The Eastasouth Journal of Information System and Computer Science
Vol. 2, No. 03, April 2025, pp. 446-458
ISSN: 3025-566X, DOI: 10.58812/esiscs.v2i03

AI-Powered Analytics Architectures for Enterprise Security and Operational Intelligence

Karthikeyan Selvarajan
Sr. Manager, Software Development Engineering, San Jose, California, United States

Article Info

Article history:

Received Apr, 2025
Revised Apr, 2025
Accepted Apr, 2025

Keywords:

Artificial Intelligence;
Cloud Security;
Enterprise Analytics;
Machine Learning;
Operational Intelligence;
Security Analytics

ABSTRACT

Cloud services, applications, networks, endpoints, and business services all generate large amounts of non-uniform security and operational data that can reside as well as be utilized by and reach the environment. These variegated streams of data cannot be related by the traditional analytics design to identify looming risks and avail timely operational insights. The current research paper introduces an AI-based analytics platform to enterprise level operations and security intelligence platform which embraces machine learning, smart data processing and real-time analytical functions under one platform. The proposed architecture will integrate with multi-source data ingestion, data normalization, feature engineering, anomaly detection, which are founded on AI, behavioral analysis, the threat intelligence correlation, and operational event processing. The hierarchical analysis framework will enable the security and operation data to be transformed to the contextualized data and make appropriate choices and continuous monitoring. Machine learning models can be used to identify abnormal behavior, prioritization of security events, identification of potential threats and establishing a relationship between infrastructure and business processes. The architecture is also seen to have cloud-native observability, centralized observability, automated feedback and alerting to enhance analytical flexibility. This paper discusses the aspects of architecture, the flow of data and the prospects of AI, integration principles, as well as the benefits of the functionality of the proposed approach. Based on the findings, AI-based analytics will be able to increase the visibility of various business security activities, increase the promptness of detecting incidents, resultant heightened awareness of the operations, and manage complex and dynamic enterprise landscapes more proactively.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Name: Karthikeyan Selvarajan
Institution: Sr. Manager, Software Development Engineering, San Jose, California, United States
Email: karthik.selvarajan83@gmail.com

1. INTRODUCTION

The data approved digital services, interconnected devices; cloud computing and distributed applications have led to rapid changes in information systems in the enterprises. This leads to a perpetually shifting host of information of security incidences, application logs, network traffic, user activities, system metrics and

operational data. Despite the fact that this information has now become a huge opportunity of improved visibility and decision making, the sheer amount, heterogeneity, velocity and complexity of this data poses new threats to the traditional monitoring mechanisms and rule-based security. The businesses therefore need analytics infrastructures which can convert operational and security mass streams information into contextual, timely and actionable intelligence.

Artificial Intelligence (AI), machine learning (ML) and deep learning (DL) has become a topical technology to assist in addressing these issues. Among things that AI-based methods are capable of doing are trend discovery (using past and current data), anomalies (patterns in expected behavior), labeling security events, and aiding in predictive analytics. Security related information in clouds can be processed with the help of ML which is capable of developing anticipatory mechanisms that can be used to identify a potential industrial cybersecurity attack [1]. These capabilities are able to turn security operations into more reactive response lent oriented responses as opposed to proactive identifications of exceptional states, when confronted with looming threats. Nevertheless, prediction model models necessitate data pipelines, data analytic components, and incorporation to be viable to execute in complicated enterprise schemes.

The complexification of managing enterprise security is also due to the increasing use of multi-cloud and distributed infrastructure. Workloads and applications can run on more than a single cloud provider, and it can be challenging to have a centralized view and coordinate threat detection. Use of cooperative intrusion detectors based on deep-learning has been observed to possess the capability of detecting malicious traffic in the multi-cloud contexts and actively understand security information [2]. Such trends imply that there is a loss of the possibility of enterprise security analytics being limited to particular aspects of the infrastructure. Security information should be gathered and compared across environments interlocks to offer a simpler image of the systems functionality, and the threats it could be vulnerable to.

The inclusion of the Internet of Things (IoT) technologies in the cloud computing presents new security and operational problems. This means that ITC spaces are made up of heterogeneous devices, communication protocols, applications and data sources which mean that there is a highly distributed attack surface. Still up to date researches have been reporting of a high number of cybersecurity threats in both IoT-cloud systems and security protocols that can support in securing the interconnected infrastructure [3]. These diverse environments are equipped with beneficial telemetry regarding the operations and security information with the environment. This implies that, effective analytics architecture is supposed to be capable of uniting the data between devices, networks, applications, cloud services, and enterprise systems as opposed to viewing them as individual entities.

