Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2020, 7(12):107-111

Research Article ISSN: 2394 - 658X

# Streamlining Enterprise Cybersecurity: Building Real-Time Threat Analytics Solutions

**Laxminarayana Korada[1], Vijay Kartik Sikha[2], Dayakar Siramgari[3]**

[1]ORCID: 0009-0001-6518-0060, laxminarayana.k@gmail.com
[2]ORCID: 0009-0002-2261-5551, vksikha@gmail.com
[3]ORCID: 0009-0004-0715-3146, reddy_dayakar@hotmail.com

## ABSTRACT

The proliferation of cybersecurity tools in enterprises has led to an overwhelming complexity in managing and responding to security threats. Since the 1990s, as organizations have increasingly invested in cybersecurity to combat growing threats and sophisticated attacks, they have accumulated a vast array of tools designed to address various aspects of their security needs. This accumulation has resulted in a fragmented security landscape where the effectiveness of individual tools is often undermined by their lack of integration. This paper explores the challenges associated with managing a multitude of cybersecurity tools and examines the emerging solutions aimed at providing near real-time threat analytics. Case studies of industry leaders such as Splunk, Microsoft Azure Sentinel, and LogRhythm illustrate how automation and advanced analytics are addressing these challenges. Additionally, the paper discusses the complexities and benefits of in-house solutions with open-source tools and the role of artificial intelligence in enhancing enterprise security. By integrating these approaches, organizations can improve their security posture, streamline their operations, and better manage their cybersecurity investments.

**Keywords:** Cybersecurity Tools, Threat Analytics, Automation, SIEM, Opensource Security Solutions, Artificial Intelligence, Splunk, Microsoft Azure Sentinel, LogRhythm

## INTRODUCTION

The need to invest in cybersecurity became clear in the 1990s when viruses like “Melissa” and “ILOVEYOU” infected millions of PCs. Companies had to create security budgets and invest wisely to protect their systems. Initially, companies hired cybersecurity experts, but experts are expensive. To support their security teams, businesses began buying various tools. During the 90s, many software and hardware solutions emerged to meet different security needs. This trend has continued for over 20 years, with many products created to secure different parts of business technology systems. Today, technology stacks are much more complex. Many companies use a mix of on-premises servers and multiple cloud services. Securing such a complicated system is a huge task. Security teams now need many different tools to protect against all possible threats (Smith, 2019).

With growing reliance on technology and the increasing sophistication of cyberattacks, organizations are compelled to invest more heavily in cybersecurity. According to Gartner, average annual security spending per employee increased from $584 in 2012 to $1,178 in 2018. Major banks and technology firms now allocate over half a billion dollars annually to cybersecurity, and these budgets continue to rise (Asen et al., 2019). IBM (2020) states that organizations utilized over 45 different security tools on average. It further states that adding more tools did not always improve security response efforts; it often made them more complicated. Using open, compatible platforms and automation technologies can simplify the response process by minimizing the challenges of managing numerous disconnected tools. Many organizations are working to create timely, relevant, and actionable cyber threat intelligence (CTI) to make better cybersecurity decisions. To enhance CTI capabilities, leading cybersecurity companies such as FireEye, Anomali, ThreatConnect, McAfee, CyLance, and ZeroFox have developed CTI platforms. These platforms help organizations prioritize threats, identify key threat actors, understand their tools, techniques, and procedures (TTP), deploy effective security measures, and ultimately improve their overall cybersecurity hygiene (Samtani et al., 2020).

