Implementing Artificial Intelligence in the Security Operation Center

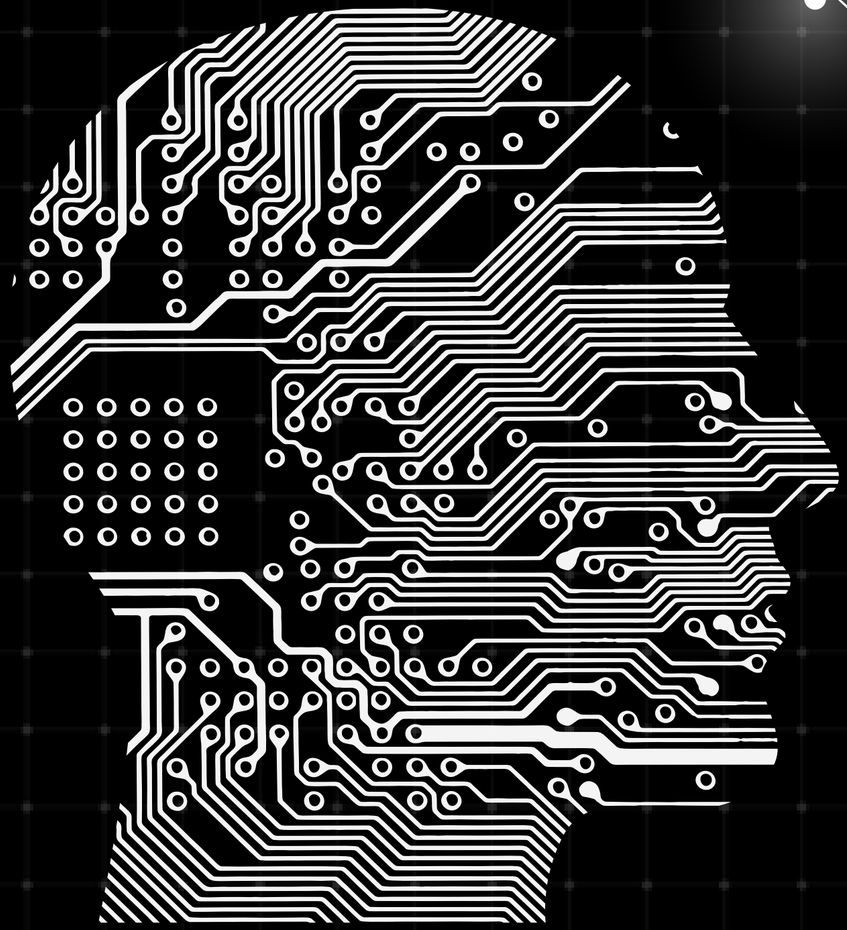
Le Minh Nguyen

Riaa Sehgal

Table of Contents

01

Introduction

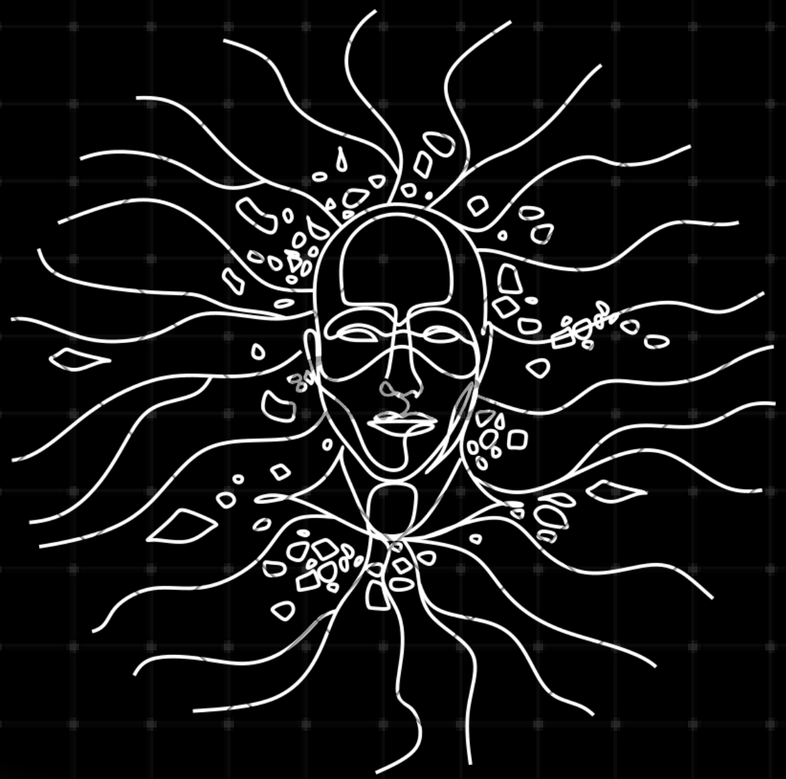


Purpose of Our Research

The rapid evolution of cyber threats has made implementing sophisticated safeguards essential for protecting digital ecosystems. Security Operation Centers (SOCs) are at the forefront of this defense, requiring cutting-edge tools to adapt and mitigate risks as threat actors employ increasingly complex tactics.

Our research aims to revolutionize the efficiency and effectiveness of Security Operation Centers (SOCs) by integrating advanced AI-driven methodologies. The focus is on optimizing the collaboration between human analysts and AI systems to address the increasing complexity of cyber threats.

