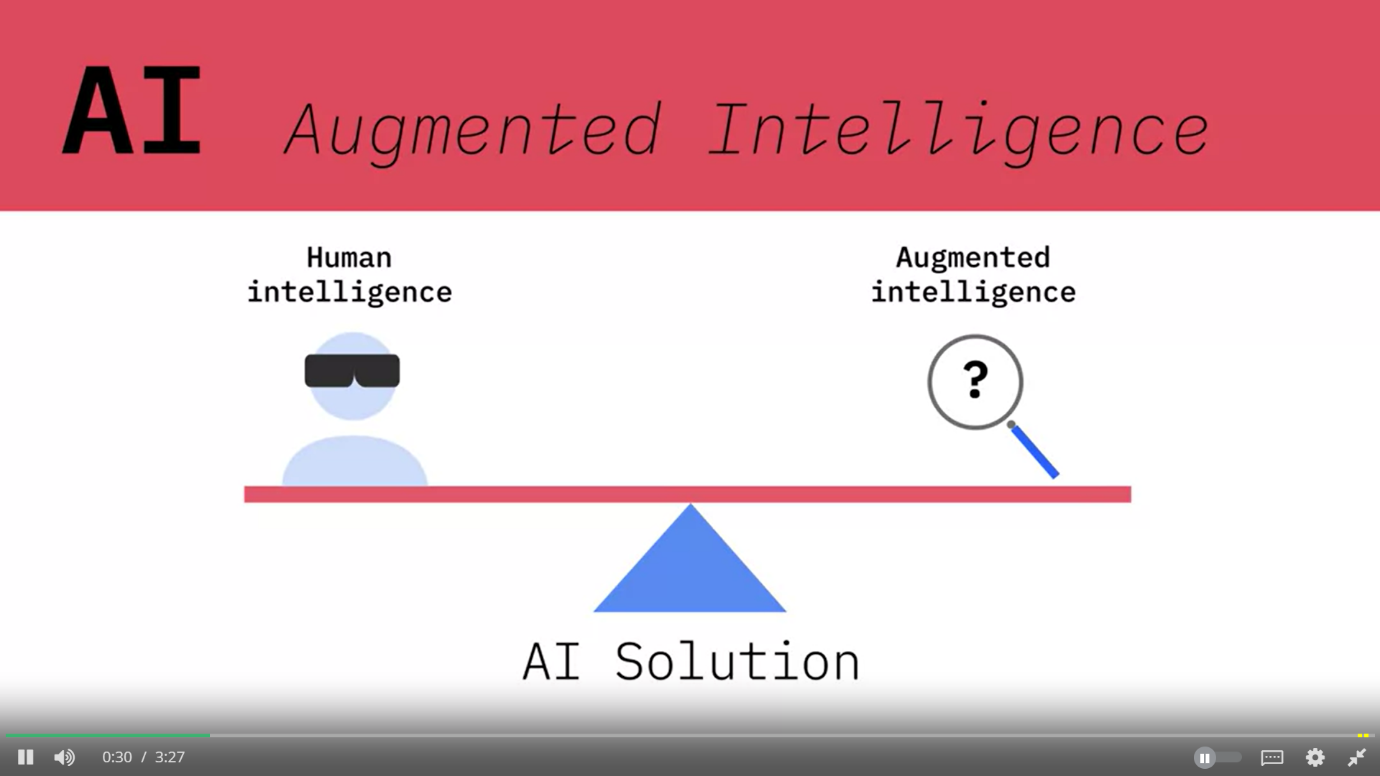
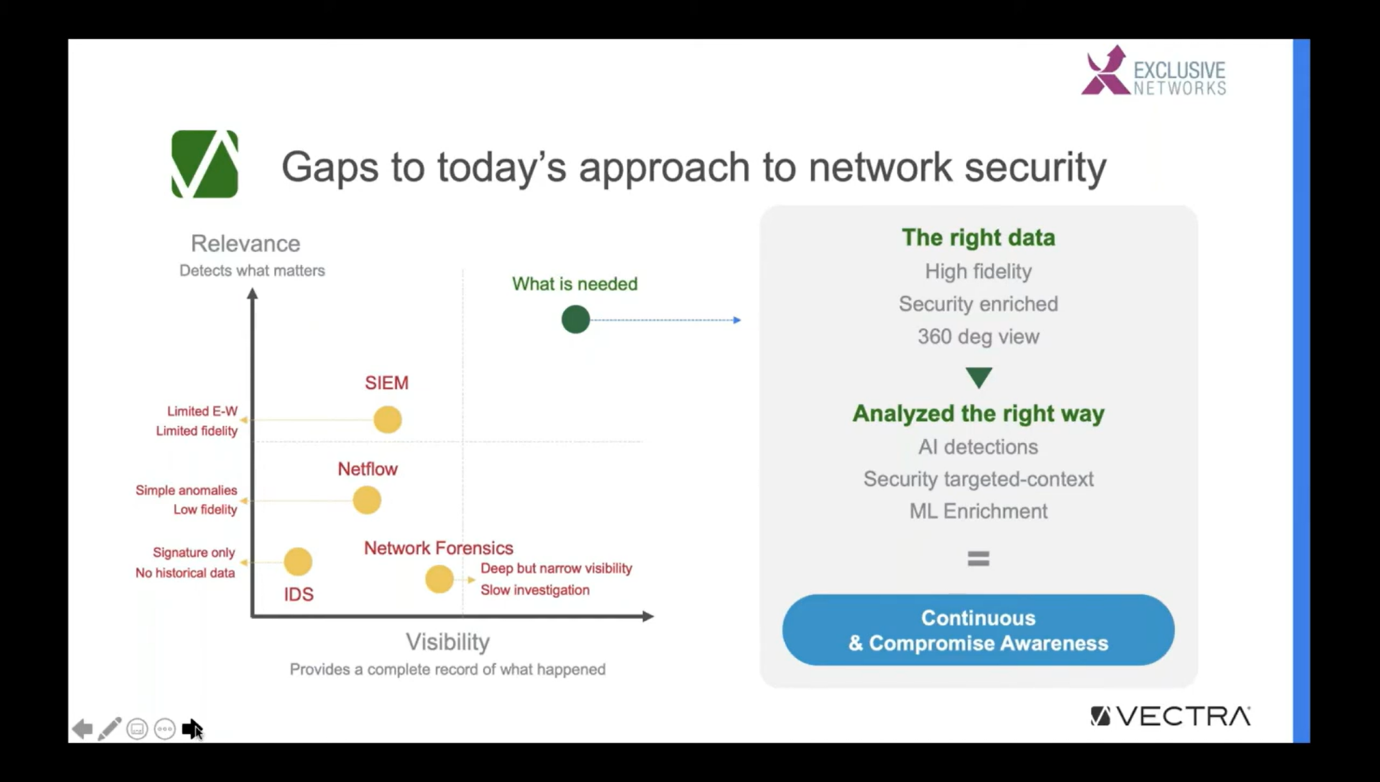
