

Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge

Dinis Cruz (v0.9 - Apr 2025)



Current presentation

This talk advocates for a shift to a semantic knowledge graph ecosystem for OWASP content – an approach that would make OWASP knowledge more accessible, customizable, and interconnected.

By leveraging semantic web technologies and large language models (LLMs), OWASP can transform its guides and standards into a machine readable, linked knowledge base that community members and tools can query, adapt, and build upon in a context-aware manner.

<https://www.linkedin.com/in/diniscruz/>



Dinis Cruz

Founder @ The Cyber Boardroom, Chief Scientist @ Glasswall,
vCISO and GenAI expert

London, England, United Kingdom · Contact info

The Cyber Boardroom (GenAI) ↗

16,113 followers · 500+ connections

in
The Cyber Board

Founder (GenAI company)

Welcome to The Cyber Boardroom, the one-stop shop boards of directors rely on their cyber readiness. The Cyber Boardroom's mission is to help you understand your organisation's cyber security agenda, as well as fulfil your duties as a board member.

To help you with any questions you might have on cyber security and the risks your organisation faces, we have created an engaging AI advisor named **Athena**.

To ensure **Athena** delivers a personalised experience, go to your profile section, scroll down, and add as many prompts as you want.

In addition, we are building a customised library of short videos and valuable content aimed at enhancing your knowledge of cyber security, which will help you optimise your engagement with **Athena**.

Previously

| | |
|-------------------|--------------|
| Holland & Barrett | CISO |
| Gasswall | CTO |
| Photobox | CISO |
| Moonpig | CISO |
| BBC | AppSec |
| The Hut Group | AppSec |
| OWASP | Board Member |

Open Source Developer

Pinned:

- owasp-shot/OSBot-AWS · Public
- owasp-shot/OSBot-LLMs · Public
- owasp-shot/OSBot-Utils · Public
- Book_SetDevOps_Risk_Workflow · Public
- Book_Generation_2_Developer · Public
- OpenSecuritySummit/oss-website · Public

Customize your pins

Dinis Cruz

190 followers · 0 following

At 190 followers · 0 following

London

dinis.cruz@owasp.org

<http://bitly.dinicruz.com/>

2,674 contributions in the last year

Contribution settings

2024

18:00 - 16:00
WS-15-16

Addressing the cyber unemployment crisis: a positive outlook
Ruchiya Perry

Threat Hunting and Detection Strategies: Practical Examples in Action (panel)
Dinis Cruz, Marius Poskus

The Rise of AI Security Engineers
Stefan Streicher

Zero trust in distributed media workflows for Hollywood
Bee Schiebold

Baseline Threat Modeling for Gen AI and Large Language Models
Yemi Adenwo

Achievements

Learn how we count contributions

@owasp-shot @the-cyber-boardroom @OpenSecuritySummit

Currently

Chief Scientist (UK tech startup)

GLASSWALL

Learn about CDR Solutions Resources Partners Company

Book a demo Try cleaning a file

We prevent malicious files from entering your network

Glasswall Content Disarm and Reconstruction (CDR) rebuilds files and documents into a safe, clean standard, free from the risks of malware.

Learn about CDR

0:00 / 0:44

Director (UK CIC company)

