How Enterprises Use ML in Cybersecurity Operations

Song Luo

March 2024

I am:

Researcher
Developer
Visionary

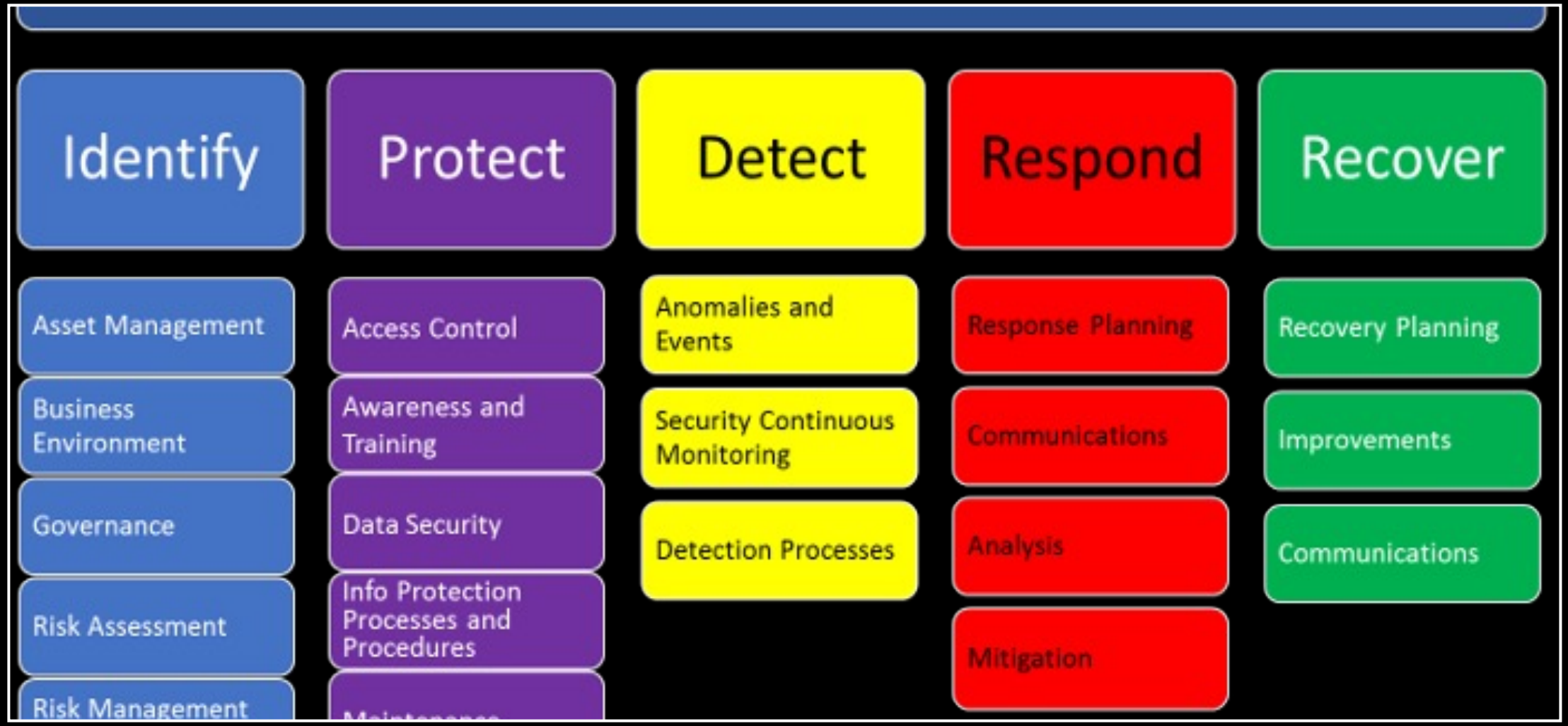
I care about:

Security
Efficiency
Happiness

- My interest:
  - Machine learning and AI
  - Security and Privacy
  - Coding and building
- My experiences :
  - Currently director of machine learning at Capital One
  - Led R&D teams in financial and tech industries
  - Focus on transforming advanced technologies into real values

