firewall.

How often should I run a SLR?

Palo Alto Networks customers can run SLRs on demand, as often as needed. We recommend regularly evaluating your security risks by running an SLR at least every 90 days or whenever there has been a significant change on your network.

Can I get a single SLR report on multiple devices?

Yes, the multi-statsdump merge feature allows you to upload statsdump files from multiple devices to generate a cumulative SLR report.

Additional Resources

- Other questions? Visit our Customer Support Portal.
- Ready to get started? Visit us online and **request an SLR** https://start.paloaltonetworks.com/security-lifecycle-review-risk-assessment.html
- Running a Customer-Driven SLR? Read our SLR QuickStart Guide.
- Need help with the SLR app? Read our technical documentation.

SLR Prerequisite Subscriptions

For the most complete view of your environment, you'll need:

- **General:** WildFire, URL Filtering, Threat Prevention subscriptions
- **IoT section:** Cortex™ Data Lake subscription and an active IoT Security instance
- **DNS section:** DNS Security subscription

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com