The research of intelligent cloud security suggests that implementing ML and DL to slacken protection tools can as well be done. Smart techniques have been applied to detect the threats and assign the anomalies and other clouds security features [4]. The techniques have the potential of improving the capability of security platforms to recognize intricate patterns which might otherwise be eluded by fixed rules or a set of signature forms. However, single AI models do not make a full-fledged enterprise analytics architecture. They require data quality, feature preparation, model administration, the organization of analysis, and contextual correlation and concerted set-up with monitoring and response mechanisms to be effective.

Machine learning, in the research on cloud security has also explained the distinction in the algorithm that can be applied in various cybersecurity

requirements [5]. The analytical capabilities can be supplemented with other learning techniques such as classification, clustering, anomaly detection, and so on. That diversity that creates a window into possible layered AI architectures in which various AI strategies can be applied to respond to various classes of events within the business. Simultaneously, more models of analytical processing coming up, could also add complexity to architecture provided the introduction of data, processing, execution of a model and relationship of events and delivery of intelligence are not well synchronized.

It is on this background, questioning the issue of an AI-driven architecture of analytics to enterprise security and operational intelligence. The described methodology makes the notion of the security and data on the operations on the level of corresponding sources of the unceasing processing of data-analyses. It encompasses the consumption of data, its standardization, feature handling, and the AI-supported identification of anomalies and threats, correlation of events, dependency-driven intelligence and the production of operational insights. The architecture is meant to offer harmonized analytic perspective not only in heterogeneous enterprise settings but also embrace scaling and context sensitive monitoring.

The main impact of this study is the contribution of an architectural framework reconciling the field of AI-based security analytics with the elementary functions of wider operations intelligence instead of viewing cybersecurity as an independent analytical process. The proposed architecture will offer enhanced visibility of the enterprise, promote the early detection of an abnormal condition and apply it to operational decisions by leveraging security events with operational telemetry and contextual relationships. The sections below describe the architecture, elements of analysis, elements of assessment and potential future directions of AI-nearby enterprise security and operational intelligence.

2. RELATED WORK

Meticulousness of enterprise IT settings has triggered the need of progressed security analytics, which can handle diverse types of data and recognize threats in adaptable cloud and distributed settings. Deep learning (DL) and machine learning (ML) as respective methods have become salient methods in preempting cybersecurity, identifying abnormalities, identifying intrusions, and automating security levels. The literature, however, predominantly discusses only a single security issue, or a computing setting, but an overall architecture fusing security analytics with more general operational intelligence is still lacking.

Abbas and Myeong explored the applications of ML to provide forecasts on security threats to industries in a cloud environment [1]. Their article illuminates the potentiality of predictive analytics to get the security operations turned into a more of an anticipatory threat recognition of security operations as opposed to a reactive identification. The research proves the relevance of using ML to data that is associated with the security generated by clouds, specifically, the industrial example, where sustainability of business and security is intertwined. Nonetheless, the emphasis is on prediction, instead of on an in-depth enterprise analytics framework that would combine various security and operational data points.

Proactive multi-cloud cooperative intrusion detector proposed by Abusitta et al. is based on the principles of deep learning [2]. In their effort, they touch on the issues that relate to the maliciousness evident in the distributed cloud platform and they stress on collaboration between the cloud platform. Complex trends of intrusion, which can be hard to detect with rule-based systems, can be learned using deep learning. The plan is however inclined towards intrusion detection more than other areas of operations

such as operational intelligence within a broader scope, cross domain operational detectives and enterprise decision support.

Ahmad et al. [3] critically assessed the issues of security of using the IoT and cloud computing. These numerous threats to IoT-cloud ecosystems are outlined in their survey, as well as security mechanisms are analysed. The heterogeneity of devices, communication systems, and cloud services and applications that form the IoT is a great challenge to any centralized solution to security monitoring. The research warrants the existence of smart security controls in the interconnected infrastructures, which are smart and can be scaled to work. However, the reviewed solutions are more aligned towards cybersecurity protection compared to integrating security analytics with a dynamic operational intelligence.

Belal and Sundaram have constructed a smart taxonomy of smart defenses of cloud security concerns comprising of security challenges, ML / DL methods, issues and research directions [4]. Their discussion reveals how intelligent approaches can be extremely used to cloud security, such as recognizing threats, their categorization, and anomaly. The work offers a valuable basis on the comprehension of how AI techniques can reinforce cloud security designs. At the same time, the abundance of specific methods through which the review has proven indicates the necessity that there is the need to integrate architecturally so that various services of analysis can then be invoked within the same almost as the enterprise security and intelligence.

