Volume 10, Issue 7, July – 2025 International Journal of Innovative Science and Research Technology
ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jul1858

Securing the Supply Chain: Automated Defenses Against Emerging Cyber Risks

Aakarsh Mavi[1]

Publication Date: 2025/08/13

Abstract: As supply chain networks become more complex, they're also becoming more vulnerable to cybersecurity threats. To stay secure, organizations need more than just automated tools that fix issues—they need systems that can constantly monitor their environment, report on compliance, and evolve with new threats. While most traditional security automation frameworks focus on enforcing policies and patching vulnerabilities, they often fall short when it comes to real-time visibility and ongoing improvement.

This paper builds on the existing SecAuto Toolkit [5] by introducing three critical additions: Monitoring, Reporting, and Continuous Improvement layers. These new components ensure that security events are tracked in real time, compliance with standards is automatically verified, and the system can adapt as new threats emerge. Additionally, integrating Software Bills of Materials (SBOMs) into the supply chain security process has proven essential for identifying vulnerabilities in third-party components and maintaining transparency in software dependencies. [9]

The enhanced framework combines Ansible automation with SIEM tools, compliance dashboards, and machine learning to deliver proactive and intelligent threat management. Designed specifically for supply chain environments, this approach helps organizations stay secure by providing real-time insights, automating audits, and continuously refining their security posture over time.

Keywords: *Cybersecurity, Supply Chain, Ansible, Nist, Siem, Compliance, Automation, Continuous Improvement.*

How to Cite: Aakarsh Mavi (2025). Securing the Supply Chain: Automated Defenses Against Emerging Cyber Risks. *International Journal of Innovative Science and Research Technology*, 10(7), 3571-3575. https://doi.org/10.38124/ijisrt/25jul1858

I. INTRODUCTION

Supply chain organizations are embedded in interconnected digital environments where cyber threats are not only on the rise but also becoming more complex. As supply chain processes digitize, the risk area grows, making it harder to protect sensitive information and assets. Cybersecurity issues, from ransomware targeting logistics to supply chain tampering through third-party weaknesses, can have severe financial, operational, and reputational impacts. Historically, security automation frameworks have concentrated on specific cybersecurity elements like patching, hardening systems, and fixing DNS and all other vulnerabilities [3].

However, many lack thorough integration for ongoing monitoring, immediate reporting, and continuous enhancements, crucial for tackling the evolving landscape of modern threats. This research aims to close this gap by enhancing the SecAuto Toolkit [5]with three additional layers—Monitoring, Reporting, and Continuous Improvement—into the security automation process. These layers are intended to function together, ensuring a supply chain organization not only responds to security incidents but also actively enhances its security measures based on real-time data and changing threats.

The core of this research is combining the NIST Cybersecurity Framework (CSF) with advanced automation tools like Ansible to establish a complete, adaptable security framework. The NIST CSF offers a flexible, structured method for handling cybersecurity risks through five main functions: Identify, Protect, Detect, Respond, and Recover. By aligning these functions with automation workflows, this research seeks to develop a strong security automation system that adheres to best practices while accommodating the unique needs of supply chain organizations.

This paper presents an upgraded version of the SecAuto Toolkit, adding three essential layers:

- *Monitoring Layer*
  Provides real-time security event tracking by integrating with SIEM tools and network monitoring systems.

- *Reporting Layer*
  Streamlines compliance and governance reporting to meet industry standards, including NIST and CIS.

- *Continuous Improvement Layer*
  Utilizes data analytics and machine learning to enhance security automation processes in response to emerging threats.

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jul1858

The suggested framework is in line with supply chain cybersecurity best practices, ensuring that security automation catches and addresses vulnerabilities while also adapting to new threats dynamically.

