ISAUnited
International Security Architects

Threat Landscape Analysis Practice Guide

Parent standard: ISAU-Std-100x-v1.2024-Threat Analysis

www.isaunited.org

Disclaimer

ISAUnited has designed and created the ISAUnited Defensible Architecture (IDA)® 2023 Design Guide: Designing security architecture utilizing a threat-based approach to ensure, emphasize, and educate governance of information and technology, assurance, risk, and security professionals (the "Work"). ISAUnited makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures, and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, enterprise governance of information and technology, assurance, risk, and security professionals should apply their own professional judgment to the specific circumstances presented by the systems or information technology environment.

Document Management

Parent document: ISAU-Std-100x-v1.2024-Threat Analysis

Child document: ISAU-add-Threat Landscape Analysis

Forward

This guide presents methods and practices for integrating cyber threat intelligence security architecture design. This guide does not designate practices or instructions for every specific situation because of the complexity of technical architecture designs.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.

This guide should be used in conjunction with the practices described in the following ISAUnited standards and publications, when appropriate (use the latest revisions):

1. Security Design Operations Model
2. Defensible Architecture Design Methodology

Contents

Threat Landscape Analysis

Practice Guide

1. Introduction

Nested within ISAUnited's Defensible Architecture methodology is Threat Intelligence Preparation in which Integrates Threat Intelligence in security design. The objective of this technical process is to seamlessly integrate threat intelligence into the security design process to fortify defenses, identify potential vulnerabilities, and enhance overall cybersecurity posture.

The integration of Cyber Threat Intelligence (CTI) is a proactive defense strategy. Security architects and architect designers must leverage cyber threat intelligence to perform comprehensive threat analysis, creating a foundation for informed security design and the implementation of focused security controls.

For security architects, the ability to anticipate, understand, and pre-empt potential threats is essential to the architecture design and review process. Security designers must be equipped not only with technical acumen but also with the insights provided by CTI. This knowledge forms strategic decision-making, allowing architects to design security measures that are not reactive but anticipatory, addressing vulnerabilities before they can be exploited.

CTI offers extensive exploration across various domains allowing security teams to go deep and wide with threat intelligence information. Specifically in security design, a more focused approach called a Threat Landscape Analysis (TLA) serves as a pivotal component, addressing critical questions about potential threat actors, their tactics, objectives, and likely targets within an organization's technical architecture.

The threat landscape is dynamic, and adversaries are becoming increasingly sophisticated, the role of security architects is more pivotal than ever. To fortify digital defenses against potential threats, security architects must harness efficient and effective CTI. This imperative becomes particularly pronounced when preparing for the ominous prospect of a bad actor's attack or intrusion.

1.1 Definitions

Threat Landscape - In the field of cyber threat intelligence, the term "threat landscape" refers to the comprehensive and dynamic overview of potential risks and hazards that an organization or system may encounter. The threat landscape encompasses a wide range of factors, including various types of cyber threats, vulnerabilities, and the potential impact of malicious activities on an organization's information technology infrastructure and network.

2. Purpose

The purpose of this technical guidance is to delve into the critical role of threat landscape analysis in the domain of security architecture. As the cyber threat landscape continues to evolve rapidly, security architects face the imperative of understanding, anticipating, and mitigating emerging risks. This journal aims to provide insights into why conducting a thorough threat landscape analysis is indispensable in the design and implementation of robust security measures. By exploring real-world case studies, methodologies, and best practices, we seek to equip security architects with the knowledge and tools necessary to fortify organizational infrastructures effectively. Ultimately, this document serves as a guide for navigating the complex terrain of cybersecurity, emphasizing the proactive stance that threat landscape analysis affords in shaping resilient security architectures. A TLA should cover:

WHO? Identify threat actors inclined to target the organization.

HOW? Analyze tactics and techniques typically employed by threat actors.

WHY? Determine the objectives pursued by threat actors in their attacks.

WHERE? Identify the resources and personnel likely to be targeted by threat actors.

NOTE: A TLA is a point-in-time analysis or a continuous assessment of active monitoring of your architecture threat landscape, the TLA ensures your resources are best placed to counter cyber threats as they emerge.

