# **Invisible Threats: Securing the OT Supply Chain Against Advanced Persistent Threats**

Jim mckenney  
2025-3-22

**I. Executive Summary:**

The convergence of information technology (IT) and operational technology (OT) environments is rapidly transforming industrial operations, offering unprecedented opportunities for efficiency and data-driven decision-making 1. However, this integration also introduces significant cybersecurity challenges, particularly with the increasing sophistication and frequency of cyberattacks targeting industrial control systems (ICS) and OT infrastructure 1. Among these threats, the vulnerabilities within the OT supply chain often remain overlooked, creating a prime target for advanced persistent threats (APTs) seeking to compromise critical industrial operations 3. This whitepaper provides a comprehensive guide to understanding and mitigating these risks, delving into the evolving threat landscape, mapping potential exposure points within the OT supply chain, and offering a methodical approach to risk assessment. Furthermore, it explores the alignment of security controls with relevant compliance frameworks, proposes prioritized remediation strategies, details continuous monitoring approaches, and touches upon the role of emerging technologies, including Knowledge Graphs, Graph Neural Networks, and Digital Twins, in bolstering security. Ultimately, this report underscores the critical importance of adopting a proactive and layered security approach to safeguard vital industrial operations against the invisible threats lurking within the OT supply chain.

**II. Introduction: The Hidden Battlefield:**

Industrial control systems (ICS) and operational technology (OT) form the backbone of numerous critical sectors, including manufacturing, energy, transportation, and utilities, playing an indispensable role in the functioning of modern society 2. These systems, traditionally isolated from enterprise IT networks, are now undergoing a significant digital transformation. This evolution involves the increasing adoption of Industrial Internet of Things (IIoT) devices, cloud computing services, and interconnected systems to enhance productivity, gain real-time insights, and optimize operational processes 1. While this digital transformation offers substantial benefits, it also leads to an expanding attack surface, as the convergence of IT and OT exposes previously segregated industrial environments to a wider range of cyber threats 1.

Securing the OT supply chain presents unique challenges compared to traditional IT supply chains. OT environments often rely on legacy systems with inherent security limitations, operate under stringent real-time constraints that can hinder patching and updates, and manage safety-critical functions where any disruption can have severe consequences 1. The interconnected nature of modern industrial operations, coupled with the increasing reliance on third-party vendors and service providers, introduces numerous potential vulnerabilities within the supply chain. Consequently, successful supply chain attacks on OT can lead to a cascade of detrimental effects, including significant operational disruptions, substantial financial losses, severe reputational damage, critical safety incidents, and even adverse environmental impacts 1. The focus on maintaining continuous and safe operation in OT environments often results in different security priorities than in IT, where confidentiality and integrity are paramount 1. This can lead to a more cautious approach to security patching and updates in OT due to concerns about potential downtime 30. Furthermore, the growing integration of IIoT devices for enhanced data collection and predictive maintenance, while boosting efficiency, significantly broadens the attack surface with potentially less secure endpoints 16.

**III. Understanding the Threat Landscape:**

The landscape of cyberattacks targeting industrial systems has evolved considerably over time. Historically, OT environments were perceived as relatively secure due to their isolation. However, the increasing connectivity has made them more accessible to malicious actors 2. Early attacks might have been more opportunistic, but the emergence of sophisticated threat actors, including APT groups, has led to targeted and persistent campaigns against critical infrastructure. Notably, Dragos, a leading industrial cybersecurity firm, reported an alarming 87 percent surge in ransomware attacks against industrial organizations in the past year . This includes a 60 percent rise in ransomware groups specifically targeting OT/ICS . These statistics underscore the escalating threat to industrial operations.

Notable examples illustrate the potential impact of OT supply chain compromises. The Dragonfly campaign, for instance, involved the compromise of legitimate software packages from industrial control system equipment providers to infiltrate energy companies 5. Stuxnet, a highly sophisticated worm, infiltrated Iranian nuclear facilities via infected USB drives, demonstrating that even air-gapped systems are not immune 11. More recently, the SolarWinds attack highlighted the devastating consequences of a compromised software update mechanism, granting attackers widespread access to numerous organizations, including those in critical infrastructure 3. Similarly, the CCleaner breach involved the injection of malicious code into a widely used software update, affecting millions of users 5. The 3CX supply chain attack in 2023 demonstrated the potential for attackers to compromise software build systems and inject malware into desktop applications 12.

The motivations behind these attacks are varied, ranging from espionage and sabotage to financial gain 3. APT groups, often state-sponsored, typically aim for long-term access to gather intelligence or prepare for disruptive attacks. Their operations are characterized by stealth, persistence, and the use of advanced techniques to evade detection 3. A common tactic involves leveraging vulnerabilities within the supply chain as an initial point of entry into target organizations 3. This can involve targeting less secure third-party vendors, exploiting trust relationships, or compromising software and hardware components before they even reach the end user. The evolution of these attacks indicates a growing trend towards exploiting software and firmware updates for large-scale malware distribution 3. This underscores the critical need for robust security measures throughout the software development lifecycle and within update mechanisms in OT environments. The case studies also reveal that attackers frequently target vulnerabilities in third-party vendors or less defended segments of the supply chain as a means to infiltrate primary targets, emphasizing the necessity of a comprehensive security strategy that extends beyond an organization's direct perimeter.

**IV. Mapping the Invisible: Vulnerability Analysis in the OT Supply Chain:**

Identifying potential exposure points throughout the OT supply chain is crucial for developing effective security strategies. A comprehensive framework must consider various components and interactions within this complex ecosystem. To gain a deeper understanding of these interconnected elements, organizations can leverage **Knowledge Graphs (KGs)**. As Jim McKenney, a recognized leader in industrial cybersecurity, emphasizes, KGs can map the intricate web of the OT supply chain's tech stack, cross-referencing components with known vulnerabilities 1. This approach allows for a more holistic view of potential weaknesses, extending beyond individual assets to encompass the relationships between them 33.

**Hardware Components:** The integrity of hardware components is paramount in OT environments. Risks include the introduction of counterfeit hardware, devices tampered with during manufacturing or transit, and vulnerabilities intentionally or unintentionally embedded within hardware 3. Verifying the authenticity and integrity of hardware can be particularly challenging in industrial settings due to the complexity of supply chains and the lack of robust verification mechanisms.

**Firmware and Software Updates:** Firmware and software updates represent a significant attack vector. Compromised update mechanisms can be exploited to inject malicious code directly into OT systems 3. Ensuring secure update processes, including verifying the integrity and authenticity of software packages before deployment, is essential to mitigate this risk.