OPEN SECURITY SUMMIT

SEARCH PROJECTS SCHEDULE MEMBERS PAST SUMMITS FUTURE SUMMITS ABOUT

Mini Summits

The Open Security Summit

Next Summit: 10th - 14th June 2024

| MONDAY - 10H | TUESDAY - 11TH | WEDNESDAY - 12TH | THURSDAY - 13TH | FRIDAY - 14TH |
|---|--|---|--|--|
| 16:00 - 16:00 WS-15-16 | ONLINE | ONLINE | ONLINE | ONLINE |
| Addressing the cyber unemployment crisis: a positive outlook Ruchiya Perry | Threat Hunting and Detection Strategies: Practical Examples in Action (panel) Dinis Cruz, Marius Poskus | The Rise of AI Security Engineers Stefan Streicher | Zero trust in distributed media workflows for Hollywood Bee Schiebold | Baseline Threat Modeling for Gen AI and Large Language Models Yemi Adenwo |
| 16:00 - 17:00 WS-16-17 | ONLINE | ONLINE | ONLINE | ONLINE |
| Supply Chain Security: Strengthening Resilience Against Exploring A Risk Approach to Software Supply Chain Security Securing Remote Work Environments: Challenges and Solutions (panel) Threat Modeling V Luis Servin | Threat Modeling V Luis Servin | Threat Modeling V Luis Servin | Threat Modeling V Luis Servin | Threat Modeling V Luis Servin |

**GenAI is a massive opportunity
and threat to AppSec**

For more details see this presentation

@DinisCruz

**It's 2024 and, with GenAI,
we can finally make
AppSec work** (v0.8 - Feb 2024)



And these two presentations

@DinisCruz

My Journey Building a GenAI Startup: The Power of MVPs and CI Pipelines - Part 1

Dinis Cruz | v0.8 | Jan 2025



@DinisCruz

My Journey Building a GenAI Startup: The Power of MVPs and CI Pipelines - PART 2

Dinis Cruz | v0.8 | Feb 2025



And the documents here

<https://docs.diniscruz.ai/>

Dinis Cruz - Documents and Research

Home

Dinis Cruz - Documents and Research

Home

2024 > This site will contain the code and PDFs for Dinis Cruz research

2025 >

Research > • Europe and Learning

Resources > • Graphs
• The Future of News
• Projects

Future of news

- Monetising Trust and Knowledge: How News Providers can leverage Personalised Semantic Graphs
- Journalists' Challenges with Digital Content Provenance and Trust
- The Future of News: Building Trust Through Fact Provenance
- The Future of News Monetization: Embracing Micro and Nano Payments
- Strengthening Trust in News: Implementing Identity Graphs for Authors and Sources

Europe GenAI Opportunity

- Scaling Europe's Regulatory Superpower: From Static Cybersecurity Standards to Semantic Graphs
- An Open-Source Sovereign Cloud for an Open Europe: The Case for a Federated, AI-Enabled, and Multilingual Digital Infrastructure
- Portuguese as a Programming Language in the AI Era
- Deterministic GenAI Outputs with Provenance (OWASP EU AppSec Lisbon)
- Europe's Strategic Opportunity in GenAI: A Deep Dive into Six Defining Trends
- Think Different, Again: Reimagining Apple's Role in the AI Era

Ontologies and Taxonomies

- From Top-Down to Organic Evolving Graphs, Ontologies, and Taxonomies
- Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge
- Enhancing Cybersecurity Event Networking with Semantic Knowledge Graphs

Cloud

- Intent-Based Feedback Loops in Cloud Environments

Standards and Governance

- Maturity Models vs. Traditional Standards in Application Security
- Graph-Powered Legal Knowledge: An Open, Distributed, and AI-Assisted Roadmap



Special mention

Session management

CRE: 177-260

Which contains CREs:

- CRE : 110-531 : Cookie-config
- CRE : 114-277 : Session integrity
- CRE : 258-115 : Re-authentication from federation or assertion
- CRE : 402-133 : Do not expose session token in URL
- CRE : 470-731 : Minimize session life
- CRE : 582-541 : Re-authenticate before sensitive transactions
- CRE : 716-526 : Session token generation

Which is linked to sources:

- Standard : NIST 800-53 v5 : AC-10 CONCURRENT SESSION CONTROL ↗
- Standard : NIST 800-53 v5 : IA-11 RE-AUTHENTICATION ↗
- Standard : NIST 800-53 v5 : SC-23 SESSION AUTHENTICITY ↗
- Standard : OWASP Top 10 2021 : A01 : Broken Access Controls ↗
- Standard : OWASP Top 10 2021 : A07 : Identification and Authentication Failures ↗

Which is part of CREs:

- ▼ CRE : 636-660 : Technical application security controls



Open CRE Explorer

A visual explorer of Open Common Requirement Enumerations (CREs). Data source: opencre.org.