**Key Categories of Cybersecurity Tools**

| Category | Purpose | Importance | Examples |
|---|---|---|---|
| Network Access Control (NAC) | Enforces security policies on devices and users accessing the network, ensuring devices meet security standards before granting access. | Essential for managing complex IT infrastructures and adapting to the increasing use of mobile and IoT devices. | Aruba ClearPass Policy Manager, CounterACT |
| Data Loss Protection (DLP) | Prevents sensitive data from being accidentally or maliciously transmitted outside the organization, with monitoring and blocking capabilities. | Crucial for detecting hacker activity and insider threats, and for compliance with privacy regulations. | Symantec Data Loss Prevention, McAfee DLP |
| Firewalls | Filters network traffic based on predefined rules to block threats and unauthorized access. | Evolved to offer deeper packet inspection and advanced threat prevention beyond traditional perimeter defense. | Fortinet FortiGate, Cisco Firepower NGFW Series |
| Intrusion Prevention Systems (IPS) | Monitors and analyzes network traffic to automatically block malicious data packets and respond to threats. | Enhances network defense by offering real-time threat mitigation. | Cisco Next Generation IPS, Trend Micro TippingPoint |
| Endpoint Protection | Safeguards desktops, laptops, and other devices from malware and malicious activities. | Vital for detecting and mitigating threats that bypass network-level defenses. | ESET Endpoint Security, Symantec Endpoint Security |
| Identity and Access Management (IAM) | Manages user access to enterprise systems and data based on roles and permissions. | Critical for securing access as the perimeter shifts from traditional boundaries to identity-based control. | SailPoint IdentityIQ, Centrify Next Gen Access |
| Cloud Access Security Brokers (CASB) | Enforces security policies for cloud service access, including authentication and malware detection. | Ensures security and compliance in increasingly complex cloud environments. | Netskope Security Cloud, McAfee Skyhigh Security Cloud |
| Antimalware Tools | Protects against a range of threats including viruses, ransomware, and spyware. | Essential for defending against modern threats that surpass traditional antivirus solutions. | Kaspersky Anti-Virus, Webroot SecureAnywhere |
| Endpoint Detection and Response (EDR) | Detects and responds to threats on endpoint devices through continuous monitoring and behavior analysis. | Enhances traditional endpoint protection by providing advanced threat detection and response capabilities. | SentinelOne EDR, CrowdStrike Falcon Insight |
| Mobile Threat Defense | Protects mobile devices from threats such as malware, phishing, and data loss. | Essential for managing security risks associated with mobile device use within the enterprise. | Wandera, Zimperium zIPS |

(Vijayan, 2018)

## MARKET SOLUTIONS

### Case Study 1: Splunk

### The Challenge

Cybersecurity professionals are inundated with a high volume of security alerts generated by various tools such as Security Information and Event Management (SIEM) systems, endpoint security solutions, firewalls, and email security platforms. Unfortunately, these alerts often lack sufficient detail, necessitating manual investigation by analysts. The time required to assess and address each alert ranges from 10 to 40 minutes, depending on its severity. The critical issue is that the sheer volume of security alerts exceeds the capacity of available personnel. Reports indicate that approximately 64% of daily security tickets remain unaddressed. This phenomenon, known as "alert fatigue," significantly increases vulnerability, as even a single overlooked alert can escalate into a major breach. Moreover, the effectiveness of alert systems is compromised by inefficiency. A 2017 study by Enterprise Management Associates (EMA) found that 46% of incidents are categorized as "critical," though only 1-5%

genuinely warrant this classification. Additionally, 30% of alerts are false positives, leading to substantial wasted time and resources (Dominguez, 2020).

**The Solution: Automation**

To mitigate these challenges, automation in security alert triage presents a transformative solution. Automated systems can analyze and categorize alerts far more swiftly than manual processes, cutting down response times from minutes to seconds. This efficiency not only reduces operational costs but also enhances the accuracy of threat detection by filtering out false positives and less critical alerts (Dominguez, 2020).

**Implementation: Splunk Phantom**

Splunk Phantom, a Security Orchestration Automation and Response (SOAR) tool, exemplifies how automation can significantly enhance cybersecurity operations. At Splunk's annual conference, .conf19, numerous organizations shared how Splunk Phantom revolutionized their security practices. By automating alert triage, Splunk Phantom has enabled businesses to streamline their response processes, allowing security analysts to focus on more strategic tasks and strengthening overall breach prevention efforts (Dominguez, 2020).

### Case Study 2: Microsoft Azure Sentinel

Security Operations Centers (SOCs) face escalating difficulties in managing vast volumes of security data. A significant 76% of organizations report increased security data, coupled with a shortage of qualified cybersecurity professionals—estimated at 3.5 million unfilled positions in 2021. This shortage contributes to the alarming statistic that 44% of security alerts within organizations remain uninvestigated. Effective security monitoring and response necessitate comprehensive data collection and analysis, which are critical for training machine learning models used in contemporary security solutions. For over a decade, SOCs have relied on Security Information and Event Management (SIEM) systems to provide a centralized view for security analysts. However, these SIEM solutions often prove to be cumbersome and costly. They generate vast amounts of data that either overwhelm analysts or require specialized data scientists to develop and deploy data analysis models. This situation creates significant operational challenges (Microsoft, 2020).

**The Challenge**

The primary issue lies in the inefficacy of traditional SIEM systems to cope with the complexity and scale of modern enterprise environments. These systems are not only expensive to implement and maintain but also struggle to deliver actionable insights due to the sheer volume of data. The problem is compounded by the need for highly skilled personnel to manage and interpret the data, leading to a frustrating cycle of inefficiency and resource strain (Microsoft, 2020).

