Maldives Journal of Engineering and Technology
ISSN: 3007-6536 (Online)
https://mjet.mnu.edu.mv/

Zero-Day APT Detection Using OpenSet Recognition with Adaptive Feature Selection

Adam Khalid

Department of Computer Science, Faculty of Engineering, Science and Technology, The Maldives National University, Maldives;
**Corresponding: adam.khalid@mnu.edu.mv;*

Abstract: Zero-day Advanced Persistent Threats (APTs) ex-ploit previously unknown vulnerabilities to evade signature-based defences and persist across the enterprise kill chain. This paper presents an end-to-end framework for zero-day APT detection that couples an adaptive feature-selection pipeline with open-set recognition. First, we apply a hybrid Mutual Information → Symmetric Uncertainty → mRMR procedure with adaptive thresholds to capture non-linear relevance while suppressing redundancy and high-cardinality bias, yielding a compact, dis-criminative feature set suitable for real-time inference. On top of this representation, we integrate OpenMax (EVT-based logit calibration) with kernel density estimation (KDE) and Monte Carlo Dropout (MCD) to jointly assess distributional fit and epistemic uncertainty, routing ambiguous samples to an explicit Unknown class. Using the multi-stage DAPT2020 enterprise dataset, we evaluate with 10-fold cross-validation and a leave-one-class-out protocol that simulates unseen (zero-day) attacks. In closed-set classification, ensemble models achieve near-perfect performance (e.g., Random Forest: Accuracy/Precision/Recall/F1 = 0.9997). Under open-set conditions, the proposed OpenMax+KDE+MCD approach attains class-wise accuracies between 0.933 and 0.995, with high-volume behaviours (e.g., brute force, network scans) exceeding 0.99 and stealthier behaviours (e.g., backdoors, web vulnerability scans) detected at 0.93-0.94 while being safely rejected as Unknown when uncertain. The results demonstrate robust zero-day recognition with reduced false negatives and operationally actionable uncertainty signals, offering a practical path toward resilient, next-generation intrusion detection.

Keywords: Advanced Persistent Threats, Zero-day, Open-set Recognition, OpenMax, Kernel Density Estimation, Monte Carlo Dropout, Mutual Information, Symmetric Uncertainty, mRMR, Intrusion Detection, DAPT2020.

Received: 1 May 2025
Accepted: 7 August 2025
Published: 30 November 2025

1. INTRODUCTION

With the proliferation of the Internet and the worldwide expansion of online services, digital connectivity now spans not only personal computers but also handheld and IoT devices. This ubiquity has driven a sustained increase in global Internet usage.

By 2021, Internet statistics indicated 4.66 billion users-approximately 59.5% of the world's population [47]1 and the number continued to grow. By 2024, Internet users reached 5.35 billion (66.2%) [47]1; the International Telecommunication Union (ITU) reported as many as 5.5 billion people online in 2024 (68%) [23]2. While this accessibility fuels innovation, it also expands the attack surface for cyber-crime.

The diversity of connected devices and the dynamic nature of modern networks have made them increasingly vulnerable to malicious actors [22]3. Zero-day exploits exacerbate this risk: in 2024, 75 zero-day vulnerabilities were exploited in the wild, 44% of which targeted enterprise networking or security systems. Moreover, in 2025 an estimated 32%of exploited vulnerabilities were zero-days or one-days, indicating continued reliance on novel or minimally remediated weaknesses [46]4.

Cyber-attacks can be broadly categorized as targeted or untargeted [14]5. Untargeted attacks indiscriminately probe for weaknesses, whereas targeted attacks are carefully planned campaigns against specific organizations. A particularly dam-aging subset of targeted attacks is the Advanced Persistent Threat (APT), which combines stealth, resources, and persistence to achieve strategic objectives.

A growing concern within this class is the zero-day APT, where adversaries exploit undisclosed vulnerabilities to in-filtrate and remain undetected for extended periods, [9]6. Because patches and signatures are unavailable at the time of exploitation, zero-day APTs can evade conventional intrusion detection and execute multi-stage operations such as privilege escalation, lateral movement, and data exfiltration. This makes proactive detection and mitigation of zero-day APTs a critical research priority.

