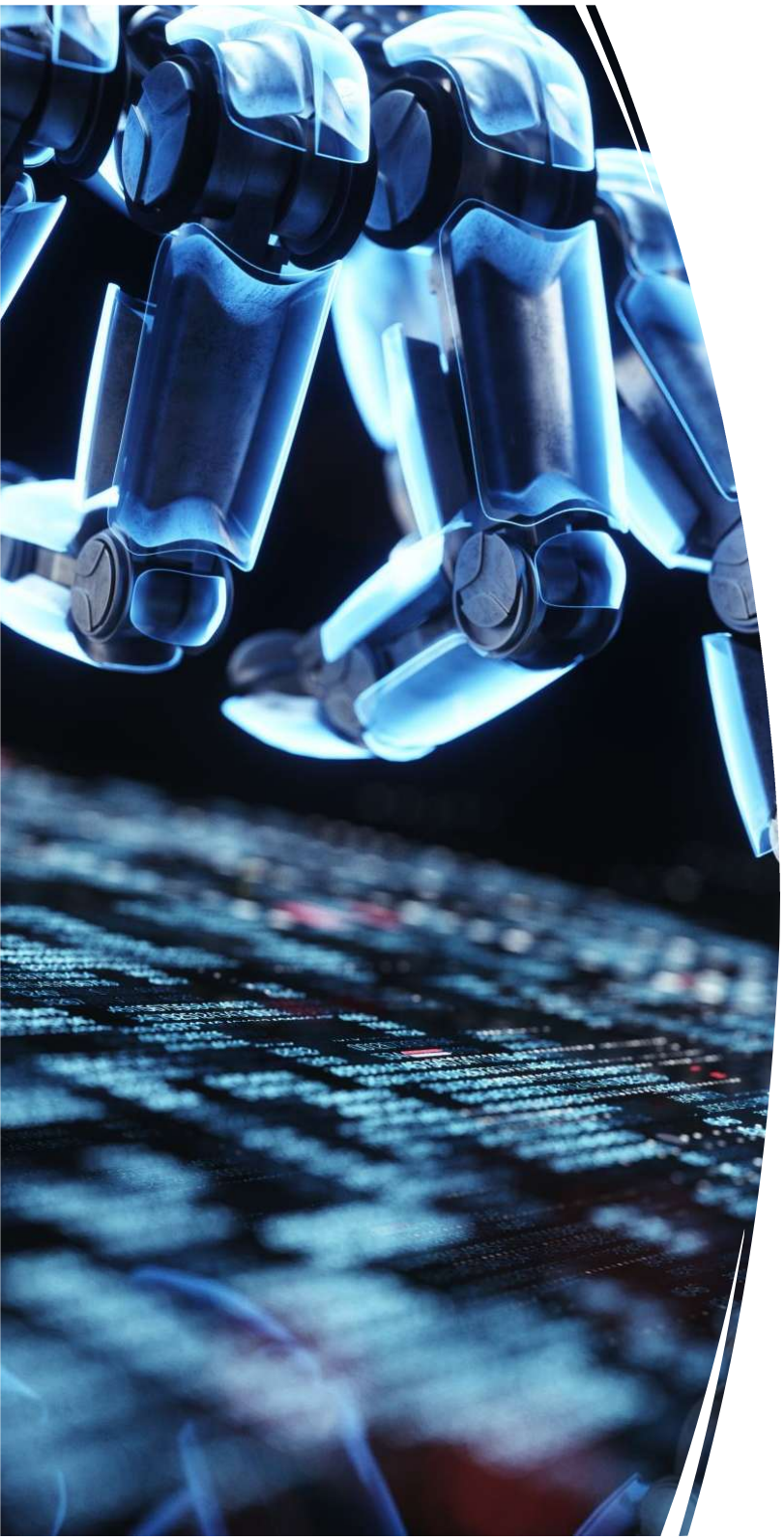


AI & Security:
Smarter Defense with Machine Learning

Leveraging AI, ML, and GenAI to Enhance Cybersecurity

Core AI Security Elements

Security Challenges, Approaches and Values

- Identify User Access Anomalies
- Spot Potential Insider Threats
- Detect Domain Generation Algorithms (DGAs)
- Identify Command Line Anomalies
- Using ML for Threat Hunting
- Detect Malicious Network Traffic
- Detect Fraudulent Activity
- Predict Data Downtime
- Demystify Security Searches with an AI Assistant

