White Paper: Enhancing IT Security with Pattern of Life Analysis

Introduction

Pattern of Life Analysis (POLA) is a technique for identifying and analyzing patterns in behavior. POLA can be used to understand the current state of an entity, detect anomalies, and predict future behavior. POLA can be used to enhance IT security in a number of ways, including:

- Detecting unauthorized access: POLA can be used to detect unauthorized access to IT systems and resources by identifying anomalous behavior. For example, POLA can be used to identify unusual login patterns or unusual patterns of access to files and data.
- Identifying insider threats: POLA can be used to identify insider threats by identifying employees whose behavior patterns indicate that they may be planning to attack the company's IT systems or data. For example, POLA can be used to identify employees who have been accessing sensitive data without authorization or who have been downloading large amounts of data without a valid reason.
- Preventing data breaches: POLA can be used to prevent data breaches by identifying patterns of behavior that indicate that a data breach is in progress. For example, POLA can be used to identify unusual patterns of data exfiltration or unusual patterns of access to sensitive data.

Use-Case Examples

Here are some specific use-case examples of how POLA can be used to enhance IT security:

- A financial services company could use POLA to detect unauthorized access to customer accounts. The company could monitor login patterns and identify any unusual activity, such as multiple login attempts from different locations or login attempts at unusual times.

SARAHAI™ Tensor Networks, Inc. All Rights Reserved www.tensornetworks.com

- A healthcare organization could use POLA to identify insider threats. The organization could monitor employee access to patient records and identify any unusual activity, such as employees accessing records of patients they are not treating or employees downloading large amounts of patient data.
- A retail company could use POLA to prevent data breaches. The company could monitor data exfiltration patterns and identify any unusual activity, such as large amounts of data being transferred to external servers or data being transferred to unusual locations.

Benefits of Using POLA for IT Security

There are a number of benefits to using POLA for IT security, including:

- Improved threat detection: POLA can help organizations to detect threats more quickly and effectively.
- Reduced risk of data breaches: POLA can help organizations to reduce the risk of data breaches by identifying threats early on.
- Improved compliance: POLA can help organizations to improve compliance with data protection and privacy regulations.

Challenges of Using POLA for IT Security

There are also some challenges associated with using POLA for IT security, including:

- Data collection and privacy: POLA systems require a large amount of data to be effective. It can be difficult and expensive to collect this data, and there are privacy concerns associated with collecting and using this data.
- Bias: POLA systems can be biased, which can lead to inaccurate or discriminatory results. It is important to take steps to mitigate bias in POLA systems.
- Transparency: It is important to be transparent about the use of POLA systems. This includes informing employees about how the systems work and what data is collected.

Conclusion

SARAHAI™ Tensor Networks, Inc. All Rights Reserved www.tensornetworks.com

POLA is a powerful tool that can be used to enhance IT security. However, it is important to be aware of the challenges associated with using POLA and to take steps to mitigate these challenges.

Recommendations

Here are some recommendations for organizations that are considering using POLA to enhance IT security:

- Start with a clear understanding of your goals. What do you hope to achieve by using POLA? Once you have a clear understanding of your goals, you can start to develop a POLA strategy that is tailored to your specific needs.
- Invest in a robust data collection and analytics platform. A good POLA platform will be able to collect and analyze data from a variety of sources, including security logs, network traffic data, and user activity logs.
- Implement appropriate privacy safeguards. It is important to implement appropriate privacy safeguards to protect the privacy of employees and customers. This includes obtaining consent before collecting data and limiting the use of data to the purposes for which it was collected.
- Be transparent about the use of POLA. It is important to be transparent about the use of POLA systems. This includes informing employees about how the systems work and what data is collected.

By following these recommendations, organizations can use POLA to improve their IT security posture and reduce the risk of cyberattacks.

SARAHAI™ Tensor Networks, Inc. All Rights Reserved www.tensornetworks.com