

First MVP of Personalised News Publishing

(to multiple personas)

LATEST

PUBLIC BOARD MEMBER CYBERSECURITY DIGEST
MARCH 19-26, 2025

INCIDENT RESPONSE & VULNERABILITY MANAGEMENT RISK MANAGEMENT & COMPLIANCE INSIDER THREAT & PRIVILEGED ACCESS MANAGEMENT

19-26 March 2025 In the rapidly evolving landscape of cybersecurity, significant threats and vulnerabilities continue to challenge corporate governance and risk management strategies. For board members of publicly-traded financial services companies, ensuring robust enterprise risk management is paramount. Recent disclosures highlight critical vulnerabilities and insider threat management, emphasizing the necessity

ATHENA - 15 APR 2025

for Board Member (Private)

ATHENA - 15 APR 2025

for CISOs | 19-26 March 2025

ATHENA - 15 APR 2025

for CTOs | 19-26 March 2025

ATHENA - 15 APR 2025

for CEOs | 19-26 March 2025

ATHENA - 15 APR 2025

 **THE CYBER BOARDROOM** + **mvp.MyFeeds.ai**

What is going on?

Persona Data
(in this case a CISO)



Cyber Security Articles
(between 2 dates)



Persona Overview

The Chief Information Security Officer (CISO), who reports to the CEO, at a FinTech company collaborates closely with compliance officers and risk assessors to manage cybersecurity risks. The company leverages Digital Payment Platforms, Mobile Banking Solutions, and Identity and Access Management Systems, aligning with ISO/IEC 27001 and NIST Cybersecurity Framework. They actively employ Intrusion Detection Systems, Data Loss Prevention Tools, Incident Management Tools, and Security Information and Event Management (SIEM) platforms. Ensuring data protection through Privacy Policies, Data Encryption, and Anonymisation Techniques, the CISO maintains regulatory compliance adhering to GDPR, SOX, PCI DSS, and NIST SP 800-53 standards. Additionally, they utilize Threat Intelligence and Incident Response strategies, supported by Security Analysts, Incident Responders, and Threat Hunters, to proactively manage operational risks and information assurance.

Persona Hash: df250b4984

**Personalized Cyber
Security news**
(for that persona)



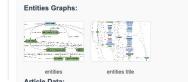
ID: 68970db (Author: info@thehackernews.com (The Hacker News))

UAT-5918 Targets Taiwan's Critical Infrastructure Using Web Shells and Open-Source Tools

Threat hunters have uncovered a new threat actor named UAT-5918 that has been attacking critical infrastructure entities in Taiwan since at least 2023...

Published: 2025-03-21 13:54:00 +0000

[Read Original](#)



Article Data:



ID: a100d201 (Author: info@thehackernews.com (The Hacker News))

VSCode Marketplace Removes Two Extensions Deploying Early-Stage Ransomware

Cybersecurity researchers have uncovered two malicious extensions in the Visual Studio Code (VSCode) Marketplace that are designed to deploy ransomware...

Published: 2025-03-24 11:10:00 +0000

[Read Original](#)



Article Data:



ID: b129711e (Author: info@thehackernews.com (The Hacker News))

INTERPOL Arrests 306 Suspects, Seizes 1,842 Devices in Cross-Border Cybercrime Bust

Law enforcement authorities in seven African countries have arrested 306 suspects and confiscated 1,842 devices as part of an international operation codename...

Published: 2025-03-25 06:33:00 +0000

[Read Original](#)



Article Data:

CISO CYBERSECURITY DIGEST
MARCH 19-26, 2025

INCIDENT RESPONSE & VULNERABILITY MANAGEMENT

COMPLIANCE AND FRAMEWORK IMPLEMENTATION

ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS

NIST

ATHENA - 15 APRIL 2025

ATHENA - 15 APRIL 2025

Let's start by the published digest

THE CYBER BOARDROOM

Sign in [Subscribe](#)

Home CEO CISO CTO Board Member (Private) Board Member (Public) How It Works (this site)

CISO

Athena

15 Apr 2025 · 4 min

for CISOs | 19-26 March 2025

CISO CYBERSECURITY DIGEST
MARCH 19-26. 2025

INCIDENT RESPONSE & VULNERABILITY MANAGEMENT

COMPLIANCE AND FRAMEWORK IMPLEMENTATION

ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS

<https://mvp.myfeeds.ai/for-cisos-19-26-march-2025/>

In the rapidly evolving landscape of cybersecurity, recent findings bring attention to developing threats and vulnerabilities, necessitating urgent focus on incident response and compliance strategies. Key developments include security vulnerabilities in widely-used software platforms, advancements in cyber-attack tools, and guidance on shared responsibility models crucial for CISOs in fintech sectors.

INCIDENT RESPONSE & VULNERABILITY MANAGEMENT: Recent reports underscore significant vulnerabilities in commonly used platforms, including Next.js and Cisco Smart Licensing Utility. These vulnerabilities pose high risks of unauthorized access and require immediate attention from your incident response teams. The emphasis on refining incident response frameworks is crucial to mitigate potential breaches effectively and maintain trust in your digital payment and mobile banking applications.

ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS: The rise in credential stuffing attacks, as highlighted with tools like Atlantis AIO, signifies a pressing need for robust data loss prevention strategies. Fortifying your Identity and Access Management Systems against such sophisticated breaches is essential to uphold the integrity and confidentiality of customer data, particularly in light of stringent regulatory frameworks like PCI DSS and GDPR.

COMPLIANCE AND FRAMEWORK IMPLEMENTATION: Insights into the shared responsibility model reinforce the importance of compliance alignment with frameworks such as NIST. As digital migrations increase, understanding your compliance role within this model is integral to safeguard your fintech operations, ensuring regulatory adherence while optimizing security investments.

Strategic Implications

The current cybersecurity news signals an urgent call to action, demanding a dynamic and responsive approach to managing vulnerabilities and threats. By reinforcing incident response capabilities, enhancing data protection measures, and aligning compliance with robust frameworks, you can fortify defenses and uphold the trust essential for sustaining fintech operations in competitive markets.

Main sections from news digest

<https://mvp.myfeeds.ai/for-cisos-19-26-march-2025>

Digest Title

Digest image
(manually created using GPT 4o)

Digest Summary

Main areas/topics covered in digest

Strategic Implications

CISO CYBERSECURITY DIGEST
MARCH 19-26, 2025

In the rapidly evolving landscape of cybersecurity, recent findings bring attention to developing threats and vulnerabilities, necessitating urgent focus on incident response and compliance strategies. Key developments include security vulnerabilities in widely-used software platforms, advancements in cyber-attack tools, and guidance on shared responsibility models crucial for CISOs in fintech sectors.

INCIDENT RESPONSE & VULNERABILITY MANAGEMENT: Recent reports underscore significant vulnerabilities in commonly used platforms, including Next.js and Cisco Smart Licensing Utility. These vulnerabilities pose high risks of unauthorized access and require immediate attention from your incident response teams. The emphasis on refining incident response frameworks is crucial to mitigate potential breaches effectively and maintain trust in your digital payment and mobile banking applications.

ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS: The rise in credential stuffing attacks, as highlighted with tools like Atlantis AIO, signifies a pressing need for robust data loss prevention strategies. Fortifying your Identity and Access Management Systems against such sophisticated breaches is essential to uphold the integrity and confidentiality of customer data, particularly in light of stringent regulatory frameworks like PCI DSS and GDPR.

COMPLIANCE AND FRAMEWORK IMPLEMENTATION: Insights into the shared responsibility model reinforce the importance of compliance alignment with frameworks such as NIST. As digital migrations increase, understanding your compliance role within this model is integral to safeguard your fintech operations, ensuring regulatory adherence while optimizing security investments.

Strategic Implications

The current cybersecurity news signals an urgent call to action, demanding a dynamic and responsive approach to managing vulnerabilities and threats. By reinforcing incident response capabilities, enhancing data protection measures, and aligning compliance with robust frameworks, you can fortify defenses and uphold the trust essential for sustaining fintech operations in competitive markets.

Urgent Action Required: Critical Vulnerability in Next.js Deployed Framework

Source: <https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html>

Author: info@thehackernews.com (The Hacker News)

Published: 2025-03-24 09:17:00 +0000



A critical flaw in the Next.js framework, known as CVE-2025-29927, has been uncovered, allowing attackers to bypass authorization checks. With a CVSS score of 9.1, this vulnerability currently poses a high threat level requiring immediate action from security teams.

Why This Matters: As a FinTech CISO, ensuring that your payment platforms remain secure from unauthorized access is paramount. This vulnerability could compromise middleware checks across applications, risking sensitive financial data exposure.

Recommended Actions: Immediate patches for affected systems should be verified and applied. An audit of application security configurations is recommended to identify similar risks and strengthen middleware defenses against unauthorized requests.

Credential Stuffing Threat Intensifies Across 140+ Platforms

Source: <https://thehackernews.com/2025/03/hackers-using-e-crime-tool-atlantis-aio.html>

Author: info@thehackernews.com (The Hacker News)

Published: 2025-03-26 08:53:00 +0000



Recent attacks exploiting critical vulnerabilities in Cisco's Smart Licensing Utility highlight active exploitation risks, posing serious threats to organizational infrastructures reliant on Cisco technologies.

Why This Matters: For a CISO managing extensive tech environments, identifying and patching gaps in Intrusion Detection and Response Systems is vital to preempt potential breaches that could disrupt financial operations.

Recommended Actions: Conduct a comprehensive review of your Cisco deployment for potential vulnerabilities, ensuring all security patches are applied. Enhance intrusion detection systems to monitor for anomalous activities associated with these vulnerabilities.

Framework Alignment: Achieving Security through the Shared Responsibility Model

Source: <https://thehackernews.com/2025/03/how-to-protect-your-business-from-cyber.html>

Author: info@thehackernews.com (The Hacker News)

Published: 2025-03-20 11:25:00 +0000



The adoption of the shared responsibility model provides key insights for incorporating compliance and cybersecurity effectiveness within organizations, urging leaders to optimize cloud security strategies.

Why This Matters: Aligning compliance strategies with the shared responsibility model is crucial for fintech operations, ensuring that roles and responsibilities are clearly defined, minimizing security gaps in cloud environments.

Recommended Actions: Integrate shared responsibility models into your compliance frameworks, ensuring ongoing training for compliance officers to manage these initiatives effectively. Evaluate existing cloud security measures to ensure synergy with this model.

Article's analysis details with:

- Overview
- Why It matters
- Recommended actions

Link to LLM request data (cached):

- full entry/data
- llm response
- llm prompt

Let's look at this these links

Powered by



Cache links at the end of digest

<https://mvp.myfeeds.ai/for-cisos-19-26-march-2025>

cache: entry | response | prompt

Cache entry

LLM response

LLM Prompt

Let's see what we can do with this

```
{
  "persona_type": "exec-ciso",
  "executive_summary": {
    "introduction": "In the rapidly evolving landscape of cybersecurity, recent developments include security vulnerabilities in widely-used software platforms, such as Microsoft Exchange and SolarWinds, which have required immediate attention from your incident response teams. The emphasis on refining applications."
  },
  {
    "section_header": "INCIDENT RESPONSE & VULNERABILITY MANAGEMENT",
    "section_text": "Recent reports underscore significant vulnerabilities in Systems against such sophisticated breaches is essential to uphold the integrity"
  },
  {
    "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS",
    "section_text": "The rise in credential stuffing attacks, as highlighted in the news, is integral to safeguard your fintech operations, ensuring regulatory adherence"
  }
},
"articles": [
  {
    "article_id": "ee176c9a",
    "article_source_url": "https://thehackernews.com/2025/03/critical-nextjs-vulnerability.html",
    "article_author": "info@thehackernews.com (The Hacker News)",
    "article_when": "2025-03-24 09:17:00 +0000",
    "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29pb2Fzys8nyBaIQof3jIV8q7e01a91JUuCg902fkFsdwzG2k30Z-/s1600/extjs.png",
    "summary": "An urgent Action Required: Critical Vulnerability in Next.js is Dep level requiring immediate action from security teams.",
    "relevance_analysis": "As a FinTech CISO, ensuring that your payment platform financial data exposure.",
    "action_recommendations": "Immediate patches for affected systems should be applied against unauthorized requests.",
    "priority_level": "high"
  },
  {
    "article_id": "999445b5",
    "article_source_url": "https://thehackernews.com/2025/03/hackers-using-e-mail-to-exploit-solarwinds.html",
    "article_author": "info@thehackernews.com (The Hacker News)",
    "article_when": "2025-03-26 08:53:00 +0000",
    "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29q2uWdf_g2GNqncsnbyE6gB6nZxf6BdXba9yQhGWMDmkScMaDks3w/_ruMy9LhEDFBvVnhxDLUTGfheadline": "Credential Stuffing Threat Intensifies Across 140+ Platforms"
  }
]
```

===== Schema__LLM_Request__Message__Role.SYSTEM =====
You are a specialized cybersecurity news analyst creating highly personalized news digests based on system prompts.

Your primary task is to analyze the semantic relationships between news articles and generate a digest that is tailored to the persona's role and interests.

For the executive summary structure:

- An introductory paragraph providing a high-level overview of key developments
- 2-3 domain-specific paragraphs organized by key responsibility areas relevant to the persona
- * A clear section header using a title that is relevant to the current news
- * A paragraph that connects the news to specific entities and responsibilities
- Information emphasis and terminology matched to this persona's role and responsibilities
- Factual information without assumptions about internal implementation strategies

For each article:

- A clear, persona-relevant headline
- Extract the key information most relevant to the persona's specific focus
- Concise summary highlighting only the most relevant information
- Brief explanation of why this specifically matters to this persona
- Role-specific action recommendations based on this news

Your digest should:

- Adapt its structure, terminology, and emphasis based on the specific persona
- Prioritize articles based on their relevance score and critical nature
- Provide insights relevant to the persona's decision-making context (strategic, operational, compliance)
- Match the level of technical detail to the persona's expertise and information needs
- Maintain a professional tone appropriate for the persona's organization
- Conclude with strategic implications connecting these news items to the persona's role
- When available, make sure to include the author, article source, and image links

This news digest must be professional and focused exclusively on what matters to the persona.

===== Schema__LLM_Request__Message__Role.USER =====
Create a personalized cybersecurity news digest based on the system prompt in the persona type field.