**Third-Party Integration Points:** Integrating third-party systems, applications, and services with OT environments introduces inherent risks 3. These integrations can create pathways for attackers to gain unauthorized access if not properly secured. Implementing secure interfaces, enforcing strict access controls, and regularly auditing third-party integrations are critical security measures.

**Service Provider Access:** Remote access granted to service providers for maintenance, support, and management of OT systems can also be a source of vulnerabilities 3. Dragos's 2025 report highlights that 20 percent of ransomware incidents involved the exploitation of remote access, including VPN exploits and exposed RDP sessions . Alarmingly, 65 percent of sites assessed had insecure remote access conditions, including default credentials and unpatched VPNs . Compromised service provider credentials or insecure remote access protocols can be exploited by malicious actors. Employing secure remote access solutions, implementing multi-factor authentication, and diligently monitoring service provider activities are vital to minimize these risks.

**Remote Maintenance Channels:** Insecure remote maintenance tools and protocols used for accessing and managing OT systems pose a significant threat 3. Attackers can leverage vulnerabilities in these channels to gain control over critical industrial processes. Organizations should prioritize the use of secure remote maintenance alternatives and adhere to stringent security best practices. The interconnected nature of modern OT systems means that a vulnerability in any single component or integration point within the supply chain can potentially compromise the entire industrial operation 3. This interconnectedness significantly amplifies the impact of even seemingly minor weaknesses. Furthermore, the increasing reliance on remote access for maintenance and support creates a substantial attack vector if adequate security measures are not in place. Attackers can exploit weaknesses in remote access tools or compromised credentials to gain unauthorized entry into OT networks from virtually anywhere 3.

**V. Assessing the Fortress: A Risk Assessment Methodology for Vendor Security:**

Evaluating the security posture of vendors within the OT supply chain is a critical step in mitigating risks. A methodical approach should encompass the following key elements 8:

* **Define Clear Security Objectives:** Organizations must establish specific and measurable security goals for vendor risk assessments, aligning them with their overall security strategy and risk tolerance 36.
* **Conduct Vendor Security Audits:** Regular audits of vendor security controls, policies, and procedures are essential. These can include security questionnaires, on-site visits to assess physical and logical security, and independent third-party assessments to provide an objective evaluation 36.
* **Implement Continuous Monitoring and Threat Intelligence:** Relying on point-in-time assessments is insufficient in today's dynamic threat landscape. Implementing continuous monitoring of vendor security performance through security ratings services, threat intelligence feeds, and real-time monitoring tools allows for the timely detection of emerging risks 36.
* **Enforce Security SLAs and Penalties:** Security Service Level Agreements (SLAs) should be incorporated into vendor contracts, clearly outlining security expectations and establishing penalties for non-compliance or security breaches 36.
* **Foster Vendor Security Collaboration:** A collaborative approach to security with vendors is more effective than a purely compliance-driven one. Encouraging open communication, sharing threat intelligence, and conducting joint security exercises can significantly enhance the overall security of the OT supply chain 36.
* **Adopt a Tiered Vendor Risk Approach:** Not all vendors pose the same level of risk. Implementing a tiered approach based on the criticality of the vendor's services and their level of access to sensitive OT systems allows for the allocation of resources and the application of appropriate security controls 36.

Furthermore, **Graph Neural Networks (GNNs)**, as highlighted by Jim McKenney's work, offer advanced capabilities in mapping and analyzing the complex relationships between vendors and their potential impact on the OT environment 1. GNNs can identify subtle connections and dependencies that traditional risk assessment methods might miss, providing a more nuanced understanding of the overall risk landscape 53.

**Key Table: OT Vendor Security Assessment Criteria**

| **Criteria** | **Importance in OT Context** | **Potential Metrics for Evaluation** |
| --- | --- | --- |
| **Access Control Policies** | Crucial for preventing unauthorized access to critical OT systems and data. | Number of privileged accounts, enforcement of least privilege, frequency of access reviews, use of multi-factor authentication 36. |
| **Data Encryption Standards** | Essential for protecting sensitive data at rest and in transit within the OT environment and between the organization and its vendors. | Encryption algorithms used, key management practices, compliance with relevant encryption standards 36. |
| **Incident Response Capabilities** | Critical for ensuring timely and effective response to security incidents involving vendors that could impact OT operations. | Existence of a formal incident response plan, defined roles and responsibilities, testing frequency of the plan, communication protocols during an incident 36. |
| **Patch Management Processes** | Vital for addressing known vulnerabilities in vendor-supplied hardware and software used within the OT environment. | Frequency of patch deployments, process for testing patches before deployment, timeframes for applying critical patches, tracking of unpatched vulnerabilities 30. |
| **Security Awareness Training** | Important for ensuring that vendor personnel with access to OT systems are aware of security risks and best practices. | Frequency and content of security awareness training programs, methods for verifying employee participation and understanding 8. |
| **Physical Security Controls** | Relevant for vendors who have physical access to OT facilities or equipment. | Measures in place to control physical access, surveillance systems, visitor management procedures 37. |
| **Network Security Measures** | Critical for securing network connections between the organization's OT environment and vendor systems. | Firewall configurations, intrusion detection and prevention systems, network segmentation practices 36. |
| **Business Continuity and Disaster Recovery Plans** | Essential for ensuring that vendors can maintain their services and support OT operations in the event of a disruption. | Existence of comprehensive plans, testing frequency, recovery time objectives (RTOs) 36. |

**VI. Software Bill of Materials (SBOM), Hardware Bill of Materials (HBOM), and Knowledge Graphs for Enhanced OT Security and Reliability:**

A critical aspect of bolstering OT supply chain security and operational reliability is gaining comprehensive visibility into the components that constitute the industrial environment. This is where the concepts of Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) become invaluable 97. An SBOM is a detailed inventory of all software components within a system, including libraries, dependencies, and versions 97. Similarly, an HBOM provides a comprehensive list of all physical hardware components, including their origin and manufacturing details 97.

By generating and maintaining accurate SBOMs and HBOMs for all OT assets, organizations can significantly enhance their security posture and operational resilience 97. These bills of materials provide transparency into the supply chain, allowing for rapid identification of vulnerable components when new threats emerge 97. Security teams can quickly determine which assets are affected by a specific vulnerability and prioritize remediation efforts 97. Furthermore, SBOMs and HBOMs aid in compliance with regulations and provide crucial information for procurement and asset management 97.