Purpose of Our Research



We investigate techniques that enhance threat detection, reduce alert fatigue, and improve decision-making processes within SOCs. By leveraging advanced frameworks like A²C and anomaly-based detection models, we seek to empower SOC analysts with tools that dynamically adjust to evolving challenges.

Ultimately, the goal is to create a robust, adaptable SOC framework that mitigates risks proactively, safeguards digital ecosystems, and stays ahead of adversaries in the ever-changing cybersecurity landscape.

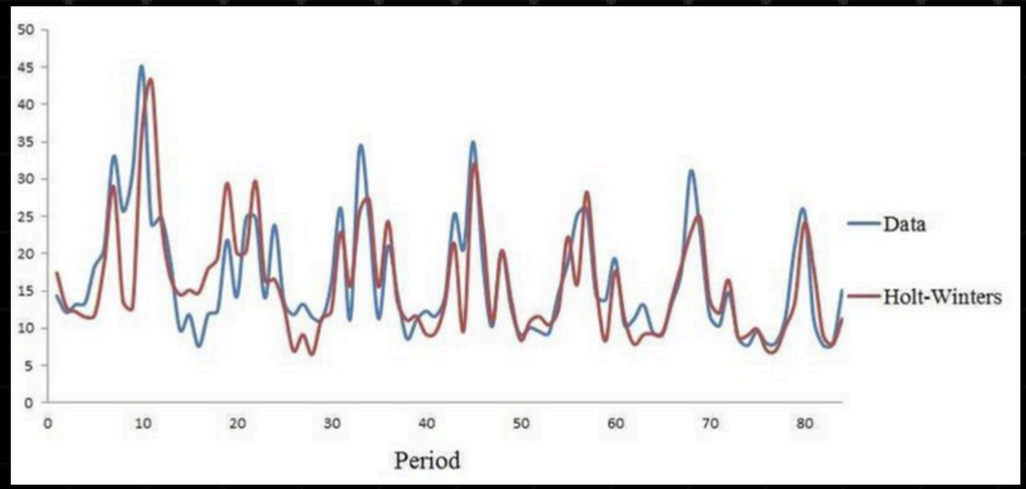
02

Related Work

Holt-Winters Forecasting

Holt-Winter Forecasting is a time-series forecasting models thats implemented in DL (Deep Learning) algorithms used for anomaly-based detection system.