**Solution: Microsoft Azure Sentinel**

To address these challenges, Microsoft introduced Azure Sentinel, a groundbreaking SIEM solution integrated into a major public cloud platform. Azure Sentinel offers intelligent security analytics across enterprise environments with automatic scalability to accommodate evolving needs. It incorporates artificial intelligence (AI) and machine learning (ML), leveraging the capabilities of the Azure cloud to deliver near-limitless speed and scale without the burden of infrastructure management. Notably, Azure Sentinel can automate up to 80% of the routine tasks typically performed by security analysts (Microsoft, 2020).

**Implementation**

For organizations to harness the full potential of Azure Sentinel, it is crucial to configure the service correctly. This involves connecting appropriate data sources and establishing robust incident response processes before any breach occurs. Azure Sentinel supports integration with a wide range of data sources, including Microsoft products, on-premises systems, leading Software as a Service (SaaS) applications, and other cloud environments such as Amazon Web Services (AWS).

Data can be ingested into Azure Sentinel through various methods:

- Utilizing pre-built data connectors for seamless integration with Microsoft and many non-Microsoft solutions.
- Employing syslog, Common Event Format (CEF), or REST-API sources for custom data ingestion.
- Connecting non-Microsoft solutions via APIs provided by the data sources.

### Case Study 3: LogRhythm Security Intelligence Platform

**The Challenge**

Organizations of all sizes face increasing cybersecurity threats, necessitating robust security measures. Smaller businesses and municipalities often struggle with limited resources and budgets, making it challenging to implement comprehensive security solutions. The complexity of integrating security information and event management (SIEM) systems with existing infrastructures adds to these difficulties (Miller, 2019).

**Solution**

LogRhythm Security Intelligence Platform offers a user-friendly and cost-effective SIEM solution that integrates seamlessly with various IT infrastructures. Its ease of use and compatibility make it particularly suitable for smaller organizations and municipalities that need comprehensive security without the high costs associated with other SIEM alternatives (Miller, 2019).

### Implementation

LogRhythm's comprehensive and accessible security solution has proven to be an invaluable asset for its clients. The platform's ability to interface smoothly with existing infrastructures, combined with its cost-effectiveness, enables smaller organizations to achieve a high level of security without significant financial strain. This has led to improved cybersecurity, demonstrating the effectiveness of LogRhythm as a reliable SIEM solution (Miller, 2019).

## IN-HOUSE SOLUTIONS WITH OPEN SOURCE

Cybersecurity solutions feature an array of Free and Opensource Software (FOSS) tools, each tailored for specific functions such as encryption, antivirus protection, email security, and internet safety. Although these tools are available for free, they are often subject to licensing agreements, and some free tools may have restrictions even if they are not opensource. Opensource cybersecurity tools provide a broad spectrum of defensive and offensive capabilities. Many of these tools are essential for protecting systems and networks and are classified into various categories by cybersecurity professionals. These categories include network security monitoring, encryption, web vulnerability assessment, penetration testing, antivirus software, network intrusion detection, and packet sniffing. The effectiveness and ease of use of these tools make them vital for maintaining strong cybersecurity defenses (Subramanian, 2019).

### Challenges Related to In-House Cybersecurity Solutions with Opensource

Implementing in-house cybersecurity solutions using opensource software offers flexibility and cost advantages, but it also presents several significant challenges:

### Cost and Resource Allocation

- Initial Setup and Maintenance Costs: Although open-source solutions often have no licensing fees, the costs associated with their implementation and maintenance can be high. Organizations need to invest in robust infrastructure and allocate substantial time and resources to configure and customize these solutions.
- Ongoing Operational Costs: The total cost of ownership for opensource solutions includes continuous patch management, updates, and integration efforts. Regular maintenance requires dedicated personnel to ensure the system remains secure and functional (Information Week, 2017).

### Skill Requirements

- Specialized Expertise: Opensource cybersecurity tools typically require personnel with specialized skills to deploy, manage, and maintain. Finding and retaining staff with the necessary expertise in tools can be challenging.
- Training and Development: Existing IT staff may need additional training to effectively use and manage open-source tools. This training can be time-consuming and costly, further straining resources (Information Week, 2017).