Butt et al. conducted a survey of the use of ML algorithms in cloud computing security and how these algorithms apply to different security challenges [5]. The paper pinpoints that ML is a significant tool in detecting abnormal behavior, attacking in classifications, and boosting automated security determination. It also throws light on the issues relating to the choice of the right algorithms and the complexity of the cloud set-ups. Despite being a fine addition to an algorithmic perspective, the work treated mainly the MI approaches in isolation and does not make a direct reference to the fact that the approaches can be considered with reference to the enterprise observability, operational metrics, and cross-source intelligence.

Another area that Chkirbene et al. have given special attention is cloud anomaly detection where they have developed a method of detecting an unusual activity in a cloud computing system using a method relying on ML [6]. Their contribution proves the worth of the data-driven methodology analysis to differentiate between normal and abnormal cloud behaviour. This anomaly-detecting capability is a crucial feature of the AI-powered enterprise security as a threat previously unknown or appeared may very well be similar to no existing signature. Nonetheless, as they are not used together with logs, network events, application telemetry, user behavior, and service dependencies, the use of anomaly detection does not provide much contextual knowledge.

Dasgupta et al. performed an extensive study of using ML in cybersecurity [7]. They have touched a few topics pertaining to cybersecurity by discussing several security applications and how their learning-based approaches could assist them in their detection and classification efforts. The paper also shows the problem of the quality of data, credibility of the models, the face-off with the opponents and the practical challenges. These concepts are particularly true in the context of the enterprise environment in which the security analytics will be required to process data of constantly varying values without compromising its ability to detect. However, it is not a set up of integrated security and activity intelligence, but just an overview of the cybersecurity.

Hassija et al. analyzed the security threats in the IoT, its areas of application, and remedies to the threats [8]. Their work has shown that effective security cannot exist based on independent security mechanisms each of which needs to be architecturally

considered and designed in terms of devices, communication networks, applications, and data-processing components. The provided design vision is valuable in the scenario of enterprise environments where security expertise is gained on different levels of infrastructure. The study, however, is not as fresh as most of the modern innovations taking place in AI-powered enterprise-wide observability and, more precisely, lacks the information about how to merge intelligent analytics and operational intelligence.

The systems of Internet of Things intrusion detection were reviewed by Heidari and Jabraeil Jamali, as well as the approaches to be taken in their further studies [9]. They discuss the methods of detection, security issues and the origin of the use of the smart techniques in the IoT environments. This paper highlights the need of adaptive intrusion detection of more and more diverse and distributed systems. Its findings validate that AI-based analytics are an efficient complement to alternative security setups within bigger companies. This ultimate aim is however intrusion detection and not the liaison between the security and operation analysis.

Hernandez-Jaimes, et al. talked about AI as the security of an IoMT with references to the intrusion detection solutions, to attacking, to data collection, and to Cloud-Fog-Edge maps [10]. Their activity can be particularly applied in the context of distributed enterprise environments as it considers the AI-driven security of different computing layers. Orchestration of distributed analytics, data processing and security has new requirements introduced by the integration of cloud and fog and edge resources. In spite of such architecture profusion, it is concentrating on the security of the IoMT and this gives a scope to apply same concepts to security and operational intelligence to a world enterprise level.

Kumar et al. have also considered the intrusion detection and intrusion prevention of cloud computing on the perspective of deep-learning [11]. Their work is a witness that EVs can be able to support the automated identification of dangerous actions and help in preventing security provisions. Such capabilities can be a layer of the enterprise security systems. Nevertheless, efficient enterprise intelligence need not simply be able to manage the identification of intrusion but must also incorporate the security events with state of affairs, service relationships, performance metrics as well as trends.

Finally, a very comprehensive review on the detection of graph anomalies using deep learning has been published by Ma et al. [12]. Graph-based analytics are specifically suitable to enterprise settings, as the interactions among users, devices, applications, services, and network elements can be modeled as intertwined networks. Graph anomaly detection could then be used to supplementary contextual analysis to detecting events with deep-learning in reporting. This study suggests an opportunity to model a complex dependency and identify suspicious relationships, but is primarily the graph anomaly identification, rather than end-to-end enterprise security, and operational intelligence architecture.

All in all, it can be noted that the literature on the topic is quite strong in stating an AI-assisted cybersecurity and cloud aberrancy detection, intrusion detection, and distributed security architecture [1], [2], [11], [12], [3]–[10]. Nevertheless, the majority of the methodology highlights individual analytic actions, distinct settings or the type of dangers. It has failed to pay attention to an integrated architecture to build heterogeneous enterprise telemetry, AI-driven anomaly and threat analytics, dependency-based correlation, security intelligence and operational insights into a unified system. The provided gap will create an AI-assisted architecture of analytics that will help bridge the gap between security surveillance and enterprise wide operational intelligence and aid in preserving contextually-sensitive decision-making.