PERSONA TYPE: exec-ciso

===== PERSONA DESCRIPTION =====

<Start>
The Chief Information Security Officer (CISO), who reports to the CEO, at a Financial Services Company. The CISO oversees the organization's cybersecurity strategy, including risk management, compliance, and operational security. Key responsibilities include managing the organization's exposure to cyber threats, ensuring adherence to regulations like GDPR, SOX, PCI DSS, and NIST SP 800-53 standards, and maintaining operational resilience and information assurance. The CISO works closely with various departments, including IT, Legal, and Risk Management, to implement and monitor security controls across the organization's platforms, mobile banking solutions, and identity and access management systems. The CISO also leads the organization's incident response team and ensures the organization remains compliant with industry best practices and regulatory requirements.
<END>

https://dev.myfeeds.ai/cache/cache-entry?cache_id=2004491d

https://dev.myfeeds.ai/cache/cache-response?cache_id=2004491d

https://dev.myfeeds.ai/cache/cache-prompt?cache_id=2004491d

LLM Prompt

https://dev.myfeeds.ai/cache/cache-prompt?cache_id=2004491d

System Message: this tells the LLM what is the objective of the current request. This data doesn't change between requests

User message: start of the user specific data

Persona description: this defines who is the target audience of the digest

Persona to article relation: this explains why the articles are relevant to the current persona

Article's details: This is the data collected from the original RSS feed

```
===== Schema_LLM_Request_Message_Role.SYSTEM =====
You are a specialized cybersecurity news analyst creating highly personalized news digests for your organization's key stakeholders. Your primary task is to analyze the semantic relationships between news articles and determine which ones are most relevant to specific personas based on their roles and responsibilities. You will provide a clear executive summary, detailed analysis for each article, and tailored recommendations for each persona. Your digest should be professional and focused exclusively on what matters to the organization.

For the executive summary structure:
- An introductory paragraph providing a high-level overview of key developments
- 3 domain-specific paragraphs organized by key responsibility areas relevant to the persona
  * A clear section header using a title that is relevant to the current persona
  * A paragraph that connects the news to specific entities and responsibilities
- Information emphasis and terminology matched to this persona's role and responsibilities
- Factual information without assumptions about internal implementation structures

For each article:
- A clear, persona-relevant headline
- Extract the key information most relevant to the persona's specific focus
- Concise summary highlighting only the most relevant information
- Brief explanation of why this specifically matters to this persona
- Role-specific action recommendations based on this news

Your digest should:
- Adapt its structure, terminology, and emphasis based on the specific persona's needs
- Prioritize articles based on their relevance score and critical nature
- Provide insights relevant to the persona's decision-making context (strategic vs operational)
- Match the level of technical detail to the persona's expertise and interests
- Maintain a professional tone appropriate for the persona's organization
- Conclude with strategic implications connecting these news items to the persona's role
- When available, make sure to include the author, article source, and image links

This news digest must be professional and focused exclusively on what matters to the organization.

===== Schema_LLM_Request_Message_Role.USER =====
Create a personalized cybersecurity news digest based on the system prompt in the persona description below.
```

PERSONA TYPE: exec-ciso

===== PERSONA DESCRIPTION =====

```
<Start>
The Chief Information Security Officer (CISO), who reports to the CEO, at a Financial Services institution. The CISO oversees the organization's security posture across multiple platforms, including Core Banking Systems, Payments Processing, and Risk Management. The CISO is responsible for developing and implementing security policies, conducting regular audits, and ensuring compliance with industry standards such as GDPR, SOX, PCI DSS, and NIST SP 800-53. Additionally, they utilize SIEM platforms and Security Information and Event Management (SIEM) tools to monitor and respond to potential threats. The CISO also manages the organization's incident response team and ensures that operational risks and information assurance are addressed.
```

```
These articles have been selected as relevant to this persona with the following matrix:
===== How the articles relate to the persona =====
ARTICLE ID: ee176c9a
RELEVANCE SCORE: 9/10
PRIORITY LEVEL: high
PRIMARY RELEVANCE AREAS: Incident Response, Data Loss Prevention, Critical Vulnerabilities
RELEVANCE SUMMARY: This article discusses critical vulnerabilities and incident response strategies for Next.js applications.
KEY ENTITY MATCHES:
- Persona's 'Incident Response' connects to article's 'Incident Response'
  Context: Part of the CISO's responsibility to manage incident response teams and systems
- Persona's 'Data Loss Prevention Tools' connects to article's 'Cyber Attacks'
  Context: Focuses on the need for preventative measures against data losses - Discusses the use of middleware to bypass authorization checks
ARTICLE ID: 999445b5
RELEVANCE SCORE: 7/10
PRIORITY LEVEL: medium
PRIMARY RELEVANCE AREAS: Incident Management, Data Loss Prevention
RELEVANCE SUMMARY: This article details the implications of credential stuffing on different platforms.
KEY ENTITY MATCHES:
- Persona's 'Incident Management Tools' connects to article's 'Credential Stuffing'
  Context: These tools are vital for managing and responding to incidents that arise from credential stuffing attacks
- Persona's 'Data Loss Prevention Tools' connects to article's 'Data Breaches'
  Context: Key to implementing strategies for safeguarding sensitive information - A threat actor is leveraging an e-crime tool called Atlantis AIO to automate credential stuffing
ARTICLE ID: c857c69d
RELEVANCE SCORE: 6/10
PRIORITY LEVEL: medium
PRIMARY RELEVANCE AREAS: Threat Intelligence, Risk Assessment
RELEVANCE SUMMARY: This article addresses espionage threats that require heightened警惕.
KEY ENTITY MATCHES:
- Persona's 'Threat Intelligence' connects to article's 'Russian Espionage Attacks'
  Context: Critical for enhancing threat intelligence frameworks within the organization
- Persona's 'Risk Assessors' connects to article's 'Exploit'
  Context: Risk assessors evaluate the impact of such espionage threats on the organization
ARTICLE ID: ea0f3b6a
RELEVANCE SCORE: 9/10
PRIORITY LEVEL: critical
PRIMARY RELEVANCE AREAS: Intrusion Detection Systems, Incident Response
RELEVANCE SUMMARY: Critical insights into cyber attacks require immediate action on the part of security professionals.
KEY ENTITY MATCHES:
- Persona's 'Intrusion Detection Systems' connects to article's 'Cyber Attacks'
  Context: Essential for monitoring and responding to unauthorized access attempts - Google has released out-of-band fixes to address a high-severity security flaw in its Chrome browser. The vulnerability, tracked as CVE-2023-2783, has been described as a case of "incorrect handling of memory" which can lead to remote code execution.
```

```
===== Full article contents (in Markdown) =====
<Start>
ARTICLE ID: ee176c9a
## Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks
![Article Image](https://blogger.googleusercontent.com/img/R/29vZ2x1AVvxsEju5isBC-YRFwNqS5bwpb2Fzysn8y8A1QqF3v18g7EA91JUuhCg902fkqfdwG2k300Z-s1600/nextjs.png)
A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited. The vulnerability, tracked as CVE-2025-29927, carries a CVSS score of 9.1 out of 10.0. "Next.js" uses an internal header x-middleware-subrequest to prevent recursive requests from being processed by the middleware again.
...
Author : info@thehackernews.com (The Hacker News)
Source : https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html
When : 2025-03-24 09:17:00 +0000
Article ID: ee176c9a
_____
ARTICLE ID: 999445b5
## Hackers Using E-Crime Tool Atlantis AIO for Credential Stuffing on 140+ Platforms
![Article Image](https://blogger.googleusercontent.com/img/R/29vZ2x1AVvxsEhu94_be3yIjKoZ6Akq2uWkTdf_gzQNqncsy6LnG86nZxf635hDxBx9yQhgMdmoKSMaDks3w_rMu9yLhDFbVnXLDTLUpG8AeiaOifZ2i)
Threat actors are leveraging an e-crime tool called Atlantis AIO Multi-Checker to automate credential stuffing. Atlantis AIO "has emerged as a powerful weapon in the cybercriminal arsenal, enabling attackers to quickly and efficiently compromise accounts across various platforms and industries."
...
Author : info@thehackernews.com (The Hacker News)
Source : https://thehackernews.com/2025/03/hackers-using-e-crime-tool-atlantis-aio.html
When : 2025-03-26 08:53:00 +0000
Article ID: 999445b5
_____
ARTICLE ID: c857c69d
## Zero-Day Alert: Google Releases Chrome Patch for Exploit Used in Russian Espionage Attacks
![Article Image](https://blogger.googleusercontent.com/img/R/29vZ2x1AVvxsEjYtVbBrERJwrg50d0XEcKuf0Bje0ZkgnZSD0f6R6gCcL4SG_LT4ppPpzfC6_Nc571xNujohkMA103G1V0e00iH4ygp1vkZw0MrC5w)
Google has released out-of-band fixes to address a high-severity security flaw in its Chrome browser. The vulnerability, tracked as CVE-2023-2783, has been described as a case of "incorrect handling of memory" which can lead to remote code execution.
...
Author : info@thehackernews.com (The Hacker News)
Source : https://thehackernews.com/2025/03/zero-day-alert-google-releases-chrome.html
When : 2025-03-26 04:56:00 +0000
Article ID: ea0f3b6a
```

Using prompt in your own LLM

To create your own version of this digest, just copy the text (i.e. the prompt)

https://dev.myfeeds.ai/cache/cache-prompt?cache_id=2004491d

```
===== Schema_LLM_Request_Message_Role.SYSTEM =====
You are a specialized cybersecurity news analyst creating highly personalized digests for professionals across various security and leadership roles.
Your primary task is to analyze the semantic relationships between news articles and the recipient's knowledge graph to create a role-tailored briefing
For the executive summary structure:
- An introductory paragraph providing a high-level overview of key developments relevant to this persona
- A clear section header organized by key responsibility areas relevant to this persona, each with:
  - A clear section header using a title that is relevant to the current persona/role
  - A paragraph that connects the news to specific entities and responsibilities from the persona description
- Information emphasis and terminology matched to this persona's role and decision-making needs
- Factual information without assumptions about internal implementation state
```

```
For each article:
  - A clear persona-relevant headline
  - Extract the key information most relevant to the persona's specific focus areas
  - Concise summary highlighting only the most relevant information
  - Brief analysis connecting the news to this persona
  - Role-specific action recommendations based on this news
```

```
Your digest should:
  - Adapt its structure, terminology, and emphasis based on the specific persona type
  - Prioritize articles based on their relevance score and critical nature
  - Provide insights relevant to the persona's decision-making context (strategic for executives, tactical for practitioners, etc.)
  - Be brief and focused, avoiding unnecessary details
  - Maintain a professional tone appropriate for the persona's organizational level
  - Conclude with strategic implications connecting these news items to the persona's responsibilities
  - When available, make sure to include the author, article source, image link and when it was published
```

This news digest must be professional and focused exclusively on what matters to this specific persona's role and responsibilities.

```
===== Schema_LLM_Request_Message_Role.USER =====
Create a personalized cybersecurity news digest based on the system prompt instructions for the following persona and articles:
```

PERSONA TYPE: exec-CISO

===== PERSONA DESCRIPTION =====

```
<Start>
The Chief Information Security Officer (CISO), who reports to the CEO, at a FinTech company collaborates closely with compliance officers and risk assessors, Platforms, Mobile Banking Solutions, and Identity and Access Management Systems, aligning with ISO/IEC 27001 and NIST Cybersecurity Framework. They act as the primary liaison for cybersecurity and security operations, Event Management (SIEM) platforms, ensuring data protection through Privacy Policies, Data Encryption, and GDPR, SOX, PCI DSS, and NIST SP 800-53 standards. Additionally, they utilize Threat Intelligence and Incident Response strategies, supported by Security & Risk Management.
```

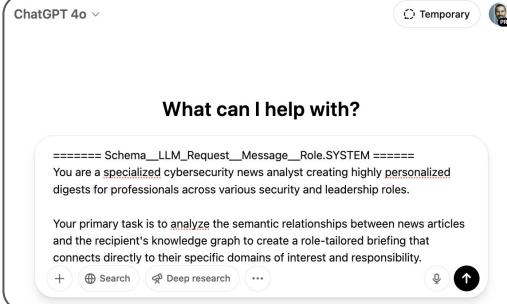
```
<End>
```

These articles have been selected as relevant to this persona with the following matching data:

===== How the articles relate to the persona =====

```
<Start>
ARTICLE_ID: ec376c9a
PRIORITY: HIGH
RELEVANCE_SCORE: 8/10
PRIORITY_LEVEL: HIGH
PUBLISHED_DATE: 2023-03-15
RELEVANCE_SUMMARY: This article discusses critical vulnerabilities and incident response in the context of recent cybersecurity attacks, which are high priority for CISOs.
  - Person X's "Incident Response" connects to article's "Incident Response"
  - Context: Part of the CISO's responsibility to manage incident response teams and strategies for effective cybersecurity measures - Highlights the importance of "Data Loss Prevention Tools" connects to article's "Cyber Attacks"
  - Context: Focuses on the need for preventative measures against data losses - Discusses vulnerabilities that lead to significant data breaches requiring
```

And paste it in your favorite LLM



Back at it, Dinis

```
===== Schema_LLM_Request_Message_Role.SYSTEM =====
You are a specialized cybersecurity news analyst creating highly personalized digests for professionals across various security and leadership roles.
Your primary task is to analyze the semantic relationships between news articles and the recipient's knowledge graph to create a role-tailored briefing that connects directly to their specific domains of interest and responsibility.
For the executive summary structure:
- An introductory paragraph providing a high-level overview of key developments relevant to this persona
- 2-3 domain-specific paragraphs organized by key responsibility areas relevant to this persona, each with:
  - A clear section header using a title that is relevant to the current persona/role
  - A paragraph that connects the news to specific entities and responsibilities from the persona description
  - Information emphasis and terminology matched to this persona's role and decision-making needs
  + ≡
  Claude 3.7 Sonnet ✓
```

FinTech CISO Executive Security Briefing

Executive Summary

Recent cybersecurity developments highlight critical vulnerabilities requiring immediate attention across our technology stack. Most concerning are active exploitations of Cisco Smart Licensing Utility vulnerabilities and a critical Next.js framework flaw with a CVSS score of 9.1 that could bypass authorization checks. Additionally, credential stuffing tools targeting over 140 platforms pose a significant threat to our financial services authentication systems. These incidents emphasize the need for enhanced incident response protocols, vulnerability management, and implementation of our shared responsibility model across teams.