- *Framework Design*

Monitoring Layer Objectives

Table 1 Framework Design

Monitoring Layer Objectives	NIST Framework	Category	Category Details
Set up real-time monitoring for security	Detect	Anomalies and Events	Establishing automated systems to identify unusual activities
Configure alerts to identify deviations from compliance standards.	Detect	Security Continuous Monitoring	Utilizing tools to track deviations from standard security measures and sending alerts accordingly.
Monitor system health and performance indicators	Respond	Analysis	Employing automated monitoring tools to evaluate system performance and health for swift responses.
Connect with SIEM tools for unified threat	Detect	Anomalies and Events	Integrating with SIEM systems for the automatic logging and

Table 2 Reporting Layer Objectives

Reporting Layer Objectives	NIST Framework	Category	Category Details
Generate reports on compliance and	Identify	Governance	Automate the creation of reports on security posture and
Produce audit logs for changes in system configuration and access	Protect	Information Protection	Generate audit trails for system configuration and access control activities automatically.
Streamline vulnerability and incident reporting	Respond	Response Planning	Create reports for incident response planning with remediation recommendations automatically.
Automate regular vulnerability assessments and compliance checks	Identify	Risk Assessment	Automatically report risks and vulnerabilities based on periodic assessments.

Table 3 Continuous Improvement Layer Objectives

Continuous Improvement Layer Objectives	NIST Framework	Category	Category Details
Implement feedback systems for enhancing security and compliance	Recover	Improvements	Utilizing feedback from security incidents to enhance playbooks and automated tasks.
Adjust automated security measures according to new threats	Identify	Risk Assessment	Modifying automated security controls to tackle emerging vulnerabilities and threats through a feedback loop.
Improve current policies based on audit results	Protect	Access Control	Regularly updating policies and automated settings based on audit results and intelligence on threats
Revise automation processes for quicker incident recovery	Respond	Response Planning	Employing automation to shorten incident response times and streamline recovery processes.

- *Implementation*

The implementation of the layered file structure for the SecAuto Toolkit aims to enhance the security automation process by dividing the framework into three main layers: Monitoring, Reporting, and Continuous Improvement. Each layer is specifically designed to target crucial aspects of security and compliance, allowing the organization to effectively manage vulnerabilities, detect irregularities, and continually improve security measures. This file structure utilizes Ansible automation, creating a clear and efficient hierarchy for tasks, roles, and variables, enabling smooth integration across systems. By aligning automation tasks with the NIST Cybersecurity Framework, the structure not only supports real-time monitoring and reporting but also promotes the ongoing advancement of security practices, ensuring adaptability to new threats and regulatory updates. This implementation fosters a scalable and robust system that aids organizations in maintaining a secure and compliant supply chain infrastructure while ensuring effective security management.

- *Monitoring Layer Implementation*

The Monitoring Layer is dedicated to real-time security monitoring, ensuring the prompt detection of any unusual activities or potential security threats in the supply chain.