Cyber Team Responsibilities

- Protection
- Incident Response
- Assessment and Audit
- Policy Development
- Compliance
- Employee Education



NIST Cybersecurity framework

Typical use of machine learning in cybersecurity: A detection-centered approach

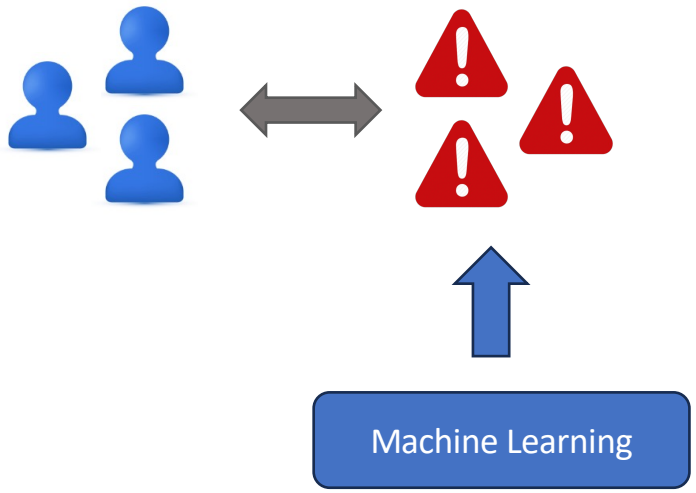
Purpose: directly identify potential threats before they escalate and cause significant damages

Examples:

- Virus and Malware detection with supervised classification and reinforcement learning
- APT detection with graph theory
- Anomaly detection with unsupervised learning

Advantages:

- It helps cybersecurity teams to be able to detect threats from large data sets, and sometimes be able to discover unknown threats



Use cases of detection-centered approach

Successful:

Detecting malicious URLs used by C&C

Detecting malicious web content

Detecting power shell commands used by virus and malwares

Not so successful:

Malware reverse engineering

Automatic signature generation

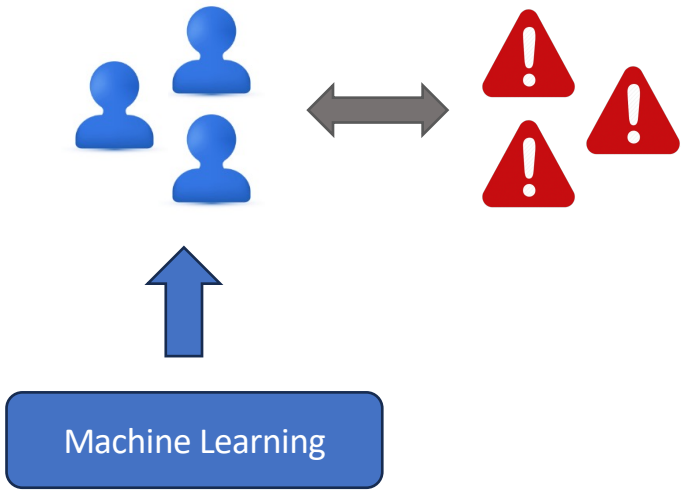
Malicious behavior detection using security logs

The challenges of detection-centered approach

- Challenges of ML in Threat Detection:
  - Scarcity of labeled data for training
  - Adversarial nature of cybersecurity
  - Rapidly evolving cyber threat landscape
  - Demand for explainable models
- Impact on ML results:
  - Low accuracy in threat detection
  - High rates of false positives
  - Sensitivity to data quality

Human-centered approach of applying ML in cybersecurity

- Human-centered AI complements detection-centered AI by enhancing human analysts' decision-making abilities.
- It provides insights and automations to allow focus on complex cybersecurity threats.
- Recognizes the irreplaceable value of human intuition and expertise in facing cybersecurity challenges.
- Fosters a collaborative dynamic between technology and human operators for more efficient threat handling.
- Maximizes the analytical capabilities and efficiency of cybersecurity teams by working alongside them.



Why human-centered approach now?

- Necessity:
  - We need more human intuition and expertise to deal with the ever-increasing complexity of cybersecurity operations.
- Capability:
  - The capability of generative AI has reached to the degree that it can help human analysts on some cognitive tasks.