3. COGNITIVE TELEMETRY FABRIC FOR AI-DRIVEN SECURITY AND OPERATIONAL INTELLIGENCE

The framework proposed sets up an integrated Cognitive Telemetry Fabric that ties together enterprise data gathering, smart analytics, security rationale, operational intelligence, and ongoing responses. The architecture considers both security and operational information as two signals of analysis, contrary to traditional security architectures that emphasize more on identification of known threats. It is used in the environment of heterogeneous enterprise, which is cloud infrastructures and apps, networks, endpoints, databases, identity systems and distributed services. This architecture is in the form of layered architecture that involves series of processing raw telemetry to normalized data, analysis properties, situational intelligence and actionable experiences.

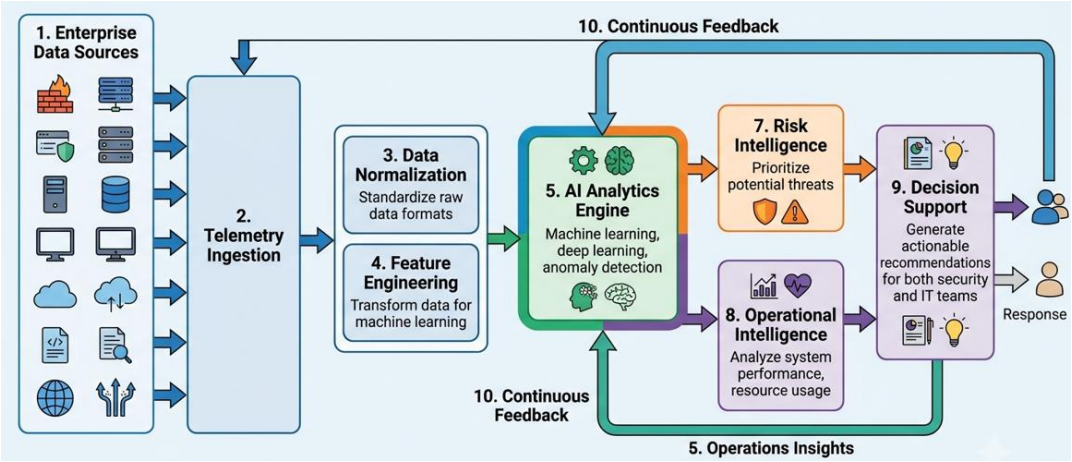


Figure 1. AI-Driven Enterprise Security and Operational Intelligence Architecture

3.1 *Enterprise Telemetry Acquisition Layer*

The former level gathers heterogeneously generated data that is generated at the enterprise level. The following are some of the key sources: cloud infrastructure, virtual machines, containers, databases, enterprise applications, network devices, endpoints, identity services, APIs, and business applications. A part of this information gathered by the information collected can encompass system metrics, application events, access event, security alert, audit trail, network flows, transaction related and service level indicators.

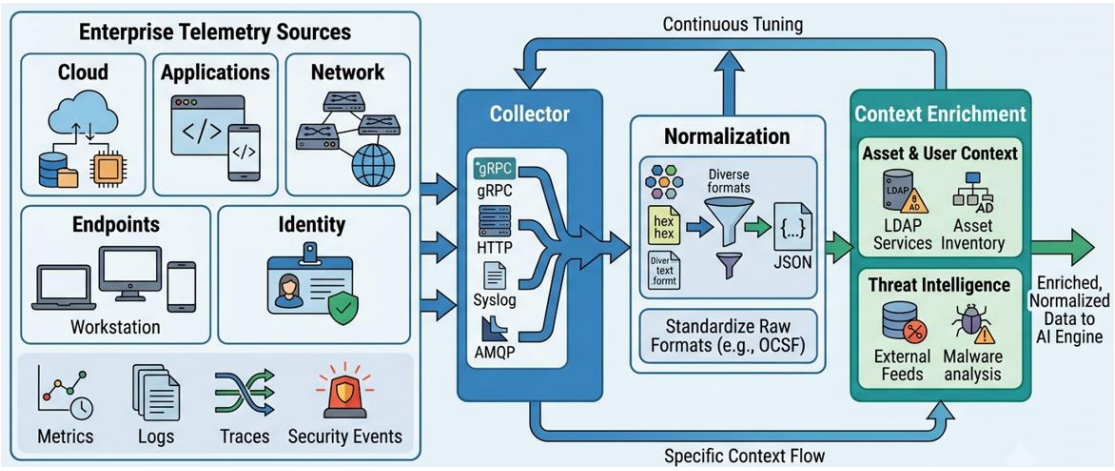


Figure 2. Enterprise Telemetry Acquisition and Contextualization Pipeline

It needs a single acquisition mechanism since the information provided by enterprise systems is in varying formats and varying rates. The model hence facilitates organized, semi-organized and eventual information. The processing of streaming data can be done continuously unlike historical data which then can be involved in the continuous processing through the use of batch-based pipelines. Such a combination assists the framework to investigate current system conditions and the trends of behavior in the past.

