Université Concordia University

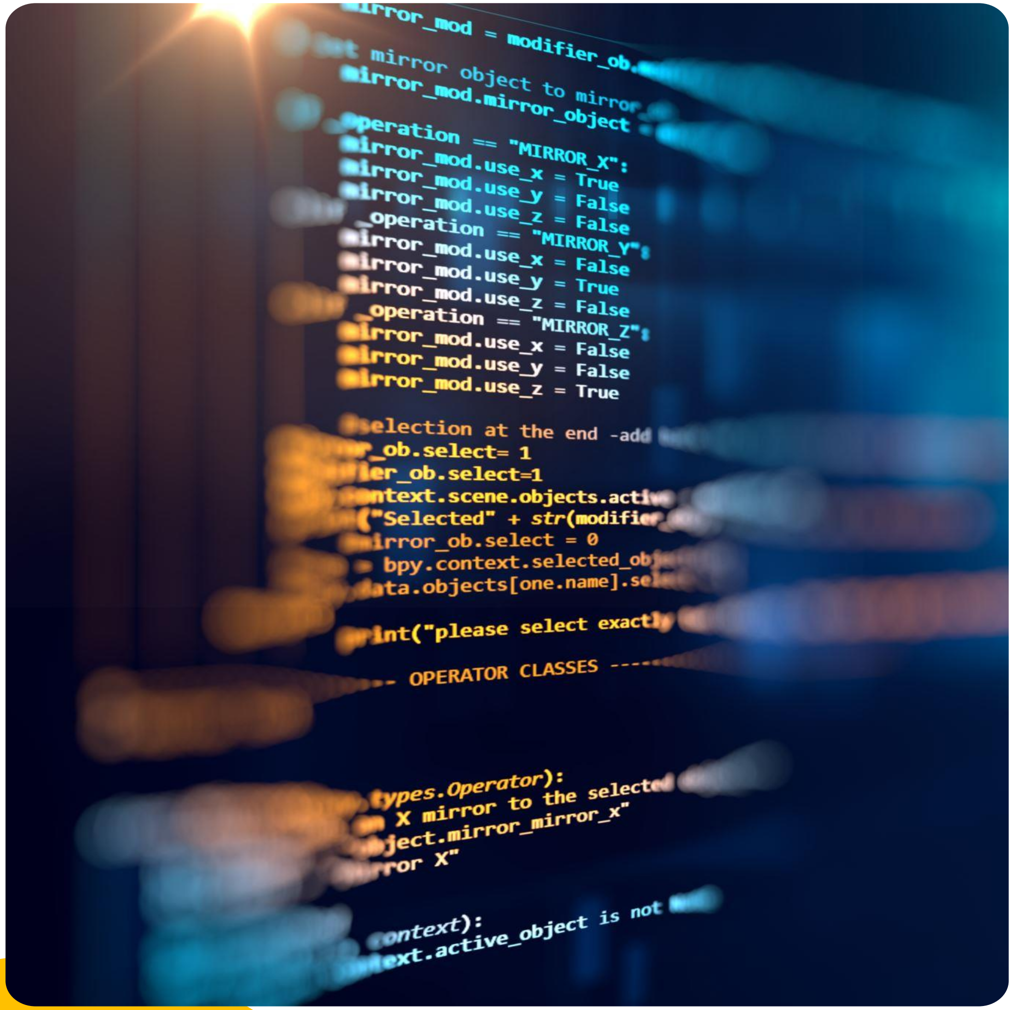
GINA CODY
SCHOOL OF ENGINEERING
AND COMPUTER SCIENCE

Log analysis for intrusion detection/investigation. Techniques using machine learning : A Survey

INSE 6610 – Cybercrime Investigation

Summer 2023

Gayatri Tangudu	40221830
Naveen Sesetti	40206610



Overview of IDS:

- Detects unauthorized access and malicious activities in networks.
- Role of IDS in Cybersecurity: Safeguarding against increasing cyber threats.
- Presentation Overview: Exploring IDS types, features, best practices, and integration with automated machine learning.

Types of IDS - Network-based IDS (NIDS) and Host-based IDS (HIDS)

- NIDS
- Monitors network traffic for suspicious patterns. Examples: Snort, Suricata.

- HIDS
- Monitors system activities on individual hosts. Examples: OSSEC, Tripwire.

Deployment Scenarios: NIDS at network entry points, HIDS on critical servers.

Key Features of NIDS and HIDS

- NIDS
- Packet analysis,
- traffic pattern recognition.

- HIDS
- File integrity monitoring,
- system log analysis.

Advantages and Disadvantages: NIDS offers network-wide view but might miss host-level threats; HIDS provides host-level insight but might miss network-wide attacks.

Comparison of Snort, Suricata, and Bro:

Snort: Widely adopted, Snort offers extensive customization and a robust community. It is ideal for various environments but may require additional configurations for high-speed networks.

Suricata: Engineered for speed and scalability, Suricata excels in high-speed network environments. However, its learning curve may demand initial effort.

Bro (Zeek): A versatile network security monitor, Bro can identify diverse network activities and allows intricate customization. Yet, its resource-intensive nature requires ample hardware.

Key Features of Each IDS:

Snort: Customizable rules for diverse threat detection.

Suricata: High-speed traffic analysis with multi-threading.

Bro: Detailed network activity analysis with scripting capabilities.

Advantages and Disadvantages of Each IDS:

- **Snort:** Pro - Large community, customizable. Con - Configuration complexity for high-speed networks.
- **Suricata:** Pro - Scalability, high-speed network support. Con - Steep learning curve.
- **Bro:** Pro - Versatility, extensive network activity detection. Con - Resource-intensive.

Best Practices for Implementing and Managing IDS Within Organizations

- Clear Objectives: Define the purpose and scope of IDS implementation.
- Up-to-date Rules: Regularly update intrusion detection rules and signatures.
- Integration with Other Tools: SIEM integration, enhanced threat visibility.
- Monitoring and Maintenance: Continuous monitoring, timely maintenance, and updates.

Integration with Security Information and Event Management (SIEM)

SIEM Overview: Centralized security management, event correlation.

IDS-SIEM Integration: Feeding IDS alerts into SIEM for comprehensive analysis.

Examples: Correlating IDS alerts with user activity logs for contextual insight.

Advantages of Automated Machine Learning in Intrusion Detection

AUTOMATED MACHINE LEARNING: UTILIZES ALGORITHMS TO IMPROVE ACCURACY AND REDUCE MANUAL EFFORTS.

BENEFITS: FASTER RESPONSE TIMES, ADAPTIVE THREAT DETECTION, SCALABILITY.

EXAMPLES: AUTOMATICALLY ADAPTING IDS RULES BASED ON EVOLVING THREATS.

Alleviating the Workload of Security Analysts with Automated Machine Learning

Analyst Workload: High volume of alerts and false positives.

Automated Machine Learning Assistance: Prioritizing alerts, reducing manual analysis.

Enhanced Efficiency: Analysts focus on complex threats, decision-making, and strategic planning.

Real-time Threat Detection and Response with Automated Machine Learning

Real-time Detection: Automated machine learning identifies threats as they occur.

Rapid Response: Automated mitigation actions triggered by machine learning algorithms.

Human Oversight: Human analysts validate and fine-tune automated responses.

Any Questions ?

Thank You!