2. DEFINITION OF ZERO-DAY APTS

APTs are highly targeted cyber-espionage campaigns [18]7. We adopt the NIST definition [31]8:

An adversary that possesses sophisticated expertise and significant resources, enabling it to achieve objectives through multiple attack vectors (e.g., cyber, physical, deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of targeted organizations for exfiltration of information, under-mining or impeding critical missions, or positioning itself to carry out these objectives in the future. The advanced persistent threat (i) pursues its objectives repeatedly over an extended period, (ii) adapts to defenders' efforts to resist it, and (iii) maintains the level of interaction needed to execute its objectives.

Within this broad definition, the zero-day APT subclass is distinguished by systematic exploitation of zero-day vulnerabilities previously unknown flaws for which no patch or

signature exists at attack time there by bypassing signature-based defences and enabling extended dwell time.

a) Characteristic properties.:
   i. Specific targets and clear objectives: High-value or-ganisations (government, finance, research, health care, aerospace) are routinely pursued [1]9.
   ii. Well-resourced, organized actors: Often state-sponsored or professional groups with access to zero-day research or markets.
   iii. Long-term, adaptive campaigns: "Low-and-slow" operations with iterative tactic shifts to evade detection.
   iv. Stealthy, zero-day exploitation: Unpatched vulnerabilities enable covert entry and lateral movement, undermining traditional IDSs.

Table 1. Contrasting Traditional Attacks and Zero-Day Apt Attacks [11]10, [39]11.

	Traditional Attacks	**Zero-Day APT Attacks**
Attacker	Often an individual hacker	State-sponsored / organized groups
Target	Opportunistic, broad	High-value entities (gov., finance, critical infra.)
Purpose	Quick financial gain / notoriety	Long-term espionage, sabotage, data theft
Approach	Rapid "smash-and-grab"	Low-and-slow, repeated attempts, zero-day use

3. ZERO-DAY APT USE CASES

APTs originated as highly targeted, long-term campaigns and now span all sectors. Below we outline landmark cases where zero-day exploitation was pivotal [40]12.

Moonlight Maze (1996-1999; disclosed 2018)

Targeted U.S. military and government networks, research institutes, and aerospace [15]13. Later analyses suggest custom exploits and stealthy persistence-traits consistent with zero-day APT tradecraft.

Operation Aurora (2009-2010)

Compromised at least 34 enterprises (e.g., Google, Yahoo, Symantec) via spear-phishing and a previously unknown Internet Explorer vulnerability (true zero-day), enabling remote code execution, backdoors, and lateral movement [45]14.

GhostNet (2009)

China-linked espionage infecting 1,295 machines across 34 countries; delivery via socially engineered emails and long-lived C&C channels-hallmarks of zero-day-enabled persistence [13]15.

Red October (2007-2012; discovered 2012)

Government and diplomatic targets; custom Office exploits, including zero-days, plus a distributed C&C infrastructure of > 60 domains [48]16.

Stuxnet (2010)

Industrial APT targeting Iranian nuclear enrichment by manipulating PLCs; propagated via removable media and exploited at least four Windows zero-days [7]17.

4. ZERO-DAY APT ATTACK MODELS

Threat modelling identifies vulnerabilities and associated risks [34]18. For zero-day APTs—where unknown flaws are exploited—modelling guides where and how to detect early signals.

4.1 Kill chain–based frameworks

The Lockheed Martin Kill Chain [17]19 covers: Recon-naissance, Weaponization, Delivery, Exploitation, Installation, C&C, and Actions on Objectives. Zero-day APTs typically exploit unpatched flaws during Delivery/Exploitation, making early-phase detection crucial. Common vectors include spear-phishing, watering-hole compromises, and direct zero-day delivery, [27]20. The Unified Kill Chain [35]21 extends this to 17 steps in three loops, offering finer granularity.