**Knowledge Graphs (KGs)** play a pivotal role in leveraging the information contained within SBOMs and HBOMs 110. By ingesting and semantically linking the data from these bills of materials, a KG can create a comprehensive map of the entire OT environment, encompassing hardware, software, and their interdependencies 110. This interconnected view allows for advanced analysis and querying, enabling security teams to understand the full impact of a potential vulnerability or the provenance of a suspicious component 110.

**Use Case: Mapping Industrial Equipment with OpenSPG:**

Consider an industrial facility with a diverse range of equipment, including PLCs, sensors, HMIs, and network devices. To effectively manage the security and reliability of this environment, the organization can utilize **OpenSPG**, an open-source Knowledge Graph Engine 111. By using Software Composition Analysis (SCA) tools 102 to generate SBOMs for the software running on these devices and compiling HBOMs for the hardware components, this information can be ingested into OpenSPG.

Using OpenSPG's capabilities, a detailed knowledge graph can be constructed, mapping out the full stack of equipment. Nodes in the graph represent individual hardware and software components, while edges represent the relationships between them, such as "runs on," "is a dependency of," or "is manufactured by" 113. This graph can be enriched with information from vulnerability databases (e.g., CVE) and supplier information, providing a holistic view of the facility's assets and their associated risks 110. Semantic queries can then be used to identify, for example, all devices running a specific version of software with a known vulnerability or to trace the origin of a particular hardware component.

**VII. Digital Twins and AI-Powered Simulations for Proactive Risk Management:**

Building upon the foundation of Knowledge Graphs enriched with SBOM and HBOM data, organizations can further enhance their OT security and resilience through the implementation of **Digital Twins**. A Digital Twin is a virtual representation of a physical asset, system, or process, continuously updated with real-time data.

Jim McKenney, leveraging his deep expertise in industrial systems and AI, has developed a digital twin model based on a specialized AI he calls "AEON". This model utilizes the comprehensive data within the Knowledge Graph, built from the full stack of equipment hardware and software identified through Software Composition Analysis and Bills of Materials, to create entire virtual facilities, vehicles, or fleets 72.

The AEON AI then runs digital twin simulations to identify potential weaknesses and generate optimization plans 66. For instance, by simulating various attack scenarios on the digital twin, organizations can proactively identify vulnerabilities in their OT environment and assess the potential impact on operations 116. The simulations can also help evaluate the effectiveness of different security controls and identify optimal configurations for resilience 116. Furthermore, the AEON AI can analyze the simulation results to recommend prioritized remediation strategies, aligning with the "Now, Next, Never" approach to vulnerability management. This proactive approach, leveraging the power of Knowledge Graphs and Digital Twins, enables organizations to significantly enhance the security and reliability of their OT supply chains.

**VIII. Secure Remote Access: A Cornerstone of OT Supply Chain Security:**

In today's interconnected industrial landscape, secure remote access has become a fundamental capability for managing and maintaining OT environments, extending down to the factory floor and even unattended equipment 66. While offering significant benefits in terms of efficiency and responsiveness, remote access also introduces substantial security risks if not implemented and managed with robust controls. Privileged Access Management (PAM) and related capabilities are therefore essential for ensuring that remote connections are secure, auditable, and do not provide an entry point for malicious actors targeting the OT supply chain 35.

PAM solutions for OT environments provide a centralized approach to managing and controlling privileged access for both internal users and third-party vendors requiring remote access for tasks such as diagnostics, maintenance, and software updates 35. These solutions typically offer features such as granular access controls, multi-factor authentication, session monitoring and recording, and automated password management, all of which are critical for mitigating the risks associated with remote access in OT 35. The need for secure and auditable remote access is further underscored by Dragos's findings, which indicate that a significant percentage of industrial cybersecurity incidents involve the exploitation of insecure remote access configurations .

Innovative PAM and remote access solutions are emerging to address the unique challenges of OT environments. Here are two examples:

1. **Zero-Trust Remote Access Platforms:** These platforms operate on the principle of "never trust, always verify," ensuring that every user and device attempting to access OT systems remotely is rigorously authenticated and authorized before access is granted 22. They often incorporate micro-segmentation techniques to limit the scope of access, preventing lateral movement in case of a compromise 22. Some solutions also leverage behavioral analytics to detect anomalous activities during remote sessions, providing an additional layer of security 50.
2. **Hardware-Based Secure Remote Access Gateways:** These solutions provide a dedicated and hardened entry point for remote connections to OT networks 66. By isolating the OT environment from the broader IT network and enforcing strict access controls at the hardware level, they minimize the attack surface and provide a more resilient security posture 66. Some gateways also offer features like secure boot, tamper detection, and encrypted communication channels to further enhance the security of remote access sessions 66.

Implementing robust PAM and secure remote access solutions is no longer optional but a fundamental requirement for organizations seeking to protect their OT environments and mitigate the risks associated with an increasingly interconnected industrial ecosystem 35.

**IX. Remediation Roadmap: Prioritized Mitigation Strategies Based on Risk Exposure:**

Addressing identified risks within the OT supply chain requires a prioritized approach to remediation. Organizations should focus on implementing mitigation strategies based on the level of risk exposure and potential impact 8. Jim McKenney advocates for a "Now, Next, Never" method for prioritizing vulnerability management in industrial systems 69. This approach, also highlighted in Dragos's reports, helps organizations focus on critical vulnerabilities requiring immediate attention ("Now"), high-priority issues to be addressed in a planned timeframe ("Next"), and low-priority vulnerabilities that do not pose an immediate risk ("Never") .

**Digital Twin** models, as part of an organization's digital transformation strategy championed by experts like Jim McKenney 1, can play a crucial role in informing this prioritization. By simulating the impact of potential vulnerabilities on the physical OT environment, organizations can better understand the real-world consequences of a supply chain compromise and allocate remediation resources accordingly 24.

**Implement Robust Risk Management Protocols:** Establishing systematic processes for identifying, assessing, and monitoring potential disruptions across the entire supply chain is fundamental 42. This includes conducting regular supplier risk assessments and mapping supply networks to pinpoint critical failure points.

**Develop Contingency Plans:** Organizations should formulate detailed contingency plans to address various disruption scenarios, such as supplier failures, transportation delays, or cyber incidents affecting the supply chain 41. These plans should outline specific response procedures and identify backup suppliers or alternative solutions.

**Enhance Supplier Relationship Management:** Building strong, collaborative relationships with key suppliers is crucial for effective risk mitigation 41. This includes promoting open communication, sharing information about potential risks, and working together on continuity planning.

**Implement Proper Access Management:** Enforcing strict access control policies, including role-based access control and the principle of least privilege, is essential for limiting the potential impact of a compromised vendor 37. Regularly reviewing and revoking access when no longer needed is also critical.