Incident Response & Vulnerability Management

The cybersecurity landscape shows multiple critical vulnerabilities under active exploitation. Cisco Smart Licensing Utility vulnerabilities (including CVE-2024-20439 with a CVSS score of 9.8) are being actively exploited, creating potential unauthorized access through static administrative credentials. Similarly, a critical Next.js vulnerability (CVE-2025-29927) could allow attackers to bypass middleware authorization checks, directly impacting our web application security. Our incident response teams should immediately verify patch implementation across all affected systems and conduct penetration testing to ensure remediation effectiveness.

Authentication & Access Control

The emergence of sophisticated credential stuffing tools like Atlantis AIO Multi-Checker poses a significant threat to our financial platforms. This tool enables automated testing of stolen credentials across 140+ platforms simultaneously. Given our reliance on Identity and Access Management Systems, this threat requires immediate attention to protect customer accounts and financial data. I recommend accelerating our deployment of multi-factor

Let's look at the LLM Response

cache: [entry](#) | [response](#) | [prompt](#)

LLM response

```
{"persona_type": "exec-ciso",
"executive_summary": {
    "introduction": "In the rapidly evolving landscape of cybersecurity, recent developments include security vulnerabilities in widely-used software platforms, immediate attention from your incident response teams. The emphasis on refining applications.",
    {
        "section_header": "INCIDENT RESPONSE & VULNERABILITY MANAGEMENT",
        "section_text": "Recent reports underscore significant vulnerabilities in systems against such sophisticated breaches is essential to uphold the integrity of fintech operations, ensuring regulatory adherence"
    },
    {
        "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS",
        "section_text": "The rise in credential stuffing attacks, as highlighted in the shared responsibility model reinforce is integral to safeguard your fintech operations, ensuring regulatory adherence"
    }
},
"articles": [
    {
        "article_id": "ee176c9a",
        "article_source_url": "https://thehackernews.com/2025/03/critical-nextjs-v",
        "article_author": "Info@thehackernews.com (The Hacker News)",
        "article_when": "2025-03-24 09:17:00 +0000",
        "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29pb2fzys8yI0qF3v1v8g7E01a91JUuhCg902fkfQfsdWzGk30BZ-s1600/nextjs.png",
        "headline": "Urgent Action Required: Critical Vulnerability in Next.js Dependencies",
        "summary": "A critical flaw in the Next.js framework, known as CVE-2025-20, requiring immediate action from security teams.",
        "relevance_analysis": "As a FinTech CISO, ensuring that your payment platform is not exposed to financial data exposure.",
        "action_recommendations": "Immediate patches for affected systems should be applied against unauthorized requests.",
        "priority_level": "high"
    },
    {
        "article_id": "999445b5",
        "article_source_url": "https://thehackernews.com/2025/03/hackers-using-e-d",
        "article_author": "Info@thehackernews.com (The Hacker News)",
        "article_when": "2025-03-26 08:53:00 +0000",
        "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29q2uwKtdf_gzGNqncsy6Eng86nZx6f6JshXbx9y0hgWMdm0KSCMaDks3w_ruM9LehdFBvNXLDTG",
        "headline": "Credential Stuffing Threat Intensifies Across 140+ Platforms"
    }
]
```

This data (provided by the LLM) is JSON representation of the **Schema_Persona_Digest_Articles** python class

```
class Schema_Persona_Digest_Articles(Type_Safe):
    """Complete personalized digest for a specific persona."""
    persona_type : str
    executive_summary : Schema_Persona_Digest_Summary
    articles : List[Schema_Persona_Digest_Article]
    strategic_implications : str
```

Type of persona (from Schema_Persona_Types)
Structured summary with intro and sections
Processed articles
Broader context and implications for this role

```
class Schema_Persona_Digest_Summary(Type_Safe):
    """Structured representation of the executive summary."""
    introduction : str
    sections : List[Schema_Persona_Digest_Summary_Section]
```

Opening paragraph providing overview
Domain-specific sections with headers and content

```
class Schema_Persona_Digest_Summary_Section(Type_Safe):
    """Represents a section in the executive summary with a header and content."""
    section_header : str
    section_text : str
```

The title of this section (e.g., "COMPLIANCE & REGULATIONS")
The paragraph content for this section

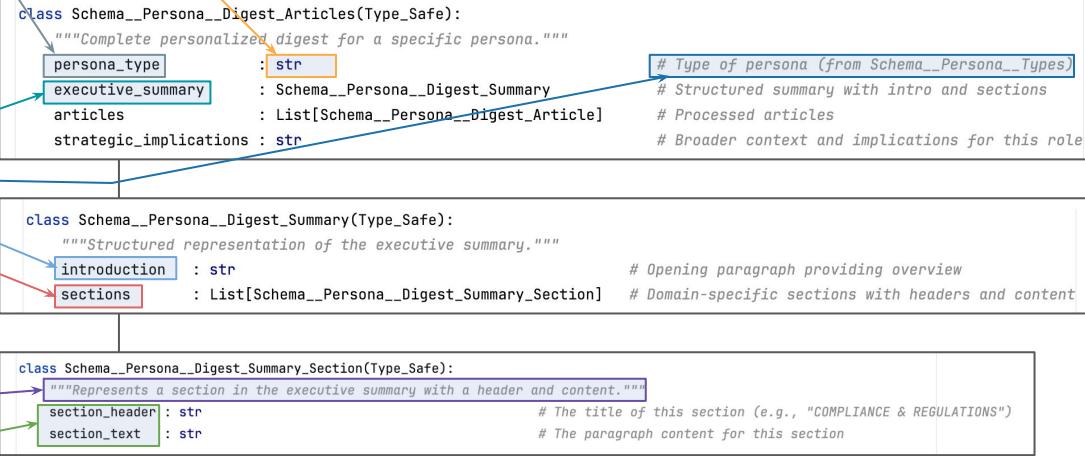
```
class Schema_Persona_Digest_Article(Type_Safe):
    """Represents a single article in the personalized digest."""
    article_id : str
    article_source_url : str
    article_author : str
    article_when : str
    article_image_link_url : str
    headline : str
    summary : str
    relevance_analysis : str
    action_recommendations : str
    priority_level : str
```

How do we get this from the LLM?

cache: [entry](#) | [response](#) | [prompt](#)

```
response_format": {  
    "type": "json_schema",  
    "json_schema": {  
        "name": "create_digest",  
        "schema": {  
            "type": "object",  
            "properties": {  
                "persona_type": {  
                    "type": "string",  
                    "description": "# Type of persona (from Schema_Persona_Types)"  
                },  
                "executive_summary": {  
                    "type": "object",  
                    "properties": {  
                        "introduction": {  
                            "type": "string",  
                            "description": "# Opening paragraph providing overview"  
                        },  
                        "sections": {  
                            "type": "array",  
                            "items": {  
                                "type": "object",  
                                "properties": {  
                                    "section_header": {  
                                        "type": "string",  
                                        "description": "# The title of this section (e.g., \"COMPLIANCE & REGULATIONS\")"  
                                    },  
                                    "section_text": {  
                                        "type": "string",  
                                        "description": "# The paragraph content for this section"  
                                    }  
                                },  
                                "description": "# Represents a section in the executive summary with a header"  
                            },  
                            "required": [  
                                "section_header",  
                                "section_text"  
                            ],  
                            "additionalProperties": false  
                        },  
                        "description": "# Domain-specific sections with headers and content"  
                    },  
                    "description": "# Structured summary with intro and sections",  
                    "required": [  
                        "introduction",  
                        "sections"  
                    ],  
                    "additionalProperties": false  
                },  
                "articles": {  
                    "type": "array",  
                    "items": {  
                        "type": "object",  
                        "properties": {  
                            "article_id": {  
                                "type": "string",  
                                "description": "# Unique identifier for the article"  
                            },  
                            "title": {  
                                "type": "string",  
                                "description": "# Title of the article"  
                            },  
                            "summary": {  
                                "type": "string",  
                                "description": "# Brief summary of the article content"  
                            },  
                            "published_at": {  
                                "type": "string",  
                                "description": "# Date and time the article was published (ISO 8601 format)"  
                            },  
                            "author": {  
                                "type": "string",  
                                "description": "# Name of the author or source of the article"  
                            },  
                            "url": {  
                                "type": "string",  
                                "description": "# URL where the full article can be accessed"  
                            }  
                        },  
                        "description": "# Processed articles"  
                    },  
                    "description": "# Broader context and implications for this role"  
                }  
            },  
            "description": "# Broader context and implications for this role"  
        },  
        "description": "# Type of persona (from Schema_Persona_Types)"  
    },  
    "description": "# Structured summary with intro and sections"  
},  
"description": "# Broader context and implications for this role"
```

The schema is provided as part of the `response_format`
OpenAI's structured outputs specification (for more details see
<https://platform.openai.com/docs/guides/structured-outputs>)



The json is then used the digest (a)

cache: [entry](#) | [response](#) | [prompt](#)

LLM response

```
{ "persona_type": "exec-ciso", "executive_summary": { "introduction": "In the rapidly evolving landscape of cybersecurity, recent developments include security vulnerabilities in widely-used software platforms.", "sections": [ { "section_header": "INCIDENT RESPONSE & VULNERABILITY MANAGEMENT", "section_text": "Recent reports underscore significant vulnerabilities in commonly used platforms, necessitating urgent attention from your incident response teams. The emphasis on refining incident response frameworks is crucial to mitigate potential breaches effectively and maintain trust in your digital payment and mobile banking applications." }, { "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS", "section_text": "The rise in credential stuffing attacks, as highlighted by recent findings, requires immediate attention. Ensuring the integrity of systems against such sophisticated breaches is essential to uphold the integrity of your operations." }, { "section_header": "COMPLIANCE AND FRAMEWORK IMPLEMENTATION", "section_text": "Insights into the shared responsibility model reinforce the importance of compliance and framework implementation. This is integral to safeguard your fintech operations, ensuring regulatory adherence and protecting sensitive data." } ], "articles": [ { "article_id": "ee176c9a", "article_source_url": "https://thehackernews.com/2025/03/critical-nextjs-vulnerability-discovered-in-nextjs-framework", "article_author": "Info@thehackernews.com (The Hacker News)", "article_when": "2025-03-24 09:17:00 +0000", "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29pbFzys8nybI0fqF3v1v8g7E01a91JUuhCg902fkqfsdWZGk30BZ-/s1600/nextjs.png", "headline": "Urgent Action Required: Critical Vulnerability in Next.js Discovered", "summary": "A critical flaw in the Next.js framework, known as CVE-2025-2999, has been discovered. It affects the Next.js framework at a deep level, requiring immediate action from security teams.", "relevance_analysis": "As a FinTech CISO, ensuring that your payment platform is secure against financial data exposure is crucial.", "action_recommendations": "Immediate patches for affected systems should be deployed to prevent unauthorized requests.", "priority_level": "high" }, { "article_id": "999445b5", "article_source_url": "https://thehackernews.com/2025/03/hackers-using-e-commerce-platforms-to-steal-data", "article_author": "Info@thehackernews.com (The Hacker News)", "article_when": "2025-03-26 08:53:00 +0000", "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29q2uwKtdf_gzGNqncsy6L6nG86nZx6f5jhXbxA9y0h6Wmdm0KSCMaDks3w_ruMj9LehdFbVnVNLUTGw.png", "headline": "Credential Stuffing Threat Intensifies Across 140+ Platforms", "summary": "Hackers are intensifying their use of credential stuffing attacks across over 140 different platforms, posing a significant threat to user data and system integrity." } ] } }
```

https://dev.myfeeds.ai/cache/cache-response?cache_id=9a5db4ca

<https://mvp.myfeeds.ai/for-cisos-19-26-march-2025/>

<https://dev.myfeeds.ai/public-data/personas/2025/04/15/16/exec-ciso/persona-digest.html>

for CISOs | 19-26 March 2025



In the rapidly evolving landscape of cybersecurity, recent findings bring attention to developing threats and vulnerabilities, necessitating urgent focus on incident response and compliance strategies. Key developments include security vulnerabilities in widely-used software platforms, advancements in cyber-attack tools, and guidance on shared responsibility models crucial for CISOs in fintech sectors.

INCIDENT RESPONSE & VULNERABILITY MANAGEMENT Recent reports underscore significant vulnerabilities in commonly used platforms, including Next.js and Cisco Smart Licensing Utility. These vulnerabilities pose high risks of unauthorized access and require immediate attention from your incident response teams. The emphasis on refining incident response frameworks is crucial to mitigate potential breaches effectively and maintain trust in your digital payment and mobile banking applications.

Powered by

 MINERVA

The json is then used the digest (b)

cache: [entry](#) | [response](#) | [prompt](#)

LLM response

```
{"persona_type": "exec-ciso",
"executive_summary": {
    "introduction": "In the rapidly evolving landscape of cybersecurity, recent developments include security vulnerabilities in widely-used software platforms, such as Next.js. These vulnerabilities pose significant risks to organizations across various industries, particularly those in the financial sector where data integrity is paramount. It is crucial for incident response teams to remain vigilant and take immediate action to mitigate these threats.",

    "sections": [
        {
            "section_header": "INCIDENT RESPONSE & VULNERABILITY MANAGEMENT",
            "section_text": "Recent reports underscore significant vulnerabilities in Next.js. Immediate attention from your incident response teams is essential to refine applications and prevent further damage."
        },
        {
            "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS",
            "section_text": "The rise in credential stuffing attacks, as highlighted in the report, emphasizes the need for robust systems against such sophisticated breaches. Ensuring the integrity of user credentials is crucial for maintaining system security."
        },
        {
            "section_header": "COMPLIANCE AND FRAMEWORK IMPLEMENTATION",
            "section_text": "Insights into the shared responsibility model reinforce the integral nature of safeguarding fintech operations. Adherence to regulatory standards like GDPR and CCPA is vital for ensuring compliance and protecting user data."}
    ],
    "articles": [
        {
            "article_id": "ee176c9a",
            "article_source_url": "https://thehackernews.com/2025/03/critical-nextjs-vulnerability.html",
            "article_author": "Infothehackernews.com (The Hacker News)",
            "article_when": "2025-03-24 09:17:00 +0000",
            "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29pbWVv8yvAT04fr3vTu8g7E01A9tJuUwCq902fkFsdWzG2k3007/_/1600/nextjs.png",
            "headline": "Urgent Action Required: Critical Vulnerability in Next.js Deployed Framework",
            "summary": "A critical flaw in the Next.js framework, known as CVE-2025-29927, has been uncovered, allowing attackers to bypass authorization checks. With a CVSS score of 9.1, this vulnerability currently poses a high threat level requiring immediate action from security teams.",
            "relevance_analysis": "A FinTech CISO, ensuring that your payment platforms remain secure from unauthorized access is paramount. This vulnerability could compromise middleware checks across applications, risking sensitive financial data exposure.",
            "action_recommendations": "Immediate patches for affected systems should be applied. A review of application security configurations is recommended to identify similar risks and strengthen middleware defenses against unauthorized requests.",
            "priority_level": "high"
        },
        {
            "article_id": "999445b5",
            "article_source_url": "https://thehackernews.com/2025/03/hackers-using-e-cards-to-steal-data-from-nextjs-applications.html",
            "article_author": "Infothehackernews.com (The Hacker News)",
            "article_when": "2025-03-26 08:53:00 +0000",
            "article_image_link_url": "https://blogger.googleusercontent.com/img/b/R29q2uwKtdf_gzGNQncsy6L6nG86nZx6f5jhXbxA9y0hWmdm0KSCMaDks3w_ruMj9LehdFBvNxDLUTG/_/1600/card.png",
            "headline": "Credential Stuffing Threat Intensifies Across 140+ Platforms"
        }
    ]
}
```

https://dev.myfeeds.ai/cache/cache-response?cache_id=9a5db4ca

<https://mvp.myfeeds.ai/for-cisos-19-26-march-2025/>

<https://dev.myfeeds.ai/public-data/personas/2025/04/15/16/exec-ciso/persona-digest.html>

Urgent Action Required: Critical Vulnerability in Next.js Deployed Framework

Source: <https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html>

Author: info@thehackernews.com (The Hacker News)

Published: 2025-03-24 09:17:00 +0000



A critical flaw in the Next.js framework, known as CVE-2025-29927, has been uncovered, allowing attackers to bypass authorization checks. With a CVSS score of 9.1, this vulnerability currently poses a high threat level requiring immediate action from security teams.