= 427 items

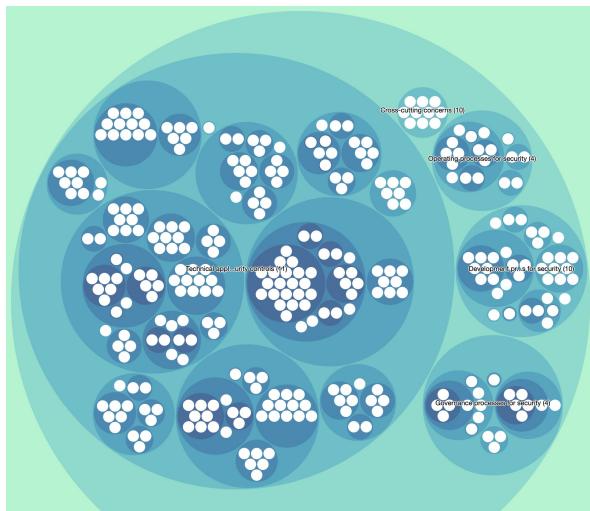
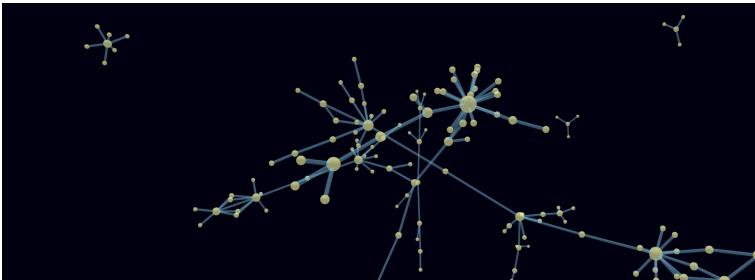
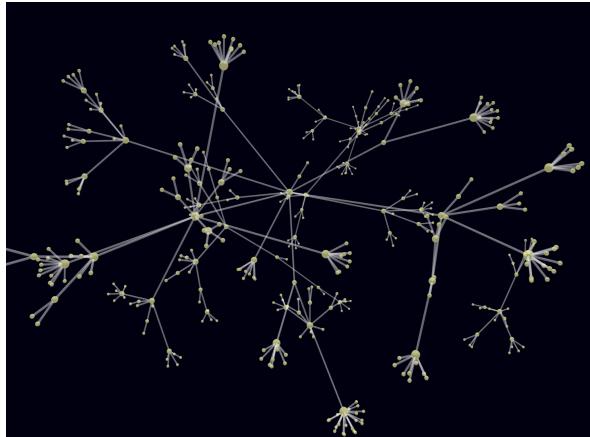
graphs (3D): [CRE dependencies - hierarchy only](#) | [related only](#) | [links to external standards](#) | [zoomable circles](#)

546-564: Cross-cutting concerns

| | |
|---|--|
| 155-155: Architecture | OWASP Top 10 2021 |
| 486-813: Configuration | NIST 800-53 v5 (2) OWASP Top 10 2021 |
| 170-772: Cryptography | OWASP Web Security Testing Guide (WSTG) Cloud Controls Matrix IS |
| 028-727: CSRF protection | |
| 623-550: Denial Of Service protection | NIST 800-53 v5 |
| 760-764: Injection protection | OWASP Top 10 2021 |
| 362-550: Personal data handling | ISO 27001 |
| 058-527: Secure name/address resolution service | NIST 800-53 v5 (2) |
| 028-728: SSRF protection | OWASP Top 10 2021 |
| 760-765: XSS protection | |