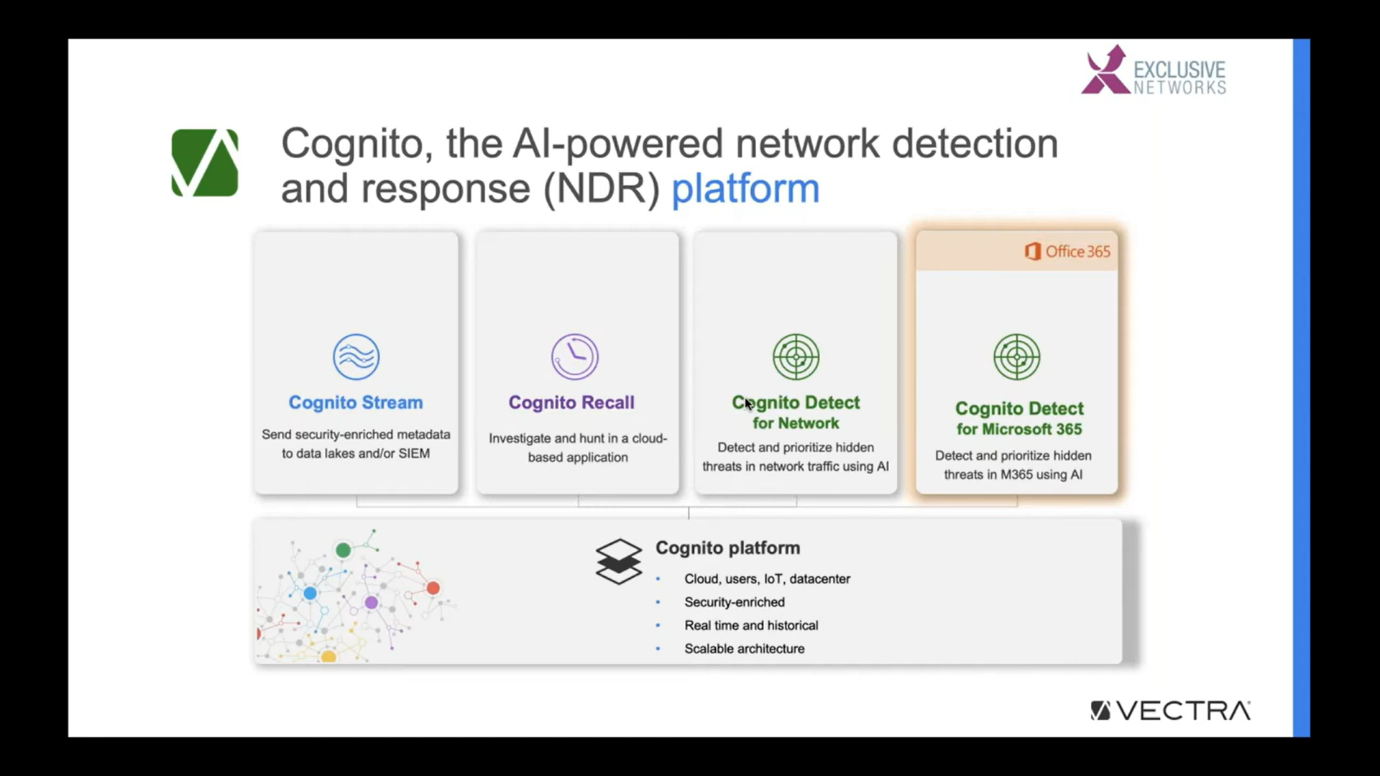
