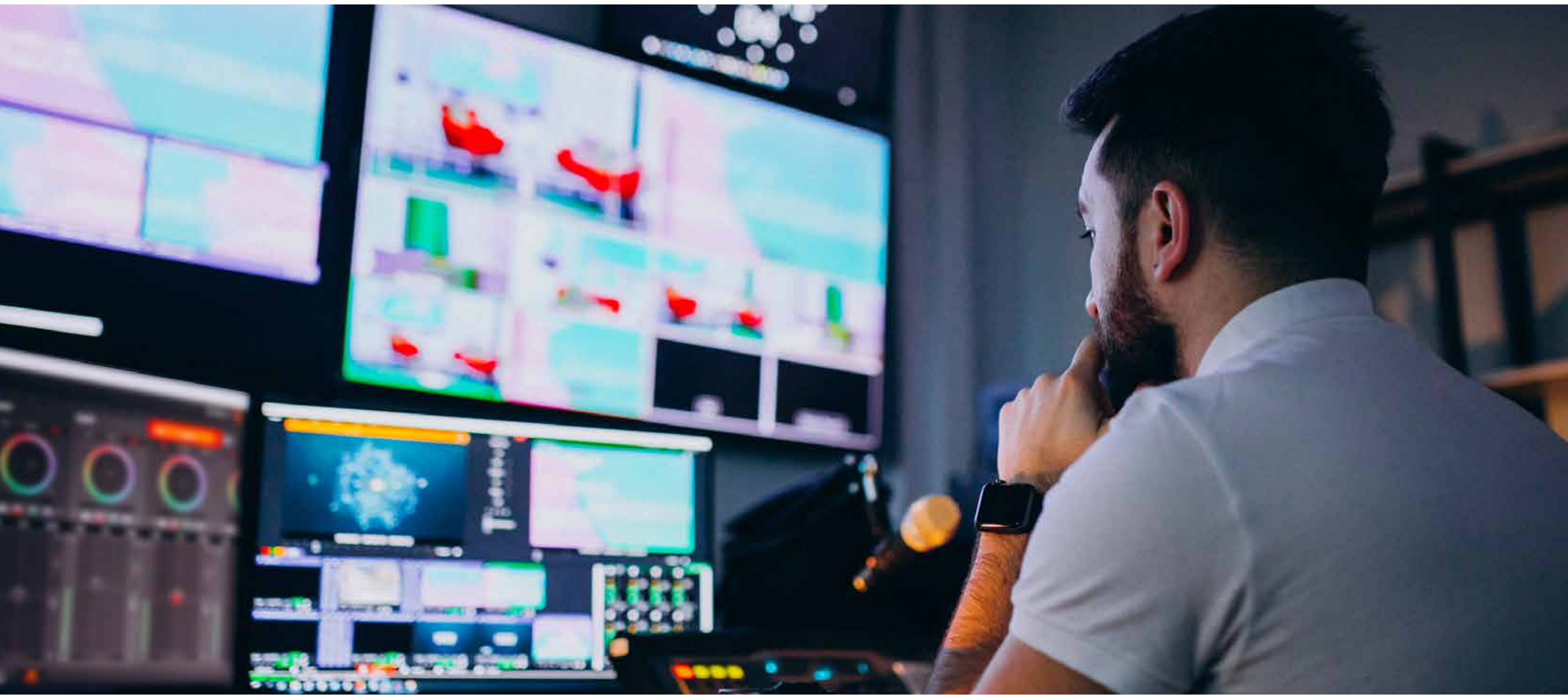
White Paper



Machine Learning for SOC (Security Operations Center)

Gireesh Sreedhar KP

Senior Technical Manager - Location Zero, GAVS

Ravindran Girikrishnan

Senior Technical Manager - Cyber Security Operations, GAVS

What is SOC?

The Security Operations Center (SOC) of an organization, also known as the Cyber Security Response Team, enforces controls that continuously monitor and prevent security incidents.