567-755: Governance processes for security

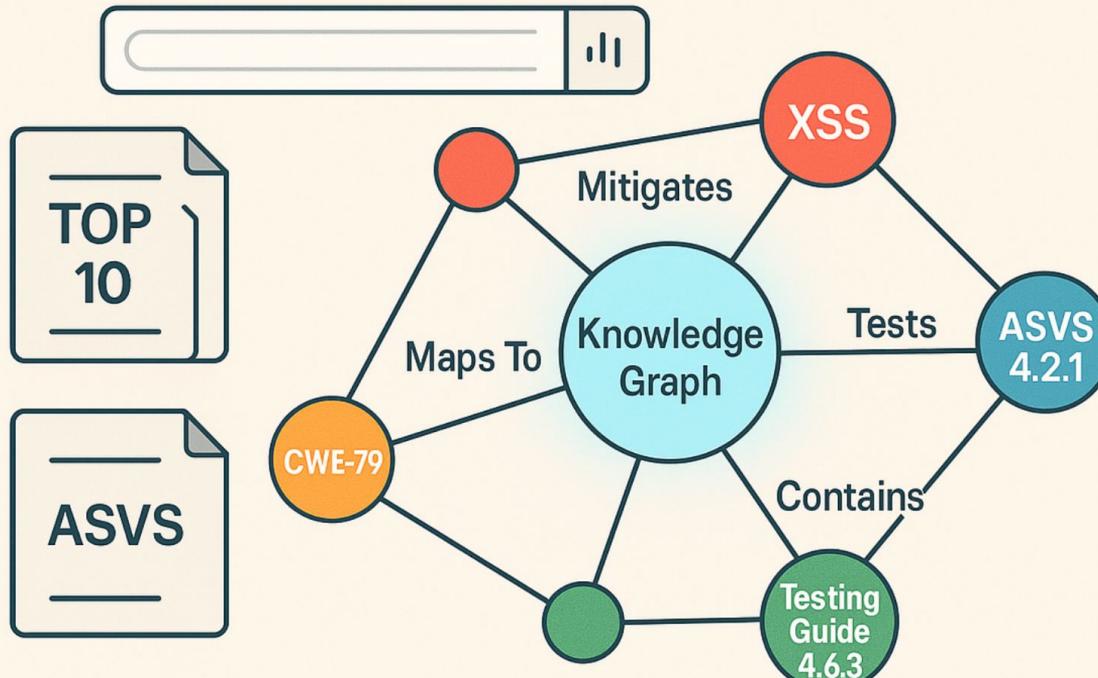
| | |
|--|---|
| 464-513: Assurance processes | Cloud Controls Matrix NIST 800-53 v5 (10) NIST SSDF |
|--|---|