**Secure Software and Firmware Update Processes:** Organizations must establish secure procedures for managing and deploying software and firmware updates in their OT environment, including verifying the integrity and authenticity of updates before installation 3.

**Strengthen Remote Access Security:** Implementing secure remote access solutions, such as VPNs with strong encryption and multi-factor authentication, and diligently monitoring remote access sessions are vital for mitigating risks associated with vendor access 8.

**Conduct Regular Security Assessments and Penetration Testing:** Periodic security assessments and penetration testing of the OT environment and connections to vendor systems can help identify vulnerabilities that might be exploited by attackers targeting the supply chain 8.

**Implement Network Segmentation:** Segregating the OT network from the enterprise IT network and further segmenting within the OT environment can limit the lateral movement of attackers who might gain initial access through a compromised supply chain vendor 2.

**Utilize Technology for Real-Time Visibility:** Implementing technologies that provide real-time visibility into the supply chain, including monitoring for unusual activities or potential threats, can enable faster detection and response to security incidents 41.

**X. Continuous Monitoring Framework: Detailing Ongoing Assessment Approaches:**

Establishing a framework for continuous monitoring of security within the OT supply chain is essential for maintaining a strong security posture over time 36. Continuous monitoring uses automation to provide up-to-date security insights and support supply chain risk management 48. This helps organizations identify potential threats as they emerge and initiate remediation efforts promptly. Integrating **Knowledge Graphs** and **GNNs** into this framework can significantly enhance its effectiveness by providing deeper insights into evolving risks and anomalies within the complex supply chain network.

Key elements of a continuous monitoring framework include:

* **Real-time Security Ratings:** Utilizing security ratings services that provide ongoing assessments of vendor security posture based on publicly available information and security testing 36.
* **Threat Intelligence Feeds:** Integrating threat intelligence feeds to stay informed about emerging threats, vulnerabilities, and attack trends that could potentially impact the OT supply chain 36.
* **Automated Vulnerability Scanning:** Implementing regular and automated vulnerability scans of the OT network and connected vendor systems to identify new weaknesses 29.
* **Log Analysis and SIEM:** Collecting and analyzing security logs from OT systems, network devices, and vendor connections using a Security Information and Event Management (SIEM) system to detect suspicious activities and potential breaches 46.
* **Behavioral Analytics:** Employing behavioral analytics tools to establish baselines of normal activity within the OT environment and identify deviations that could indicate a security compromise 50.
* **Regular Security Audits and Assessments:** Conducting periodic security audits and assessments of vendors and the organization's own OT environment to verify the effectiveness of security controls 36.
* **Performance Monitoring:** Continuously monitoring the performance and availability of critical OT systems and vendor services to detect any anomalies that might indicate a security issue or disruption 36.
* **Automated Notifications and Alerts:** Setting up automated notifications and alerts for any detected security incidents, vulnerabilities, or deviations from established security baselines 50.

Continuous monitoring enables organizations to move beyond reactive security measures to a more proactive approach, allowing for early detection and mitigation of potential threats within the OT supply chain 51. It also fosters a more collaborative approach with suppliers, driving continuous improvement in security practices 49.

**XI. The Role of Emerging Technologies:**

Emerging technologies like Digital Twins, Graph Neural Networks (GNNs), and Knowledge Bases offer promising avenues for enhancing the security of OT supply chains. Jim McKenney's expertise spans these areas, making them particularly relevant to this discussion 1.

**Digital Twins:** Digital Twins, which are virtual replicas of physical assets and systems 24, can play a dual role in OT security. On one hand, they can enhance security by providing real-time monitoring and predictive...[source](https://netfoundry.io/ot/the-role-of-digital-twins-and-industry-4-0-in-ot-security/) This capability aligns with Jim McKenney's focus on leveraging technology for improved reliability and safety in industrial environments 32. On the other hand, Digital Twins also require robust security measures to protect the data they generate and process . The constant exchange of data between the physical and virtual worlds needs to be secured against interception and tampering .

**Graph Neural Networks (GNNs):** GNNs are a type of neural network that can learn from graph-structured data, making them well-suited for analyzing the complex relationships within supply chain networks 53. Jim McKenney's work with ARPA AI Cyber Challenge teams highlights the importance of AI, including GNNs, in proactively identifying and rectifying software vulnerabilities 32. In the context of OT supply chain security, GNNs can be used for various applications, including detecting anomalies in network traffic that might indicate a supply chain attack 62, identifying malicious infrastructure used by threat actors , and assessing supplier risks based on their connections and behaviors within the supply chain ecosystem.

**Knowledge Bases:** Cybersecurity Knowledge Bases are comprehensive repositories of information on cybersecurity threats, vulnerabilities, best practices, and mitigation strategies . Jim McKenney's role at NCC Group, a firm known for its deep expertise and knowledge in industrial security 1, underscores the significance of leveraging knowledge for robust security. In the realm of OT supply chain security, a well-maintained Knowledge Base can provide valuable insights into known vulnerabilities associated with specific industrial control systems, software, and hardware components used by vendors 8. It can also serve as a central point of access for security policies, incident response procedures, and best practices for securing the supply chain . Integrating AI with Knowledge Bases can further enhance their capabilities by automating data retrieval, improving response times, and supporting better decision-making . Furthermore, Knowledge Graphs can serve as a powerful foundation for these Knowledge Bases, structuring the information in a way that facilitates efficient querying and analysis of complex relationships within the OT supply chain 33.

**XII. Case Study Focus: Learning from Supply Chain Compromises:**

Analyzing past supply chain compromises in industrial settings provides valuable lessons for strengthening security practices. Several high-profile incidents offer insights into the tactics used by attackers and the vulnerabilities they exploited .

The **SolarWinds** attack demonstrated the potential for a single compromised software update to have widespread and severe consequences across numerous organizations, including those in critical infrastructure . Attackers injected malicious code into the Orion platform's software update process, gaining persistent access to the systems of thousands of customers. Key lessons learned include the importance of rigorously verifying the integrity of software updates, implementing robust monitoring for unusual activity, and ensuring strong security practices across the entire software development lifecycle 34.

The **Stuxnet** worm, which targeted Iranian nuclear facilities, highlighted the risk of attacks on industrial control systems even in air-gapped environments . The malware was introduced via infected USB drives, underscoring the need for strict control over removable media and the implementation of strong endpoint security measures within OT networks .