### Support and Reliability

- Community Support: While open-source tools benefit from community support, this support can be inconsistent and unreliable. Organizations may face delays in addressing critical security vulnerabilities or operational issues.
- Lack of Formal Support: Unlike commercial solutions that offer dedicated customer support, open-source tools may not have formal support channels. This can lead to prolonged downtimes and unresolved issues (Sarmah, 2019).

### Security and Compliance

- Vulnerability Management: Open-source tools can be susceptible to vulnerabilities that require prompt attention. Organizations must have processes in place to regularly monitor, identify, and patch these vulnerabilities (Sarmah, 2019).
- Regulatory Compliance: Ensuring that open-source solutions comply with industry regulations and standards (such as GDPR, HIPAA, etc.) can be challenging. Organizations must validate that their implementations meet all compliance requirements, which may necessitate.

## EVOLUTION OF ENTERPRISE SECURITY WITH AI

Modern security teams encounter numerous obstacles in their efforts to protect data. These include sophisticated hackers, an ever-expanding attack surface, a deluge of data, and increasing infrastructure complexity. These challenges complicate their ability to manage user access, promptly detect threats, and respond effectively to security incidents, especially those involving AI-driven attacks (IBM, n.d.).

### Securing Data in Hybrid Cloud Environments

AI tools play a crucial role in identifying shadow data, monitoring data access for anomalies, and alerting cybersecurity professionals to potential threats. These capabilities enable real-time detection and remediation of issues, thereby enhancing the protection of sensitive information against malicious actors (IBM, n.d.).

### Enhancing Accuracy and Prioritization of Threats

AI-powered risk analysis can generate comprehensive incident summaries for high-fidelity alerts and automate incident responses, significantly speeding up alert investigations and triage by an average of 55%. This technology also aids in identifying vulnerabilities across various threat landscapes, bolstering defenses against cybercriminal activities (IBM, n.d.).

### Balancing Security with User Access Needs

AI models facilitate a balance between security and user experience by assessing the risk associated with each login attempt and verifying users through behavioral data. This approach simplifies access for authenticated users while reducing fraud costs by up to 90%. Additionally, AI systems are effective in preventing phishing, malware, and other malicious activities, thereby maintaining a robust security posture (IBM, n.d.).

## CONCLUSION

The increasing number of cybersecurity tools within enterprises has created a complex and often inefficient security environment. While the initial response to escalating cyber threats involved acquiring diverse tools, this approach has led to issues of fragmentation and alert fatigue. The need for cohesive and efficient threat management has driven the development of solutions that focus on real-time analytics and automation. Tools such as Splunk Phantom and Microsoft Azure Sentinel exemplify the shift towards integrating automation and AI to enhance threat detection and response. Additionally, open-source solutions offer flexibility but come with their own set of challenges, including cost and resource allocation. The integration of AI in cybersecurity is proving transformative, enabling more accurate threat detection and response while balancing security with user access needs. By adopting a strategic approach to tool integration and leveraging advanced technologies, enterprises can better navigate the complexities of modern cybersecurity and strengthen their defenses against evolving threats

## REFERENCES

[1]. IBM (2020, June 30). IBM Study: Security Response planning on the rise, But containing attacks remains an issue. https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue

[2]. IBM (n.d.). Artificial intelligence (AI) cybersecurity. https://www.ibm.com/ai-cybersecurity

[3]. Information Week (2017, December 08). The Hidden Costs of Open Source Security Software. https://www.informationweek.com/it-infrastructure/the-hidden-costs-of-open-source-security-software#close-modal

[4]. Miller, J. (2019, April 19). Top SIEM Products for Cybersecurity. https://www.bitlyft.com/resources/top-siem-products-cyber-security

[5]. Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 135-154.

[6]. Sarmah, H. (2019, July 31). 6 Challenges in using open source cybersecurity tools. AIM. https://analyticsindiamag.com/ai-origins-evolution/6-challenges-in-using-open-source-cybersecurity-tools/

[7]. Security Scorecard (2019, December 19). What is a Cybersecurity Posture and How Can You Evaluate It? https://securityscorecard.com/blog/what-is-a-cybersecurity-posture/

[8]. Smith, R. (2019, November 14). Companies have too many security tools. Here's how we're solving that. - Armor Resources. Armor Resources. https://res.armor.com/resources/blog/too-many-security-tools/

[9]. Subramanian, B. (2019). An Overview List of Free Cybersecurity Tools. A Data Science Foundation White Paper

[10]. Vijayan, J. (2018, October 4). 10 essential enterprise security tools (and 11 nice-to-haves). CSO Online. https://www.csoonline.com/article/566389/10-essential-enterprise-security-tools-and-11-nice-to-haves.html