3.2 Data Normalization and Contextualization Layer

The diverse AI models are not capable of receiving the raw telemetry because different sources have different schema, names, time stamps and other data representations. Data normalization and contextualization is therefore done in the second layer. The event transformation also entails the derivation of similar representations of event, time alignment, duplication eradication/enrich events meaningful attributes.

Contextualization contextualizes events to enterprise entities such as users, devices, applications, services, workloads and network segments. An example of this is that an authentication anomaly will be of greater importance when detected in relation to any of the following: a single identity, a device, an application, a location or dependency on a service. Higher level security reasoning can thus be provided by context enrichment.

Metadata of the original, reliability, sensitivity and time, of a particular piece of data is also stored in the layer. These metadata can be used to support the downstream choices of analytics as well as help to isolate events of operational importance over telemetry that is not valuable.

3.3 Feature Engineering and Behavioral Representation

The third layer converts normalized telemetry to forms that are analytical and can be dealt with through the assistance of AI. Attributes can be frequency of events, request behavior and authentication behavior, resource utilization, network behavior, service response behavior and the correspondence between the enterprise entities.

The framework does not merely indicate that only indicators are developed manually and the framework supports behavioral representations depending on previous observations. Baselines can be constructed around the users, services, applications, devices and workloads. The anomaly detection models can then be used to analyze deviations in terms of these baselines.

Temporal properties are particularly important because the behavior of an enterprise is different, the load changes, the business cycles, and maintenance operations, and the demand on the application. As a result, the framework takes into account temporal context in creating behavioral representations. This constrains such possibilities to make bona fide operating change as security inconsistencies.

3.4 AI Security Analytics Engine

The central component (AI) is an engine of AI Security Analytics with different analysis complementary functions. The framework is artificially encouraging a set of methods of analysis, which do not lie on a single ML model.

Any irregularities between the patterns in behavior are signaled by anomaly detection. In classification of models, events are based on a collection of security or operating categories. The clustering mechanism can indicate previously unknown set of behaviors and the predictive models have the ability to determine the probability of

the occurrence of the abnormal conditions in the future. High-dimensional shapes can be also complex to model with general statistical laws and are also handled easily with deep learning.

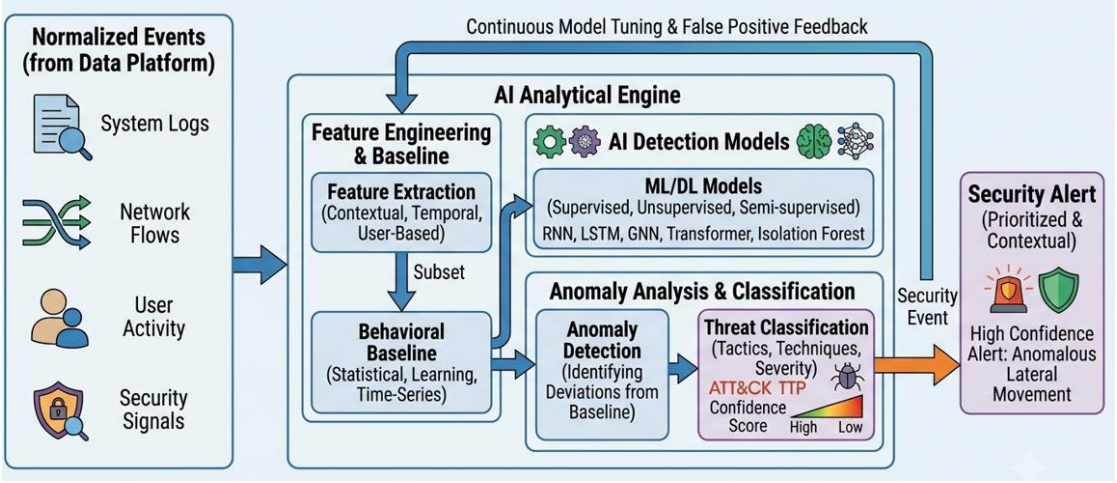


Figure 3. AI-Based Security Analytics and Anomaly Detection Flow

The framework also aids behavioral analytics in the identification of abnormal activity with regard to identities, applications, devices, and workloads. An incidence of abnormal authentication behavior, unexpected consumption of the resources, and abnormal network communication between them can also serve to relay a stronger signal of security than any select occurrence.