- It performs statistical analysis to calculate and predicts the volume of incoming network traffic at different periods of time.
- The data on the volume of traffic are collected to compute the standard threshold, any activities that cause the traffic volume to surpass the calculated point will be count as an anomaly, this is effective in spotting DDos attacks.



Holt-Winter Forecasting

In order to calculate the threshold, it first needs 3 components, the Baseline, Linear Trend and Seasonal Trend.

$$y_{t+1} = a_t + b_t + c_{t+1-m}.$$

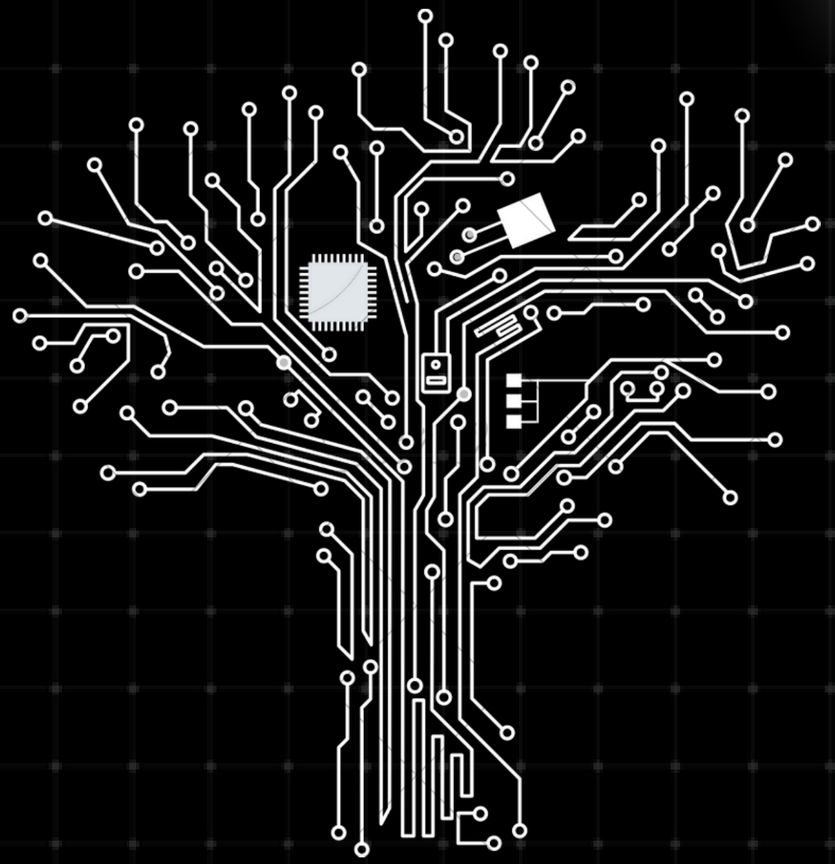
- Baseline (at): average volume of data at any given time of the day.
- Linear Trend (bt): data volume resulting from organizational changes (network growth or policy changes).
- Seasonal Trend (ct) shows the fluctuations of data during the day, (ct+1-m) is the prediction of the seasonal coefficient based on the previously computed coefficient within the same period of the cycle.
- The addition of all three components creates the future forecast of the data (yt+1).