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jul1858

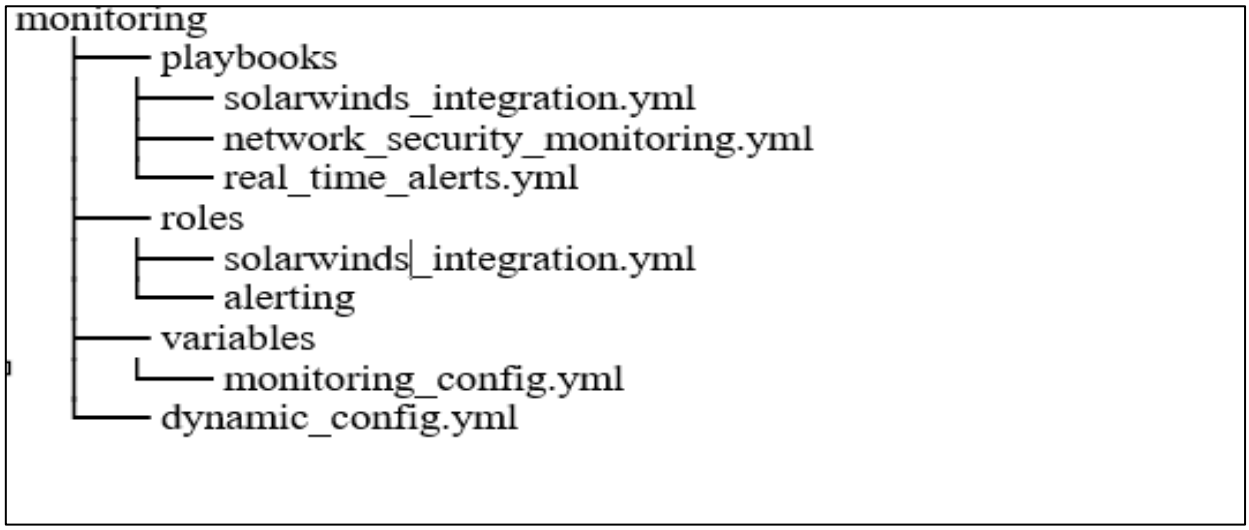

Fig 1 Monitoring Layer Implementation

➢ *How it Operates:*

- *Integration with SolarWinds:*

You can connect SolarWinds to track network performance and vital infrastructure like servers, routers, switches, and firewalls. This ensures your supply chain systems run smoothly without performance issues or vulnerabilities.

- *Monitoring Security Events:*

SolarWinds can identify anomalies such as unusual traffic patterns, unauthorized access attempts, or modifications to system settings, triggering automated alerts or responses.

- *Unified Log Management:*

SolarWinds offers centralized logging and monitoring, which can be connected to your security operations center (SOC) for enhanced proactive response management.

- *Reporting Layer Implementation*

The Reporting Layer generates automated reports on compliance and security for stakeholders, ensuring the safety and regulation adherence of supply chain activities.

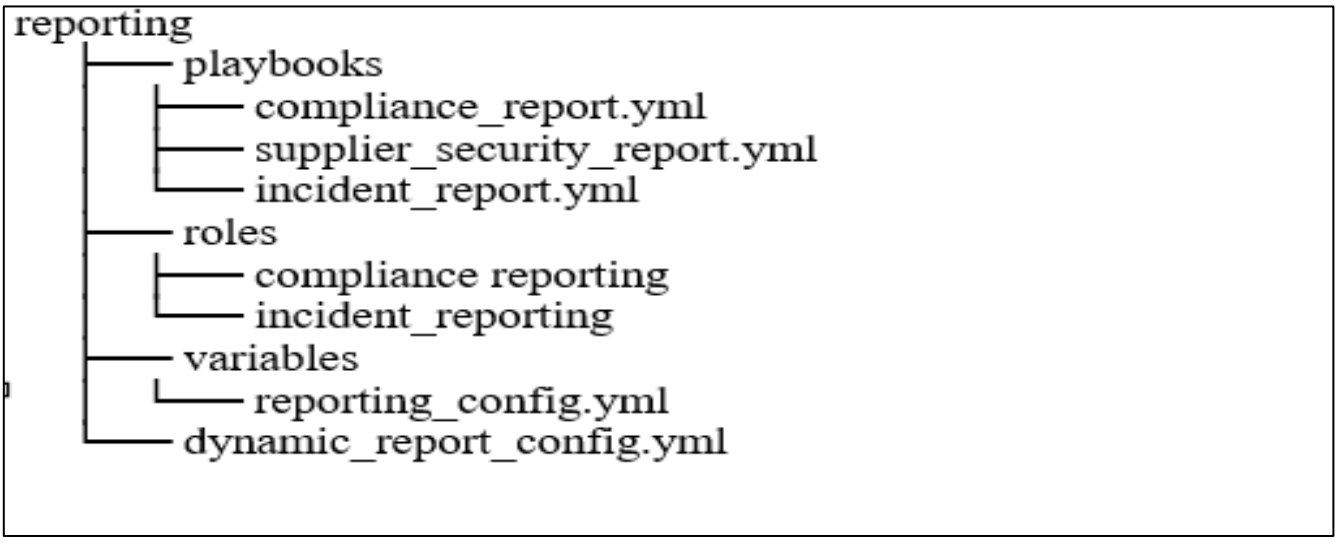

Fig 2 Reporting Layer Implementation

➢ *How it Works:*

- *Regulatory Compliance Reporting:*

Producing reports that demonstrate compliance with regulations like GDPR, CMMC, and specific supply chain standards such as ISO 28000 for security management.

- *Supplier Security Posture:*

Streamlining the generation of reports on suppliers' cybersecurity status, focusing on third-party risks and vulnerabilities.