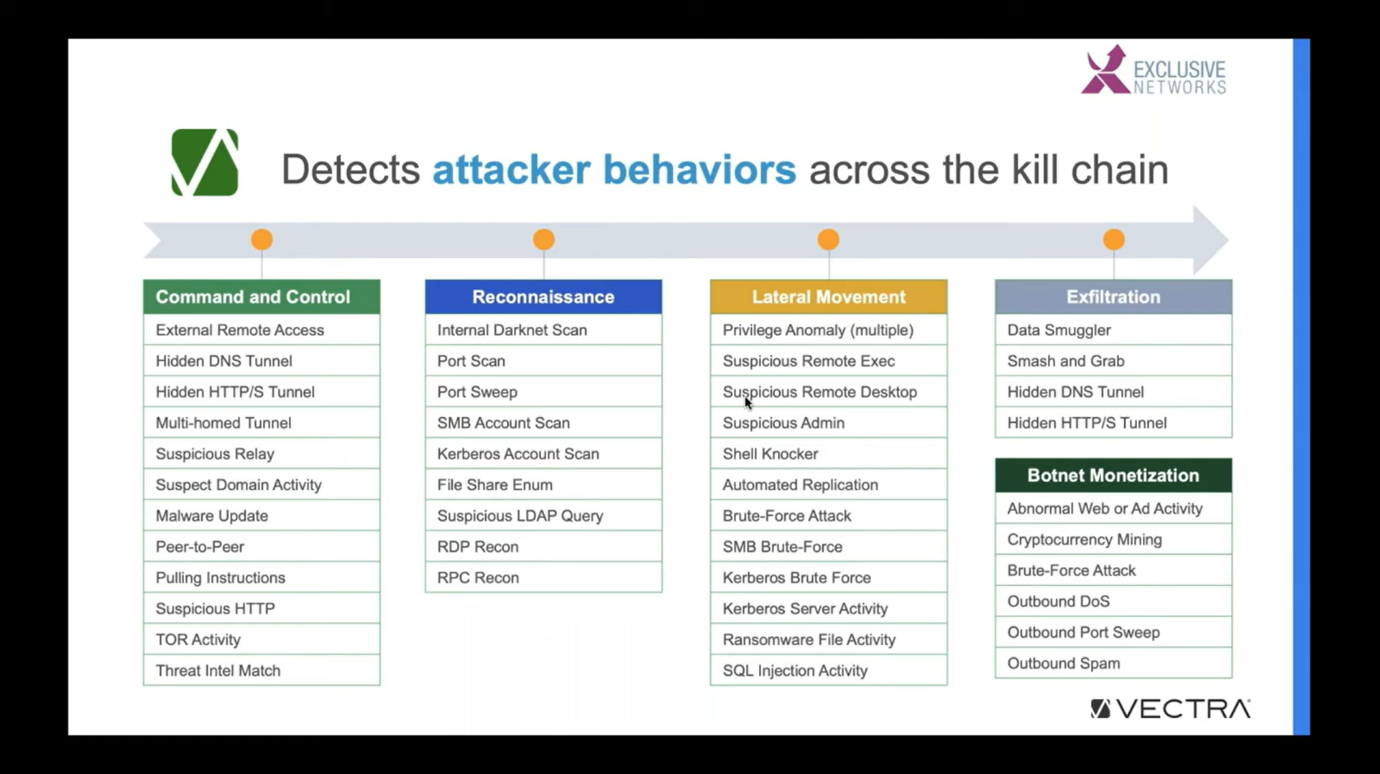
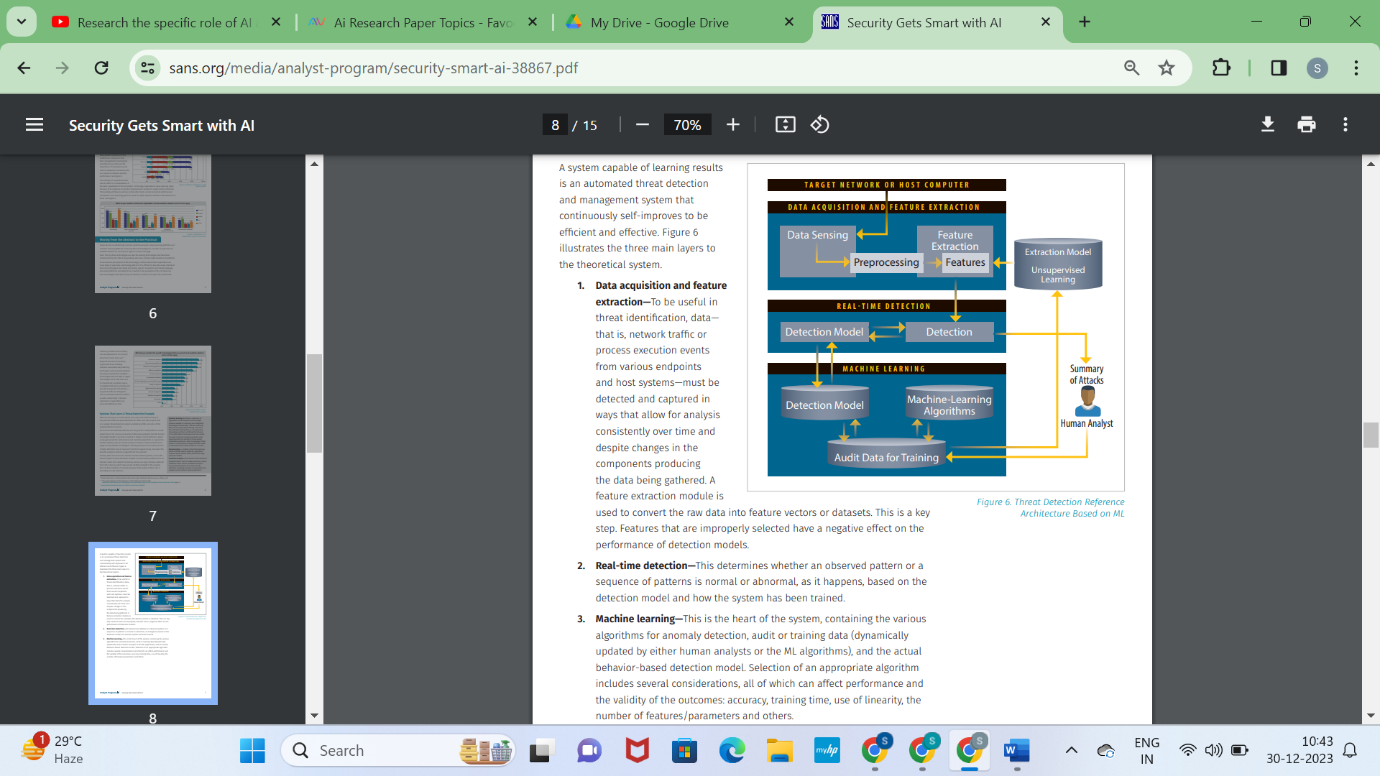
**AI-Based Threat Identification Within SANS 20**











