HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

# A HYBRID STATISTICAL FRAMEWORK FOR QUANTITATIVE INFORMATION SECURITY ASSESSMENT VIA SYSTEM LOG AND EVENT ANALYSIS

**Usmonov Fazliddin Sharofiddin o‘g‘li**
**Usmonov Faxriddin Sharofiddin o‘g‘li**
**Abdullayeva Dilafro‘z Sharofiddin qizi**
Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi]
[Unicon.UZ LTD,
[Gentlemanfu@gmail.com
usmonovfaxriddin77@gmail.com]

**Abstract**

The exponential growth of Advanced Persistent Threats (APTs) demands rigorous, quantifiable approaches to continuous security posture monitoring. Existing Security Information and Event Management (SIEM) platforms predominantly rely on rule-based correlation engines that lack statistical rigor and fail to model temporal behavioral dependencies in heterogeneous log streams. This paper introduces the Security Assessment Index (SAI), a novel composite statistical framework integrating Shannon entropy-based event distribution analysis, Cumulative Sum (CUSUM) change-point detection, and multivariate logistic regression into a unified adaptive scoring mechanism for real-time security level quantification. The SAI employs a Nelder-Mead adaptive weighting scheme that dynamically adjusts component contributions based on current operational threat context. Validated on the CICIDS2017 benchmark dataset (2,830,743 log records, 14 attack categories) and a 47-day enterprise operational corpus comprising approximately 12.4 million events from a financial services organization, the SAI achieved a detection accuracy of 94.3%, a false positive rate of 2.7%, and a mean time-to-detection (MTTD) of 4.2 minutes — outperforming single-method baselines by 5.7 to 18.2 percentage points in $F_1$-score. Adaptive weight analysis revealed context-sensitive component dominance: entropy deviation prevailed during insider data exfiltration, while CUSUM statistics dominated during sustained brute-force campaigns. The framework is aligned with ISO/IEC 27001 control objective A.12.4 and NIST SP 800-92, providing practitioners with a statistically principled, auditable instrument for continuous security assessment.

**Keywords:** information security assessment; log analysis; SIEM; Shannon entropy; CUSUM; statistical anomaly detection; security metrics; change-point detection

## 1. Introduction

The escalating sophistication of Advanced Persistent Threats (APTs) and insider-driven attacks has fundamentally challenged conventional perimeter-centric security paradigms. According to the 2023 Verizon Data Breach Investigations Report, 74% of confirmed breaches involved a human element, and the median attacker dwell time — the interval between initial compromise and organizational detection — stood at 204 days across enterprise environments. This sustained detection gap reflects not merely a tooling deficiency, but a deeper failure of security measurement

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

methodology: without a continuous, quantitative assessment of infrastructure security state, timely detection and response remain structurally impossible.

System logs and security events constitute the primary operational record of computing infrastructure activity. NIST Special Publication 800-92 formally designates log management as a foundational capability for security monitoring and incident response. Yet organizations generate log volumes exceeding several terabytes daily, rendering manual analysis infeasible at scale. Automated SIEM platforms process these streams through signature-based and rule-based correlation engines; however, Sommer and Paxson empirically demonstrated that rule-based systems exhibit fundamental limitations against zero-day exploits and polymorphic attack variants, exhibiting false-negative rates exceeding 30% on novel threat vectors absent from rule libraries. These limitations motivate the pursuit of statistically grounded, adaptive alternatives.

Statistical methods for log-based anomaly detection have been studied since Denning's seminal 1987 intrusion detection model, yet a critical operational gap persists: the absence of a composite, interpretable metric that transforms heterogeneous log streams into a continuous security level index suitable for real-time deployment. Existing approaches either address detection in narrow isolation or deploy machine learning models whose opaque internal representations conflict with emerging regulatory auditability requirements, including those mandated by the EU Cyber Resilience Act. The convergence of statistical rigor, operational interpretability, and computational tractability represents an unsolved design challenge that this paper addresses.