4.2 Lifecycle and analytical models

The Mandiant Attack Lifecycle emphasizes persistence and lateral movement—both central to long-dwell zero-day intrusions [20]22. MITRE ATT&CK enumerates tactics/techniques (e.g., initial access, privilege escalation, defense evasion) that can be mapped to indicators for proactive zero-day detection.

4.3 Diamond Model

The Diamond Model relates adversary, capability, infrastructure, and victim [10]23, [42]24. Correlating these with kill-chain phases supports tracking from reconnaissance to exfiltration even without malware signatures.

4.4 Key detection opportunities

- Delivery/Exploitation: abnormal traffic, exploit-kit arte-facts, unpatched software use.
- Command & Control: low-and-slow encrypted channels over common protocols (HTTP/HTTPS).
- Lateral movement: anomalous privilege escalation and internal reconnaissance [4]25.

5. DATASETS USED FOR ZERO-DAY APT DETECTION

Robust APT detection requires datasets capturing full life-cycle stages (reconnaissance, initial compromise, C&C, lateral movement, privilege escalation, exfiltration). Such datasets are scarce due to (i) sensitivity of real logs, (ii) multi-stage complexity, and (iii) evolving adversary tradecraft [26]26, [41]27.

Researchers typically employ:

- Real datasets (e.g., CTU-13, LANL): realistic but stage-incomplete and privacy-restricted [6]28, [33]29.
- Synthetic datasets (e.g., DARPA 1999, CICIDS2017/2018): controllable but may under-represent real-world variability [5]30, [38]31.
- Semi-synthetic datasets (e.g., UNSW-NB15, APT-Sim): balance realism and control [12], [32].

Table 2. Selected Datasets for Apt Research [33], [34], [35]

Dataset	**Summary**
CICIDS2017	Multi-attack traffic; lacks explicit APT stage labels and extended stealth.
UNSW-NB15	IXIA PerfectStorm synthetic packet data; realis-tic yet limited for multi-stage APTs [36].
DARPA 1998–1999	Historical baseline; no APT-specific scenarios.
DAPT2020	Multi-stage APT traces with realistic class im-balance [35].

TABLE 3. Coverage of Apt Life-Cycle Stages

Dataset	**Recon.**	**Init. Comp.**	**Foothold**	**Priv. Esc.**	**Exfil.**
DAPT2020	Yes	Yes	Yes	Yes	Yes
SCVIC-APT-2021	Yes	Yes	Yes	Partial	
CICIDS2017	Yes	Yes	Yes	Yes	Yes
KDD Cup 99	Yes	Yes	No	No	No

Representative datasets

Stage coverage

Dataset used in this study: DAPT2020

We employ **DAPT2020** [35], a five-day enterprise traffic collection designed to represent the full APT kill chain (recon-naissance, foothold, lateral movement, privilege escalation, exfiltration). It includes internal/external flows, simulated stealth traffic, and real-world class imbalance properties well-suited to open-set, zero-day evaluation.

6. FEATURE SELECTION FOR ZERO-DAY APT DETECTION

Effective feature selection is vital for accuracy and effi-ciency. APT campaigns evolve, so static selection often lags attacker behaviour [27]. High-dimensional logs embed non-linear and contextual dependencies, and severe class imbalance can obscure rare attack indicators.

We adopt a hybrid pipeline: Mutual Information (MI) to capture linear/non-linear relevance; Symmetric Uncertainty (SU) to normalise MI and penalise redundancy; and Minimum Redundancy Maximum Relevance (mRMR) to select a compact, diverse subset [37]. Combined with cost-sensitive learning and domain knowledge, MI â†' SU â†' mRMR supports accurate, real-time detection.

Normalisation

We use min–max scaling,

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

to harmonize feature ranges and stabilize MI/SU estimates [38], [39].