The SOC consists of information security experts who are certified in various aspects of cyber security. The SOC works 24/7 for the organization to continuously monitor and detect threats that can breach the integrity, confidentiality, and availability of their data, services, and IT assets. It relies on different threat sources that are highlighted in real time, empowering the team to mitigate cyber attacks before they can cause any damage.

The SOC plays a critical role by providing front-end protection to an organization, helping build a strong security posture by continuous monitoring and reviewing of logs from various sources.

Maintenance of Security Monitoring Tools

To effectively secure and monitor systems, the SOC requires a suite of technology products that provide a holistic view into the organization's security environment that the team must maintain and update on a regular basis. This involves collecting data from security tools and all the systems in the network and feeding them into log analytics tools (SIEM).

Investigation of Suspicious Activities

With the assistance of security monitoring tools, the SOC is responsible for investigating suspicious and potentially malicious activities within the organization's networks and systems. Typically, this is done by receiving and analyzing alerts from the SIEM which may contain signs of compromise, and related threat intelligence.

Key Responsibilities of SOC

Routine Checks & Advisory

The SOC needs to constantly advise on and implement necessary changes required to effectively prevent & counter attacks and improve security standards.

Ensuring Regulatory Compliance

The SOC is often responsible for auditing systems to ensure they meet compliance requirements of government, corporate, and industry regulations.

Machine Learning (ML)

Machine Learning provides systems the ability to automatically learn and improve from experience, without being explicitly programmed.

The two phases of ML are Training and Inference.

Training: This phase is used to teach and perfect the ML models on how to achieve desired outcomes, using two types of training data -

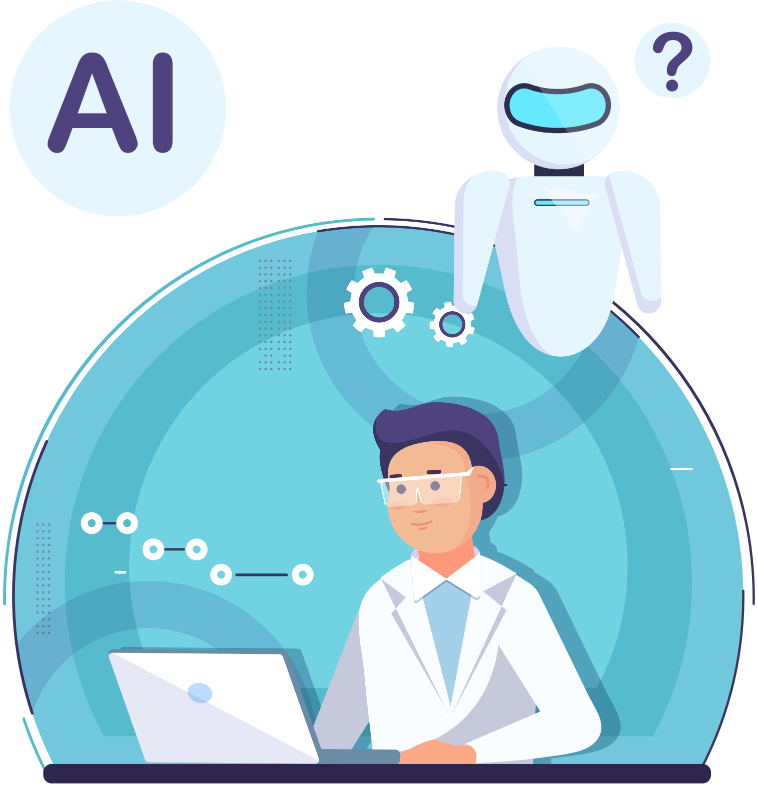
Labelled data: Labelled data refers to data that has labels to capture the expected outcomes. This is used for training supervised models.

Unlabelled data: Unlabelled data refers to data without labels. This is used for training unsupervised models.

Inference: In this phase the trained model(s) are deployed in a live environment to achieve desired outcomes and are continuously monitored for performance.

Main ML Methods:

Supervised Machine Learning Algorithms: This class of algorithms uses labelled training data (with known outcomes) to train models so that the algorithms can classify new data from what has been learned from labelled inputs.