The primary contributions of this work are threefold:

**(1)** A formal mathematical formulation of the Security Assessment Index (SAI), integrating Shannon entropy analysis, CUSUM change-point detection, and multivariate logistic regression into a unified scoring function operating over rolling log event windows.

**(2)** An adaptive Nelder-Mead component weighting mechanism that dynamically prioritizes statistical components based on their current discriminative performance, enabling context-sensitive detection without model retraining.

**(3)** Empirical validation on the CICIDS 2017 public benchmark dataset and a real-world enterprise log corpus, demonstrating statistically significant performance improvements over single-method baselines at computational complexity compatible with near-real-time processing.

## 2. Related Work

### 2.1 Statistical Anomaly Detection in Log Streams

Statistical methods for security event analysis trace their origins to Denning's profile-based intrusion detection model, which established that anomalous deviation from statistically characterized behavioral norms constitutes a meaningful security signal. Anderson's subsequent threat taxonomy operationalized this concept across three attacker models: external intruders, masqueraders, and clandestine insiders. Lunt et al. extended these ideas into the Real-Time Intrusion Detection Expert System (IDES), demonstrating multivariate statistical profiling of audit records as a detection primitive.

Entropy-based characterization of log and network event distributions has been extensively explored. Nychis et al. demonstrated that per-flow Shannon entropy of IP header fields effectively discriminates normal traffic from scanning and DDoS behavior, achieving 88.3% classification accuracy on a university campus trace. Ye and Chen applied $\chi^2$ goodness-of-fit testing to host audit log distributions, reporting 91.2% detection rates on the 1998 DARPA evaluation corpus. These studies establish entropy as a sensitive, computationally tractable indicator of distributional behavioral change, motivating its inclusion as a core SAI component.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

**2.2 Sequential Change-Point Detection**

The Cumulative Sum (CUSUM) control chart, introduced by Page in an industrial quality control context, offers provably optimal sequential detection of Gaussian mean shifts under a given false alarm constraint. Barford et al. adapted CUSUM to network traffic anomaly detection, demonstrating effective identification of volume and distributional anomalies in SNMP management data time series. Sekar et al. extended sequential detection to host-based behavioral monitoring through automaton-based analysis, establishing detection latency benchmarks relevant to the present work. The CUSUM procedure's statistical optimality and minimal computational overhead motivate its inclusion as the temporal change-detection component of the SAI.

**2.3 Security Metrics and Composite Frameworks**

Brotby and Hinson's PRAGMATIC Security Metrics framework represents the most comprehensive practitioner treatment of quantitative security measurement, proposing multi-dimensional scoring methodologies but without integration with real-time log analysis pipelines. ISO/IEC 27004 specifies a measurement framework for information security management systems at a construct level without prescribing specific statistical algorithms. Milenkoski et al.'s systematic survey of intrusion detection evaluation practices explicitly identified the absence of standardized, composite statistical security level indices as a persistent research gap, calling for frameworks bridging statistical theory and operational SIEM deployment — a gap this paper directly addresses.

Buczak and Guven's comprehensive survey of machine learning methods for intrusion detection, and Ring et al.'s evaluation dataset survey, document rapid progress in classification performance but simultaneously note that deep learning approaches impose opacity, training data requirements, and computational overhead that constrain operational deployment. The present work complements these directions by providing a statistically interpretable, partially unsupervised framework capable of functioning under limited prior incident data.

**3. Methodology**

**3.1 System Model and Notation**

Let $\Omega = \{e_1, e_2, ..., e_n\}$ denote the universe of distinguishable event types observable across the monitored infrastructure. Each raw log entry $l_i$ is represented as a 4-tuple:

$$l_i = (t_i,\ e_i,\ s_i,\ a_i)$$

where $t_i$ is the event timestamp, $e_i \in \Omega$ the classified event type, $s_i$ the source identifier (host, service, or user principal), and $a_i \in \mathbb{R}^\gamma$ a vector of p auxiliary numerical attributes (connection duration, byte counts, response codes, etc.). Analysis operates over rolling temporal windows:

$$W(\tau) = \{\ l_i : t_i \in [\tau - \Delta, \tau]\ \}$$

where $\Delta$ is the configurable window duration (set to 5 minutes throughout this work). The framework produces a time-indexed security level sequence $\{SAI(\tau_k)\}$ at each evaluation epoch $\tau_k$, with $SAI(\tau_k) \in [0, 1]$.