- *Incident and Breach Reporting:*

Automatically creating detailed incident reports after breaches, outlining the impact on the supply chain and the measures taken to address them.

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jul1858

- *Continuous Improvement Layer Implementation for Supply Chain Company*

The Continuous Improvement Layer keeps security processes up-to-date to tackle new supply chain challenges, especially with rising cybersecurity threats. Integrating real-time data sources significantly enhances the accuracy and responsiveness of threat detection in supply chain systems. Approaches like these help correlate live security events with known threat patterns, improving detection speed and decision-making [10].

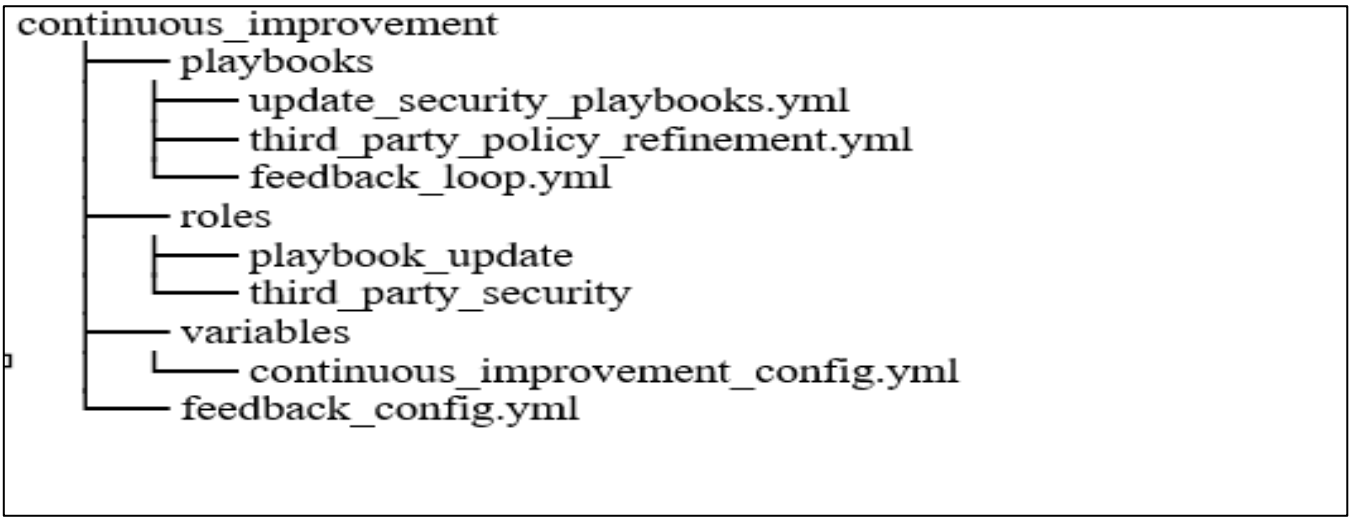

Fig 3 Continuous Improvement Layer Implementation for Supply Chain Company

➢ *How it works:*

- *Supply Chain Risk Feedback:*

Collecting insights from real-time monitoring and compliance reports to strengthen security measures, focusing on sensitive data management and vendor relations.

- *Automating Security Playbook Updates:*

Updating security playbooks automatically based on feedback, such as enforcing stricter controls for vulnerable systems or vendors with lower security ratings.

- *Policy Refinement for Third-party Integrations:*

Revising policies and procedures for interacting with third parties based on newly discovered vulnerabilities or breach attempts.

II. CONCLUSION

The SecAuto Toolkit detailed in this paper combines the NIST Cybersecurity Framework with Ansible automation for a strong, scalable, and flexible security automation approach. It features three key layers—Monitoring, Reporting, and Continuous Improvement—ensuring a proactive security stance crucial for handling vulnerabilities and meeting compliance in supply chain settings. By using tools like SolarWinds for immediate monitoring and automated reporting, the toolkit boosts the organization's capacity to spot anomalies, create compliance reports, and improve security policies based on real-time insights. This method simplifies vulnerability management and helps organizations stay aligned with industry standards.