Mutual Information and Symmetric Uncertainty

Entropy is defined as $H(X) = -\sum_i p(x_i)\ logp\ (x_i)$,

joint entropy as $H(X,Y) = -\sum_{i,j} p(x_i, y_j)\ log\ p\ (x_i, y_j)$, and MI

as $I(X;\ Y) = H(X) + H(Y) - H(X,\ Y)$. SU normalizes MI:

$$SU(X,Y) = 2\frac{I(X;\ Y)}{H(X)\ +\ H(Y)},$$

mitigating MI's bias toward high-cardinality features and reducing redundancy [40], [41].

mRMR objective

For a candidate feature fi, target c, and selected subset S,

$$\max_{f_i}\left(I(f_i; c) - \frac{1}{S}\sum_{f_i \in S} I(f_i; f_j\right),$$

balancing relevance and redundancy [42], [43]. Adaptive selection procedure

a) Pre-process (clean, encode, min–max scale).
b) Rank by MI; apply adaptive MI thresholds (mean ± SD) to discard extremes.
c) Compute pairwise SU; prune features above an SU re-dundancy threshold (retain higher-MI member).
d) Apply mRMR for final subset.
e) Validate and, if needed, tune MI/SU thresholds based on macro-F1 and APT recall.

Evaluation protocol

We use 10-fold cross-validation and report Accuracy, Precision, Recall, and F1. Classifiers include Random Forest [44], SVM [45], Decision Trees, Neural Networks [46], Gradient Boosting, and XGBoost. (Results summarized in Table 4.).

Table 4. Classifier Performance After Mi→Su→Mrmr Feature Selection

Classifier	Accuracy	Precision	Recall	F1
Random Forest	0.9997	0.9997	0.9997	0.9997
SVM	0.9692	0.9708	0.9692	0.9686
Gradient Boost	0.8432	0.9651	0.8432	0.8469
Naive Bayes	0.9658	0.9741	0.9658	0.9685
XGBoost	0.995	0.9994	0.9995	0.9994

a) Observations.: Ensembles (RF, XGBoost) achieve near-perfect scores, likely due to variance reduction and robust handling of heterogeneous features. Gradient Boost shows high Precision but lower Recall, reflecting conservative decision boundaries on stealthier classes.

7. ZERO-DAY DETECTION FRAMEWORK AND EVALUATION

Zero-day attacks exploit unknown vulnerabilities before patches exist [47]; APT actors frequently use them for initial access or privilege escalation [48]. We propose a hybrid open-set framework integrating OpenMax, Kernel Density Estimation (KDE), and Monte Carlo Dropout (MCD). OpenMax uses EVT calibration to reject samples inconsistent with known classes; KDE provides density-based novelty checks; MCD estimates epistemic uncertainty at inference.

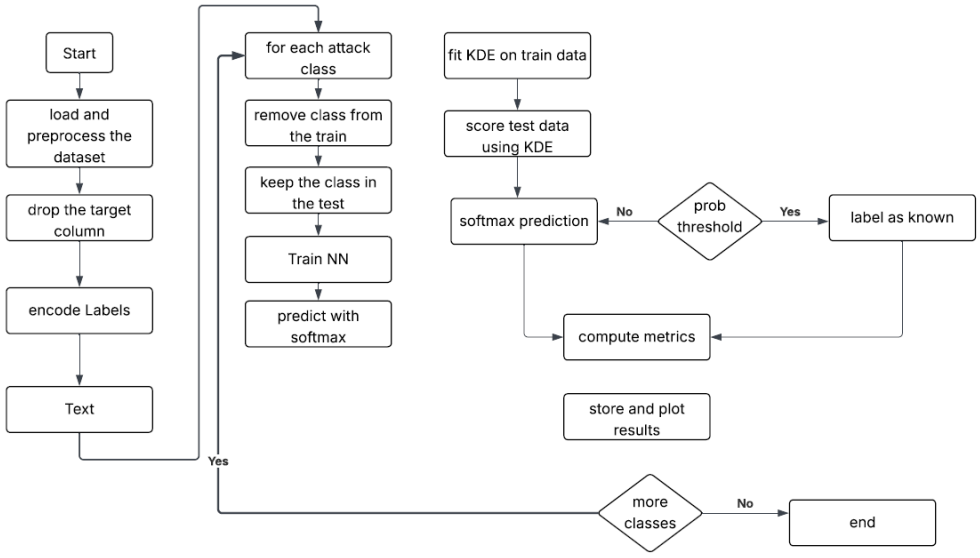

Figure. 1. Overview of the proposed zero-day detection framework (Open-Max+KDE+MCD).

a) Leave-one-class-out protocol.: For a class set C, remove c ∈ C from training to simulate a zero-day; test on the full set and measure unknown-class rejection and misclassification.