Interval of deviation

$$\hat{y}_t \pm \delta \times d_{t-m}.$$

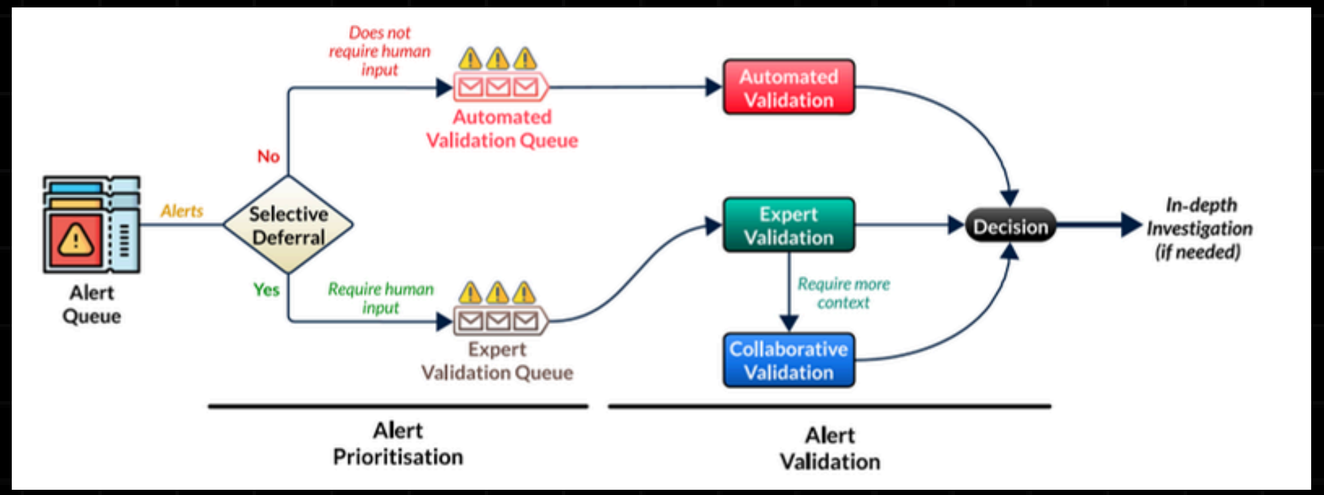
03

Proposed Solutions



Enhancing SOC Efficiency with A²C Framework and Human-AI Collaboration

Incorporating machine learning into Security Operations Centers (SOCs) presents challenges in adapting to real-world business operations. The A²C framework offers flexibility in adjusting AI's automation levels —Full Automation, Selective Deferral, and Collaborative Exploration. This adaptability supports SOC analysts by reducing their mental workload during the triage analysis process.

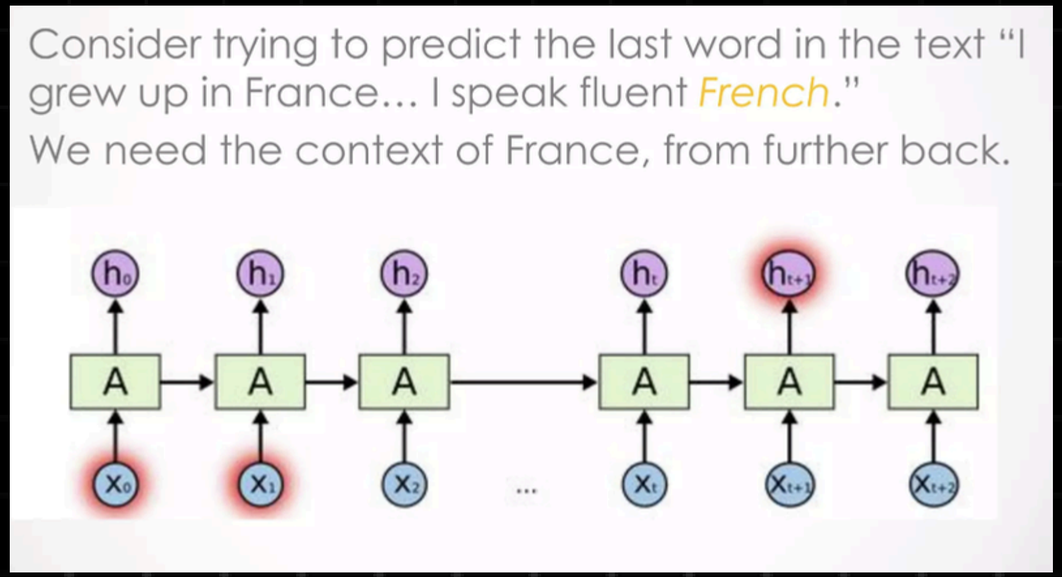


If AI encounters uncertainty, the alert is deferred to human experts for in-depth analysis, this is a feature of Shared situational awareness (SA)

In Threat Hunting, AI collaborates with analysts to spot vulnerabilities and mitigate potential threats before they escalate.