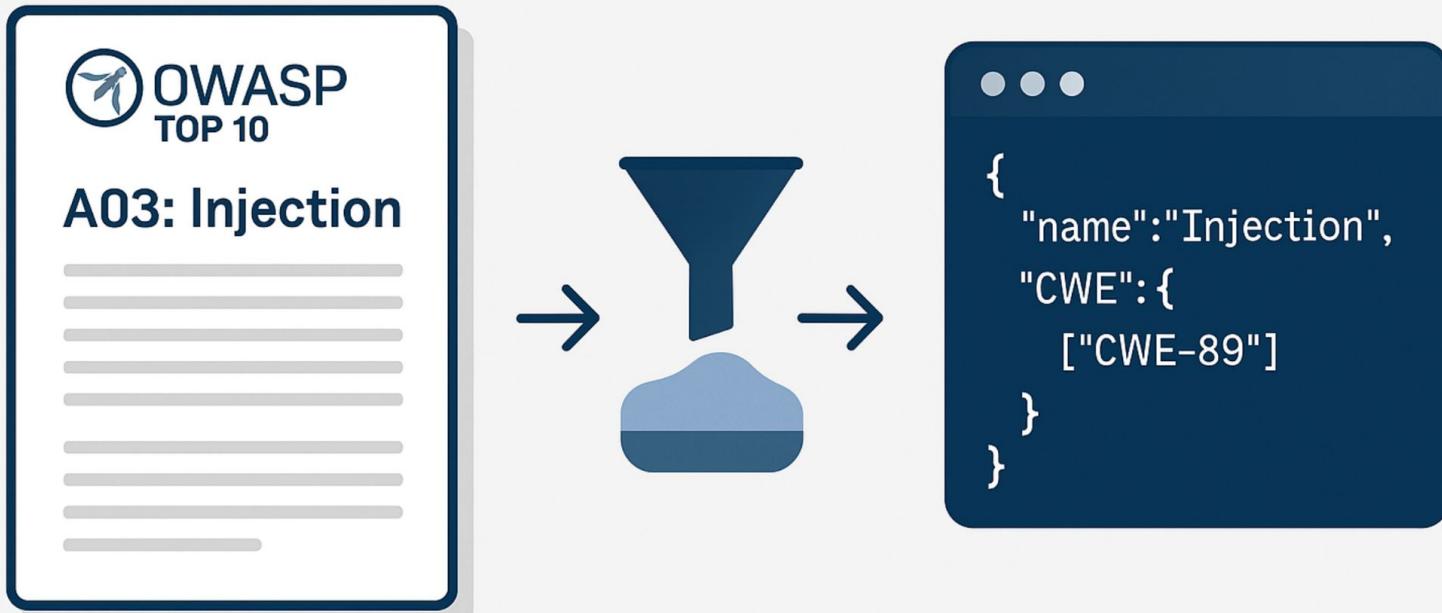
Semantic OWASP

(key concepts)

What If OWASP Were a Knowledge Graph?



From Human-Readable to Machine-Usable



Customizing OWASP for Your Context

Industry:

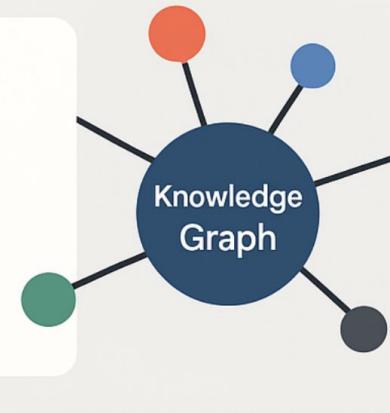
Healthcare

Kubernetes

EU

A03: Injection

- Use safe APIs
- Perform input validation
- Utilize ORM



ASVS Controls for API Security



Apply misics

- Use safe APIs
- Perform input validation
- Utilize ORM

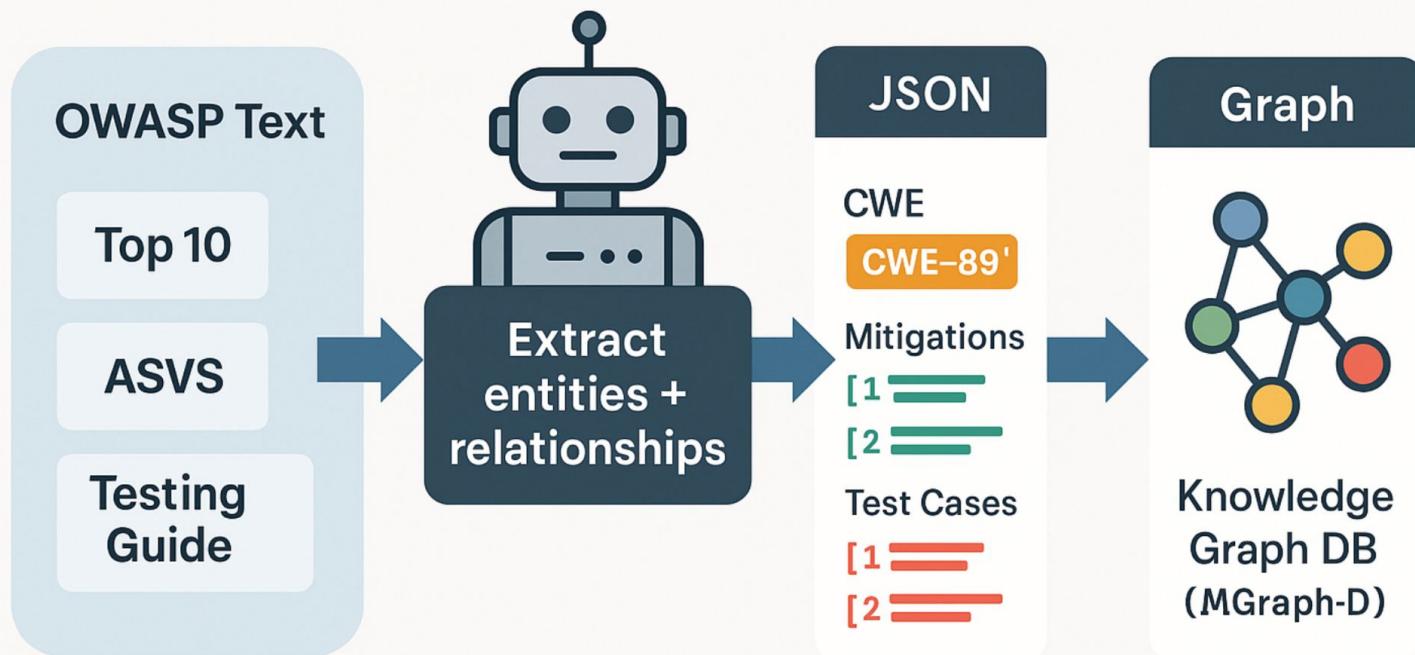


Connected, Not Siloed

OWASP projects become interlinked – making navigation seamless



How LLMs Help OWASP Evolve



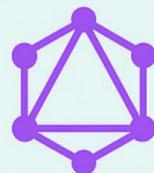
Why This Matters: Benefits of Semantic OWASP

Traditional OWASP (Today)



- Static docs,
one-size-filt-all

Semantic OWASP



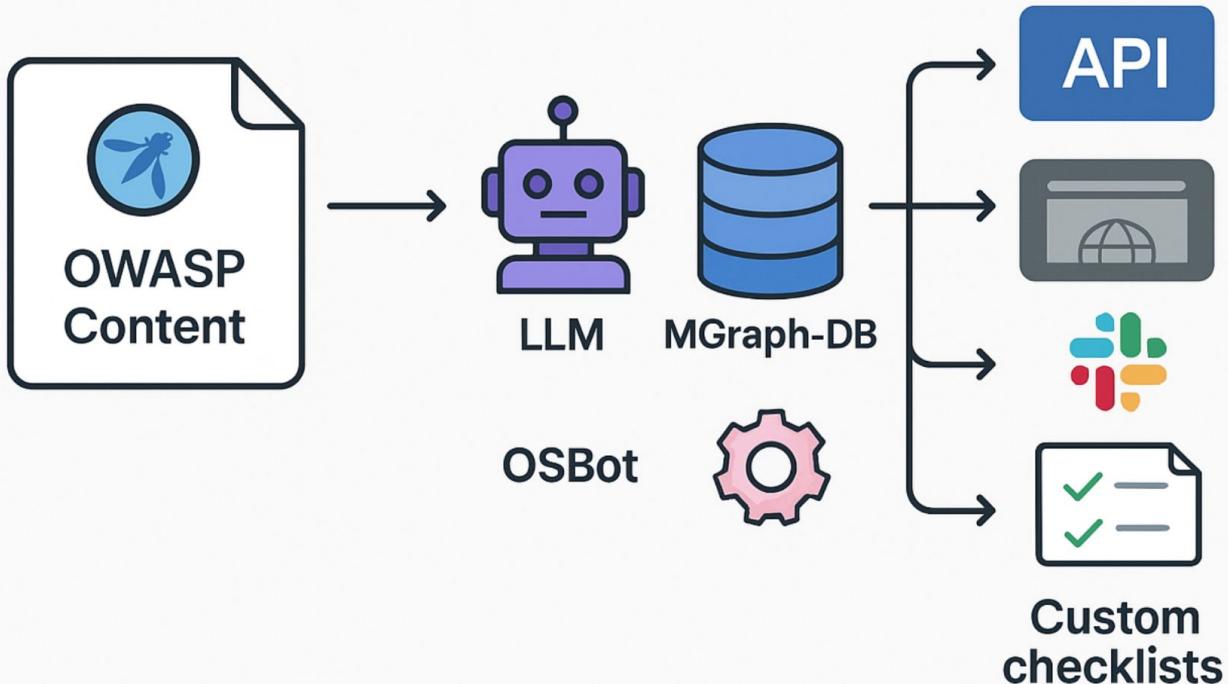
Filtered, linked,
personalized

Use Cases



- Chatbots
- Dashboards
- IDE Plugins

The Tools Making This Possible



OWASP's Future: Dynamic. Open. AI-Ready.