Unsupervised Machine Learning Algorithms: This class of algorithms uses unlabelled training data (with no information on outcomes) to train models. Unsupervised learning studies how systems can infer a function to describe a hidden structure from data. The system explores the data and can draw inferences to describe hidden structures from data.

Reinforcement Learning Algorithms (RL): This class of algorithms creates their own data by interacting with the environment, takes action to receive feedback, and learns from feedback received. RL algorithms automatically determine the ideal behavior in a specific context that would maximize performance.

Why Machine Learning for SOC?

To understand this, let us look at some challenges with traditional SIEM tools:

Manual Intervention: Most organizations use a wide variety of disjoint security tools. This leads to operational inefficiencies since it necessitates manual translation of the security alerts and policies between different environments.

Resources: There is a shortage of competent SOC analysts in the market, which means that many SOC teams are not sufficiently equipped to handle threats effectively.

Lack of a Unified View: When it comes to 24/7 monitoring, SOC analysts need tools that can correlate logs from various systems in a network. There are some disadvantages & gaps when this is done by SIEM:

> Complex: Collecting the right data, aggregating & correlating it from different tools & technologies in order to get a unified view is an enormous task. This requires coordinating with the data owners, making sense of the data, and then sending relevant information to SIEM.
>
> Undiscovered Devices: Most often SIEMs are unaware of unregistered devices in the organization, for instance IoT and mobile devices, resulting in many devices remaining hidden and unmonitored.
>
> Expensive: In addition to costs of licenses, organizations would need to invest in experts to integrate the data from various sources and design relevant event correlation rules to extract meaningful insights from the data – in the security context of the organization.
>
> Alert Fatigue: Too many alerts can result in alert fatigue and cause critical alerts to be missed. To minimize noise, SIEM needs to be periodically fine-tuned.
>
> Inadequate Context: Although SIEMs aggregate logs, they may not provide context or insights into how best to respond now and how to prevent future occurrences.
>
> Time Consuming: It can take too much time to mitigate threat with SIEM. Since the generated alerts require human intervention to analyze and take actions, the threat mitigation process is delayed and could lead to extended downtime.

To overcome these challenges and to handle the volume and complexity of modern-day hybrid and dynamic IT infrastructure, the SOC must leverage Machine Learning, as ML can identify security threats with high reliability using the same data sources as SIEM, while also reducing the time and experience required in the SOC. By adoption of Machine Learning, the entire process can be streamlined with algorithms identifying critical events and automatically triggering remediation.

How ZIF Machine Learning Works:

Zero Incident Framework™ (ZIF™) is an Artificial Intelligence led technology platform powered by Machine Learning techniques, offering Machine Learning solutions across multiple domains.

ZIF has a suite of anomaly detection machine learning algorithms which can learn from log data to benchmark normal behavior and flag when abnormal or unexpected deviations are observed. Further, the algorithms can learn appropriate remedial action for an identified threat and trigger automatic remediation.

ZIF algorithms learn continuously from latest data and user feedback to incorporate behavioral changes happening in systems over time.
This ensures that abnormal behavior is flagged with current understanding of system behavior rather than behavioral understanding from some point in the past.

Conclusion

Traditional SIEM tools have not been able to scale up to handle the volume and complexity of modern-day hybrid and dynamic IT infrastructure. We have reached a point where SOC needs have surpassed the limits of traditional SIEM and human capabilities, and so, supplementing SIEM and human intelligence with Artificial Intelligence and Machine Learning have now become indispensable.

ZIF

ZIF (**Zero Incident Framework™**), is an award-winning AIOps platform for IT Operations. ZIF delivers business outcomes by leveraging unsupervised pattern-based machine learning algorithms. Infrastructure and application telemetry data are aggregated, correlated, and potential failures are predicted. To enable faster resolution and better user experience, ZIF deploys intelligent bots for proactive remediation. Developed by GAVS Technologies (www.gavstech.com), ZIF is available as an on-premise and SAAS solution.

To find out how ZIF can help your organization, please visit **www.zif.ai** or write to **inquiry@zif.ai**