For a supply chain organization, the toolkit is vital for defense against cyber threats by providing constant monitoring of critical systems and sensitive data, swiftly identifying and addressing vulnerabilities, and ensuring compliance is consistently met. As supply chains face increasing cyberattack risks—largely due to dependence on numerous third-party vendors—this toolkit is essential. Automating tasks like patching, updating security settings, and sending real-time alerts helps protect data exchanges between suppliers, partners, and internal systems. The Continuous Improvement Layer guarantees security strategies adaptively respond to new threats, protecting the entire supply chain from end to end and across interconnected systems. Through this thorough and adaptable approach, the SecAuto Toolkit empowers supply chain organizations to reduce risks, prevent disruptions, and uphold operational integrity amid rising cybersecurity challenges.

➢ *Future Work*

The SecAuto Toolkit is a developing framework with numerous opportunities for future enhancements. A major focus is on adding more AI and Machine Learning capabilities. This could lead to better anomaly detection and predictive analytics, allowing the toolkit to spot potential threats before they occur. Another improvement could be enhancing the Continuous Improvement Layer by including more detailed feedback loops. This would facilitate real-time updates to security protocols based on threat information and performance data. Additionally, as supply chain systems become increasingly complex and interconnected, the toolkit can be adapted to tackle the specific challenges related to third-party vendor integrations and global supply chain security, focusing on managing risks from distributed systems and remote access. Lastly, the toolkit could be modified for wider use in enterprises by integrating with cloud-native [4] environments and enhancing its features to keep pace with the shifting cybersecurity landscape. These advancements will help organizations maintain secure,

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jul1858

resilient, and compliant operations amid a continuously evolving threat environment.

REFERENCES

[1]. National Institute of Standards and Technology (NIST**).** (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. NIST. Retrieved from https://www.nist.gov/cyberframework

[2]. Zhang, Y., & Zhang, X**.** (2019). *Automated Security Monitoring and Compliance Management using Ansible*. International Journal of Computer Applications.

[3]. Talwar, S., & Mavi, A. (2023). AN OVERVIEW OF DNS DOMAINS/SUBDOMAINS VULNERABILITIES SCORING FRAMEWORK. International journal of applied engineering and technology, 5(S4), 274–280. https://romanpub.com/resources/Vol.%205%20No.%20S4%20(July%20-%20Aug%202023)%20-%2027.pdf

[4]. Talwar, S. (2022). Securing Cloud-Native Dns Configurations: Automated Detection of Vulnerable S3-Linked Subdomains. International journal of applied engineering and technology, 4(2), 270–278. https://romanpub.com/resources/Vol.%204%20No.%202%20(September%2C%202022)%20-%2033.pdf

[5]. Talwar, S., & Mavi, A. (2023). SECAUTO TOOLKIT - HARNESSING ANSIBLE FOR ADVANCEDSECURITY AUTOMATION. International Journal of Applied Engineering & Technology, 5(5S), 2478–2491. https://romanpub.com/resources/Vol.%205%20No.%20S5%20(Sep%20-%20Oct%202023)%20-%2013.pdf

[6]. Barker, K., & Harris, D. (2020). *Cybersecurity Automation in Supply Chain Management: A Case Study Approach*. International Journal of Cybersecurity, 12(3), 45-62

[7]. Cameron, S., & Thomas, E. (2018). *Leveraging Ansible for Security Automation: Best Practices and Frameworks*. Journal of Information Security and Applications, 44, 51-62 Almeida, M., & Rodrigues, L. (2019). Integrating Risk

[8]. Management and Automation in Supply Chain Security: A Comprehensive Framework. Journal of Industrial Engineering and Management, 12(4), 201-217

[9]. Osha Shukla, 2025, *Software Supply Chain Security: Designing a Secure Solution with SBOM for Modern Software Ecosystems*, IJERT, Vol. 14, Issue 04. https://www.ijert.org/software-supply-chain-security-designing-a-secure-solution-with-sbom-for-modern-software-ecosystems

[10]. Osha Shukla, 2025, *Enhancing Threat Intelligence and Detection with Real-Time Data Integration*, IJERT, Vol. 14, Issue 04. https://www.ijert.org/research/enhancing-threat-intelligence-and-detection-with-real-time-data-integration-IJERTV14IS040201.pdf