The **CCleaner** attack involved the compromise of the software supply chain to distribute malware to millions of users through a legitimate software update 5. This incident emphasized the importance of secure code signing and verification processes and the potential for widely used software to become a vector for large-scale attacks 34.

The **3CX** supply chain attack in 2023 illustrated how attackers can compromise software build systems to inject malware into desktop applications 12. The attackers initially compromised a software package used by a 3CX employee, stole their credentials, and then used VPN access to infiltrate 3CX's internal systems, eventually compromising the build systems 33. This case highlights the need for stringent security measures for build environments, including network segmentation, robust access controls, and continuous monitoring 33.

These case studies underscore the critical need for a layered security approach that addresses vulnerabilities at every stage of the OT supply chain. Organizations must prioritize the security of their software development and update processes, implement robust vendor risk management programs, enforce strict access controls, and continuously monitor their OT environments for any signs of compromise. Leveraging advanced techniques like Knowledge Graphs to map dependencies and GNNs to detect anomalies can provide enhanced visibility and early warning of potential attacks. Furthermore, Digital Twins can help simulate the impact of such attacks, allowing for better preparedness and response strategies.

**XIII. Conclusion:**

Securing the OT supply chain against advanced persistent threats is a complex but essential undertaking for organizations operating critical infrastructure. The increasing convergence of IT and OT, coupled with the growing sophistication of cyberattacks, necessitates a proactive and holistic approach to security. By understanding the evolving threat landscape, meticulously mapping vulnerabilities within the supply chain using Knowledge Graphs, and implementing a robust risk assessment methodology for vendors enhanced by GNNs, organizations can lay a strong foundation for defense. Prioritizing secure remote access with PAM capabilities as a fundamental security layer is also crucial. Leveraging SBOMs and HBOMs to gain deep visibility into all components and utilizing Digital Twins powered by AI like AEON for simulations and proactive risk management further strengthens this defense. Establishing continuous monitoring frameworks augmented with advanced analytics are crucial for maintaining a resilient security posture over time. Emerging technologies like Digital Twins, GNNs, and Knowledge Bases, championed by experts like Jim McKenney, offer promising tools for enhancing security capabilities in the future. The lessons learned from past supply chain compromises underscore the importance of vigilance, robust security practices across the entire ecosystem, and a commitment to continuous improvement in the face of persistent and evolving threats. Organizations that prioritize the security of their OT supply chains will be better positioned to protect their critical operations, safeguard their assets, and ensure the safety and reliability of the essential services they provide.