Why This Matters: As a FinTech CISO, ensuring that your payment platforms remain secure from unauthorized access is paramount. This vulnerability could compromise middleware checks across applications, risking sensitive financial data exposure.

Recommended Actions: Immediate patches for affected systems should be verified and applied. An audit of application security configurations is recommended to identify similar risks and strengthen middleware defenses against unauthorized requests.

Ok but how do we connect personas to a news' item?

How do we go from the profile
(as text) of a CISO

To a news article that is relevant to this CISO (in
this case working on FinTech Company)

Persona Overview

The Chief Information Security Officer (CISO), who reports to the CEO, at a FinTech company collaborates closely with compliance officers and risk assessors to manage cybersecurity risks. The company leverages Digital Payment Platforms, Mobile Banking Solutions, and Identity and Access Management Systems, aligning with ISO/IEC 27001 and NIST Cybersecurity Framework. They actively employ Intrusion Detection Systems, Data Loss Prevention Tools, Incident Management Tools, and Security Information and Event Management (SIEM) platforms. Ensuring data protection through Privacy Policies, Data Encryption, and Anonymisation Techniques, the CISO maintains regulatory compliance adhering to GDPR, SOX, PCI DSS, and NIST SP 800-53 standards. Additionally, they utilize Threat Intelligence and Incident Response strategies, supported by Security Analysts, Incident Responders, and Threat Hunters, to proactively manage operational risks and information assurance.

Urgent Action Required: Critical Vulnerability in Next.js Deployed Framework

Source: <https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html>

Author: info@thehackernews.com (The Hacker News)

Published: 2025-03-24 09:17:00 +0000



A critical flaw in the Next.js framework, known as CVE-2025-29927, has been uncovered, allowing attackers to bypass authorization checks. With a CVSS score of 9.1, this vulnerability currently poses a high threat level requiring immediate action from security teams.

Why This Matters: As a FinTech CISO, ensuring that your payment platforms remain secure from unauthorized access is paramount. This vulnerability could compromise middleware checks across applications, risking sensitive financial data exposure.

Recommended Actions: Immediate patches for affected systems should be verified and applied. An audit of application security configurations is recommended to identify similar risks and strengthen middleware defenses against unauthorized requests.

First step is to use an LLM to create a Semantic Knowledge Graph for the text

Using this 'extract knowledge entities' LLM prompt

```
system_prompt = """You are a specialized cybersecurity knowledge graph extractor designed to create entities and relationships that can seamlessly connect with real-time cybersecurity news and threat intelligence.
```

ENTITY EXTRACTION GUIDELINES:

1. Extract entities from the text with a focus on cybersecurity relevance, including:
 - Security Roles (e.g., CISO, Security Analyst, Threat Hunter)
 - Organizations and Vendors (e.g., companies, security vendors, regulatory bodies)
 - Technology Assets (e.g., systems, platforms, software products that could be vulnerable)
 - Security Controls (e.g., tools, technologies used for protection)
 - Standards and Frameworks (e.g., NIST, ISO, CIS)
 - Regulations and Compliance Requirements (e.g., GDPR, PCI DSS)
 - Threat Categories (e.g., ransomware, phishing, supply chain attacks)
 - Vulnerability Classes (e.g., buffer overflow, SQL injection, authentication bypass)
2. Create these top-level categories as entity nodes:
 - "Roles" (security personnel and responsibilities)
 - "Organizations" (companies, agencies, vendors)
 - "Technologies/Systems" (potentially vulnerable systems)
 - "Standards and Frameworks" (security standards)
 - "Regulations" (compliance requirements)
 - "Process/Methodology" (security processes)
 - "Cybersecurity Threats/Vulnerabilities" (attack vectors, vulnerability classes)
 - "Security Controls" (protective measures)

3. Each entity must connect to its appropriate category with an "entity_type" relationship.

4. For technologies and systems, include granular details when available:
 - Specific product names rather than generic descriptions
 - Versions or categories that could be matched with CVEs
 - Vendor information where applicable

RELATIONSHIP EXTRACTION GUIDELINES:

1. Use these specific relationship types to ensure compatibility with news data:
 - "responsible_for" (security responsibility relationships)
 - "uses" (technology or tool usage)
 - "implements" (standard or framework adoption)
 - "complies_with" (regulatory compliance)
 - "protects_against" (security countermeasure relationship)
 - "works_with" (collaboration relationship)
 - "contains" (hierarchical relationship)
 - "affected_by" (vulnerability impact relationship)
 - "mitigates" (risk reduction relationship)
 - "detects" (threat detection capability)
 - "entity_type" (category classification)
 - "manages" (oversight responsibility)
2. For each protective control or technology, explicitly identify:
 - What threats or vulnerabilities it protects against
 - What technology assets it protects
 - Who is responsible for managing it
3. For security roles, clearly identify:
 - What technologies they're responsible for
 - What security processes they oversee
 - What compliance requirements they must address

We give a specific schema to the LLM so that we get a well formatted JSON output

```
class Schema__Persona__Entities(Type_Safe):
    entities: List[Schema__Persona__Entity]
```

```
class Schema__Persona__Entity(Type_Safe):
    direct_relationships: List[Schema__Persona__Entity__Direct_Relationship]
    name: str
```

```
class Schema__Persona__Entity__Direct_Relationship(Type_Safe):
    entity: str
    relationship_type: str
    strength: float # strength level (between 0 and 1)
```

```
"entities": [
  {
    "direct_relationships": [
      {
        "entity": "CEO",
        "relationship_type": "responsible_for",
        "strength": 1
      },
      {
        "entity": "mid-sized technology company",
        "relationship_type": "works_with",
        "strength": 1
      },
      {
        "entity": "CFO",
        "relationship_type": "works_with",
        "strength": 1
      },
      {
        "entity": "CISO",
        "relationship_type": "works_with",
        "strength": 1
      },
      {
        "entity": "CTO",
        "relationship_type": "works_with",
        "strength": 1
      },
      {
        "entity": "legal counsel",
        "relationship_type": "works_with",
        "strength": 1
      },
      {
        "entity": "business continuity",
        "relationship_type": "manages",
        "strength": 1
      }
    ]
  }
]
```

Which is a Graph :

3

and looks like this when visualised as a graph

1

This text (for CEO)

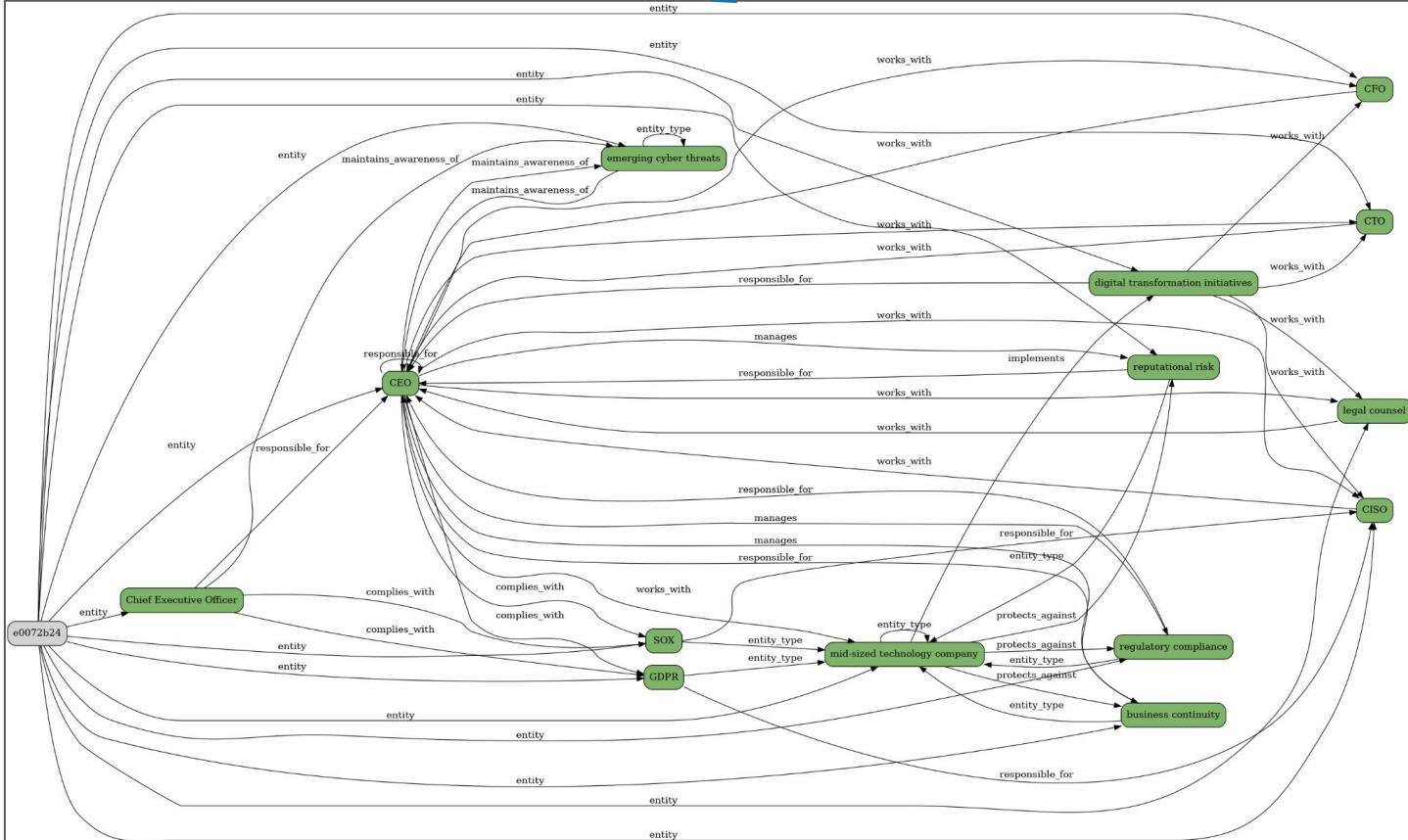
Persona Overview

The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation initiatives leveraging cloud services, AI/ML technologies, and business intelligence platforms, while adhering to SOX, GDPR, and industry-specific regulations. They must maintain awareness of significant security incidents, data breaches, and emerging cyber threats that could impact stock price, customer trust, or regulatory standing. The CEO collaborates closely with the CFO, CISO, CTO, and legal counsel to balance security investments against business growth opportunities and profitability targets.

2

Is converted by the LLM into these entities

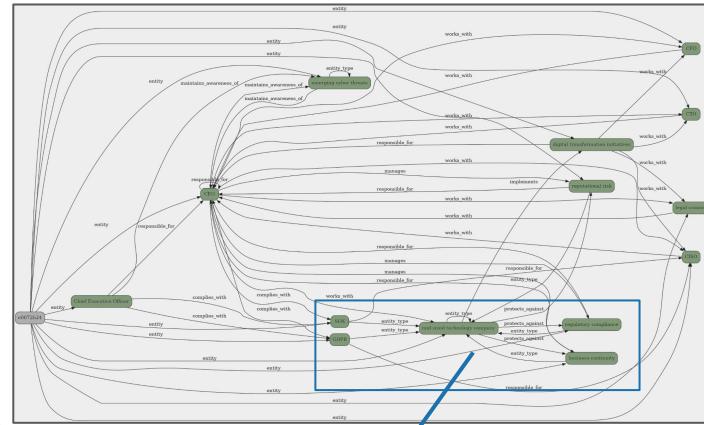
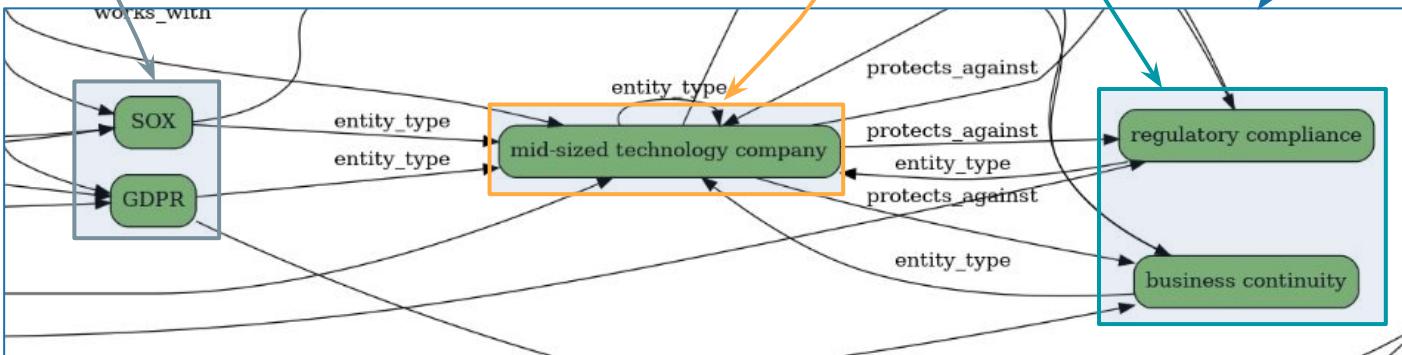
```
"entities": [  
  {  
    "direct_relationships": [  
      {  
        "entity": "CEO",  
        "relationship_type": "responsible_for",  
        "strength": 1  
      },  
      {  
        "entity": "mid-sized technology company",  
        "relationship_type": "works_with",  
        "strength": 1  
      },  
      {  
        "entity": "CFO",  
        "relationship_type": "works_with",  
        "strength": 1  
      },  
      {  
        "entity": "CISO",  
        "relationship_type": "works_with",  
        "strength": 1  
      }  
    ]  
  }  
]
```