The outputs generated by AI receive a sense of contextual trust, and analytical importance, as opposed to being considered final judgments. This enables the latter to correlate and construct policy elements with multiple signals then create high-priority alerts.

3.5 Multi-Signal Correlation and Dependency Intelligence

The compatibility of security and operational signals is one of the main points of the framework. One time situations are not able to provide sufficient context on whether an event is significant. Measure, journals, follow-ups, warns, personal data and behaviour notes are thus considered towards a correlation layer.

The ERs assume the form of interrelationship between applications, services and infrastructure, users and data resources. Graph representations may be graphed to identify a relationship that is not normal or propagation pattern. This comes in handy especially when an abnormal event takes place involving several interacting services.

In order to illustrate the argument, a higher scale of resource consumption might seem like a problem at the outset and is coupled with a process. It may be a state of security relevance when combined with out of chain authentication behavior, and abnormal network communication. But in the opposite also where traffic increases abruptly during the operating period of expected business event one then should consider it differently where the situation of running up business is accessible. Correlation can then be utilized to enhance contextual discrimination of true danger, dynamic operation and work load change of a reactive character.

3.6 Security Intelligence and Risk Prioritization

The results of the analysis are correlated and sent to a security intelligence layer which integrates analytical results and lays priority on the occurrences. The framework does

not result in large amounts of autonomous warnings, instead taking into group connections amongst the observing that are associated with security circumstances with greater levels.

The risk prioritization takes into account: the intensity of the incident that occurred, the impacted assets, the diversion of behavior, dependency on service, the rate of confidence or confidence levels, and the instance of the event and dependency impact. Such a methodology can enable a reduction in the load of alert since it can be used to target those events with more favorable context or enterprise-level influence.

The intelligence layer can also absorb pre-set requirements and policies of the organization in the context of security. Consequently, when two priority in consideration of the criticality of service or asset is considered, separate priority can be given to the same technical anomaly.

3.7 Operational Intelligence Layer

The model extends the sphere of cybersecurity with the help of integration of operational intelligence. Security incidents are monitored, availability of services, resource utilization, and performance of the application, latency, throughput and error rate among other operations indications.

Such co-location can help the security teams, and the operations ones, make an opinion concerning the state of the enterprise shared. Security event can thus be analyzed based on the possible impact of such an event on business operation and performance of the service. Similarly, a security investigation can be undertaken on an operational anomaly with the potential causes of security.

Operational intelligence dashboard information is shown in summaries in the form of analytical views, trends, dependency and prioritized events. These visualization systems may be able to provide real time and historical data to enable monitoring, interrogation and management decision making.

3.8 Automated Response and Decision Support

The latter turns the analysis findings to the response and where possible response approval to the organization to automatic response in accordance with the policies. The categories of responses may involve creating notifications, requesting further investigation, and further monitoring acuity, making authentication verifications, isolating impacted workloads or initiating procedures aimed at dealing with pre-established incident management.

Analysis and reply authorization is separated by the framework. The evidence and patterns are identified, respectively; AI models are the decision makers to whether the action needs to be executed automatically or not, i.e. in policy and governance terms. This particular type of segregation is significant as any form of business can be derailed due to counterfeit automatization in an organization.

3.9 Continuous Learning and Feedback

The last element forms a loop of the feedback connecting the result of the work and the analytical engine. Security analysts have the ability to verify alerts, categorize false positives, and verify incidents as well as giving other contextual information. Operational findings can also be helpful to detect an identified anomaly as a genuine service problem.

These are all the kinds of feedback that can be used in the model refinement process, where baselines are tweaked and features of the model optimize, and updating policies run analytical processes. The form is thus an ever-changing intelligence system as

opposed to a fixed set of detection models.

Overall, the Cognitive Telemetry Fabric embraces heterogeneous enterprise telemetry and AI-driven analytics, contextual correlation, dependency intelligence, security prioritization, and operational tracking. It has stratified architecture that enables the outflow of raw data off collection in more significant intelligence and provides feedback between the products of analytical output and enterprise business practices. The created architecture offers a common core to the operational intelligence of proactive security checks and context in the complex cloud and enterprise environment.

4. INTELLIGENCE ASSURANCE AND ARCHITECTURE VALIDATION

Cognitive Telemetry Fabric is characterized against the scalability, analytical effectiveness, contextual intelligence, operational integrations and flexibility. The evaluation is on the ability of the architectural components to individually contribute to enterprise security and operational intelligence as opposed to assessing AI models individually.