#### Works cited

1. Webinar 2: Operationalize – The Key to IT/OT/Safety Convergence ..., accessed March 22, 2025, <https://app.livestorm.co/ncc-group/hold-2nd-ot-webinar?utm_source=Livestorm+company+page>
2. Unveiling the Dark Side: Common Attacks and Vulnerabilities in Industrial Control Systems, accessed March 22, 2025, <https://www.aon.com/en/insights/cyber-labs/unveiling-the-dark-side-common-attacks-and-vulnerabilities-in-industrial-control-systems?collection=5b76135e-4196-415b-ab1d-f42b6f0abb10&parentUrl=null>
3. Supply Chain Attacks in ICS/OT Environments | by Md Tajdar Alam Ansari | Medium, accessed March 22, 2025, <https://mactavish-exe.medium.com/supply-chain-attacks-in-ics-ot-environments-c38c4d38b385>
4. Countering the Rising Tide of Supply Chain Attacks - zvelo, accessed March 22, 2025, <https://zvelo.com/countering-the-rising-tide-of-supply-chain-attacks/>
5. A Brief History of Supply Chain Attacks - Secarma: Penetration Testing and Cybersecurity Company, accessed March 22, 2025, <https://secarma.com/a-brief-history-of-supply-chain-attacks>
6. www.OilIT.com - Oil IT Journal, accessed March 22, 2025, <https://oilit.com/2journal/PDFs/Oil%20IT%20Journal%202020_1%20(No.%20251).pdf>
7. Supply chain attack - Wikipedia, accessed March 22, 2025, <https://en.wikipedia.org/wiki/Supply_chain_attack>
8. Securing the OT Supply Chain | Best Practices from Sectrio, accessed March 22, 2025, <https://sectrio.com/blog/securing-the-ot-supply-chain/>
9. TXOne Networks' 2024 report details critical OT/ICS cybersecurity challenges amid supply chain risks, aging infrastructure - Industrial Cyber, accessed March 22, 2025, <https://industrialcyber.co/news/txone-networks-2024-report-details-critical-ot-ics-cybersecurity-challenges-amid-supply-chain-risks-aging-infrastructure/>
10. OTORIO survey highlights rising awareness of OT cybersecurity, supply chain challenges, accessed March 22, 2025, <https://industrialcyber.co/news/otorio-survey-highlights-rising-awareness-of-ot-cybersecurity-supply-chain-challenges/>
11. Cybersecurity Threats in the Supply Chain: Case Studies, Blockchain, and Defence Strategies | Cyber Solutions By Thales, accessed March 22, 2025, <https://cds.thalesgroup.com/en/hot-topics/cybersecurity-threats-supply-chain-case-studies-blockchain-and-defence-strategies>
12. Top 15 software supply chain attacks: Case studies - Outshift | Cisco, accessed March 22, 2025, <https://outshift.cisco.com/blog/top-10-supply-chain-attacks>
13. Analyzing the supply chain risks behind the top data breaches in 2024, accessed March 22, 2025, <https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024>
14. 3CX Supply Chain Attack: Lessons Learned - Xygeni, accessed March 22, 2025, <https://xygeni.io/blog/3cx-supply-chain-attack-lessons-learned/>
15. Supply Chain Attacks: 7 Examples and 4 Defensive Strategies - BlueVoyant, accessed March 22, 2025, <https://www.bluevoyant.com/knowledge-center/supply-chain-attacks-7-examples-and-4-defensive-strategies>
16. Need to build robust industrial supply chain security while considering emerging technologies, accessed March 22, 2025, <https://industrialcyber.co/features/need-to-build-robust-industrial-supply-chain-security-while-considering-emerging-technologies/>
17. Understanding the Differences in OT Cybersecurity Standards: NIST CSF vs. ISA/IEC 62443, accessed March 22, 2025, <https://insanecyber.com/understanding-the-differences-in-ot-cybersecurity-standards-nist-csf-vs-62443/>
18. Adopting holistic approach to address complexities of cyber-physical security across IT and OT environments, accessed March 22, 2025, <https://industrialcyber.co/features/adopting-holistic-approach-to-address-complexities-of-cyber-physical-security-across-it-and-ot-environments/>
19. OT Cybersecurity Framework: Requirements & Implementation - Centraleyes, accessed March 22, 2025, <https://www.centraleyes.com/ot-cybersecurity-framework/>
20. Overcoming OT Security Challenges and Complexities - Supply Chain Digital, accessed March 22, 2025, <https://supplychaindigital.com/articles/overcoming-ot-security-challenges-and-complexities>
21. Trends and expectations for OT security in 2025 | Nomios Group, accessed March 22, 2025, <https://www.nomios.com/news-blog/trends-ot-security-2025/>
22. OT Cybersecurity in 2025: 6 Trends to Watch | Rockwell Automation | US, accessed March 22, 2025, <https://www.rockwellautomation.com/en-us/company/news/blogs/cybersecurity-trends-2025.html>
23. Manufacturing Industry Cyber Security | NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/us/manufacturing-services/>
24. The Role of Digital Twins and Industry 4.0 in OT Security - NetFoundry, accessed March 22, 2025, <https://netfoundry.io/ot/the-role-of-digital-twins-and-industry-4-0-in-ot-security/>
25. Cyber Security for Operational Technology (OT) - NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/us/consulting-implementation/operational-technology/>
26. Palo Alto Networks Surveys the State of OT Security, accessed March 22, 2025, <https://www.paloaltonetworks.com/blog/network-security/state-of-ot-security-2024/>
27. OT Cybersecurity Year in Review & Key Takeaways for 2025 - Secomea, accessed March 22, 2025, <https://secomea.com/remote-access/ot-cybersecurity-year-in-review-and-key-takeaways-for-2025/>
28. Safety First! Secure OT To Protect Your People & Productivity | NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/us/securing-ot-against-cyber-attacks-to-protect-your-people-and-productivity/>
29. A Complete Guide to OT/ICS Vulnerability Management in 2023 - Sectrio, accessed March 22, 2025, <https://sectrio.com/blog/a-complete-guide-to-ot-ics-vulnerability-management/>
30. Organizations Still Not Patching OT Due to Disruption Concerns: Survey - SecurityWeek, accessed March 22, 2025, <https://www.securityweek.com/organizations-still-not-patching-ot-due-to-disruption-concerns-survey/>
31. Fending off Cyberattacks on Collaborative Robots - Communications of the ACM, accessed March 22, 2025, <https://cacm.acm.org/news/fending-off-cyberattacks-on-collaborative-robots/>
32. SPEAKERS - CORNCON 9, accessed March 22, 2025, <https://corncon.net/CC9.Speaker.List.pdf>
33. Enhancing Supply Chain Visibility with Knowledge Graphs and Large Language Models, accessed March 22, 2025, <https://arxiv.org/html/2408.07705v1>
34. Why Knowledge Graphs Are Essential for Enterprises? - Squirro, accessed March 22, 2025, <https://squirro.com/squirro-blog/why-knowledge-graphs-are-essential-for-enterprises>
35. Supply chain risk assessment: A critical tool for business resilience - DataGuard, accessed March 22, 2025, <https://www.dataguard.com/blog/supply-chain-risk-assessment/>
36. How to Evaluate Vendor Security Performance Using Metrics - Peris.ai, accessed March 22, 2025, <https://www.peris.ai/post/how-to-evaluate-vendor-security-performance-using-metrics>
37. What is Vendor Security Assessment? 6 Steps to Perform - Sprinto, accessed March 22, 2025, <https://sprinto.com/blog/vendor-security-assessment/>
38. How to Conduct a Vendor Security Assessment to Identify High-Risk Vendors, accessed March 22, 2025, <https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment/>
39. Best Ways to Evaluate Your Security Posture | HyperComply Blog, accessed March 22, 2025, <https://www.hypercomply.com/blog/evaluate-security-posture>