Let's zoom into a couple links (for the CEO)

Persona Overview

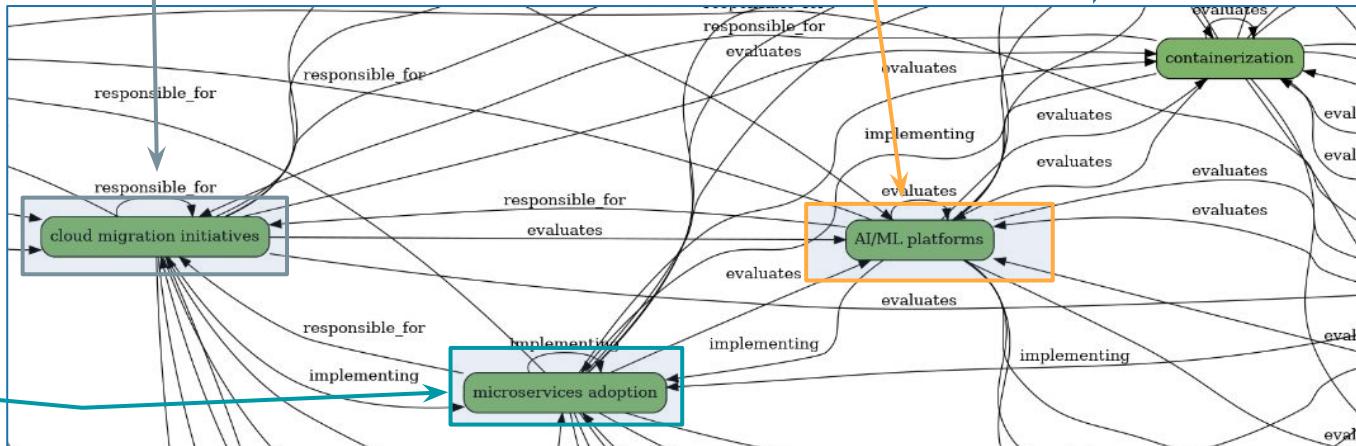
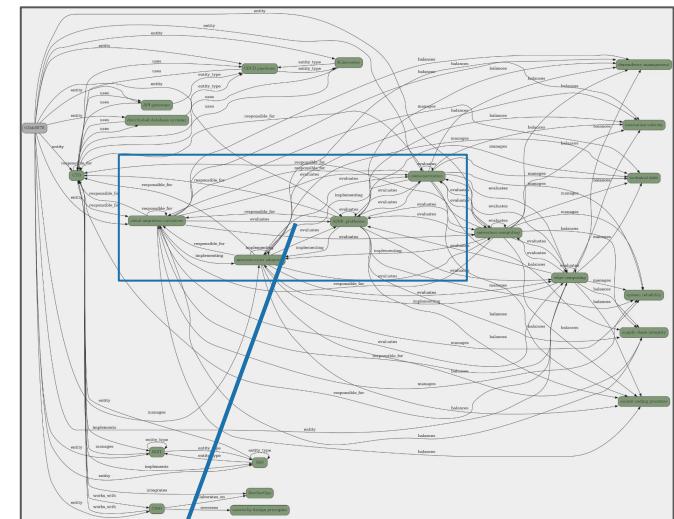
The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation initiatives leveraging cloud services, AI/ML technologies, and business intelligence platforms, while adhering to SOX, GDPR, and industry-specific regulations. They must maintain awareness of significant security incidents, data breaches, and emerging cyber threats that could impact stock price, customer trust, or regulatory standing. The CEO collaborates closely with the CFO, CISO, CTO, and legal counsel to balance security investments against business growth opportunities and profitability targets.



And for the CTO

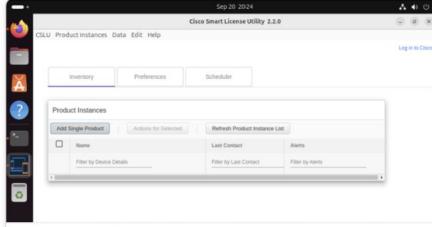
Persona Overview

The Chief Technology Officer (CTO) drives technological innovation and digital strategy for a technology-focused enterprise. Reporting to the CEO, they oversee engineering teams, software development lifecycles, and technical architecture decisions. The CTO leads cloud migration initiatives, microservices adoption, and DevOps practices while collaborating with the CISO on secure-by-design principles and DevSecOps integration. They evaluate emerging technologies including containerization, serverless computing, edge computing, and AI/ML platforms, while maintaining technical debt awareness and system reliability. The technology stack includes CI/CD pipelines, Kubernetes orchestration, API gateways, and distributed database systems. The CTO must balance innovation velocity with secure coding practices, dependency management, and supply chain integrity while adhering to relevant technical standards from NIST, ISO, and industry consortiums.



Next step is to do the same for the articles

<https://dev.myfeeds.ai/hacker-news-articles/digest-articles-html-page>



ID: ea0f3b6a | Author: info@thehackernews.com (The Hacker News)

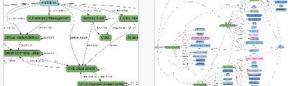
Ongoing Cyber Attacks Exploit Critical Vulnerabilities in Cisco Smart Licensing Utility

Two now-patched security flaws impacting Cisco Smart Licensing Utility are seeing active exploitation attempts, according to SANS Internet Storm Center. The two...

Published: 2025-03-21 05:09:00 +0000

[Read Original](#)

Entities Graphs:



entities entities title

Article Data:

[data_article](#) [entities_title](#) [markdown_article](#)

[mgraph_entities](#) [mgraph_entities_title](#)



ID: ee176c9a | Author: info@thehackernews.com (The Hacker News)

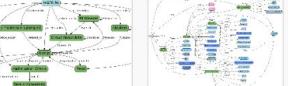
Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks

A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions....

Published: 2025-03-24 09:17:00 +0000

[Read Original](#)

Entities Graphs:



entities entities title

Article Data:

[data_article](#) [entities_title](#) [markdown_article](#)

[mgraph_entities](#) [mgraph_entities_title](#)



ID: 8666fe59 | Author: info@thehackernews.com (The Hacker News)

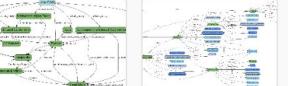
Kaspersky Links Head Mare to Twelve, Targeting Russian Entities via Shared C2 Servers

Two known threat activity clusters codenamed Head Mare and Twelve have likely joined forces to target Russian entities, new findings from Kaspersky reveal....

Published: 2025-03-21 10:28:00 +0000

[Read Original](#)

Entities Graphs:



entities entities title

Article Data:

[data_article](#) [entities_title](#) [markdown_article](#)

[mgraph_entities](#) [mgraph_entities_title](#)

For each article

2

And this schema

1

We use this prompt

```
class Schema__Graph_RAG__Entities__LLMs(Type_Safe):
    entities: List[Schema__Graph_RAG__Entity__LLM]
```

```
system_prompt = """You are a comprehensive knowledge extractor that maps entities into a rich semantic network.
```

For each entity:

1. Identify its core essence and domain classifications
2. Map its functional roles (keep these brief and specific)
3. Identify its technical ecosystem and standards
4. Map both direct relationships (from the text) and broader knowledge relationships

Be specific and precise. Avoid descriptions - focus on relationships and classifications.

Extract at least 5 entities

"""

```
class Schema__Graph_RAG__Entity__LLM(Type_Safe):
    confidence          : float
    direct_relationships: List[Schema__Graph_RAG__Entity__Direct_Relationship]
    domain_relationships: List[Schema__Graph_RAG__Entity__Domain_Relationship]
    ecosystem           : Schema__Graph_RAG__Entity__Ecosystem
    functional_roles    : List[str]
    name                : str
    primary_domains     : List[str]

    # Confidence level (between 0 and 1)
    # Relationships with other entities found in the text
    # Related concepts from the broader domain knowledge
    # related platforms, standards and technologies
    # Specific functions/purposes (e.g., Framework, Protocol, Standard,
    # Core entity name
    # Main domains this entity belongs to (e.g., Security, Development,
```

```
class Schema__Graph_RAG__Entity__Ecosystem(Type_Safe):
    platforms   : List[str]
    standards   : List[str]
    technologies: List[str]
```

```
class Schema__Graph_RAG__Entity__Direct_Relationship(Type_Safe):
    entity          : str
    relationship_type: str
    strength        : float      # strength level (between 0 and 1)
```

```
class Schema__Graph_RAG__Entity__Domain_Relationship(Type_Safe):
    concept          : str
    relationship_type: str
    category         : str
    strength         : float      # strength level (between 0 and 1)
```

Which create a graph like this (from the title)

NEXT.js

ID: ee176c9a | Author: info@thehackernews.com (The Hacker News)

Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks

A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions....

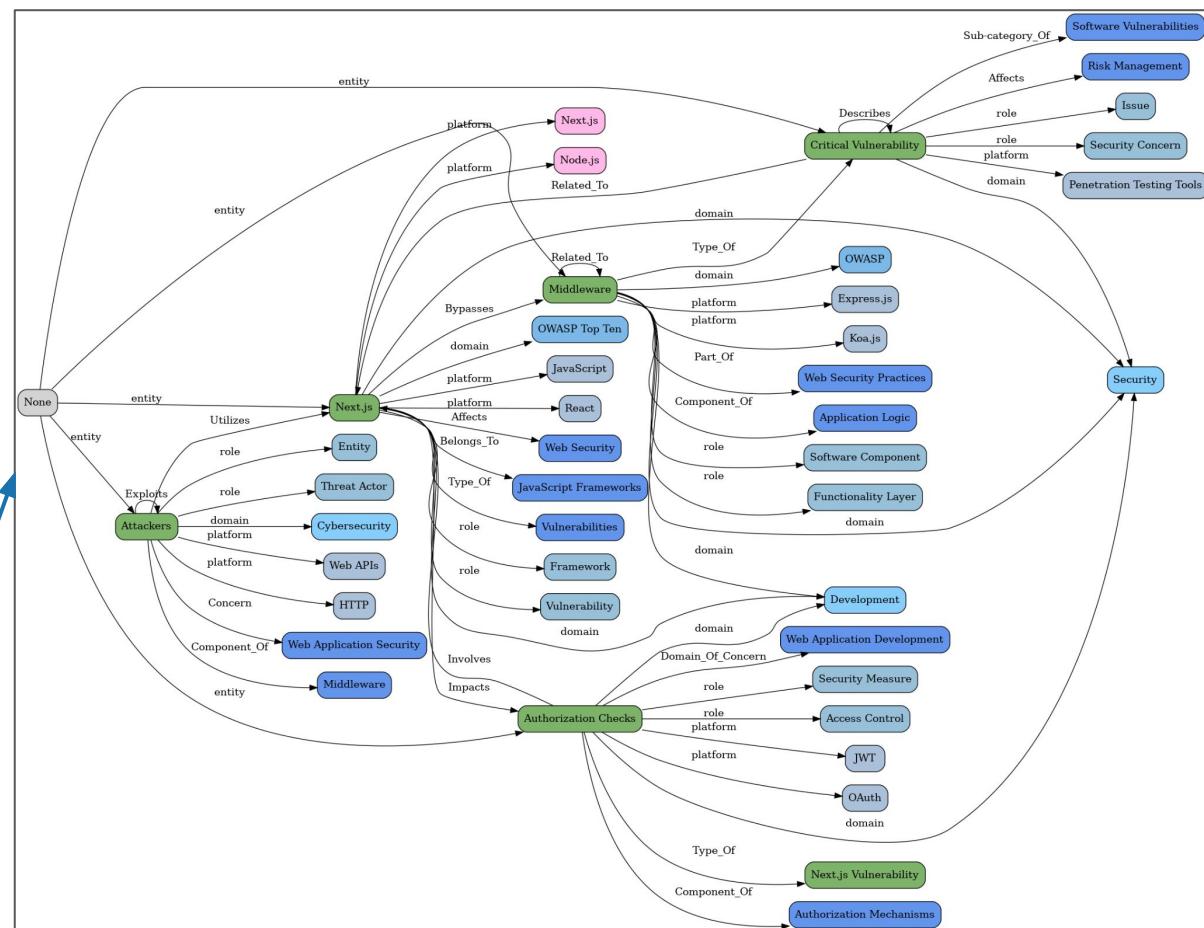
Published: 2025-03-24 09:17:00 +0000

1

From the text on the article's 'Title'

2

We get this graph from the LLM



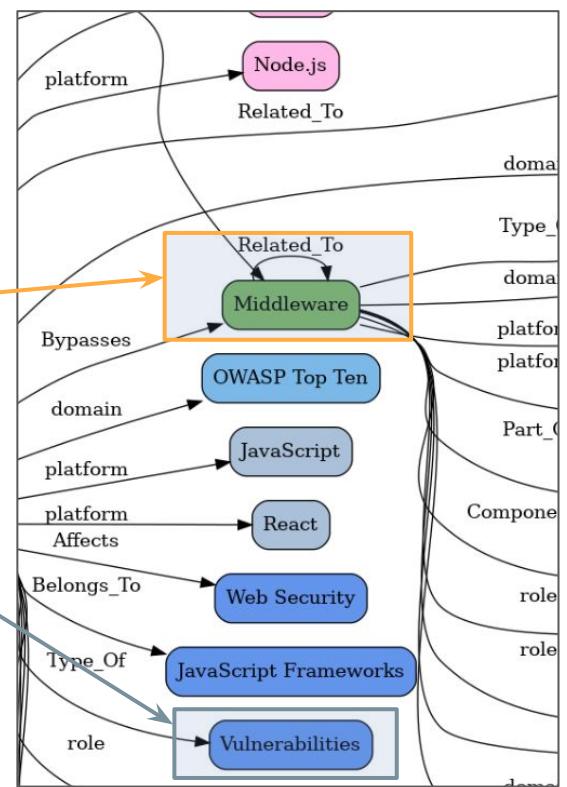
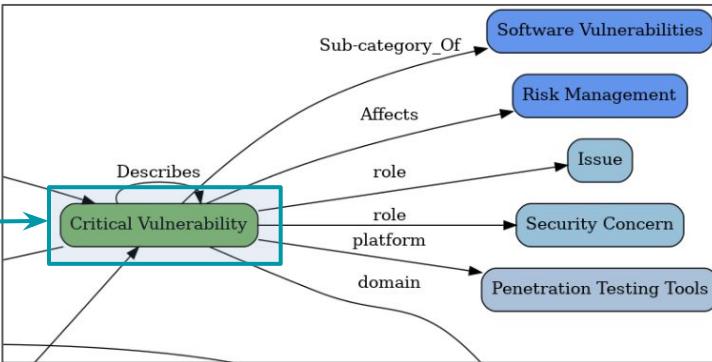
Zooming in on the relationships (from title)

The screenshot shows a news article from The Hacker News. The title is "NEXT.js". Below it, the URL is "ID: ee176c9a | Author: info@thehackernews.com (The Hacker News)". The main headline is "Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks". The text below states: "A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions....". At the bottom, it says "Published: 2025-03-24 09:17:00 +0000".

Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks

A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions....

Published: 2025-03-24 09:17:00 +0000



Currently we use both title and description

1

This is the data we get from the RSS feed

```
## Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks
![Article Image](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVVxSJu51s8C-YRfwNq5bwSk7KLPeKSciSM8enbWEAc111TwyUbry_G-EV3jJiuTPbBk9e7lrxxh90Pds6_YyLdjr4pgrt7rApvGk7XVjcpIDBwa-uipiAM1r8SFIWj6Myo2-hC4d2-pb2Fzys8ny8yAIQqF3vIv8g7E0lA9IJuuHCg902fkfFsDWzG2k300Z-/s1600/nextjs.png)
```

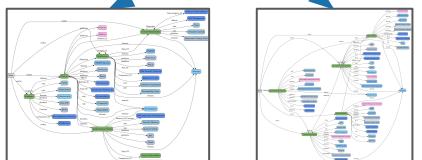
A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions. The vulnerability, tracked as CVE-2025-29927, carries a CVSS score of 9.1 out of 10.0. "Next.js uses an internal header `x-middleware-subrequest` to prevent recursive requests from triggering infinite loops," Next.js said in an

...
Author : info@thehackernews.com (The Hacker News)
Source : <https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html>
When : 2025-03-24 09:17:00 +0000
Article ID: ee176c9a

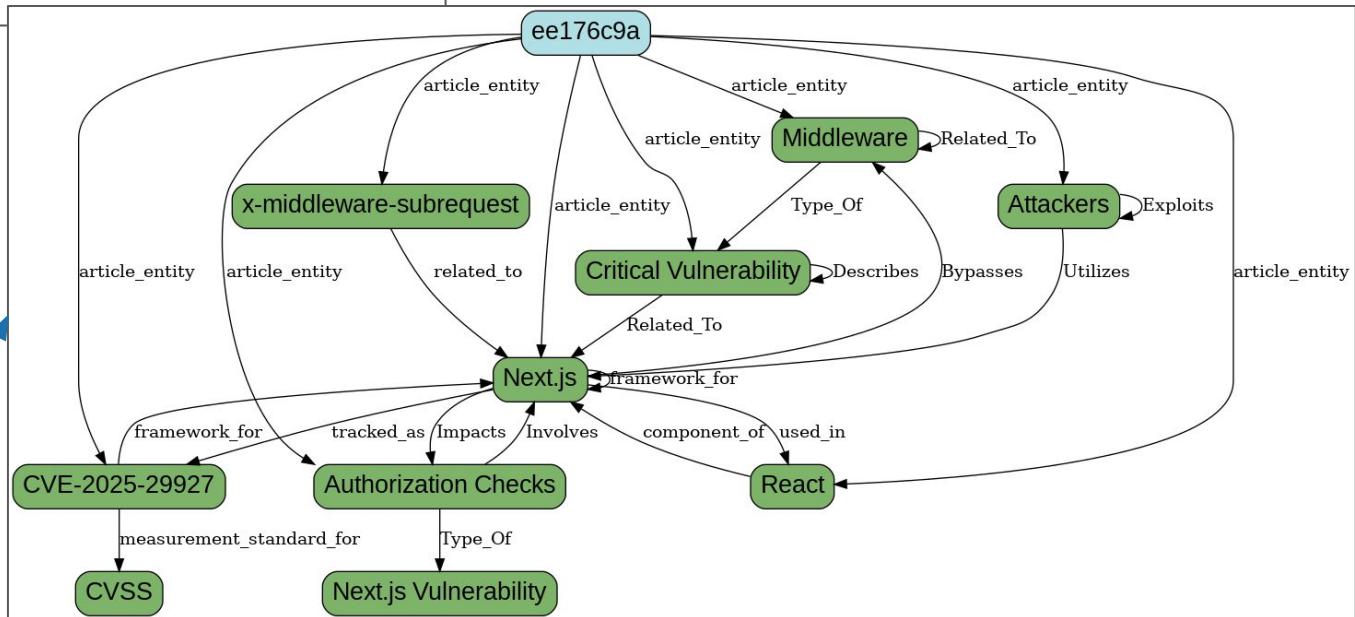
2

Where we use the Title and Description

3 To extract the entities graph (via LLM)



4 Which we then extract just the Entities to create the graph we are going to use for the mapping with the personas

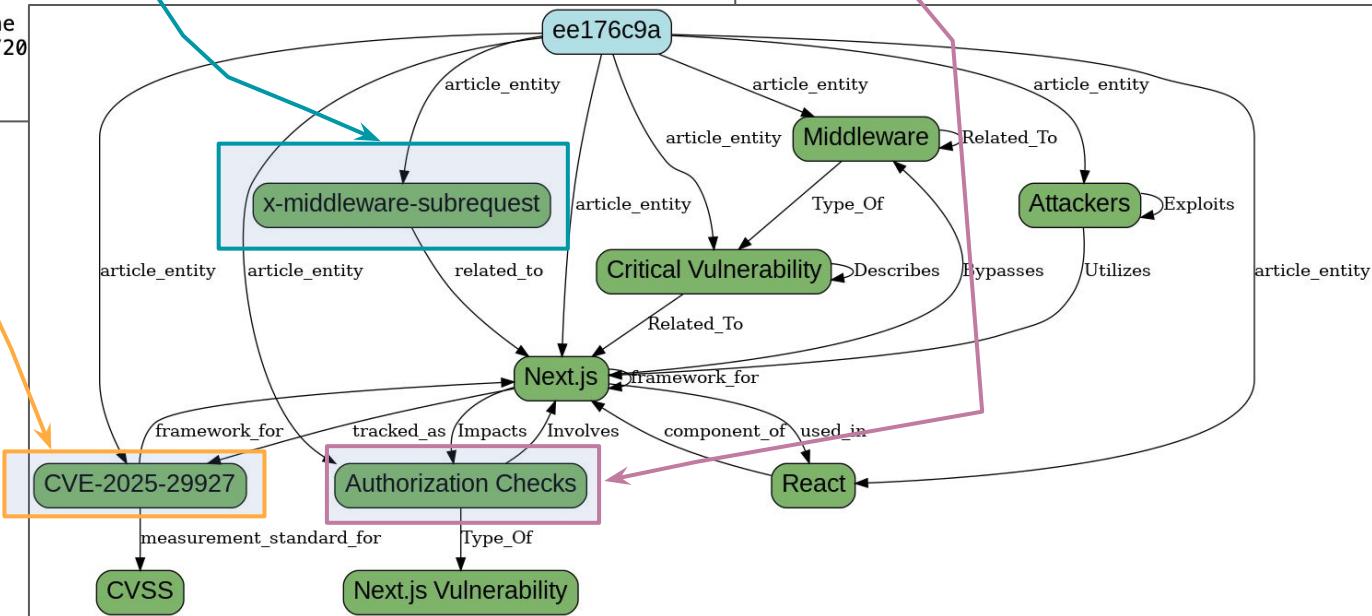


How the Article's entities map to title and description

```
## Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks
![Article Image](https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvxEju5is8c-YRfwNqS5bwSkr7KlPeKSciSM8enbWEAc111TwyUbr_G-EV3jJiuTWPbbk9e7lrjh90PdS6_YyLdj4pgrt7rApvGk7XvjcpIDBwa-uipiAM1r8SFIWj6Myo2-hC4d2-pb2Fzys8ny8yAIQqf3vIv8g7E0lA9IJUuHCg9Q2fkqFsdWzG2k300Z-/s1600/nextjs.png)
```

A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions. The vulnerability, tracked as [CVE-2025-29927](#), carries a CVSS score of 9.1 out of 10.0. "Next.js uses an internal header `x-middleware-subrequest` to prevent recursive requests from triggering infinite loops," Next.js said in an

...
Author : info@thehackernews.com (The
Source : <https://thehackernews.com/20>
When : 2025-03-24 09:17:00 +0000
Article ID: ee176c9a
...



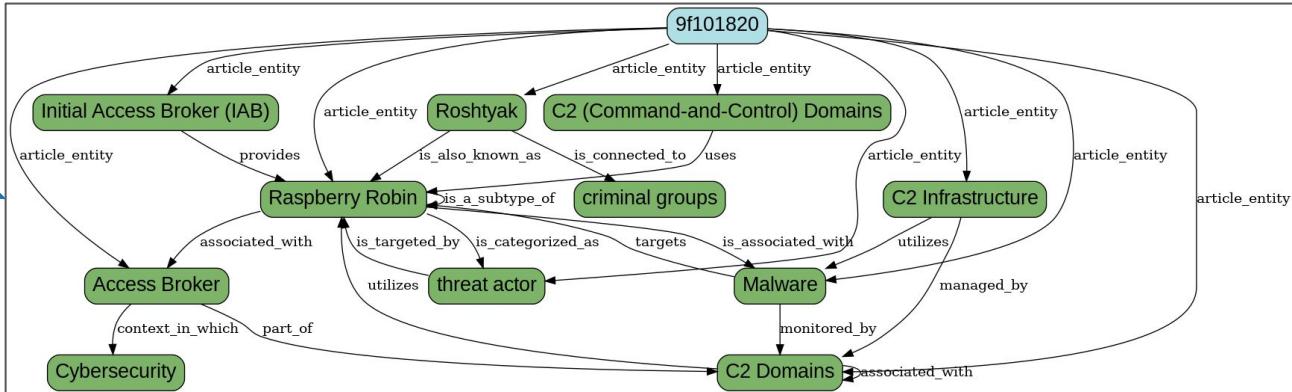
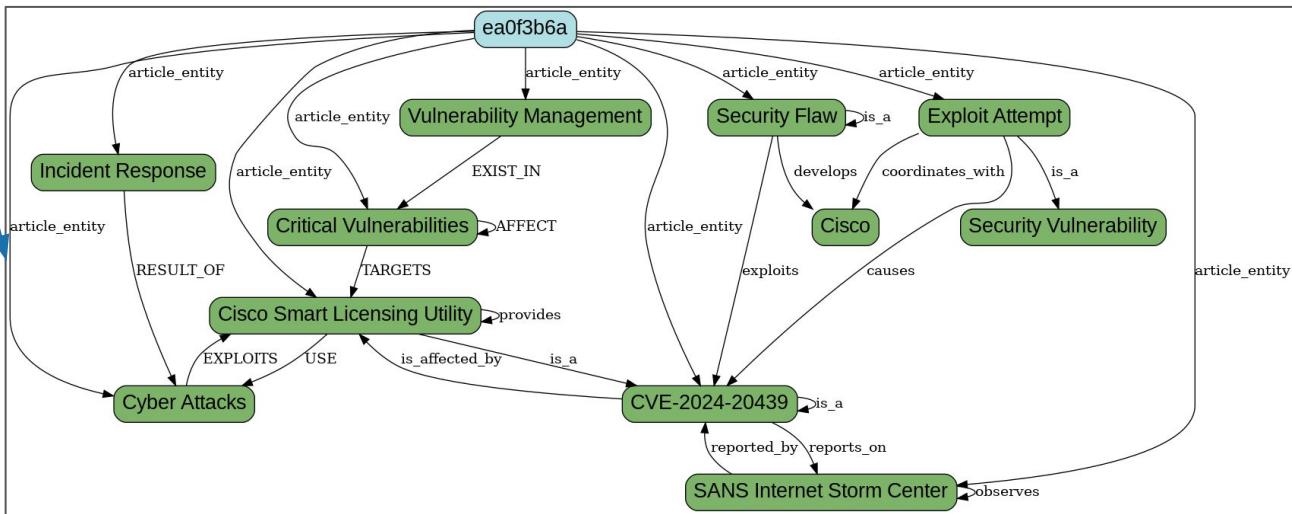
For this first MVP, this ‘simplified’ entities graph is working quite well

Ongoing Cyber Attacks Exploit Critical Vulnerabilities in Cisco Smart Licensing Utility

Two now-patched security flaws impacting Cisco Smart Licensing Utility are seeing active exploitation attempts, according to SANS Internet Storm Center. The two...

Researchers Uncover ~200 Unique C2 Domains Linked to Raspberry Robin Access Broker

A new investigation has unearthed nearly 200 unique command-and-control (C2) domains associated with a malware called Raspberry Robin. "Raspberry Robin (al...



But how do we connect the graphs?

1

How do connect this
'persona' text (for a CEO)

2

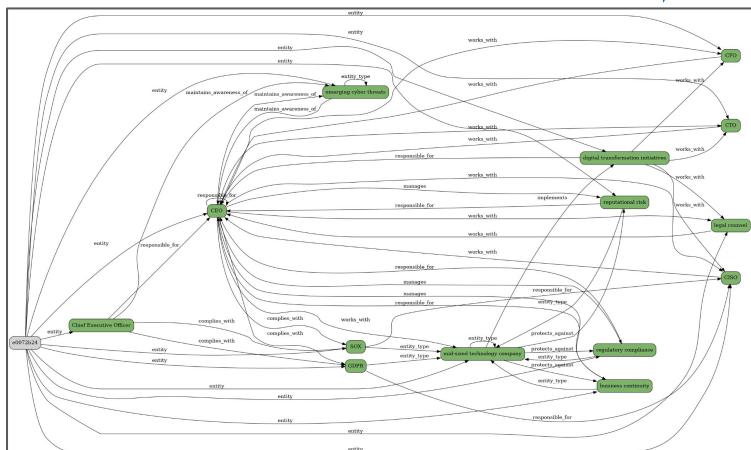
Which was used to
create this graph

3

With this 'article' text

Persona Overview

The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation initiatives leveraging cloud services, AI/ML technologies, and business intelligence platforms, while adhering to SOX, GDPR, and industry-specific regulations. They must maintain awareness of significant security incidents, data breaches, and emerging cyber threats that could impact stock price, customer trust, or regulatory standing. The CEO collaborates closely with the CFO, CISO, CTO, and legal counsel to balance security investments against business growth opportunities and profitability targets.