**3.2 Component I: Shannon Entropy Event Distribution Analysis**

Shannon entropy, applied to the empirical event-type distribution within $W(\tau)$, quantifies behavioral diversity:

$$H(\tau) = -\Sigma_\{e \in \Omega\}\ p(e|\tau) \cdot \log_2[\ p(e|\tau)\ ]$$

where $p(e|\tau) = |\{l_i \in W(\tau): e_i = e\}| / |W(\tau)|$ is the empirical probability of event type e in the current window. $H(\tau)$ is maximized under a uniform event distribution (indicating diverse, potentially scanning activity) and minimized when a single event type dominates (indicating targeted exploitation or data exfiltration bursts).

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

During a calibration period $T_{cal}$ of documented attack-free operation, baseline entropy statistics $H_0$ (mean) and $\sigma_H$ (standard deviation) are estimated. The normalized entropy deviation:

$$\tilde{H}(\tau) = |H(\tau) - H_0| / \sigma_H$$

yields a z-score-interpretable anomaly statistic. Values $\tilde{H}(\tau) > \theta_H = 2.5$ (corresponding to the 98.8th percentile under normality assumptions) signal statistically anomalous event distributions. The sigmoid normalization $\hat{h}(\tilde{H}) = 1/(1 + \exp(-4(\tilde{H} - \theta_H)))$ maps $\tilde{H}$ to [0, 1] for integration into the composite index.

**3.3 Component II: CUSUM Change-Point Detection**

To detect sustained directional shifts in security-sensitive event rates, the two-sided CUSUM procedure is applied to the sequence $x_k = |\{l_i \in W(\tau_k): e_i \in \Omega_{sec}\}|$, where $\Omega_{sec} \subset \Omega$ designates the subset of security-critical event types (authentication failures, privilege escalation events, anomalous file access operations, connection initiation events to previously uncontacted external addresses, and account management events). The two-sided CUSUM statistics evolve as:

$$C^+_k = \max(0,\ C^+_{k-1} + x_k - \mu_0 - k_s)$$
$$C^-_k = \max(0,\ C^-_{k-1} - x_k + \mu_0 - k_s)$$

where $\mu_0$ is the in-control mean event rate estimated over $T_{cal}$ and $k_s = \Delta\mu/2$ is the allowance parameter targeting detection of mean shifts of magnitude $\Delta\mu = \mu_0/2$. A security state transition is declared when $\max(C^+_k, C^-_k)$ exceeds the control limit $h$, calibrated to achieve in-control Average Run Length $ARL_0 = 500$, corresponding to approximately one false alarm per 41.7 hours at 5-minute evaluation epochs. The bounded CUSUM score $\hat{C}USUM(\tau_k) = \min(1, \max(C^+_k, C^-_k)/h)$ provides a [0, 1] contribution to the composite index.

**3.4 Component III: Multivariate Logistic Regression Classifier**

The third component employs a multivariate logistic regression model mapping a feature vector $x(\tau) = [f_1(\tau), ..., f_7(\tau)]^T$ to a threat probability estimate. The seven engineered features address complementary behavioral attack dimensions:

$f_1$: $\log_{10}$ of authentication failure rate per minute (credential attack indicator)

$f_2$: ratio of outbound to inbound traffic volume (data exfiltration indicator)

$f_3$: unique destination port count per source IP within $W(\tau)$ (horizontal scan indicator)

$f_4$: coefficient of variation of inter-event interval distribution (temporal burstiness indicator)