2.1 Key Questions

Addressed by the Threat Landscape Analysis (TLA):

- **Adversaries-**Identify real adversaries targeting the organization.
- **Tactics, Techniques, and Procedures (TTPs)-**Understand the TTPs employed by adversaries.
- **Defense Strategies-**Determine how to effectively defend against identified threats.
- **Opportunities-**Identify opportunities for enhancing security measures.
- **Security Posture-**Evaluate the alignment of security posture with the threat profile.
- **Industry-Specific Threats-**Assess threats of significance to the industry vertical.

2.2 Key Components

Understanding the adversary's tactics, techniques, and procedures is necessary to decipher a constantly evolving puzzle. Efficient CTI acts as a force multiplier for security architects, providing timely and relevant insights into the ever-changing threat landscape. Why integration of such intelligence is indispensable:

Proactive Defense Posture- Efficient cyber threat intelligence empowers security architects to adopt a proactive defense posture. By staying ahead of potential bad actor activities, architects can anticipate and preemptively address vulnerabilities before they are exploited.

Understanding Adversarial Tactics- To counter a bad actor effectively, security architects need to comprehend the methods employed by potential attackers. Cyber threat intelligence offers a detailed understanding of the tactics, techniques, and procedures utilized, enabling architects to design defenses that specifically target these methodologies.

Risk Mitigation and Prioritization all threats are equal, and effective cyber threat intelligence aids security architects in assessing and prioritizing risks. This allows for resource allocation based on the severity and likelihood of potential attacks, optimizing defense mechanisms.

Tailored Security Controls- Armed with intelligence on specific threats and attack vectors, security architects can design and implement security controls that are precisely tailored to counteract the identified risks. This ensures a more effective defense against bad actor intrusions.

Incident Response Preparedness- Cyber threat intelligence plays a pivotal role in incident response preparedness. Architects, armed with insights into potential bad actor behaviors, can develop and refine incident response plans, ensuring a swift and coordinated reaction to emerging threats.

Continuous Adaptation- The cybersecurity landscape is in constant flux. Efficient cyber threat intelligence facilitates continuous adaptation by providing real-time updates on emerging threats. This agility allows security architects to evolve their defense strategies in tandem with the changing threat landscape.

Enhanced Situational Awareness- To effectively prepare for a bad actor attack, security architects require enhanced situational awareness. Cyber threat intelligence provides a comprehensive view of the threat landscape, enabling architects to make informed decisions and rapidly respond to evolving risks.

The integration of efficient and effective cyber threat intelligence is not merely an advantage but a necessity for security architects preparing for the specter of a bad actor attack. It empowers architects with the knowledge required to stay ahead of adversaries, fortify defenses, and proactively safeguard organizational assets against the ever-present threat of intrusion.

2.3 Key Preparation Steps

As you enter the threat analysis phase of security design, the Threat Landscape Analysis (TLA) is conducted. While conducting the TLA process, the gathering and reviewing of cyber threat intelligence information allows for the appropriate assessment of the organization's asset data, components, and systems.

- The initial phase in optimizing the utilization of threat intelligence involves identifying your intelligence requirements. An intelligence requirement refers to any specific information you seek to gain insights into. This could encompass a broad spectrum of subjects, including comprehending threat groups, obtaining details about a novel malware variant or ransomware group, and staying informed about the most recent indicators of compromise or threats specific to your industry.
- Once you have defined and prioritized your intelligence needs, the next step is to communicate them to your intelligence team. Because they work pro-actively to find threats before they have an impact, Intelligence teams typically can't guarantee what they will be able to report on, but their jobs are made a lot easier if they understand directly from customers what their intelligence needs and priorities are.

A proactive approach to identifying intelligence requirements not only aids in the communication process but also proves advantageous when reviewing published threat intelligence in platforms. By prioritizing intelligence needs, you circumvent the need for your team to sift through an extensive array of intelligence reports to find relevant information. This strategic prioritization allows for a more efficient workflow, enabling timely review of crucial reporting while deferring less critical information for later consideration.