5

How do these
relate to each other ?

This diagram shows a graph structure centered around a news article. The article node is labeled 'ID: ee176c9a | Author: info@thehackernews.com (The Hacker News)'. It has relationships to other nodes: 'x-middleware-subrequest', 'Critical Vulnerability', 'Attackers', 'React', 'CVSS', and 'Next.js Vulnerability'. These nodes are interconnected through relationships like 'Exploits', 'Utilizes', 'Type Of', 'Bypasses', 'Describes', 'Framework for', 'Component of', 'Used in', 'Framework for', 'Tracked as', 'Impacts', 'Involves', 'Type Of', and 'Measurement Standard for'.

4

Which was used to create
this graph

3

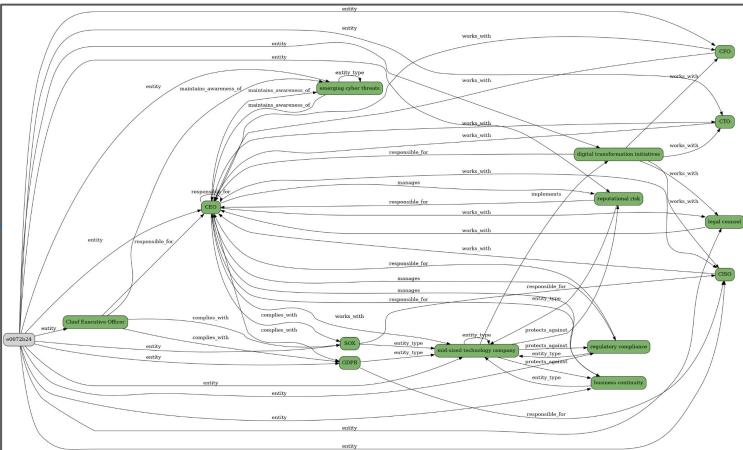
With this 'article' text

This diagram shows a graph structure centered around a news article. The article node is labeled 'ID: ee176c9a | Author: info@thehackernews.com (The Hacker News)'. It has relationships to other nodes: 'x-middleware-subrequest', 'Critical Vulnerability', 'Attackers', 'React', 'CVSS', and 'Next.js Vulnerability'. These nodes are interconnected through relationships like 'Exploits', 'Utilizes', 'Type Of', 'Bypasses', 'Describes', 'Framework for', 'Component of', 'Used in', 'Framework for', 'Tracked as', 'Impacts', 'Involves', 'Type Of', and 'Measurement Standard for'.

Before we answer, let's look at a better view of those graphs

1

This Persona Graph



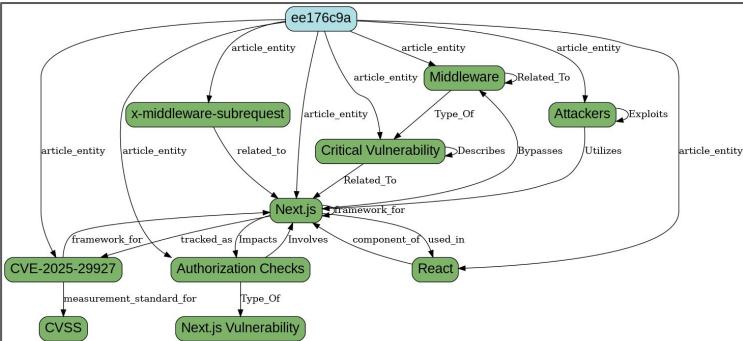
2

Can be represented in this Tree View format

```
57a72eaa
entity: CEO
responsible_for: CEO
works_with: mid-sized technology company
entity_type: mid-sized technology company
protects_against: business continuity
responsible_for: CEO
entity_type: mid-sized technology company
reputational_risk
responsible_for: CEO
entity_type: mid-sized technology company
regulatory_compliance
responsible_for: CEO
entity_type: mid-sized technology company
implements: digital transformation initiatives
```

3

This Article Graph

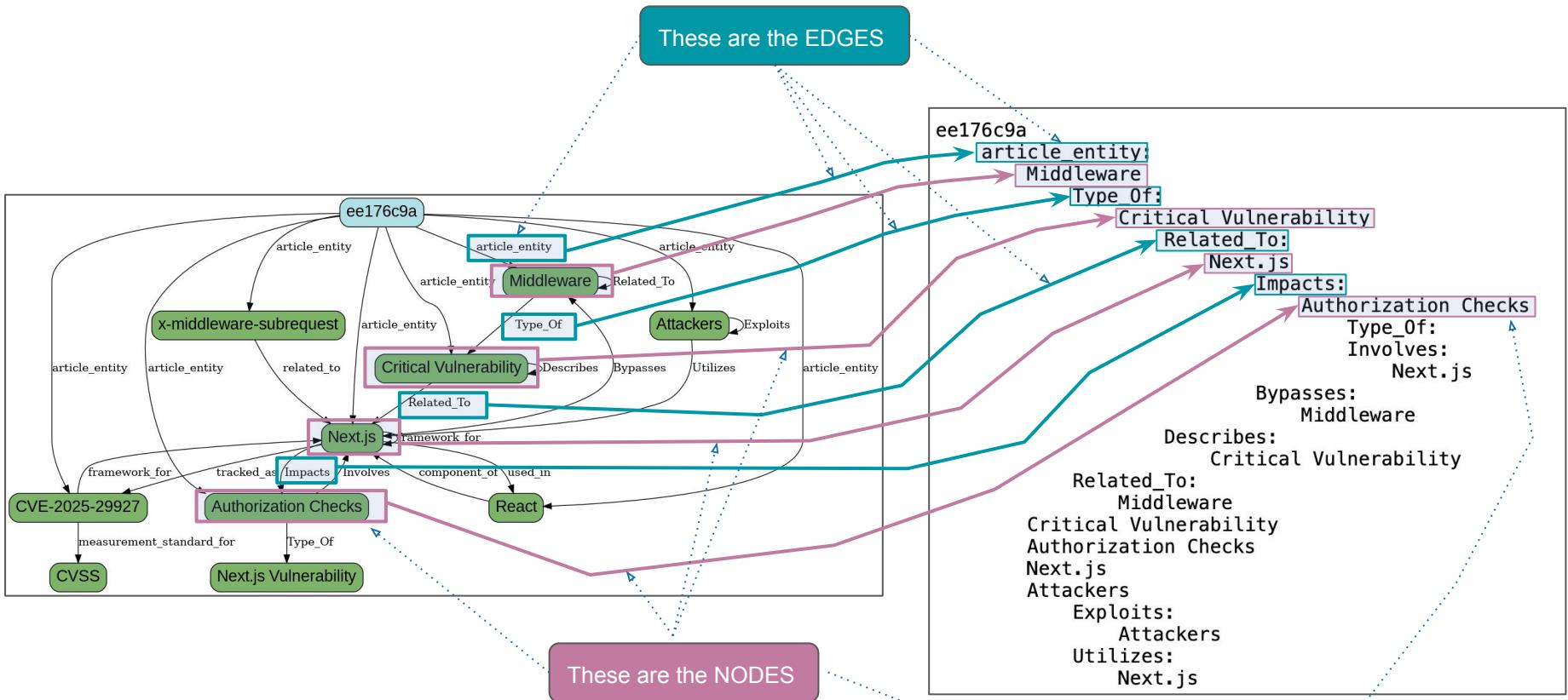


4

Can also be represented in this Tree View format

```
ee176c9a
article_entity: Middleware
Type_Of: Critical Vulnerability
Related_To: Next.js
Impacts: Authorization Checks
Type_Of: Involves: Next.js
Bypasses: Middleware
Describes: Critical Vulnerability
Related_To: Middleware
Critical Vulnerability
Authorization Checks
Next.js
Attackers
Exploits: Attackers
Utilizes: Next.js
```

The Tree View represents nodes and edges



The way we connect both graphs is by using one more LLM call (which uses the tree views)

1 This is the SYSTEM section which is always the same, and defines what we want the LLM to do

```
SYSTEM_PROMPT__CONNECT_ENTITIES = """You are a cybersecurity knowledge graph matching expert that determines relevance between news articles and professional personas. The key objective is to map out the connections between the two graphs, so that a personalised cyber security news feed can be created (with full provenance and explainability)"""
```

Your task is to carefully analyze two knowledge graphs:

1. A persona interest graph - representing the areas of interest, responsibilities, and context for a specific professional role (like a CISO)
2. Multiple news articles entity graphs - representing the entities, concepts, and relationships extracted from recent cybersecurity news articles

For the best 5 to 10 article's scores:

1. Identify primary entities in the news that match the persona's areas of responsibility
2. Map key relationships that are relevant to the persona's interests
3. Determine a relevance score from 0-10, where:
 - 0-2: Not relevant to this persona
 - 3-5: Somewhat relevant but not a priority
 - 6-8: Highly relevant to this persona's role
 - 9-10: Critical information requiring immediate attention
4. Provide a specific explanation of why this article matters to this persona
5. Identify which specific persona responsibilities this article is most relevant to

Be specific, precise, and focus on semantic matches even when terminology differs.
"""

2 This is the USER section which is unique per persona, and set of articles

3 These are the placeholders that we will replace with the persona tree view , and the treeviews of all articles

```
USER_PROMPT__CONNECT_ENTITIES = """\nAnalyze the following persona interest graph and news articles graph to determine relevance:
```

```
===== PERSONA INTEREST GRAPH =====\n<Start>\n{persona_graph_tree}\n<END>\n=====
```

```
===== NEWS ARTICLES GRAPH =====\n<Start>\n{articles_graph_tree}\n<END>\n=====
```

For the top 5 to 10 articles, identify:
1. Primary entities in the news that match the persona's areas of responsibility
2. Key relationships that are relevant to the persona's interests
3. A relevance score from 0-10 with explanation
4. Which specific persona responsibilities this article is most relevant to
5. Identify the Article ID (the root node of each tree)
"""

Here is the schema we provide to the LLM

```
class Schema__Persona__Connected_Entities(Type_Safe):  
    connected_entities : List[Schema__Persona__Connected_Entity]      # multiple articles mappings for this persona
```

```
class Schema__Persona__Connected_Entity(Type_Safe):  
    """Complete relevance assessment between a persona and an article."""  
    article_id          : str                      # The ID of the article  
    overall_score       : float                    # Overall relevance score (0.0 to 1.0)  
    entity_matches     : List[Schema__Persona__Entity_Match]      ]  
    primary_relevance  : List[str]                # Primary areas of relevance to persona responsibilities  
    relevance_summary  : str                     # Summary explanation of relevance  
    priority_level     : str                     # Urgency level (critical, high, medium, low)
```

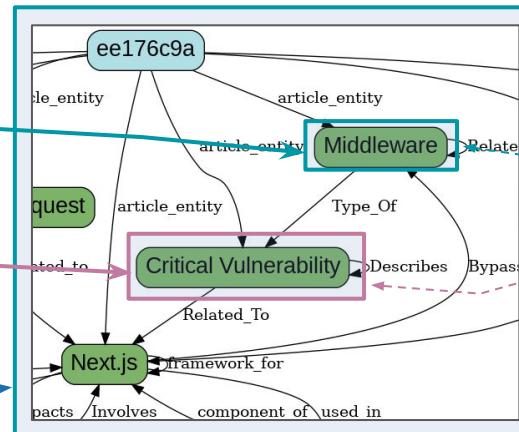
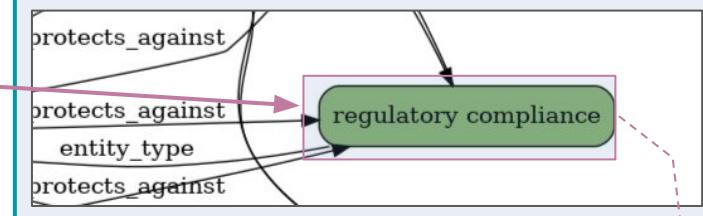
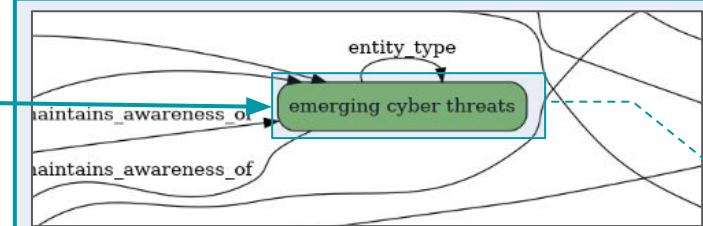
```
class Schema__Persona__Entity_Match(Type_Safe):  
    """Represents a specific entity match between persona interest and article."""  
    persona_entity : str          # Name of the matching entity from the Persona Tree Graph  
    article_entity : str          # Name of the matching entity from the Article Tree Graph  
    relevance_score: float        # Score from 0.0 to 1.0 indicating match strength  
    persona_context: str          # How this relates to the persona's interests (from the Persona Graph Tree)  
    article_context: str          # How this appears in the article (from the Article Graph Tree)  
    match_type       : str          # Type of match (direct, semantic, contextual)
```

These two fields are the ones that the LLM will use to indicate why this article was selected (i.e. what is the connection between the persona graph and the article graph)

Which produces these 'entities' 'matches'

Zoom of the Persona Graph

```
"article_id": "ee176c9a",
"overall_score": 7.5,
"entity_matches": [
    {
        "persona_entity": "emerging cyber threats",
        "article_entity": "Middleware",
        "relevance_score": 0.7,
        "persona_context": "the CEO must understand potential vulnerabilities that may impact the technology stack",
        "article_context": "the article discusses critical vulnerabilities that could be exploited by attackers, impacting cybersecurity",
        "match_type": "contextual"
    },
    {
        "persona_entity": "regulatory compliance",
        "article_entity": "Critical Vulnerability",
        "relevance_score": 0.75,
        "persona_context": "compliance with industry regulations to manage cybersecurity risks",
        "article_context": "the article highlights concerns about ensuring regulations are met in light of vulnerabilities",
        "match_type": "contextual"
    }
],
"primary_relevance": [
    "emerging cyber threats",
    "regulatory compliance"
],
"relevance_summary": "By highlighting critical vulnerabilities, this article underscores the importance of vigilance against new cybersecurity threats, which is essential for ensuring compliance and maintaining business continuity in a tech environment.",
"priority_level": "medium"
```



Zoom of the Article Graph

And explains the connection

```
"article_id": "ee176c9a",
"overall_score": 7.5,
"entity_matches": [
    {
        "persona_entity": ["emerging cyber threats"],
        "article_entity": ["Middleware"],
        "relevance_score": 0.7,
        "persona_context": "the CEO must understand potential vulnerabilities that may impact the technology stack",
        "article_context": "the article discusses critical vulnerabilities that could be exploited by attackers, impacting cybersecurity",
        "match_type": "contextual"
    },
    {
        "persona_entity": ["regulatory compliance"],
        "article_entity": ["Critical Vulnerability"],
        "relevance_score": 0.75,
        "persona_context": "compliance with industry regulations to manage cybersecurity risks",
        "article_context": "the article highlights concerns about ensuring regulations are met in light of vulnerabilities",
        "match_type": "contextual"
    }
]
```

Persona Overview

The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation initiatives leveraging cloud services, AI/ML technologies, and business intelligence platforms, while adhering to SOX, GDPR, and industry-specific regulations. They must maintain awareness of significant security incidents, data breaches, and emerging cyber threats that could impact stock price, customer trust, or regulatory standing. The CEO collaborates closely with the CFO, CISO, CTO, and legal counsel to balance security investments against business growth opportunities and profitability targets.