Use Case No. 1: Correlation for Anomaly Detection

- Anomaly Detection in Cybersecurity:
  - Utilizes systems to identify abnormal activities in logs.
  - Targets anomalies caused by attacks or valid operations under unusual conditions.
  - Primarily operates on time series data from single sources (e.g., firewalls, endpoint protection software).

- Challenges with Anomaly Detection:
  - Difficulty in pinpointing root causes from a single data source.
  - Necessity to correlate alerts with additional data for comprehensive understanding.

- AI-Assisted Solution:
  - Understands the nature of the anomaly from event reports, including data source and statistical characteristics.
  - Identifies relevant additional data sources for context enrichment.
  - Automatically retrieves and consolidates data from these sources, generating insightful summaries.

Use Case no. 2: text-to-detection with AI

- Text-to-Detection AI for Cybersecurity:
  - Automates the process of building new detection rules for emerging threats.
  - Reads and interprets cyber threat intelligence reports to understand new challenges.
  - Identifies necessary data sources for effective threat detection.
  - Generates and translates detection rules into query formats like SQL for testing.
- Positive Impacts:
  - Enhances speed and accuracy in developing detection rules.
  - Improves the cybersecurity team's ability to rapidly and accurately counter new threats.

Use Case no. 3: remediation for software vulnerabilities.

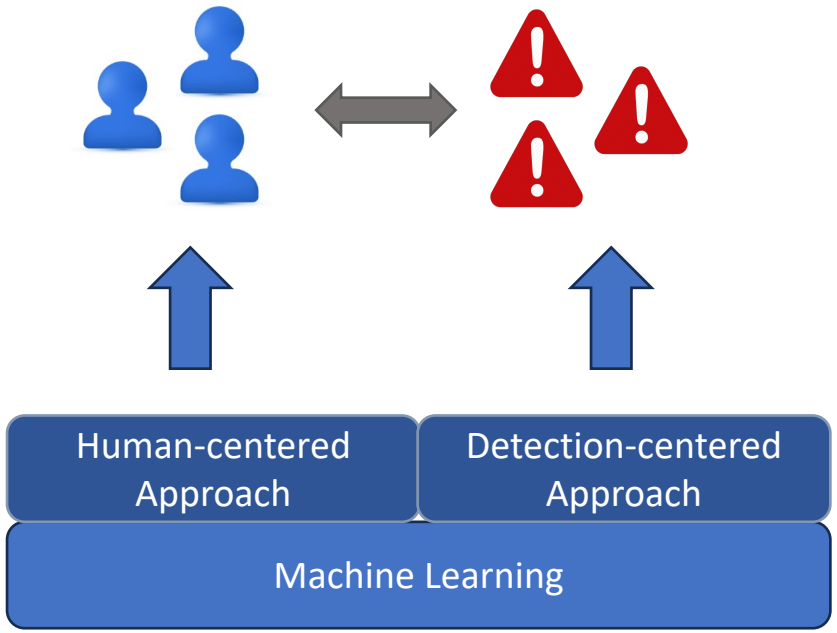
- Software Vulnerability Remediation AI Tool:
  - Identifies software vulnerabilities scanned by tools like Checkmarx.
  - Recommends remediation strategies by referencing similar, previously fixed cases.
  - Consumes and analyzes internal documentation on past vulnerability fixes.
- Positive Impact:
  - Provides specific remediation guidance to engineering teams lacking expertise.
  - Reduces the time taken to fix vulnerabilities by leveraging internal knowledge.
  - Minimizes false positives in vulnerability scanning, streamlining the development process.

Potential Challenges and Limitations of Using Generative AI

- Difficulty in understanding the context and nuances of cybersecurity incidents.
- Potential for bias and hallucinations in AI-generated recommendations.
- Challenges in integrating with existing cybersecurity tools and processes.

Conclusion

- Both human-centered and detection centered approaches are important for cybersecurity operations
- They complement to each other
- Human-centered approach may receive more attention in the near future
- Generative AI is expected to be used in both detection-centered and human-centered approaches, with cautions



Q&A