Advancing Malware Detection with LSTM Networks

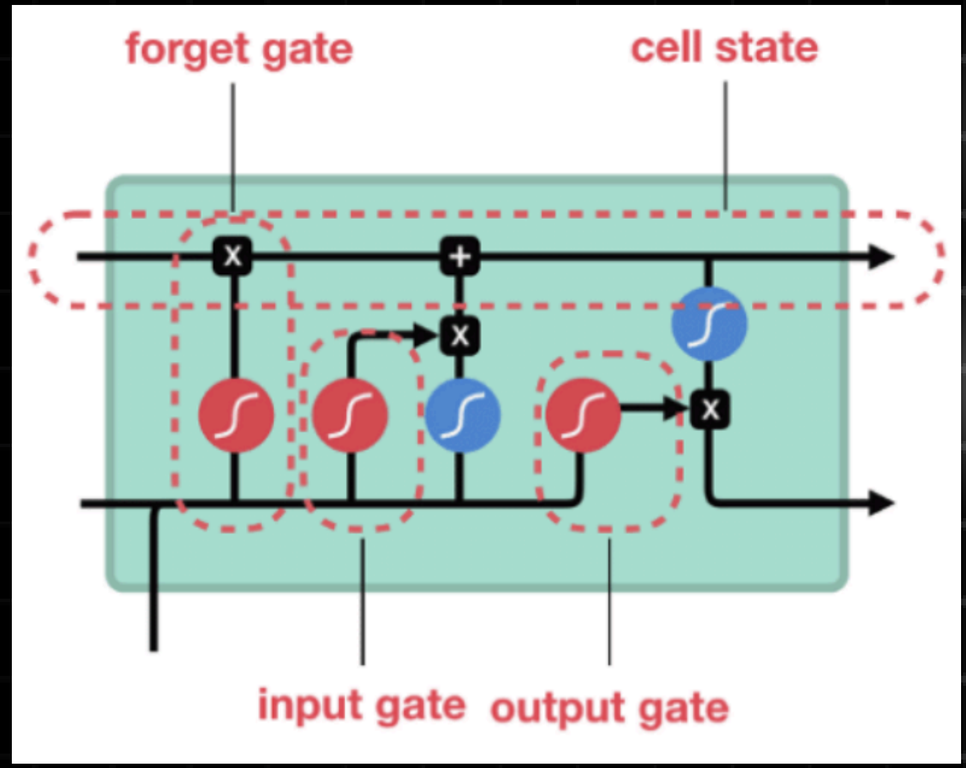
Anomaly-based detection techniques offer clear advantages over signature-based system which struggle to detect unknown threats. Deep learning algorithms, such as Recurrent Neural Networks (RNNs), are effective in identifying sequential data patterns, but they face limitations, including vanishing gradients and difficulty managing long-term dependencies.