Algorithm 1 OpenMax-based Zero-Day Detection with KDE and MCD

Require: Dataset (X, y), KDE threshold $\theta_{,}$, class set C

1. for c ϵ C do
2. Train on (X, y) with c removed; hold out Xc for testing.
3. Obtain class logits → OpenMax EVT calibration.
4. Apply MCD for predictive uncertainty; compute KDE density.
5. Flag samples as Unknown if low density or high uncertainty; otherwise assign calibrated class.
6. Record Accuracy/Precision/Recall/F1 for class c.

8. RESULTS

Table 5. Leave-One-Class-Out Performance (Openmax+Mcd).

Removed Class	Accuracy	Precision	Recall	F1
Account Brute Force	0.9953	0.9953	0.9953	0.9953
Network Scan	0.9937	0.9937	0.9937	0.9937
Web Vulnerability Scan	0.9379	0.9398	0.9379	0.9369
Account Discovery	0.9414	0.9437	0.9414	0.9402
SQL Injection	0.9380	0.9396	0.9380	0.9374
Backdoor	0.9329	0.9443	0.9329	0.9280
Privilege Escalation	0.9363	0.9422	0.9363	0.9336

High-volume signatures (e.g., scans, brute-force) are detected with >99% accuracy; stealthier behaviors (e.g., back-doors, web vulnerability scans) show reduced recall (93–94%), reflecting overlap with benign traffic.

b) Key insights.:

- Robustness: Distinct signatures yield near-perfect detection.
- Stealth challenge: Low-footprint attacks overlap with benign baselines; improved representation helps.

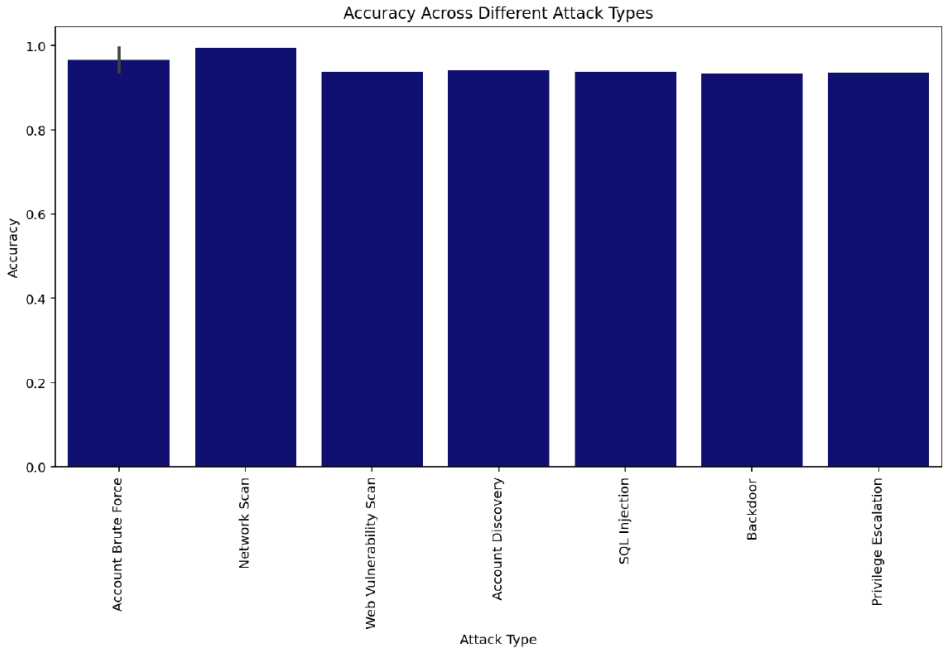

Figure 2. Accuracy across removed classes (OpenMax+MCD).