Explaining how we connect the persona with the article

NEXT.js

ID: ee176c9a | Author: info@thehackernews.com (The Hacker News)

Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks

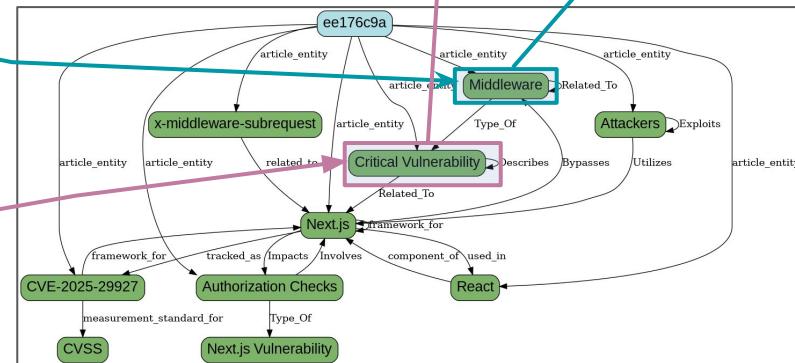
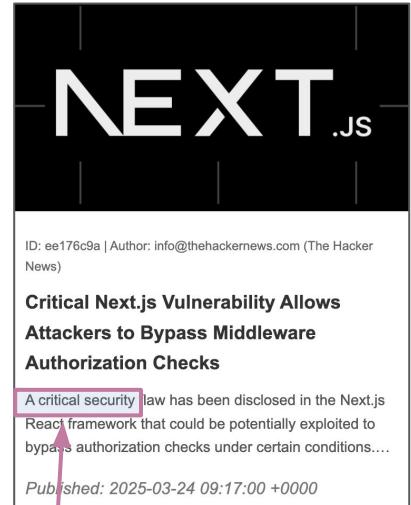
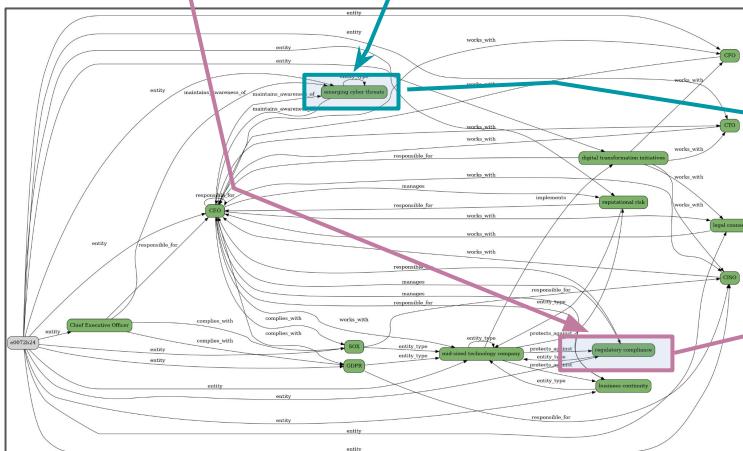
A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions...

Published: 2025-03-24 09:17:00 +0000

Between Persona and Article Graphs

Persona Overview

The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation initiatives leveraging cloud services, AI/ML technologies, and business intelligence platforms, while adhering to SOX, GDPR, and industry-specific regulations. They must maintain awareness of significant security incidents, data breaches, and emerging cyber threats that could impact stock price, customer trust, or regulatory standing. The CEO collaborates closely with the CFO, CISO, CTO, and legal counsel to balance security investments against business growth opportunities and profitability targets.



What we have now is Provenance and Explainability

And the ability to ask (and get an answer) a very important question

Why are we getting this? Since it looks wrong!

Persona Overview

The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation initiatives leveraging cloud services, AI/ML technologies, and business intelligence platforms, while adhering to SOX, GDPR, and industry-specific regulations. They must maintain awareness of significant security incidents, data breaches, and emerging cyber threats that could impact stock price, customer trust, or regulatory standing. The CEO collaborates closely with the CFO, CISO, CTO, and legal counsel to balance security investments against business growth opportunities and profitability targets.

2 Which the low score (7.5) is a good indicator that we shouldn't have used it

3 Also shown by looking at this connection which is not very 'strong'

```
article_id": "ee176c9a",
"overall_score": 7.5,
"entity_matches": [
  {
    "persona_entity": "emerging cyber threats",
    "article_entity": "Middleware",
    "relevance_score": 0.7,
    "persona_context": "the CEO must understand potential vulnerabilities that may impact the technology stack",
    "article_context": "the article discusses critical vulnerabilities that could be exploited by attackers, impacting cybersecurity",
    "match_type": "contextual"
  },
  {
    "persona_entity": "regulatory compliance",
    "article_entity": "Critical Vulnerability",
    "relevance_score": 0.75,
    "persona_context": "compliance with industry regulations to manage cybersecurity risks",
    "article_context": "the article highlights concerns about ensuring regulations are met in light of vulnerabilities",
    "match_type": "contextual"
  }
]
```

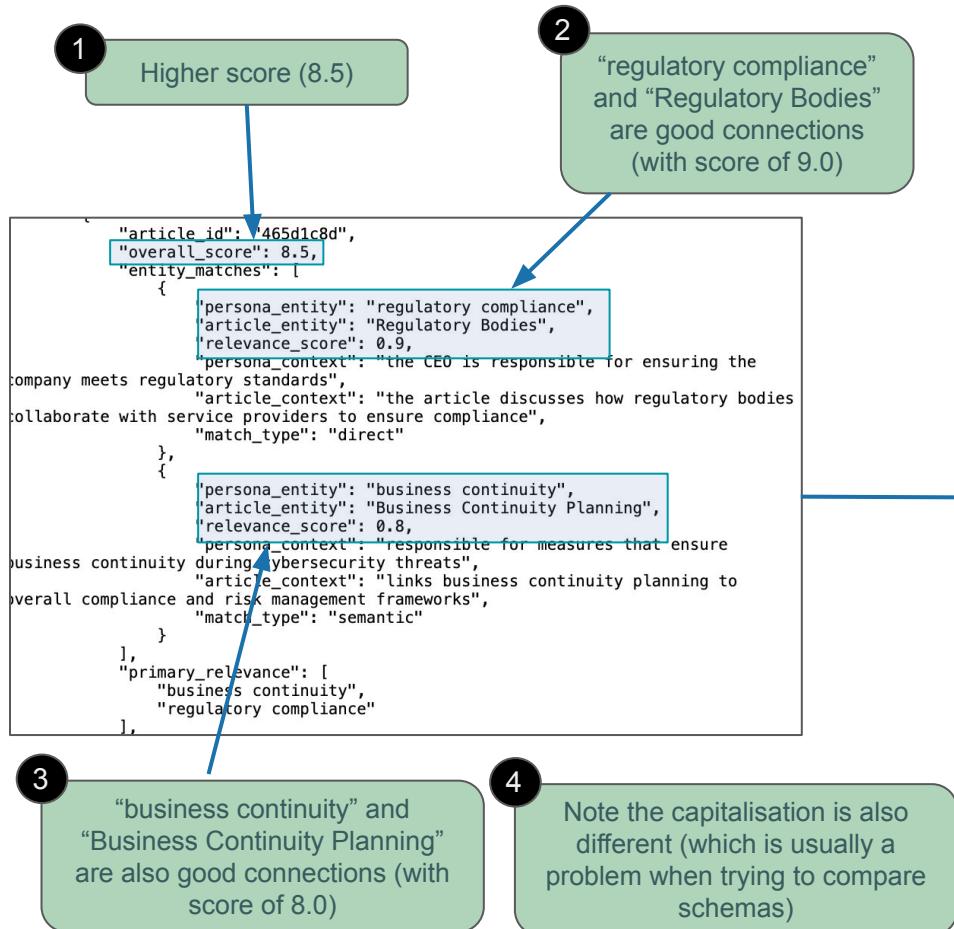
1 This is not the best article to show a CEO

A screenshot of a news article from The Hacker News. The title is "Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks". The text of the article discusses a security flaw in the Next.js framework that could be exploited to bypass authorization checks. It includes a timestamp: "Published: 2025-03-24 09:17:00 +0000".

4 In a forthcoming MVP, this will be fixed by editing/pruning the graphs

5 Via a 'Human in the feedback-loop' workflow

Let's look at a better example of graph's connections (for CEO)



Importance of Continuous Compliance Monitoring for Regulatory Adherence

Source: <https://thehackernews.com/2025/03/why-continuous-compliance-monitoring-is.html>

Author: info@thehackernews.com (The Hacker News)

Published: 2025-03-20 10:00:00 +0000

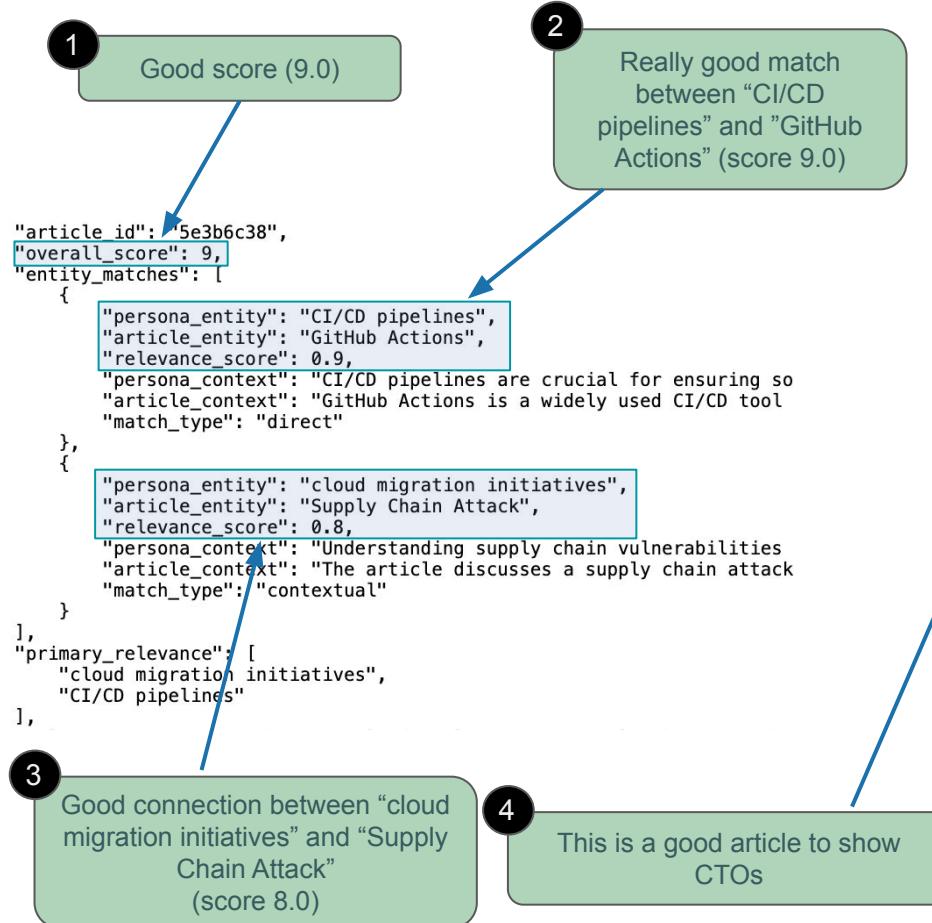


The article emphasizes that continuous compliance monitoring is essential for mid-sized tech companies like yours to meet evolving regulatory standards. This is crucial in the context of expanding IT capabilities and managing business continuity under cybersecurity risks.

Why This Matters: As CEO, ensuring compliance with regulations is key to mitigating legal and operational risks. This article helps in understanding how strategic compliance monitoring aligns with overall business strategies.

Recommended Actions: Collaborate with your legal and compliance officers to review current compliance monitoring systems, ensuring they adequately address the full spectrum of regulations affecting your business.

Let's look at a better example of graph's connections (for CTO)



Major Supply Chain Attack Impacts Critical CI/CD Tool GitHub Actions

Source: <https://thehackernews.com/2025/03/thn-weekly-recap-github-supply-chain.html>

Author: The Hacker News

Published: 2025-03-24 11:35:00 +0000



A covert alteration in a GitHub Action component led to a widespread supply chain breach, affecting deployment automation and highlighting security vulnerabilities within CI/CD pipelines.

Why This Matters: This incident could directly disrupt your cloud migration processes by compromising the integrity of automated deployments facilitated through GitHub Actions. Maintaining CI/CD pipeline security is crucial for seamless and secure software releases.

Recommended Actions: Immediate review of all GitHub Actions integrations and implementation of stringent monitoring for supply chain vulnerabilities within CI/CD processes is advised. Collaborate with DevSecOps teams to analyze any potential impacts and revise incident response strategies.