Advancing Malware Detection with LSTM Networks

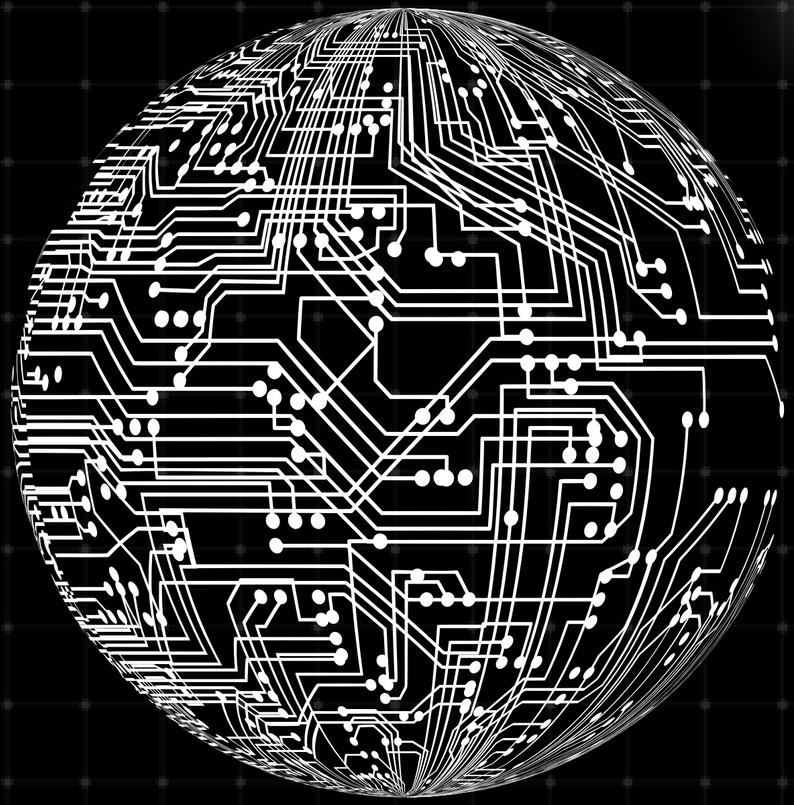
To address these issues, Long Short-Term Memory (LSTM) networks are integrated into the anomaly detection process. LSTM networks utilize memory cells and gating mechanisms—input, forget, and output gates—to efficiently store relevant data over extended periods, enabling detection of changes in long-term patterns.

- Forget gate: Determine which information from the previous cell state should be discarded
- Input gate: Decides which part of the input should be written
- Output gate: Choose which part of the cell state to influence the current output, filtering only useful information for the next cell state



04

Limitations



Challenges of Anomaly-Based Detection

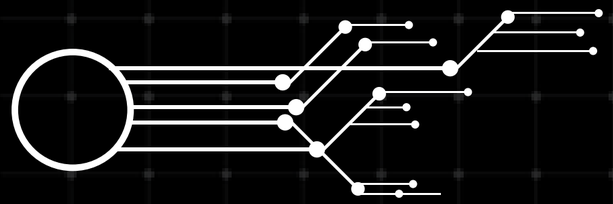
While anomaly-based detection systems using advanced deep learning algorithms like Holt-Winters Forecasting and LSTM networks represent a breakthrough, they face significant real-world challenges.

One critical issue is model bias and false positives, often caused by insufficient or non-diverse training data. These false alarms can overwhelm analysts, leading to alert fatigue and the risk of real threats being overlooked.

Another challenge is integration with existing SOC workflows. Many AI models prioritize computational efficiency over practical operational compatibility, forcing SOC analysts to adapt their processes to the technology rather than vice versa.

How do we Overcome these Limitations?

Enhancing adaptability is key to ensuring that AI systems can dynamically respond to the demands of complex, ever-changing cybersecurity environments.