Q How do I prevent SQLi?



¿Cómo evito SQLi?



SQL Injection

SQL injections are mitigated by the use of parameterized queries and ORM.

Linked Results

Testing Procedure 1

ASVS 4.3.2

Cheat Sheet

A vision for semantic, AI-integrated knowledge service

Read more at

Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge

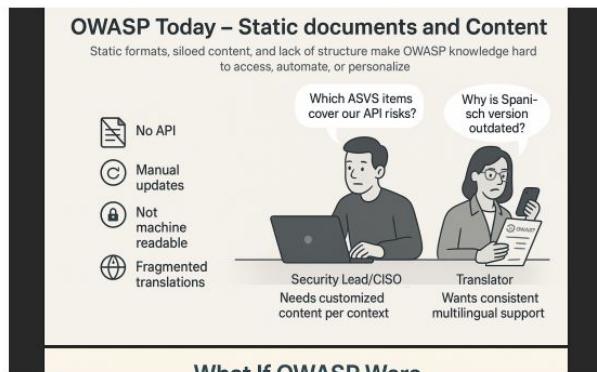
by Dinis Cruz and ChatGPT Deep Research, 2025/04/02

[Download](#) [Listen Audio](#)

Podcast



Infographic



Introduction

Open Web Application Security Project (OWASP) documentation projects – such as the OWASP Top 10, Application Security Verification Standard (ASVS), the Web Security Testing Guide and many others – are widely used to educate and guide the security community. These resources have become de-facto standards for identifying risks, defining security requirements, and outlining testing practices.

However, as the volume and diversity of software grows—and new technologies like AI change how information is consumed—the current format of OWASP knowledge bases is starting to show limitations.

Most OWASP documentation exists as static text (PDFs or web pages), which is great for human reading but makes it difficult to extract specific information, automate usage, or tailor content to different needs.

This paper advocates for a shift to a semantic knowledge graph ecosystem for OWASP content – an approach that would make OWASP knowledge more accessible, customizable, and interconnected.

By leveraging semantic web technologies and large language models (LLMs), OWASP can transform its guides and standards into a machine-readable, linked knowledge base that community members and tools can query, adapt, and build upon in a context-aware manner.

To remain impactful, OWASP must evolve its content delivery to support greater accessibility, customization, and interoperability across tools, industries, and languages.

https://docs.diniscruz.ai/2025/04/02/semantic-owasp_leveraging-genai-and-graphs-to-customise-and-scale-security-knowledge.html

Listen about it (Spotify podcast)

The screenshot shows a Spotify podcast episode page. At the top left is the show's logo, "Semantic OWASP", with the subtitle "Leveraging GenAI & Knowledge Graphs to Scale Security Knowledge". Below the logo is a small illustration of two people, one holding a book titled "OWASP ASVS Testing Guide" and the other working on a laptop, with a brain icon and a network graph in the background. The main title of the episode is "Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge", with the subtitle "Cyber Boardroom GenAI Insights". Below the title, it says "3 Apr • Finished ✓". Underneath are standard Spotify controls: a green play button, a download icon, an add-to-library icon, and a more options menu. The "Episode Description" section contains text about the podcast's focus on transforming security knowledge through semantic technology and AI, and it mentions Cruz's paper "Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge".

Semantic OWASP
Leveraging GenAI & Knowledge Graphs
to Scale Security Knowledge

Transforming static documentation into dynamic, queryable knowledge

Podcast Episode

Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge

Cyber Boardroom GenAI Insights

3 Apr • Finished ✓

...

