Building an Intelligence-Led Security Program

In today's rapidly evolving threat landscape, organizations need to be more proactive than ever in protecting their assets. Traditional security approaches that rely solely on reactive measures are no longer enough. Organizations need to be able to identify and mitigate threats before they can cause damage.

An intelligence-led security program (ILSP) is a proactive approach to security that uses threat intelligence to inform security decision-making. By collecting, analyzing, and disseminating threat intelligence, organizations can gain a better understanding of the threats they face and take steps to mitigate those threats.

This guide will provide you with a comprehensive overview of how to build an ILSP. We will cover the following topics:

Building an Intelligence-Led Security Program by Allan Liska

4 out of 5

Language	: English
File size	: 4581 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 178 pages

- What is an ILSP?
- The benefits of an ILSP

- The key components of an ILSP
- How to build an ILSP
- Measuring the effectiveness of an ILSP

An ILSP is a security program that uses threat intelligence to inform security decision-making. Threat intelligence is information about potential or actual threats to an organization. This information can come from a variety of sources, including:

- Internal sources, such as security logs and incident reports
- External sources, such as threat intelligence feeds and reports from law enforcement and intelligence agencies

By collecting, analyzing, and disseminating threat intelligence, organizations can gain a better understanding of the threats they face and take steps to mitigate those threats.

There are many benefits to implementing an ILSP, including:

- **Improved threat visibility:** An ILSP provides organizations with a more comprehensive view of the threats they face. By collecting and analyzing threat intelligence from a variety of sources, organizations can identify threats that they may not have otherwise been aware of.
- **Improved threat detection and response:** An ILSP can help organizations to detect and respond to threats more quickly and effectively. By using threat intelligence to identify potential threats, organizations can take steps to mitigate those threats before they can cause damage.

- **Improved decision-making:** An ILSP can help organizations to make better security decisions. By providing security decision-makers with access to timely and accurate threat intelligence, organizations can make more informed decisions about how to allocate their security resources.
- **Reduced costs:** An ILSP can help organizations to reduce their security costs. By identifying and mitigating threats before they can cause damage, organizations can avoid the costs associated with responding to and recovering from security incidents.

There are four key components of an ILSP:

- **Threat intelligence:** Threat intelligence is the foundation of an ILSP. Without threat intelligence, organizations cannot effectively identify and mitigate threats. Threat intelligence should be collected from a variety of sources and should be timely, accurate, and relevant to the organization's needs.
- **Threat analysis:** Threat analysis is the process of analyzing threat intelligence to identify potential threats. Threat analysis should be conducted by a team of experienced security analysts who are familiar with the organization's security posture and the threats it faces.
- **Threat mitigation:** Threat mitigation is the process of taking steps to reduce the risk of a threat. Threat mitigation strategies should be based on the results of threat analysis and should be tailored to the specific threats that the organization faces.
- **Threat monitoring:** Threat monitoring is the process of tracking threats over time to identify changes in the threat landscape. Threat

monitoring should be conducted on a regular basis and should be used to update the organization's security posture accordingly.

Building an ILSP is a complex process that requires careful planning and execution. The following steps will help you to build an ILSP that meets the needs of your organization:

1. **Define your goals and objectives.** Before you can build an ILSP, you need to define your goals and objectives. What do you want to achieve with your ILSP? What are the specific threats that you are trying to mitigate?
2. **Identify your intelligence needs.** Once you have defined your goals and objectives, you need to identify your intelligence needs. What type of threat intelligence do you need? From what sources do you need to collect threat intelligence?
3. **Build a threat intelligence team.** The success of your ILSP depends on the quality of your threat intelligence team. Your threat intelligence team should be composed of experienced security analysts who are familiar with the organization's security posture and the threats it faces.
4. **Develop a threat intelligence collection plan.** Your threat intelligence collection plan should outline how you will collect threat intelligence from a variety of sources. Your plan should include both internal and external sources of threat intelligence.
5. **Implement a threat analysis process.** Your threat analysis process should be designed to identify potential threats and assess their risk. Your threat analysis process should be conducted by a team of experienced security analysts.

6. **Develop a threat mitigation strategy.** Your threat mitigation strategy should outline how you will reduce the risk of a threat. Your threat mitigation strategy should be based on the results of threat analysis and should be tailored to the specific threats that the organization faces.
7. **Implement a threat monitoring process.** Your threat monitoring process should be designed to track threats over time and identify changes in the threat landscape. Your threat monitoring process should be conducted on a regular basis and should be used to update the organization's security posture accordingly.

The effectiveness of an ILSP should be measured by its ability to improve the organization's security posture and reduce the risk of a security incident. The following metrics can be used to measure the effectiveness of an ILSP:

- **Number of threats identified:** The number of threats identified by an ILSP is a measure of the program's ability to identify potential threats.
- **Accuracy of threat assessments:** The accuracy of threat assessments is a measure of the program's ability to assess the risk of a threat.
- **Time to respond to threats:** The time to respond to threats is a measure of the program's ability to detect and respond to threats in a timely manner.
- **Cost of security incidents:** The cost of security incidents is a measure of the program's ability to reduce the financial impact of a security incident.

By tracking these metrics, organizations can measure the effectiveness of their ILSP and make adjustments as needed.

An ILSP is a powerful tool that can help organizations to improve their security posture and reduce the risk of a security incident. By collecting, analyzing, and disseminating threat intelligence, organizations can gain a better understanding of the threats they face and take steps to mitigate those threats.

If you are interested in building an ILSP for your organization, there are a number of resources available to help you. The following resources provide additional information on ILSPs:

- NIST Special Publication 800-53: Guide for Developing Security Programs
- DHS Intelligence-Led Security Primer
- Gartner Report: How to Build an Intelligence-Led Security Program: A Step-by-Step Guide

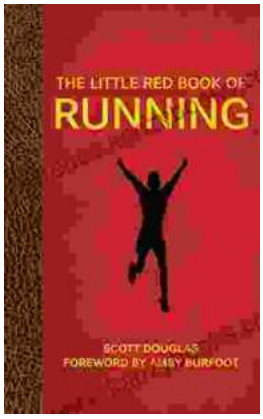
Building an Intelligence-Led Security Program by Allan Liska

4 out of 5

Language	: English
File size	: 4581 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 178 pages

Book Review: In Controluce Scatti Di Epilessia

In Controluce Scatti Di Epilessia Author: Elisa Serafini Publisher: Postcart Edizioni Publication Date: 2019 ...



The Little Red Book of Running: A Comprehensive Guide to the World's Most Popular Sport

Running is one of the most popular sports in the world. It's a great way to get fit, lose weight, and relieve stress. But if you're new to...