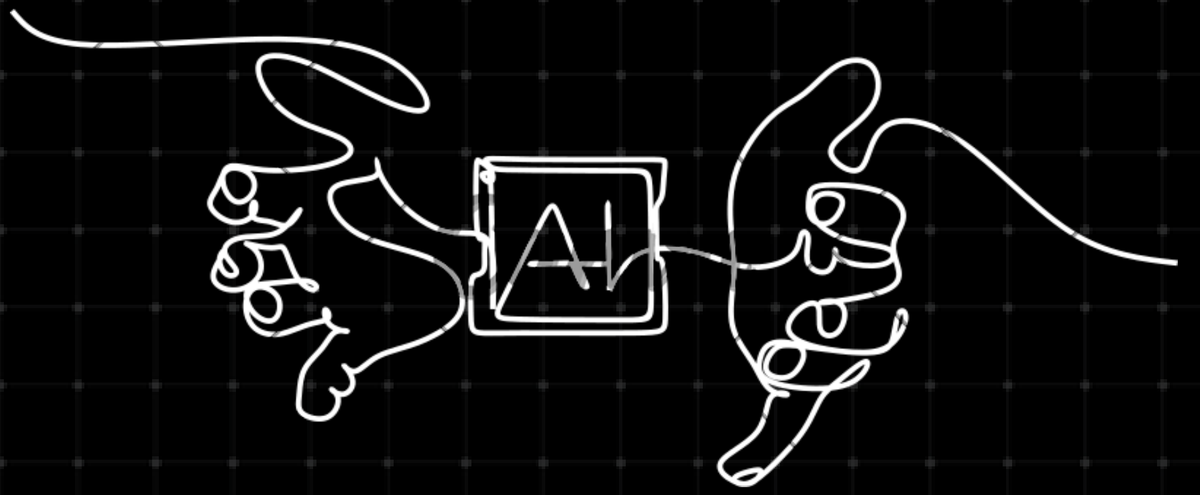


Efforts must also focus on reducing resource requirements to make these models more practical for real-world adoption. This includes minimizing false positives and streamlining system efficiency.

Seamless integration with SOC processes is essential. Future advancements should prioritize building AI systems that enhance existing workflows rather than disrupt them, creating a harmonious human-AI collaboration for robust digital security

05

Conclusion



Closing Insights

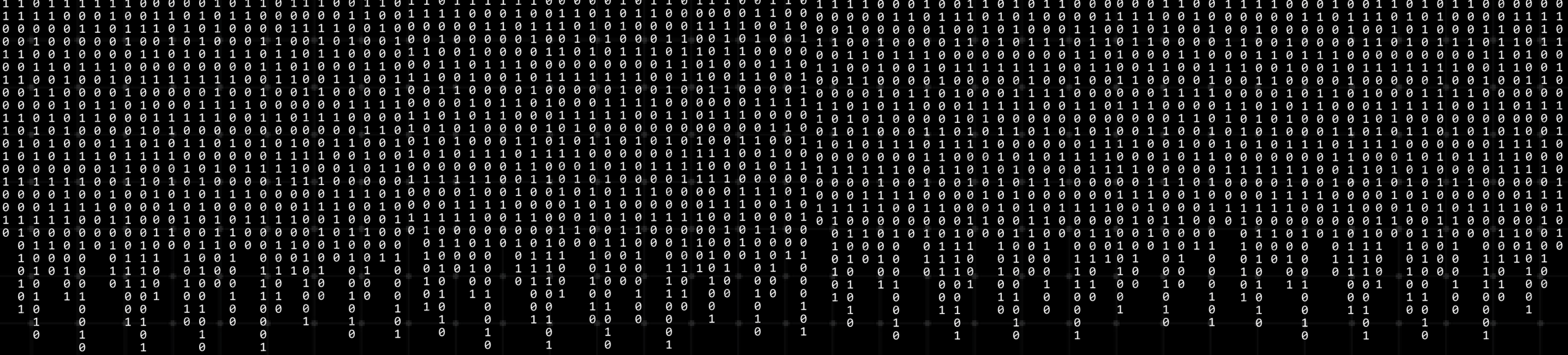
The integration of cutting-edge AI technologies, including deep learning and generative AI, marks a pivotal advancement in the capabilities of Security Operations Centers (SOCs) to address modern cyber threats. Tools such as Holt-Winters Forecasting and LSTM networks empower SOCs to detect intricate anomalies and proactively counter evolving attack vectors.

This exploration reaffirms the potential of AI-driven solutions to redefine SOC operations, equipping them to protect dynamic digital ecosystems against an ever-evolving threat landscape.

Thank You

Le Minh Nguyen

Riaa Sehgal



Q&A

Feel free to ask any questions!