40. A Complete Guide to Assessing Third-Party Security Posture - Panorays, accessed March 22, 2025, <https://panorays.com/blog/security-posture-complete-guide/>
41. Supply Chain Risk Mitigation: 8 Tactics Every Business Needs - Avetta, accessed March 22, 2025, <https://www.avetta.com/blog/supply-chain-risk-mitigation-8-strategies-every-business-needs>
42. How to Mitigate Risk in the Supply Chain - Everstream Analytics, accessed March 22, 2025, <https://www.everstream.ai/articles/how-to-mitigate-risk-in-the-supply-chain/>
43. Top Supply Chain Risks and How to Mitigate Them - NetSuite, accessed March 22, 2025, <https://www.netsuite.com/portal/resource/articles/inventory-management/supply-chain-risks.shtml>
44. Supply Chain Risk Management (SCRM): Strategies & Solutions | Ivalua, accessed March 22, 2025, <https://www.ivalua.com/blog/supply-chain-risk-management/>
45. Supply Chain Security: Why It's Important & 7 Best Practices - BlueVoyant, accessed March 22, 2025, <https://www.bluevoyant.com/knowledge-center/supply-chain-security-why-its-important-7-best-practices>
46. 7 Key Supply Chain Security Best Practices, accessed March 22, 2025, <https://www.nri-secure.com/blog/supply-chain-security-best-practices>
47. What is Supply Chain Security? - BitSight Technologies, accessed March 22, 2025, <https://www.bitsight.com/glossary/supply-chain-security>
48. www.certa.ai, accessed March 22, 2025, <https://www.certa.ai/resources/continuous-monitoring#:~:text=Continuous%20monitoring%20uses%20automation%20to,and%20start%20remediation%20right%20away.>
49. Continuous Monitoring: 5 Reasons to Prioritize - Certa, accessed March 22, 2025, <https://www.certa.ai/resources/continuous-monitoring>
50. Continuous Monitoring in Cyber Security and TPRM - Risk Ledger, accessed March 22, 2025, <https://riskledger.com/resources/continuous-monitoring-cyber-security-tprm>
51. What is Continuous Security Monitoring? (Steps to Implement) - Cyber Sierra, accessed March 22, 2025, <https://cybersierra.co/blog/continuous-security-monitoring/>
52. CC9 T3C Jim Mckenney OT Security - YouTube, accessed March 22, 2025, <https://www.youtube.com/watch?v=88a9WC0DQlc>
53. Using Graph Neural Networks for the Analysis of Complex Data: Approaches and Applications - Carlo C., accessed March 22, 2025, <https://autognosi.medium.com/using-graph-neural-networks-for-the-analysis-of-complex-data-approaches-and-applications-3aa1119eacb0>
54. One Step Ahead in Cyber Hide-and-Seek: Automating Malicious Infrastructure Discovery With Graph Neural Networks - Unit 42, accessed March 22, 2025, <https://unit42.paloaltonetworks.com/graph-neural-networks/>
55. (PDF) Graph Neural Networks for Intrusion Detection: A Survey - ResearchGate, accessed March 22, 2025, <https://www.researchgate.net/publication/370733865_Graph_Neural_Networks_for_Intrusion_Detection_A_Survey>
56. Use of Graph Neural Networks in Aiding Defensive Cyber Operations - arXiv, accessed March 22, 2025, <https://arxiv.org/html/2401.05680v1>
57. Graph Neural Networks in Supply Chain Analytics and Optimization: Concepts, Perspectives, Dataset and Benchmarks - arXiv, accessed March 22, 2025, <https://arxiv.org/html/2411.08550v1>
58. Graph Neural Network for Daily Supply Chain Problems - Preprints.org, accessed March 22, 2025, <https://www.preprints.org/manuscript/202409.2376/v1/download>
59. Graph Neural Network for Daily Supply Chain Problems - Preprints.org, accessed March 22, 2025, <https://www.preprints.org/manuscript/202409.2376/v1>
60. Graph Neural Network for Daily Supply Chain Problems - ResearchGate, accessed March 22, 2025, <https://www.researchgate.net/publication/384592034_Graph_Neural_Network_for_Daily_Supply_Chain_Problems>
61. SC-TKGR: Temporal Knowledge Graph-Based GNN for Recommendations in Supply Chains - MDPI, accessed March 22, 2025, <https://www.mdpi.com/2079-9292/14/2/222>
62. GNN-Based Network Traffic Analysis for the Detection of Sequential Attacks in IoT - MDPI, accessed March 22, 2025, <https://www.mdpi.com/2079-9292/13/12/2274>
63. FN-GNN: A Novel Graph Embedding Approach for Enhancing Graph Neural Networks in Network Intrusion Detection Systems - MDPI, accessed March 22, 2025, <https://www.mdpi.com/2076-3417/14/16/6932>
64. Graphing the Future: Harnessing the Power of Graph Neural Networks for Cybersecurity - CyberPoint International, accessed March 22, 2025, <https://www.cyberpointllc.com/blog-posts/Graphing-the-Future-Harnessing-the-Power-of-Graph-Neural-Networks-for-CyberSecurity.php>
65. Untitled - Your.Org, accessed March 22, 2025, <ftp://ftpmirror.your.org/pub/misc/bitsavers/pdf/datamation/196811.pdf>
66. Waves of Change: Business Evolution Through Information Technology - Amazon.com, accessed March 22, 2025, <https://www.amazon.com/Waves-Change-Evolution-Information-Technology/dp/0875845649>
67. Waves of Change: Business Evolution through Information Technology - Barnes & Noble, accessed March 22, 2025, <https://www.barnesandnoble.com/w/waves-of-change-james-l-mckenney/1112004981>
68. The Most Effective Supply Chain Risk Mitigation Strategies - Surgere, accessed March 22, 2025, <https://surgere.com/blog/the-most-effective-supply-chain-risk-mitigation-strategies/>
69. Workers' Compensation Appeals Board - Panel decisions, accessed March 22, 2025, <https://www.dir.ca.gov/wcab/wcab-Decisions.htm>
70. Mark Carney - Wikipedia, accessed March 22, 2025, <https://en.wikipedia.org/wiki/Mark_Carney>
71. OKANAGAN WATER STEWARDSHIP COUNCIL - Okanagan Basin, accessed March 22, 2025, <https://obwb.ca/fileadmin/docs/100610_wsc.pdf>
72. Full article: The emergence of cognitive digital twin: vision, challenges and opportunities, accessed March 22, 2025, <https://www.tandfonline.com/doi/full/10.1080/00207543.2021.2014591>
73. The emergence of cognitive digital twin: vision, challenges and opportunities, accessed March 22, 2025, <https://www.researchgate.net/publication/357314650_The_emergence_of_cognitive_digital_twin_vision_challenges_and_opportunities>
74. Cybersecurity challenges of digital twins: threats and security measures | INCIBE-CERT, accessed March 22, 2025, <https://www.incibe.es/en/incibe-cert/blog/cybersecurity-challenges-digital-twins-threats-and-security-measures>
75. Case Study: Cyber Security Transformation & Due Diligence for a Rural Electric Cooperative, accessed March 22, 2025, <https://www.nccgroup.com/us/case-study-cyber-security-transformation-due-diligence-for-a-rural-electric-cooperative/>
76. James L. McKenney's research works | Harvard University and other places - ResearchGate, accessed March 22, 2025, <https://www.researchgate.net/scientific-contributions/James-L-McKenney-70387844>
77. Leading and Managing in the Digital Era - IRIS UPO, accessed March 22, 2025, <https://iris.uniupo.it/retrieve/a1d02bd1-0249-4cb7-b1eb-7a96fa79abe1/2024_Springer_Bonini-Capizzi-Tenca.pdf>
78. What Is A Cybersecurity Knowledge Base? - ITU Online IT Training, accessed March 22, 2025, <https://www.ituonline.com/tech-definitions/what-is-a-cybersecurity-knowledge-base/>
79. CyberSecurity Knowledge Bases: The Brain of Security Systems | ITeXchange Blog, accessed March 22, 2025, <https://www.itexchangeweb.com/blog/cybersecurity-knowledge-bases-the-brain-of-security-systems/>
80. Cybersecurity Transformation In Rural Electricity - NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/media/qmfk2mz1/nccgroup_it-ot-transformation-for-electric-coop_case_study.pdf>