Table 6. Illustrative Confusion Matrix Emphasizing Stealth Misclassification.

True ↓ / Pred. →	**Brute**	**Scan**	**WebVuln**	**Backdoor**	**Unknown**
Brute Force	98	1	0	0	1
Scan	0	97	1	0	2
Web Vuln. Scan	0	2	85	5	8
Backdoor	0	1	6	82	11
Unknown (Zero-Day)	0	0	3	4	93

Uncertainty helps: MCD calibration meaningfully routes ambiguous cases to Unknown, reducing false negatives.

Operations: An explicit Unknown channel prioritizes SOC triage for potential zero-days

c) Comparison to open-set baselines.: OpenMax alone [49] can miss subtle deviations; distance-based rejection [?] and Deep SAD [?] require careful tuning and are scale-sensitive. Our OpenMax+KDE+MCD combination adds density checks and epistemic uncertainty, improving robustness for stealthy APT behaviors and yielding actionable uncertainty estimates for operations.
d) Future work.: Time-series models (e.g., Transformers) and adaptive EVT scaling for thresholding may further re-duce false positives. Integration with streaming IDS pipelines will advance real-time zero-day defence.

9. CONCLUSION

This paper presented a practical framework for detecting zero-day Advanced Persistent Threats by combining an adaptive feature-selection pipeline with open-set recognition. The MI→SU→mRMR procedure, equipped with adaptive thresholds, yields a compact and

discriminative representation that curbs high-cardinality bias and redundancy-key failure modes in high-dimensional network telemetry. Building on this representation, the integration of OpenMax (EVT-based calibration), kernel density estimation, and Monte Carlo Dropout jointly assesses distributional fit and epistemic uncertainty, routing ambiguous samples to an explicit Unknown class for analyst triage.

On the multi-stage DAPT2020 dataset, ensembles achieved near-perfect closed-set performance, while the proposed open-set detector sustained strong leave-one-class-out results (per-class accuracy ≈0.933-0.995), detecting high-volume behaviors (e.g., brute force, scans) with >0.99 accuracy and safely rejecting stealthier behaviors (e.g., backdoors, web vulnerability scans) when uncertainty was high. These outcomes demonstrate that uncertainty-aware open-set recognition can materially reduce false negatives and provide actionable signals for SOC operations.

Limitations and future work.: Our evaluation is con-strained by dataset availability and the fidelity of simulated stealth traffic. Future efforts will target (i) sequence-aware models (e.g., Transformers) for long-horizon behaviors and lateral movement, (ii) adaptive EVT scaling and calibrated thresholds for better precision-recall trade-offs, (iii) online/streaming deployment with concept-drift handling, (iv) cross-domain generalization studies and transfer/federated learning, and (v) operational metrics (latency, throughput, alert volume) with human-in-the-loop feedback. We view these directions as the next steps toward resilient, real-time zero-day APT detection in production networks.

10. REFERENCE

[1] Chao Wang and Leen d'Haenens. Report-based interpretation of 2024 digital literacy and skills in china and the eu: Status, differences, and future directions. In International Conference on New Media Pedagogy, pages 3–18. Springer, 2024.

[2] Katelyn Lynch. Modeling internet use in the global development context: Preliminary findings and future directions. In 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K), pages 1-6. IEEE, 2024.

[3] Jinping Liu, Jiezhou He, Wuxia Zhang, Tianyu Ma, Zhaohui Tang, Jean Paul Niyoyita, and Weihua Gui. Anid-seokelm: Adaptive network intrusion detection based on selective ensemble of kernel elms with random features. Knowledge-Based Systems, 177:104-116, 2019.

[4] Azheen Waheed, Bhavish Seegolam, Mohammad Faizaan Jowaheer, Chloe Lai Xin Sze, Ethan Teo Feng Hua, and Siva Raja Sindiramutty. Zero-day exploits in cybersecurity: Case studies and countermeasure. 2024.