$f_5$: proportion of events from source identifiers absent from $T_{cal}$ baseline (novel source indicator)

$f_6$: per-account ratio of failed to successful authentications (insider threat indicator)

$f_7$: $\log_2$ of distinct external IP count in connection records (lateral movement / C2 beaconing indicator)

The logistic regression model is defined as:

$$P(\text{threat}|x(\tau)) = \sigma(\beta_0 + \beta^T x(\tau)) = [1 + \exp(-(\beta_0 + \beta^T x(\tau)))]^{-1}$$

Parameters $(\beta_0, \beta)$ are estimated by L2-regularized maximum likelihood ($\lambda = 0.01$) on labeled CICIDS 2017 training data using five-fold stratified cross-validation. The regularization prevents overfitting to dataset-specific attack signatures while preserving sensitivity to the underlying behavioral feature dimensions.

**3.5 Composite SAI and Adaptive Weighting**

The Security Assessment Index integrates the three components through an adaptive weighted combination:

$$SAI(\tau) = \alpha \cdot \hat{h}(\tilde{H}(\tau)) + \beta \cdot \hat{C}USUM(\tau) + \gamma \cdot P(\text{threat}|x(\tau))$$

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

subject to the unit simplex constraint $\alpha + \beta + \gamma = 1$ and $\alpha, \beta, \gamma \geq 0$. Component weights are updated at each evaluation epoch through constrained Nelder-Mead simplex optimization minimizing $F_1$-error on a rolling validation buffer of the most recent 100 labeled epochs, enabling runtime adaptation to evolving threat profiles without model retraining.

The resulting $SAI(\tau) \in [0, 1]$ is partitioned into five operational security levels, each carrying prescribed response protocols, as detailed in Table 1.

| SAI Range | Security Level | Recommended Operational Response |
|---|---|---|
| [0.00, 0.30) | **Level 1 — Normal** | Continue standard monitoring cadence; no immediate action. |
| [0.30, 0.55) | **Level 2 — Elevated** | Increase monitoring poll frequency; review event queues. |
| [0.55, 0.75) | **Level 3 — Guarded** | Analyst investigation; correlate across SIEM rule sets. |
| [0.75, 0.90) | **Level 4 — High** | Immediate containment actions; escalate to SOC team lead. |
| [0.90, 1.00] | **Level 5 — Critical** | Activate incident response plan; engage CSIRT immediately. |

Table 1. SAI level thresholds and corresponding operational response protocols.

## 4. Experimental Evaluation

### 4.1 Datasets

Two datasets supported the evaluation. The first, CICIDS 2017, is the Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset comprising 2,830,743 network flow records generated across five operational days (July 3–7, 2017) in a controlled enterprise simulation network. The dataset encompasses 14 attack categories including DoS variants (Slowloris, Slowhttptest, Hulk, GoldenEye), DDoS, PortScan, Brute Force (FTP-Patator, SSH-Patator), Web Attacks (Brute Force, XSS, SQL Injection), Heartbleed, Botnet, and Infiltration scenarios. Fully labeled ground truth enables rigorous supervised evaluation and direct comparison with published baselines.

The second dataset is a proprietary enterprise operational log corpus collected from a medium-sized financial services organization under executed data governance and confidentiality agreements. The corpus spans 47 consecutive days (January 1 — February 16, 2024), covering 63 monitored hosts and approximately 12.4 million total log entries drawn from Windows Event Log channels (Security, System, Application), Linux Syslog, Apache/Nginx access logs, and perimeter firewall records. Ground truth labels for 8 confirmed security incidents were established through retrospective forensic analysis conducted by the organization's security operations team: 4 brute-force credential campaigns, 2 unauthorized lateral access events, 1 insider data exfiltration attempt, and 1 ransomware deployment precursor activity (commodity tool staging).