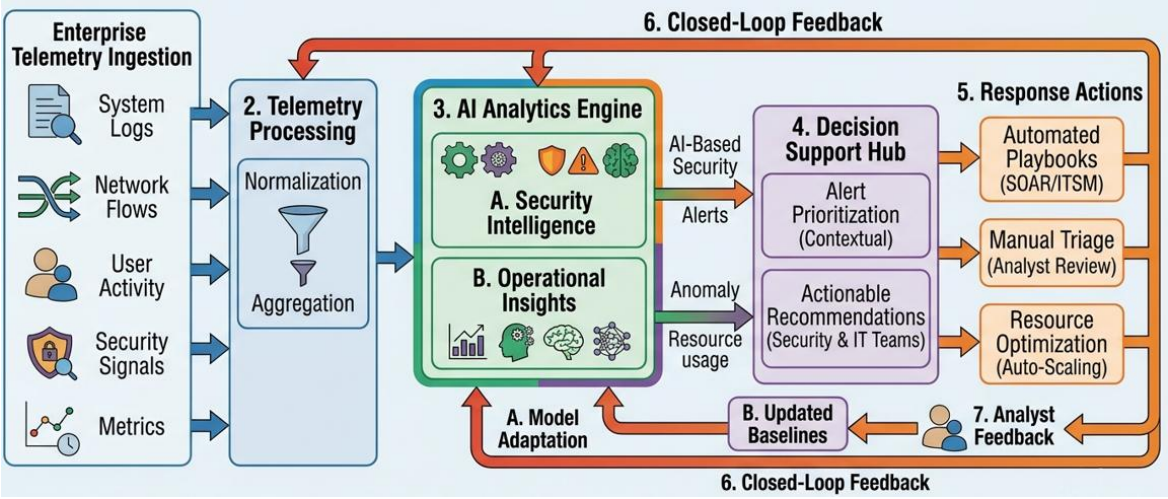


Figure 4. Closed-Loop Security and Operational Intelligence

4.1 *Analytical Effectiveness*

The architecture has several analytic capabilities which include: anomaly detection, classification, behavioral analysis and predictive intelligence. When combined with these capabilities, the framework will be able to concentrate on both the well-known and unknown trends in history. Multi-signal correlation can be used in conjunction with a mixture of metrics, logs, traces, identity events, and security alerts to enhance the interpretation of analytics. This makes the reliance on individual indicators less necessary, and allows more contextual happening of potentially important events.

4.2 *Contextual Security Intelligence*

One of the important architectural capabilities is a mix of security information and business background. Before the prioritization, there will be user, workload, application and service dependency and infrastructure dependency events. We can therefore obtain the identical technical incidents, which depending on the asset criticality or the operating condition could be subjective. A dependency informed analysis may also give a clear picture about the propagation that may happen between the interdependent services. Such a contextual approach can increase

meaning in prioritization as compared to independent event-based alerting.

4.3 Scalability and Distributed Processing

The enterprise reality is not only creating vast amounts of telemetry on a steady basis but it is also originating at a geographically distributed as well as non-homogenous locations. Our proposed layered architecture has been designed in a manner that acquisition and normalization and feature processing, analytics and correlation and visualization are completely decoupled and hence each of them can be made to scale to the work load autonomously. It can be combined with streaming and batch processing, which will allow a real-time positioning and historical analysis. Collector and analytical services can also be distributed in a decentralized manner in order to decentralize the processing load to centrally placed elements.

4.4 Operational Intelligence Integration

The framework does more than just the basic surveillance of security but also comprises operational indicators of availability, latency, resource utilization, error rates and performance of the services. The integration allows analyzing the security and operational incidents in a shared analysis environment. One such exclusion is that an anomaly in application-performance might be correlated with a network event or authentication to identify relationships that might exist. Security alerts on the other hand can be rated in accordance with the operational damage that the alert may have.

4.5 Adaptability and Continuous Learning

It is dynamic in that as time goes by the workloads, the application releases, the infrastructure and the changing user activity of an enterprise lead to a change in behavior of an enterprise. With this dynamic work conditions the laws can be less efficient. The behavioral baselines and operational models are also honed with the input of analysts and operational performance within the framework. Attentiveness to new trends and minimization of the ongoing false-positive situations can be facilitated using on-the-fly feedback.

4.6 Governance and Explainability

The security systems that will be produced on the basis of AI will not need a lot of decision making, as there will be a possibility of unpredictability of the product of the analysis. Automated response and AI inference and policy enforcement is not supported by the architecture. The analytics can be output accompanied with confidence, contextual evidence, and affected assets, and correlated event hence security personnel might scrutinize the premises of prioritized alerting. Those actions with high impacts can thereby be delegated to human control.