Summary of AI Security Elements

Core AI Security Elements

Detect anomalies & outliers

– Identify unusual behaviors in data and responses

Forecast deviations

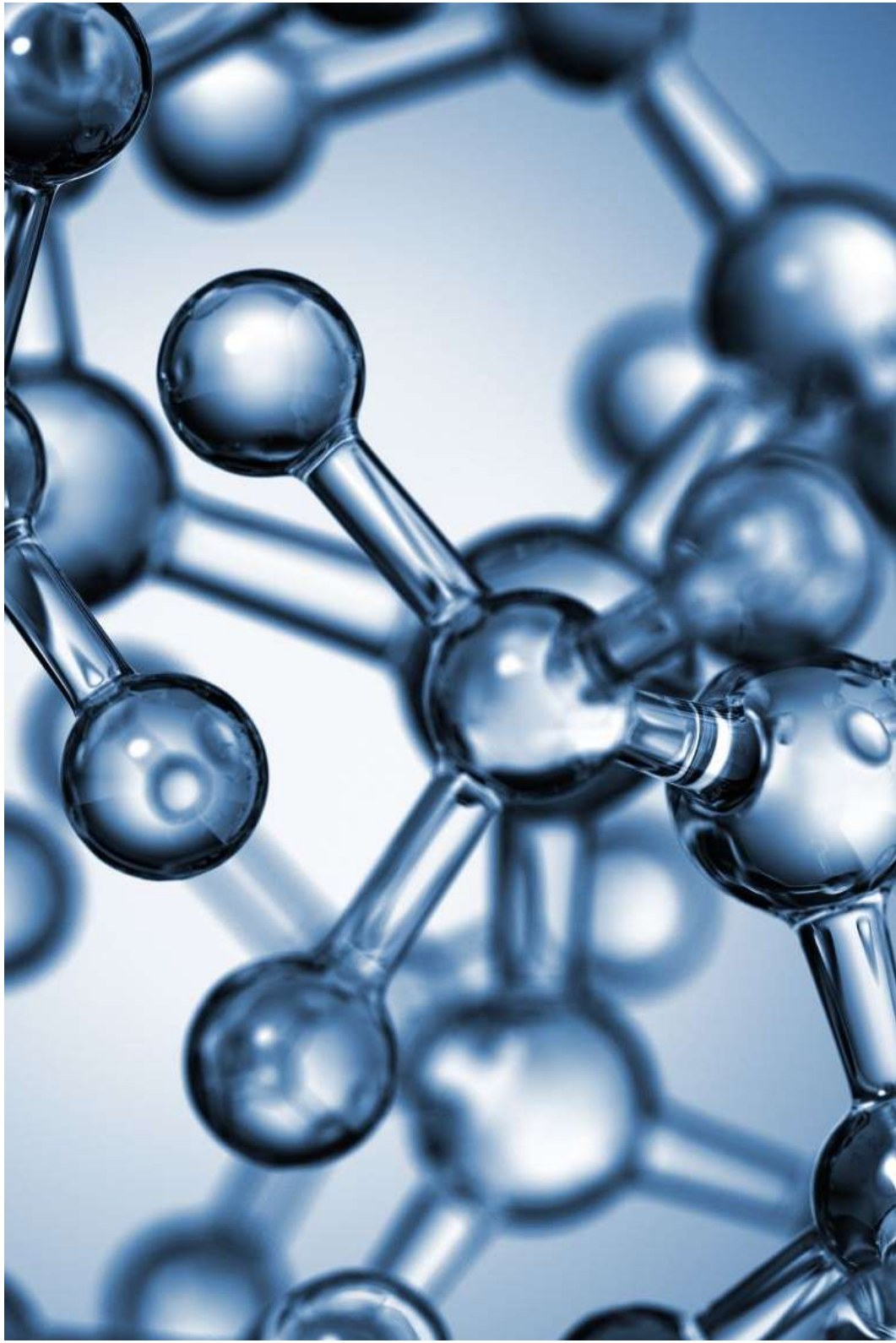
– Predict irregular activity before it escalates

Predict threats

– Spot potential botnet or malware activity

Cluster suspicious logs

– Group unusual patterns for faster triage



Identify User Access Anomalies

- **Business Challenge:**
  - 71% of cyberattacks start with compromised credentials
- **Approach:**
  - Use ML agents to baseline login activity
  - Detect brute force attempts via failed logins
  - Create profiles of user behavior
- **Value:**
  - Faster detection of compromises
  - Reduced manual log analysis
  - Lower overall risk exposure

Spot Potential Insider Threats

Business Challenge:

- Insider threats can involve data leaks, espionage, or misuse of privileges
- Hard to differentiate between normal and malicious behavior

Approach:

- Monitor changes in user behavior
- Use ML analytics for data exfiltration & unusual access patterns

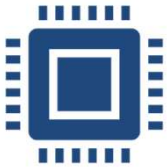
Value:

- Detect risks earlier
- Reduce false positives
- Guide analysts to focus on high-priority threats

Detect Domain Generation Algorithms (DGAs)

- **Business Challenge**:
  - Attackers use DGAs to create thousands of new domains daily
  - Traditional deny lists cannot keep up
- **Approach:**
  - Apply classification algorithms to detect algorithm-generated domains
  - Automate detection in real-time
- **Value:**
  - Faster and more efficient detection
  - Reduced manual domain tracking
  - Improved defense against C2 infrastructure

Identify Command Line Anomalies



Business Challenge:

Attackers use common tools or commands already present in the system

Hard to detect as they blend in with normal activity

Approach:

Train AI models to baseline normal command usage

Detect deviations indicating malicious use

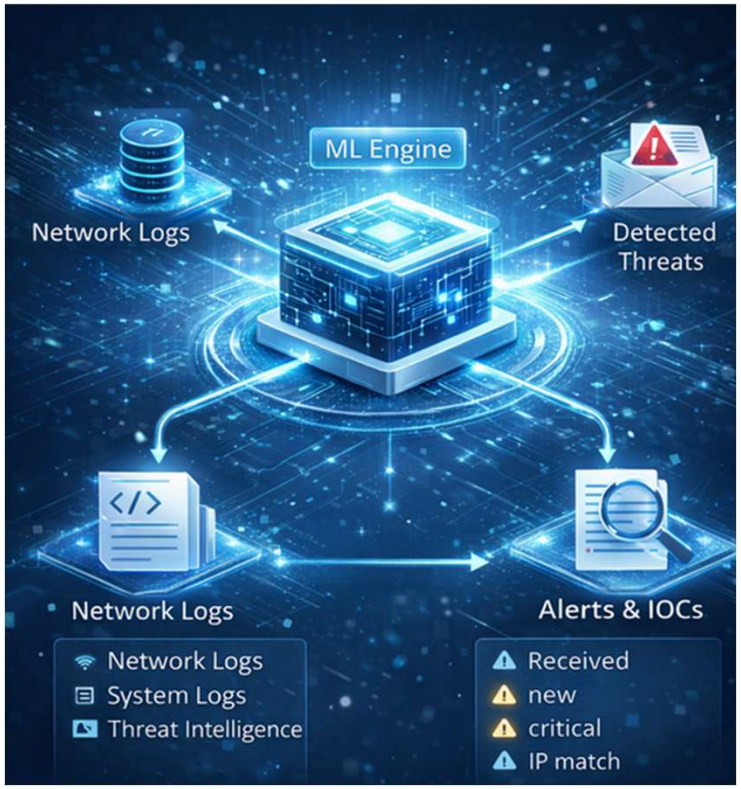
Value:

Early identification of malicious commands

Reduced time spent analyzing logs

Prevent attacks leveraging native tools

Use ML for Hunting Threats



Business Challenge:

Attackers constantly evolve tactics, bypassing traditional detection rules

Approach:

Deploy AI agents to scan security logs

Flag unusual events and anomalies for review

Value:

Identify sophisticated, previously unseen attacks

Enhances analyst efficiency

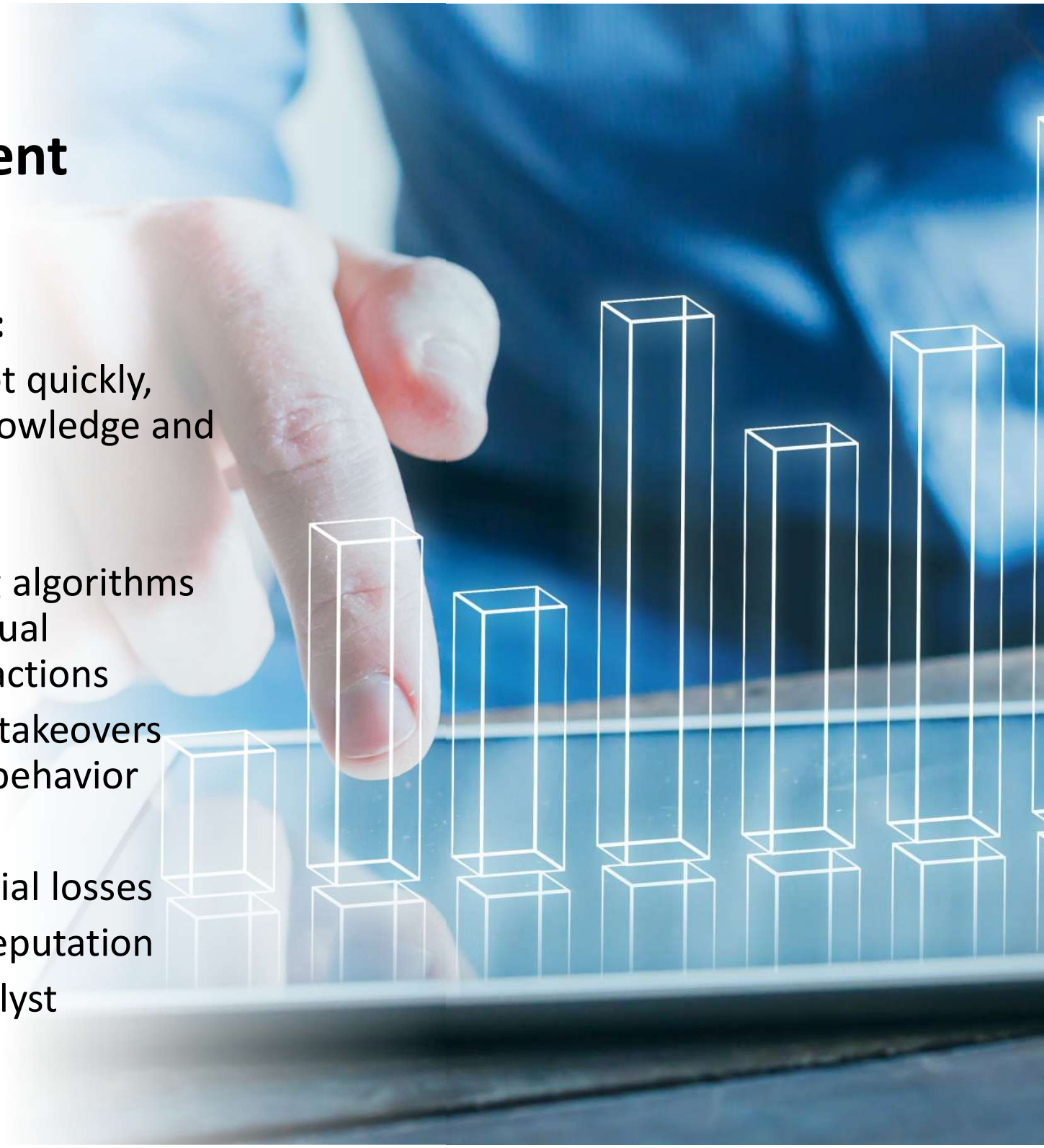
Builds new Indicators Of Compromise (IOCs)

Detect Malicious Network Traffic

- **Business Challenge:**
  - Network traffic generates large volumes of data, hiding malicious activity
- **Approach:**
  - Use AI agents to baseline normal network behavior
  - Detect unusual traffic spikes, port activity, and lateral movement
- **Value:**
  - Faster identification of network threats
  - Reduced noise for analysts
  - Improved network defense capabilities

Detect Fraudulent Activity

- **Business Challenge:**
  - Fraudsters adapt quickly, using insider knowledge and pivoting tactics
- **Approach:**
  - Apply clustering algorithms to identify unusual customer transactions
  - Detect account takeovers and suspicious behavior
- **Value:**
  - Minimize financial losses
  - Protect brand reputation
  - Boost fraud analyst efficiency



Predict Data Downtime

Business Challenge:

Data interruptions reduce visibility into system performance

Approach:

Collect host/system data using connectors

Train ML models to track normal event volumes

Flag anomalies in throughput and ingestion

Value:

Prevent service disruptions

Maintain operational resilience

Improve visibility of critical systems

Demystify Security Searches with an AI Assistant

Business Challenge:

Hundreds of detection rules make it hard to track purpose and logic

Employees rely heavily on tribal knowledge

Approach:

Use an AI Assistant to translate security requests into queries

Automatically generate documentation for search logic

Value:

Improves efficiency

Reduces reliance on a few experts

Provides transparency into detection rules

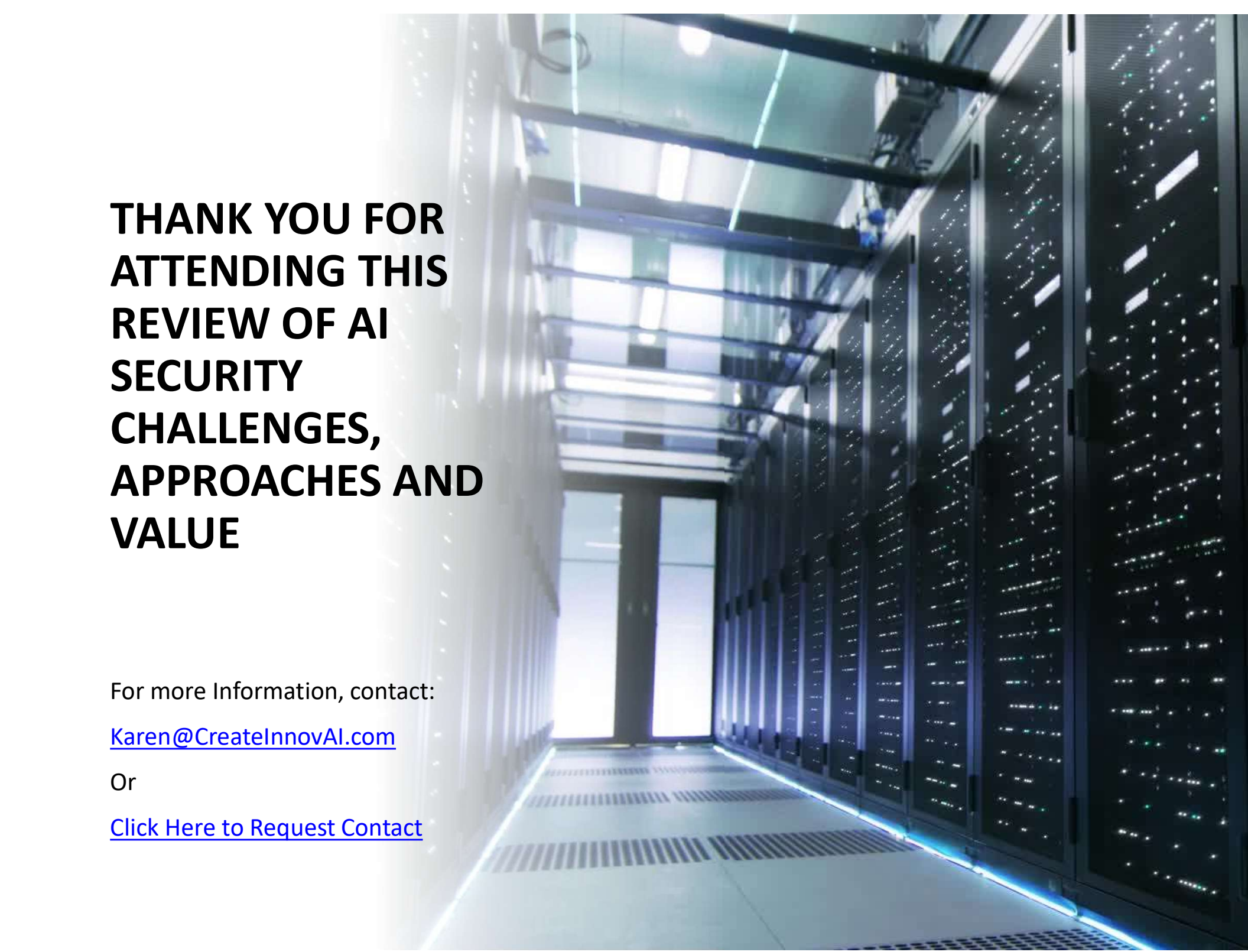
Summary of AI Security Elements

1. **User Access Anomalies** → Detect compromised credentials faster
2. **Insider Threats** → Spot suspicious insider behavior
3. **Domain Generation Algorithms** → Real-time DGA detection
4. **Command Line Anomalies** → Identify unusual command executions
5. **Threat Hunting** → Catch unknown sophisticated attacks
6. **Malicious Network Traffic** → Spot unusual network behaviors
7. **Fraudulent Activity** → Detect abnormal transaction patterns
8. **Data Downtime** → Monitor and prevent service disruptions
9. **AI Assistant** → Simplify complex searches and documentation

Overall Value:

- Faster detection
- Reduced manual effort
- Identification of unknown threats

THANK YOU FOR ATTENDING THIS REVIEW OF AI SECURITY CHALLENGES, APPROACHES AND VALUE



For more Information, contact:

Karen@CreateInnovAI.com

Or

Click Here to Request Contact