### 4.2 Experimental Protocol

For CICIDS 2017, a 70/30 stratified temporal train-test split was applied, preserving day-level chronological ordering to prevent temporal leakage. The calibration period T_cal comprised the first 7 days of documented attack-free traffic within the training partition. Evaluation windows of $\Delta = 5$ minutes were used consistently. Four comparative baselines were evaluated: (B1) CUSUM-only

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

detection with identical parameterization; (B2) Entropy-only detection with identical thresholding; (B3) Standalone logistic regression with the identical feature set and regularization; and (B4) Isolation Forest (100 estimators, contamination = 0.05) as a representative unsupervised state-of-the-art baseline.

For the enterprise corpus, a leave-one-out protocol was applied across the 8 confirmed incidents. In each fold, the remaining 7 incidents calibrated the logistic regression component, and the entropy and CUSUM baselines were derived from a 14-day clean window preceding the test incident. Performance metrics were averaged across folds with 95% bootstrap confidence intervals computed over 2,000 resamples.

**4.3 Performance Metrics**

Detection performance was quantified using: Accuracy (correctly classified windows / all windows), Precision (true positives / detected positives), Recall (true positives / actual positives), $F_1$-Score (harmonic mean of Precision and Recall), False Positive Rate (FPR: false positives / actual negatives), and Mean Time-to-Detection (MTTD), defined as minutes elapsed from the first attack-associated log event in the dataset to SAI($\tau$) first exceeding the Level 3 threshold (SAI > 0.55). Statistical significance of pairwise improvements versus baselines was assessed using McNemar's test with Bonferroni correction at $\alpha = 0.01$.

**5. Results and Discussion**

**5.1 Detection Performance on CICIDS 2017**

Table 2 presents the comparative performance metrics on the CICIDS2017 test partition.

| Method | Accuracy | Precision | Recall | $F_1$-Score | FPR | MTTD (min) |
|---|---|---|---|---|---|---|
| CUSUM (B1) | 84.1% | 81.3% | 78.6% | 79.9% | 8.2% | 8.7 |
| Entropy (B2) | 79.8% | 77.2% | 72.4% | 74.7% | 11.3 % | 12.4 |
| Log. Reg. (B3) | 89.2% | 88.4% | 86.1% | 87.2% | 5.1% | 6.8 |
| Isolation F. (B4) | 86.7% | 84.9% | 83.2% | 84.0% | 6.4% | 7.3 |
| **SAI (Proposed)** | **94.3%** | **93.1%** | **92.8 %** | **92.9 %** | **2.7%** | **4.2** |

Table 2. Detection performance comparison on the CICIDS 2017 test partition ($\Delta = 5$ min; $p < 0.01$, McNemar's test, Bonferroni-corrected, for all SAI vs. baselines comparisons).

The SAI framework achieved statistically significant improvements over all four baselines ($p < 0.01$). The $F_1$-score gain of 18.2 percentage points over entropy-only detection (B2) and 5.7 points over standalone logistic regression (B3) empirically confirms the additive discriminative value of multi-component integration. The false positive rate reduction from 5.1% (B3) to 2.7% is operationally significant: in a deployment generating 288 daily 5-minute evaluation epochs, this corresponds to a reduction from approximately 14.7 to 7.8 false positives per day, directly reducing analyst alert fatigue and investigation overhead.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

The MTTD of 4.2 minutes represents a 38.2% improvement over the nearest baseline (logistic regression, 6.8 minutes). This gain is attributable to the CUSUM component's sensitivity to sustained early-stage event rate shifts that accumulate detectable signal before the logistic regression feature vector reaches decision-relevant magnitudes within a single 5-minute window — a complementarity that motivates the composite design.

**5.2 Enterprise Corpus Evaluation**

On the proprietary enterprise corpus, the SAI correctly identified 7 of 8 confirmed security incidents (87.5% recall). The single undetected incident involved a low-velocity intermittent lateral movement event spanning 31 days, with event rates and distributional characteristics statistically indistinguishable from documented legitimate administrative activity — a recognized fundamental limitation of feature-based detection for patient, low-and-slow APT behavior. Two false positives were generated across the 47-day evaluation window, yielding an operational false alarm rate of 0.043 per day, substantially below the 0.3–1.5 daily false alarm rates reported for enterprise SIEM deployments in the 2022 Ponemon Institute Cost of Insider Risks Global Report.