Overall, the assessment has revealed that the suggested architecture presents an architecture which can provide a global framework of scalable, contextual and adaptable enterprise security analytics. It fills these gaps inherent in separate detection systems and forms a larger scale system of situational awareness continuously available in the enterprise through its combination of telemetry, artificial intelligence, dependency analysis and operational intelligence.

5. CONCLUSION

The growing popularity of distributed cloud systems, multifaceted apps, a plethora of various devices and the constant production of operational data is all set to become a common feature on the enterprise environment. These are great challenges to the past security monitoring paradigms that used a single notification, reestablished rules, and analysis systems that were not integrated. The study showed a heterogeneous telemetry and machine learning-driven AI-based analytics architecture to enterprise security and

operational intelligence to overcome these issues.

The suggested Cognitive Telemetry Fabric is a layered design that converts crude enterprise telemetry to useful and valuable intelligence. Telemetry acquisition and normalization features ensure an equal platform on which to handle cloud infrastructure, application, network, endpoint, identity and service data. The layer of AI analytics then goes through the algorithms of anomaly detection, classification, behavioral analysis, and predictive to discover potential meaningful patterns. Multi-Signal correlation and dependency intelligence will also be in a position to provide some insights on how security events will correlate to operation situations and enterprise entities and vice versa.

Among the significant contributions of the framework is the fact that it has incorporated the security analytics with the operational intelligence. The architecture also takes the risk measurement as something that is to be accounted along with service availability, resource utilization, application performance, latency and other performances of operations as opposed to treating each event of cybersecurity as a single event. The resultant perspective can be used to increase the presence of the enterprise, and more informed exploration and decision-making. Ongoing feedback also makes it possible to develop improved analytical models and behavioral baseline with changes in the conditions at the enterprise.

The framework analysis shows that the architecture can be beneficial in terms of scalability, contextual analysis, distributed telemetry processing, adaptive intelligence and ability of operational coordination to security. Nevertheless, practically, the data quality, explainability of the models, computation overhead, privacy, governance, interoperability and the handling of false-positives need to be taken into consideration.

It can be generalized to explainable AI, graph-based security reasoning, federated analytics, organising autonomous responses, privacy preserving learning and multimodal telemetry analysis in the future.

REFERENCES

[1] Z. Abbas and S. Myeong, "Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in Cloud Computing Environment," *Electronics*, vol. 12, no. 12, p. 2650, 2023, doi: https://doi.org/10.3390/electronics12122650.

[2] A. Abusitta, M. Bellaïche, M. R. Dagenais, and T. Halabi, "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," *Futur. Gener. Comput. Syst.*, vol. 98, pp. 308–318, 2019, doi: https://doi.org/10.1016/j.future.2019.03.043.

[3] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, no. 1, p. 16, 2022, doi: https://doi.org/10.3390/electronics11010016.

[4] M. M. Belal and D. M. Sundaram, "Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9102–9131, 2022, doi: https://doi.org/10.1016/j.jksuci.2022.08.035.

[5] U. A. Butt *et al.*, "A Review of Machine Learning Algorithms for Cloud Computing Security," *Electronics*, vol. 9, no. 9, p. 1379, 2020, doi: https://doi.org/10.3390/electronics9091379.

[6] Z. Chkirbene, A. Erbad, R. Hamila, A. Gouissem, A. Mohamed, and M. Hamdi, "Machine Learning Based Cloud Computing Anomalies Detection," *IEEE Netw.*, vol. 34, no. 6, pp. 178–183, 2020, doi: https://doi.org/10.1109/MNET.011.2000097.

[7] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *J. Def. Model. Simul.*, vol. 19, no. 1, pp. 57–106, 2022, doi: https://doi.org/10.1177/1548512920951275.

[8] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2924045.

[9] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," *Cluster Comput.*, vol. 26, no. 6, pp. 3753–3780, 2023, doi: https://doi.org/10.1007/s10586-022-03776-z.

[10] M. L. Hernandez-Jaimes, A. Martínez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures," *Internet of Things*, vol. 23, p. 100887, 2023, doi: https://doi.org/10.1016/j.iot.2023.100887.

[11] A. Kumar *et al.*, "An intrusion identification and prevention for cloud computing: From the perspective of deep learning," *Optik (Stuttg).*, vol. 270, p. 170044, 2022, doi: 10.1016/j.ijleo.2022.170044.

[12] X. Ma *et al.*, "A Comprehensive Survey on Graph Anomaly Detection With Deep Learning," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 12, pp. 12012–12038, 2023, doi: https://doi.org/10.1109/TKDE.2021.3118815.