AI algorithms and techniques employed in threat identification, such as anomaly detection, behavior analysis, and predictive analytics, as per SANS 20's guidelines.

**Anomaly Detection:**

1. **Role in SANS 20:** Anomaly detection plays a pivotal role in Control 1 - Inventory of Authorized and Unauthorized Devices and Control 2 - Inventory of Authorized and Unauthorized Software.
2. **AI Techniques:** Employing machine learning algorithms like unsupervised learning (e.g., clustering, isolation forests) and neural networks to identify deviations from normal patterns in device or software behavior. Any anomalies could indicate potential security threats or unauthorized activities.

**Behavior Analysis:**

1. **Relevance in SANS Controls:** Control 5 - Controlled Use of Administrative Privileges and Control 8 - Malware Defenses emphasize behavior analysis.
2. **AI Approaches:** Utilizing machine learning models for behavior analysis, including supervised learning for user behavior profiling, reinforcement learning for anomaly detection in privileged access, and natural language processing (NLP) for identifying suspicious patterns in logs or communication.

**Predictive Analytics:**

1. **Alignment with SANS Controls:** Control 4 - Continuous Vulnerability Assessment and Remediation and Control 10 - Data Recovery Capability benefit from predictive analytics.
2. **AI Methods:** Leveraging predictive modeling using machine learning techniques like regression, decision trees, or ensemble methods to forecast vulnerabilities, prioritize risks, and preemptively identify potential data loss or system failure scenarios.

**Machine Learning for Threat Detection:**

1. **Embedded in SANS Controls:** Control 11 - Secure Configuration for Network Devices, Control 14 - Wireless Access Control, and Control 19 - Application Software Security focus on secure configurations and access control.
2. **AI Application:** Utilizing supervised learning to establish baseline configurations and anomaly detection models to continuously monitor network settings, identify deviations, and secure access points, such as wireless networks or application security gaps.

**Natural Language Processing (NLP) for Log Analysis:**

1. **Within SANS Controls:** Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs and Control 13 - Data Protection benefit from NLP-driven analysis.

**AI Integration:** Utilizing NLP techniques to parse and analyze logs, extract meaningful insights, detect patterns, and identify potential security incidents or data breaches from unstructured log data.

**Integrating AI-Driven Threat Identification into the SANS 20 Framework**

The integration of AI-driven threat identification within the SANS 20 framework demands a strategic approach encompassing several best practices and recommended methodologies.

**Comprehensive Familiarization:** Gain a deep understanding of the SANS 20 Critical Security Controls framework, its objectives, and the specific security areas it addresses.

**Identify Alignment Points:**

**Mapping Controls to AI Capabilities:** Identify which SANS controls can benefit from AI-driven threat identification. Align AI capabilities with control objectives, emphasizing areas where AI can enhance threat detection, response, or risk mitigation.

**Select Appropriate AI Technologies:**

**Tailored AI Solutions:** Choose AI technologies based on the specific requirements of each control. For instance, anomaly detection, machine learning models, NLP, or predictive analytics might suit different controls within the SANS framework.

**Data Collection and Preprocessing:**

**Quality Data Acquisition:** Collect high-quality, diverse data relevant to the security controls. Ensure data preprocessing to clean, normalize, and prepare datasets for AI model training.

**Model Development and Testing:**

**Customized Model Building:** Develop AI models tailored to SANS controls' objectives. Test these models rigorously, validating their accuracy, precision, and recall rates in identifying threats aligned with control requirements.

**Continuous Monitoring and Adaptation:**

**Dynamic Model Maintenance:** Implement mechanisms for continuous monitoring of AI models. Regularly update and adapt models based on evolving threats, new attack patterns, or changes in the IT environment.

**Collaboration and Cross-Functional Integration:**

**Interdepartmental Collaboration:** Foster collaboration between cybersecurity, IT, and data science teams. Encourage knowledge sharing and alignment of AI-driven threat identification initiatives with broader organizational security strategies.

**Documentation and Reporting:**

**Clear Documentation:** Document integration processes, AI model configurations, and alignment strategies with SANS controls. Maintain detailed reports on AI model performance and their impact on threat identification within the framework.

**Compliance and Ethical Considerations:**

**Adherence to Standards:** Ensure AI integration complies with industry standards, regulations, and ethical considerations. Address privacy concerns and ethical use of data in AI-driven threat identification practices.

**Continuous Improvement and Adaptation:**

**Iterative Approach:** Embrace an iterative approach to refine AI-driven threat identification. Continuously assess and refine AI models, methodologies, and integration practices based on feedback, new threats, or technological advancements.