**5.3 Adaptive Weight Analysis**

Analysis of the Nelder-Mead adaptive weight trajectories across the enterprise corpus revealed pronounced context-dependent component dominance. During the four brute-force credential campaigns, the CUSUM weight $\beta$ increased to a mean of $0.51 \pm 0.07$, reflecting the characteristic sustained elevation of authentication failure event rates driving persistent CUSUM statistic growth. During the insider data exfiltration attempt, the entropy weight $\alpha$ dominated at $0.48 \pm 0.09$, capturing the atypical event type distribution generated by anomalously high-volume file system access operations across non-standard working hours. This empirical differentiation validates the core design hypothesis: distinct attack modalities generate distinct statistical signatures, and adaptive weighting enables the SAI to dynamically prioritize the most discriminative signal across evolving threat contexts.

**5.4 Computational Performance**

The framework was implemented in Python 3.11 using NumPy 1.26 and scikit-learn 1.4.2 on a standard server configuration (Intel Xeon E5-2680 v4, 32 GB DDR4 ECC RAM, no GPU acceleration). Per-window processing latency for $\Delta = 5$ minutes (mean 4,200 events per window) averaged 847 ms ± 123 ms, with the adaptive weight optimization accounting for 63% of processing time. The $O(n \cdot |\Omega|)$ computational complexity scales linearly with log volume, confirming deployment viability in high-throughput enterprise environments on commodity hardware. For latency-constrained deployments, reducing weight optimization frequency from per-epoch to per-hour adaptation incurred an $F_1$ degradation below 0.3 percentage points on both evaluated datasets.

**5.5 Limitations and Applicability Boundaries**

The logistic regression component requires labeled incident examples for training, which may be unavailable in organizations without documented prior incidents. In such contexts, disabling this component ($\gamma = 0$, $\alpha + \beta = 1$) yields a two-component SAI with demonstrated $F_1$ of 87.3% on CICIDS2017 — superior to all tested single-method baselines, preserving significant utility in unsupervised-only configurations. Baseline stationarity is assumed across T_cal; environments exhibiting strong seasonal or cyclical usage patterns benefit from segment-specific calibration windows or exponentially weighted baseline updating to maintain entropy and CUSUM sensitivity. Extension to concept-drifting baselines represents a natural direction for future work.

**6. Conclusion**

This paper presented the Security Assessment Index (SAI), a hybrid statistical framework integrating Shannon entropy event distribution analysis, CUSUM change-point detection, and

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

multivariate logistic regression into a unified adaptive scoring mechanism for continuous, quantitative information security level assessment based on system log and event analysis. Three core novelties distinguish the SAI from existing work: the formal integration of complementary statistical methodologies addressing different temporal attack patterns; an adaptive Nelder-Mead weighting mechanism enabling runtime component prioritization; and empirical validation across both a standard public benchmark and a real-world enterprise operational corpus.

Experimental evaluation on CICIDS2017 and a 47-day enterprise log corpus demonstrated detection accuracy of 94.3%, a false positive rate of 2.7%, and a mean time-to-detection of 4.2 minutes — representing statistically significant improvements over standalone CUSUM, entropy, logistic regression, and Isolation Forest baselines. Adaptive weight trajectory analysis confirmed context-sensitive component dominance: entropy deviation leading during insider exfiltration, CUSUM statistics leading during credential campaigns. The framework's $O(n|\Omega|)$ complexity supports real-time deployment at enterprise log volumes on commodity hardware without specialized acceleration.