3. Techniques Deployed

Several cyber threat intelligence techniques can be employed to determine an organization's threat landscape. These techniques involve gathering, analyzing, and interpreting information about potential cyber threats. Here are some common techniques:

Open-Source Intelligence (OSINT):

- **Description:** OSINT involves collecting information from publicly available sources.
- **Use Case:** Monitor social media, forums, news articles, and other public platforms for information related to potential threats targeting the organization.

Human Intelligence (HUMINT):

- **Description:** HUMINT involves gathering intelligence through human sources, such as employees, partners, or industry contacts.
- **Use Case:** Engage with industry forums, attend conferences, and establish contacts to gather insights into potential threats.

Technical Intelligence (TECHINT):

- **Description:** TECHINT involves analyzing technical information related to threats, such as malware analysis, network traffic analysis, and forensic investigations.
- **Use Case:** Investigate and analyze the technical aspects of previous incidents to understand potential threats and their capabilities.

Indicator-Based Intelligence (IBI):

- **Description:** IBI involves analyzing indicators of compromise (IoCs) and patterns associated with previous cyber-attacks.
- **Use Case:** Identify and analyze IoCs, such as malicious IP addresses, domains, and file hashes, to detect potential threats targeting the organization.

Tactics, Techniques, and Procedures (TTPs) Analysis:

- **Description:** Analyzing the TTPs used by threat actors provides insights into their methods and behaviors.
- **Use Case:** Study past incidents to understand the tactics, techniques, and procedures employed by threat actors, helping in the identification of potential future threats.

Threat Feeds and Intelligence Sharing:

- **Description:** Subscribing to threat intelligence feeds and participating in information-sharing communities to receive real-time updates on emerging threats.
- **Use Case:** Stay informed about the latest threat intelligence from reputable sources and collaborate with other organizations to share insights.

Scenario-Based Threat Modeling:

- **Description:** Develop hypothetical scenarios to model potential threat scenarios and assess the organization's readiness.
- **Use Case:** Create and simulate threat scenarios to identify gaps in current security measures and develop proactive defense strategies.

Vulnerability Intelligence:

- **Description:** Monitor and analyze information about vulnerabilities in software, systems, and networks.
- **Use Case:** Stay updated on vulnerabilities relevant to the organization's infrastructure and prioritize patching or mitigation efforts accordingly.

NOTE: Whether security teams opt to develop CTI internally or collaborate with external vendors, it remains the responsibility of the security teams to ensure that cyber threat intelligence is delivered to key stakeholders, including security designers.

4. Guiding Process

Following the ISAUnited's Defensible Architecture methodology preparations guidance of 'Know Your Architecture' and 'Threat Intelligence Preparation', using the guiding process below will allow the organization and its security design practitioners to conduct the threat landscape analysis.

Prerequisites:

Review the attack surface or entry points to be assessed and researched against the most realistic, current, and future threats.

Understanding the data flow, data in use, and data at rest from public-facing internet assets inside and outside the infrastructure and network.

Identifying architecture components and systems that integrate with third-party entities and analyzing the vulnerabilities and threats of any outside security risks.

Guidance Steps:

1 - Define and scope the threat landscape of architecture assets such as data, development source code, components and systems, infrastructure, and networks.

2 - Describe and identify the operations of each scoped asset in the technology operations to the best of your knowledge.

3 - Using the above 'Techniques Deployed', gather, and evaluate the threat intelligence information provided to analyze and identify the threats for the defined assets and scoped architectural segments to determine your pre-determine threat landscape scope.

4 – By now the security design practitioner has determine threats associated with the defined assets and scoped architectural segments the design. Determine the course of action to remediate the threat and develop the technical controls necessary to close the gap.

5. Conclusion

The Threat Landscape Analysis (TLA) serves as a dynamic tool, answering crucial questions about adversaries, tactics, defense strategies, opportunities, security posture alignment, and industry-specific threats. As security architecture designers navigate the complex threat landscape, conducting a TLA becomes a vital step, encompassing a strategic process of cyber defense and assisting with providing specific security controls.

5.1 References:

1. ISAUnited's Defensible Architecture Methodology
2. Threat and Vulnerability Analysis-IDA-Template-05

Revision	Date
Created Date	11-17-2023
Institute Date	01-05-2024
Published Date	01-05-2024

End of Document.