Module 2: Anomaly Detection and Attack Prediction with Machine Learning

Adarsh KUMAR

Universitat Politècnica de Catalunya
Department of Computer Science

Project Coordinator:
Prof. Ilker Demirkol

MERiT Project
September 3, 2025

Co-funded by
the European Union

Outline of

Co-funded by
the European Union

Types of Anomalies in Cybersecurity

Anomaly detection identifies unusual patterns deviating from normal behavior. Understanding anomaly types helps tailor detection methods.

Three main types:

- Point anomalies
- Contextual anomalies
- Collective anomalies

MERIT

Co-funded by the European Union

Point Anomalies

Definition: A single data point significantly different from the rest.

Characteristics:

- Evaluated individually
- Single event suspicious on its own

Cybersecurity examples:

- IP sending unusually high traffic volume
- Login from an unseen geographic location
- Rare or never-before-seen system calls

MERIT

Co-funded by the European Union

Point Anomalies

Detection approaches:

- Statistical thresholds (e.g., z-score)
- Distance-based methods (k-nearest neighbors)
- Isolation Forest

MERIT

Co-funded by the European Union

Contextual Anomalies

Definition: Data anomalous in a specific context but normal otherwise.

Characteristics:

- Depends on surrounding context/environment
- Requires joint modeling of data and context

Cybersecurity examples:

- High traffic volume during off-hours
- User accessing sensitive files while on vacation
- Login failure spikes only suspicious during work hours

MERIT

Co-funded by the European Union

Contextual anomalies

Detection approaches:

- Time-series analysis
- Sequence modeling (e.g., LSTM)
- Context-aware statistical methods

MERIT

Co-funded by the European Union

Collective Anomalies

Definition: A group of related data points anomalous together, even if individuals are normal.

Characteristics:

- Pattern-based anomaly in groups of instances
- Often linked to coordinated or complex attacks

Cybersecurity examples:

- Sequence of slow port scans appearing normal individually
- Multiple failed logins across different accounts
- Coordinated malware activity on multiple hosts

MERIT

Co-funded by the European Union

Collective anomalies

Detection approaches:

- Clustering methods
- Sequence and graph-based models
- Hidden Markov Models (HMM), LSTM

MERIT

Co-funded by the European Union

Anomaly Types Summary

Anomaly Type	**Description**	**Example**	**Detection Technique**
Point Anomaly	Single unusual instance	Unusually large data packet	Statistical methods, Isolation Forest
Contextual Anomaly	Anomalous in context/environment	Login at unusual time	Time-series, LSTM, context-aware stats
Collective Anomaly	Group of related instances anomalous	Coordinated port scans	Sequence models, clustering, HMM

Choosing the right anomaly type is essential for precise detection, reducing false positives, and tailoring cybersecurity defenses effectively.

MERIT

Co-funded by the European Union

Attack Prediction in Cybersecurity

Goal: Predict cyberattacks before significant damage occurs using advanced ML techniques.

Key Aspects:

- Predicting lateral movement within networks
- Modeling attacker behavior over time
- Correlating threat intelligence feeds with local event logs

Co-funded by
the European Union

Predicting Lateral Movement

Definition: Attackers moving through a network post-compromise to escalate privileges/access resources.

Why predict?

- Prevent privilege escalation and data exfiltration
- Contain breaches before critical asset compromise

MERIT

Co-funded by the European Union

Predicting Lateral

ML Approaches:

- Sequence modeling (LSTM) to learn attacker paths
- Graph analysis of connectivity and access patterns
- Anomaly detection on unusual host access

Example Features: Frequency and sequence of host-to-host connections, user account usage, timing of suspicious activities.

MERIT

Co-funded by the European Union

Modeling Attacker Behavior Over Time

Attackers adapt tactics dynamically; modeling helps predict future actions.
Why model behavior?

- Capture evolving tactics, techniques, and procedures (TTPs)
- Detect multi-stage attacks more effectively

MERIT

Co-funded by
the European Union

Modeling Attacker Behavior Over Time

ML Approaches:

- Hidden Markov Models (HMMs) for attacker states inference
- Reinforcement learning simulating attacker-defender dynamics
- Behavioral clustering to identify attacker profiles

Applications: Forecast attack chains, identify APT patterns, understand attack timing/sequences.

MERiT

Co-funded by the European Union

Correlating Threat Intelligence with Local Logs

Purpose: Enhance situational awareness by linking global threat data with local events.

Why correlate?

- Detect external threats targeting your environment
- Validate suspicious local events against known threats
- Prioritize alerts based on external threat severity

MERIT

Co-funded by the European Union

Correlating Threat Intelligence with Local Logs

ML Techniques:

- Data fusion of heterogeneous sources
- Feature enrichment of logs with threat intelligence data
- Anomaly detection on enriched datasets

Use Cases: Flag connections to malicious IPs, detect malware via hash signatures, enhance behavioral models.

MERIT

Co-funded by the European Union

Attack Prediction Summary

Aspect	Purpose	ML Techniques	Examples
Predicting Lateral Movement	Anticipate attacker's network traversal	Sequence modeling, graph analysis	Unusual host-to-host connections
Modeling Attacker Behavior	Understand and forecast attacker tactics	HMM, reinforcement learning, clustering	Multi-stage attack prediction
Correlating Threat Intelligence	Combine global threat data with local logs	Data fusion, feature enrichment	Detecting known malicious IPs

MERIT

Co-funded by the European Union

Attack Prediction Summary

Attack prediction leverages machine learning to provide early warnings and deeper insight into attacker strategies. By anticipating lateral movements, dynamically modeling behaviors, and enriching local data with external threat intelligence, defenders can strengthen their proactive cybersecurity posture.

MERIT

Co-funded by
the European Union