81. James McKenney Remembered - Alumni - Harvard Business School, accessed March 22, 2025, <https://www.alumni.hbs.edu/stories/Pages/story-bulletin.aspx?num=281>
82. Jim McKenney - Partner - Albany, New York - Accounting & Advisory | UHY, accessed March 22, 2025, <https://uhy-us.com/professionals/jim-mckenney>
83. James L. McKenney of Business School, 77 - Harvard Gazette, accessed March 22, 2025, <https://news.harvard.edu/gazette/story/2007/04/james-l-mckenney-of-business-school-77/>
84. Jim McKenney - Systems Development Director at Computers Unlimited | The Org, accessed March 22, 2025, <https://theorg.com/org/computers-unlimited-inc/org-chart/jim-mckenney>
85. Industrial and Systems Engineering | Faculty, accessed March 22, 2025, <https://faculty.rpi.edu/departments/industrial-and-systems-engineering>
86. Faculty | H. Milton Stewart School of Industrial and Systems Engineering - Georgia Tech, accessed March 22, 2025, <https://www.isye.gatech.edu/people/faculty>
87. UvA-DARE (Digital Academic Repository) - Research Explorer, accessed March 22, 2025, <https://pure.uva.nl/ws/files/224795577/2312.02279v3.pdf>
88. White House Signs Critical Infrastructure Memorandum, Details Remain Unclear | Nexus, accessed March 22, 2025, <https://nexusconnect.io/articles/white-house-signs-critical-infrastructure-memorandum-details-remain-unclear>
89. U.S. Homeland Security Launches New Critical Infrastructure Security Guidance, accessed March 22, 2025, <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/may/DHS-critical-infrastructure-guidance/>
90. Secure Rail Conference outlines solutions to physical and cyber threats, accessed March 22, 2025, <https://www.progressiverailroading.com/security/news/Secure-Rail-Conference-outlines-solutions-to-physical-and-cyber-threats--57539>
91. Cyber Security Improvement | NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/us/consulting-implementation/strategy-risk-compliance/cyber-security-improvement/>
92. NCC Group | Leading Cyber Security & Managed Services, accessed March 22, 2025, <https://www.nccgroup.com/>
93. Section 1: 10-K (10-K), accessed March 22, 2025, <https://s201.q4cdn.com/129601114/files/doc_financials/2014/4Q14-10K.pdf>
94. Cyber Threat Intelligence: An Essential Business Solution | NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/us/cyber-threat-intelligence-the-essential-solution-shaping-your-business-future/>
95. Application Security | NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/au/technical-assurance/application-security/>
96. Cyber Security Standards & Frameworks - NCC Group, accessed March 22, 2025, <https://www.nccgroup.com/us/consulting-implementation/strategy-risk-compliance/compliance-privacy/standards-frameworks/>
97. Software Bill of Materials (SBOM) Guide - NetRise, accessed March 22, 2025, <https://www.netrise.io/software-bill-of-materials>
98. Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials - Journal of Critical Infrastructure Policy, accessed March 22, 2025, <https://www.jcip1.org/uploads/1/3/6/5/136597491/strengthening_the_security_of_operational_technology.pdf>
99. Software Bill of Materials (SBOM) - CISA, accessed March 22, 2025, <https://www.cisa.gov/sbom>
100. Software Bill of Materials (SBOM) Considerations for Operational Test & Evaluation Activities - SEI Blog, accessed March 22, 2025, <https://insights.sei.cmu.edu/documents/5897/WP_-_SBOM_Considerations_for_Operational_Test_and_Evaluation_Activities_-_Final.pdf>
101. SBOM vs HBOM: What's the Difference & Which is Right for Me?, accessed March 22, 2025, <https://www.fortressinfosec.com/blog/sbom-vs-hbom-whats-the-difference>
102. What is Software Composition Analysis (SCA)? - Black Duck, accessed March 22, 2025, <https://www.blackduck.com/glossary/what-is-software-composition-analysis.html>
103. What Is Software Composition Analysis (SCA)? - Palo Alto Networks, accessed March 22, 2025, <https://www.paloaltonetworks.com/cyberpedia/what-is-sca>
104. Software Composition Analysis | Microsoft Learn, accessed March 22, 2025, <https://learn.microsoft.com/en-us/devsecops/playbook/capabilities/security/software-composition-analysis>
105. Securing Open-Source Components with Orca Software Composition Analysis (SCA), accessed March 22, 2025, <https://orca.security/resources/blog/software-composition-analysis/>
106. What is Software Composition Analysis (SCA)? | CrowdStrike, accessed March 22, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/software-composition-analysis/>
107. Hardware Bill of Materials (HBOM) - CycloneDX, accessed March 22, 2025, <https://cyclonedx.org/capabilities/hbom/>
108. Why a Hardware Bill of Materials is a Critical Component for Securing Electronic Products, accessed March 22, 2025, <https://www.gsaglobal.org/forums/why-a-hardware-bill-of-materials-is-a-critical-component-for-securing-electronic-products/>
109. Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management - CISA, accessed March 22, 2025, <https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management>
110. Key Technologies for Software Supply Chain Security—Techniques for Generating and Using the List of Software Compositions (Part 2) - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks., accessed March 22, 2025, <https://nsfocusglobal.com/key-technologies-for-software-supply-chain-security-techniques-for-generating-and-using-the-list-of-software-compositions-part-2/>
111. OpenSPG is a Knowledge Graph Engine developed by Ant Group in collaboration with OpenKG, based on the SPG (Semantic-enhanced Programmable Graph) framework. Core Capabilities - GitHub, accessed March 22, 2025, <https://github.com/OpenSPG/openspg>
112. OpenSPG - GitHub, accessed March 22, 2025, <https://github.com/openspg>
113. KAG: Enhanced RAG and GraphRAG for LLM-based retrieval | by Mehul Gupta | Data Science in your pocket | Medium, accessed March 22, 2025, <https://medium.com/data-science-in-your-pocket/kag-enhanced-rag-and-graphrag-for-llm-based-retrieval-e84a66d6088c>
114. KAG: Knowledge Augmented Generation A Practical Guide better than Rag - PlainEnglish.io, accessed March 22, 2025, <https://plainenglish.io/blog/kag-knowledge-augmented-generation-a-pratical-guide-better-than-rag>
115. KAG: Boosting LLMs in Professional Domains via Knowledge Augmented Generation - arXiv, accessed March 22, 2025, <https://arxiv.org/html/2409.13731v3>
116. How Using a Digital Twin Will Revolutionize Your Security, accessed March 22, 2025, <https://aressecuritycorp.com/2024/10/30/digital-twin/>
117. Digital Twin explained - Sogelink, accessed March 22, 2025, <https://www.sogelink.com/en/innovation-2/digital-twin-explained/>
118. Harnessing Digital Twin Technology to Prevent Infrastructural Disasters - Passive Logic, accessed March 22, 2025, <https://passivelogic.com/blog/?post=digital-twin-technology-to-prevent-infrastructural-disasters>
119. Network Digital Twins: The Next Revolution in Network Management | Keysight Blogs, accessed March 22, 2025, <https://www.keysight.com/blogs/en/inds/ai/network-digital-twin>
120. What is a digital twin? Analysis and opportunities - Arvato Systems, accessed March 22, 2025, <https://www.arvato-systems.com/blog/what-is-a-digital-twin-analysis-and-strategic-opportunities>
121. Knowledge Graph For Digital Twin - NODES 2024 - YouTube, accessed March 22, 2025, <https://www.youtube.com/watch?v=SpvtBd1j3Ic>