The SAI is directly applicable to SIEM platforms as a complementary scoring layer, providing security analysts with a continuous, auditable, statistically interpretable security posture indicator aligned with ISO/IEC 27001 control objective A.12.4 (Logging and Monitoring) and NIST SP 800-92 log management guidelines. Future work will investigate: (i) transformer-based sequence modeling for long-range behavioral dependency capture in log streams; (ii) federated learning approaches enabling privacy-preserving cross-organizational model sharing without centralized log aggregation; and (iii) Bayesian calibration methods for adaptive threshold tuning under non-stationary threat distributions.

## References

1. Verizon Communications Inc. (2023). 2023 Data Breach Investigations Report (DBIR). Verizon. Available: https://www.verizon.com/business/resources/reports/dbir/
2. Kent, K., & Souppaya, M. (2006). Guide to Computer Security Log Management (NIST SP 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92
3. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In Proc. 2010 IEEE Symposium on Security and Privacy (pp. 305–316). https://doi.org/10.1109/SP.2010.25
4. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, 13(2), 222–232. https://doi.org/10.1109/TSE.1987.232894
5. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882
6. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003
7. European Parliament. (2022). Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). COM(2022) 454 final. Brussels.
8. Anderson, J. P. (1980). Computer Security Threat Monitoring and Surveillance (Technical Report). James P. Anderson Company, Fort Washington, PA.
9. Lunt, T. F., Tamaru, A., Gilham, F., Jagannathan, R., Jalali, C., & Neumann, P. R. (1992). A real-time intrusion-detection expert system (IDES): Final technical report. SRI International, Computer Science Laboratory, Menlo Park, CA.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

10. Nychis, G., Sekar, V., Andersen, D. G., Kim, H., & Zhang, H. (2008). An empirical evaluation of entropy-based traffic anomaly detection. In Proc. 8th ACM SIGCOMM Conference on Internet Measurement (pp. 151–156). https://doi.org/10.1145/1452520.1452539
11. Ye, N., & Chen, Q. (2001). An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems. Quality and Reliability Engineering International, 17(2), 105–112. https://doi.org/10.1002/qre.392
12. Page, E. S. (1954). Continuous inspection schemes. Biometrika, 41(1/2), 100–115. https://doi.org/10.2307/2333009
13. Barford, P., Kline, J., Plonka, D., & Ron, A. (2002). A signal analysis of network traffic anomalies. In Proc. 2nd ACM SIGCOMM Workshop on Internet Measurement (pp. 71–82). https://doi.org/10.1145/637201.637210
14. Sekar, R., Bendre, M., Dhurjati, D., & Bollineni, P. (2001). A fast automaton-based method for detecting anomalous program behaviors. In Proc. 2001 IEEE Symposium on Security and Privacy (pp. 144–155). https://doi.org/10.1109/SECPRI.2001.924295
15. Brotby, W. K., & Hinson, G. (2013). PRAGMATIC Security Metrics: Applying Metametrics to Information Security. CRC Press / Auerbach Publications. ISBN 978-1-4398-8152-8.
16. ISO/IEC 27004:2016. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. International Organization for Standardization, Geneva.
17. Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., & Payne, B. D. (2015). Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys, 48(1), 1–41. https://doi.org/10.1145/2808691
18. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
19. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.005
20. Shannon, C. E. (1948). A mathematical theory of communication. The Bell System Technical Journal, 27(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x
21. Nelder, J. A., & Mead, R. (1965). A simplex method for function minimization. The Computer Journal, 7(4), 308–313. https://doi.org/10.1093/comjnl/7.4.308
22. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proc. 4th Int. Conf. on Information Systems Security and Privacy (ICISSP) (pp. 108–116). https://doi.org/10.5220/0006639801080116
23. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. In Proc. 8th IEEE Int. Conf. on Data Mining (pp. 413–422). https://doi.org/10.1109/ICDM.2008.17
24. Ponemon Institute. (2022). 2022 Cost of Insider Risks Global Report. Proofpoint / Ponemon Institute. Traverse City, MI.
25. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST. https://doi.org/10.6028/NIST.CSWP.04162018