[5] Ibrahim Ghafir and Vaclav Prenosil. Proposed approach for targeted attacks detection. In Advanced Computer and Communication Engineering Technology, pages 73-80. Springer, 2016.

[6] Leyla Bilge and Tudor Dumitras¸. Before we knew it: an empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 833–844, 2012.

[7] Inkyung Jeun, Youngsook Lee, and Dongho Won. A practical study on advanced persistent threats. In Computer applications for security, control and system engineering, pages 144–152. Springer, 2012.

[8] SP NIST. 800-39-managing information security risk: Organization. Mission, and Information System View, 2011.

[9] Fireeye advanced threat report. 2013.
[10] Ping Chen, Lieven Desmet, and Christophe Huygens. A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security, pages 63–72. Springer, 2014.
[11] Murtaza A Siddiqi and Naveed Ghani. Critical analysis on advanced persistent threats. International Journal of Computer Applications, 975:8887, 2016.
[12] Branka Stojanovi´c, Katharina Hofer-Schmitz, and Ulrike Kleb. Apt datasets and attack modeling for automated detection methods: A review. Computers & Security, 92:101734, 2020.
[13] Juan Andres Guerrero-Saade, Costin Raiu, Daniel Moore, and Thomas Rid. Penquins moonlit maze, 2017.
[14] Rohit Varma. Mcafee labs: combating aurora, 2010.
[15] Ronald J Deibert, Rafal Rohozinski, A Manchanda, Nart Villeneuve, and GMF Walton. Tracking ghostnet: Investigating a cyber espionage network. 2009.
[16] KL Zao. Red october diplomatic cyber attacks investigation. Retrieved from.
[17] Marie Baezner and Patrice Robin. Stuxnet. Technical report, ETH Zurich, 2017.
[18] Keith L Pendergrass, Walker Sampson, Tim Walsh, and Laura Alagna. Toward environmentally sustainable digital preservation. The American Archivist, 82(1):165–206, 2019.
[19] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1):80, 2011.
[20] Trend Micro. Spear-phishing email: Most favored apt attack bait. Trend Micro, http://www. trendmicro. com. au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait. pdf (accessed 1 October 2014), 2012.
[21] Paul Pols and Jan van den Berg. The unified kill chain. CSA Thesis, Hague, pages 1–104, 2017.
[22] Meicong Li, Wei Huang, Yongbin Wang, Wenqing Fan, and Jianfang Li. The study of apt attack stage model. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), pages 1–5. IEEE, 2016.
[23] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz. The diamond model of intrusion analysis. Technical report, Center For Cyber Intelligence Analysis and Threat Research Hanover Md, 2013.
[24] Matt Tatam, Bharanidharan Shanmugam, Sami Azam, and Krishnan Kannoorpatti. A review of threat modelling approaches for apt-style attacks. Heliyon, 7(1):e05969, 2021.
[25] Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 2019.
[26] Mohamad Erfan Mazaheri and Alireza Shameli-Sendi. Aptracker: A comprehensive and analytical malware dataset, based on attribution to apt groups. IEEE Access, 2024.
[27] Manar Abu Talib, Qassim Nasir, Ali Bou Nassif, Takua Mokhamed, Nafisa Ahmed, and Bayan Mahfood. Apt beaconing detection: A systematic review. Computers & Security, 122:102875, 2022.
[28] Md Monowar Anjum, Shahrear Iqbal, and Benoit Hamelin. Analyzing the usefulness of the darpa optc dataset in cyber threat detection research. In Proceedings of the 26th ACM Symposium on Access Control Models and Technologies, pages 27–32, 2021.
[29] Anagha Patil and Arti Deshpande. Evaluating ml models on ctu-13 and iot,-23 datasets. In 2023 International Conference on Advanced Computing Technologies and Applications (ICACTA), pages 1–6. IEEE, 2023.

[30] Tertsegha J Anande and Mark S Leeson. Synthetic network traffic data generation and classification of advanced persistent threat samples: A case study with gans and xgboost. In International Conference on Deep Learning Theory and Applications, pages 1–18. Springer, 2023.
[31] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. To-ward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1:108–116, 2018.
[32] Robert Techentin, Daniel Foti, Sinan Al-Saffar, Peter Li, Erik Daniel, Barry Gilbert, and David Holmes. Characterization of semi-synthetic dataset for big-data semantic analysis. In 2014 IEEE High Performance Extreme Computing Conference (HPEC), pages 1–6. IEEE, 2014.
[33] Defense Advanced Research Projects Agency. Darpa 1999 dataset. https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset, 1999.
[34] David Mudzingwa and Rajeev Agrawal. A study of methodologies used in intrusion detection and prevention systems (idps). In 2012 Proceedings of IEEE Southeastcon, pages 1–6. IEEE, 2012.
[35] Sowmya Myneni, Ankur Chowdhary, Abdulhakim Sabur, Sailik Sen-gupta, Garima Agrawal, Dijiang Huang, and Myong Kang. Dapt 2020-constructing a benchmark dataset for advanced persistent threats. In International Workshop on Deployable Machine Learning for Security Defense, pages 138–163. Springer, 2020.
[36] Nour Moustafa and Jill Slay. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In 2015 military communications and information systems conference (MilCIS), pages 1–6. IEEE, 2015.
[37] A. Maleki. Title of the article. Journal Name, 12(5):67–89, 2021.
[38] Ian Connick Covert, Wei Qiu, Mingyu Lu, Na Yoon Kim, Nathan J White, and Su-In Lee. Learning to maximize mutual information for dynamic feature selection. In International Conference on Machine Learning, pages 6424–6447. PMLR, 2023.
[39] Minghong Li, Yuqian Zhao, Fan Zhang, Biao Luo, Chunhua Yang, Weihua Gui, and Kan Chang. Multi-scale feature selection network for lightweight image super-resolution. Neural Networks, 169:352-364, 2024.
[40] Pooja V Agrawal, Deepak D Kshirsagarb, and Anish R Khobragadec. Symmetric uncertainty-based feature selection method in android mal-ware detection. In Recent Advances in Material, Manufacturing, and Machine Learning, pages 934–941. CRC Press, 2023.
[41] Cl´audia Pascoal, M Ros´ario Oliveira, Ant´onio Pacheco, and Rui Valadas. Theoretical evaluation of feature selection methods based on mutual information. Neurocomputing, 226:168–181, 2017.
[42] Amin Hashemi, Mohammad Bagher Dowlatshahi, and Hossein Nazamabadi-pour. Minimum redundancy maximum relevance ensemble feature selection: A bi-objective pareto-based approach. Journal of Soft Computing and Information Technology (JSCIT) Vol, 12(1), 2023.
[43] Yang Lyu, Yaokai Feng, and Kouichi Sakurai. A survey on feature se-lection techniques based on filtering methods for cyber attack detection. Information, 14(3):191, 2023.
[44] Suthakaran Ratnasingam and Jose Mu˜noz-Lopez. Distance correlation-based feature selection in. Entropy, 25(9):1250, 2023.
[45] Dirk Valkenborg, Axel-Jan Rousseau, Melvin Geubbelmans, and Tomasz Burzykowski. Support vector machines. American Journal of Orthodontics and Dentofacial Orthopedics, 164(5):754–757, 2023.
[46] Atin Roy and Subrata Chakraborty. Support vector machine in structural reliability analysis: A review. Reliability Engineering & System Safety, 233:109126, 2023.

[47] Jingci Zhang, Jun Zheng, Ning Shi, Zhaohui Ci, Yajie Wang, and Liehuang Zhu. Towards mitigating apt attacks with zero-trust networks access control model. IEEE Internet of Things Journal, 2025.

[48] Bilge Karabacak and Todd Whittaker. Zero trust and advanced persistent threats: who will win the war. In International conference on cyber warfare and security, volume 17, pages 92–101. Academic Conferences International Limited, 2022.

[49] Abhijit Bendale and Terrance E Boult. Towards open set deep networks. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 1563–1572, 2016.