Episode Description

In this NotebookLM-powered podcast, two moderators dive into Dinis Cruz's groundbreaking research on transforming security knowledge through semantic technology and AI.

The conversation explores key insights from Cruz's paper "Semantic OWASP: Leveraging GenAI and Graphs to Customise and Scale Security Knowledge," examining:

<https://open.spotify.com/embed/episode/3cFm0lvdD33VPSBsl121px>

And this 20 page research paper

The OWASP community has always been about empowering organizations and developers with knowledge to build secure software. As we move deeper into the digital era, the way knowledge is consumed is changing – it's more interactive, on-demand, and tailored. To keep pace, OWASP's own knowledge delivery should evolve from static documents to a **dynamic, semantic knowledge graph ecosystem**. By doing so, OWASP content becomes more accessible (to both humans and machines), more customizable to diverse needs, and more interconnected for a holistic understanding of application security.

In this paper, we highlighted the current pain points: important OWASP guidelines locked in PDFs and web pages that can't easily talk to each other or adapt to specific contexts. We then painted a vision of how semantic web technologies and LLMs can transform this situation, turning OWASP's collective wisdom into a living knowledge graph that is rich with relationships and machine-readable meaning. We drew inspiration from Dinis Cruz's MyFeeds.ai and Cyber Boardroom projects, which proved that even complex narratives can be distilled into graphs and reassembled into personalized outputs using AI – a blueprint OWASP can follow using open source tools like MGraph-DB and OWASP SBot that are already at our disposal.

The benefits of this shift are immense. Consider a future where a developer in Brazil can query OWASP in Portuguese for the top risks in her fintech web application, and instantly get a curated list with implementation guidance and test checklists drawn from OWASP Top 10, ASVS, and Cheat Sheets – all relevant, up-to-date, and in her language. Or a future where an OWASP Top 10 release isn't just a PDF, but an interactive data set that companies can import directly into their risk tracking systems, and a knowledge base that AI assistants reference to give developers accurate advice. In such a future, OWASP's impact would be even greater than it is today, because the knowledge would integrate seamlessly into the workflows and tools developers use.

Importantly, moving to a semantic knowledge graph model keeps OWASP on the cutting edge of how information is shared, ensuring the organization remains the go-to source for application security guidance in a form that modern platforms (and brains) can readily digest. It also reinforces OWASP's open philosophy: an open knowledge graph is easier for the community to contribute to, remix, and build upon than static docs. The underlying data being open means researchers, educators, and tool builders can create new innovations on top of OWASP content, driving further our mission of spreading security knowledge.

https://docs.diniscruz.ai/2025/04/02/semantic-owasp_leveraging-genai-and-graphs-to-customise-and-scale-security-knowledge.html

Semantic OWASP

In Practice

Let's look at OWASP Top 10 (non Semantic version)

OWASP Top 10:2021

Home
Notice
Introduction
How to use the OWASP Top 10 as a standard
How to start an AppSec program with the OWASP Top 10
About OWASP
Top 10:2021 List
[A01 Broken Access Control](#)
[A02 Cryptographic Failures](#)
[A03 Injection](#)
[A04 Insecure Design](#)
[A05 Security Misconfiguration](#)
[A06 Vulnerable and Outdated Components](#)
[A07 Identification and Authentication Failures](#)
[A08 Software and Data Integrity Failures](#)
[A09 Security Logging and Monitoring Failures](#)
[A10 Server Side Request Forgery \(SSRF\)](#)
Next Steps

A01:2021 – Broken Access Control



Factors

| CWEs Mapped | Max Incidence Rate | Avg Incidence Rate | Avg Weighted Exploit | Avg Weighted Impact | Max Coverage | Avg Coverage |
|-------------|--------------------|--------------------|----------------------|---------------------|--------------|--------------|
| 34 | 55.97% | 3.81% | 6.92 | 5.93 | 94.55% | 47.72% |

Overview

Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor*, *CWE-201: Insertion of Sensitive Information Into Sent Data*, and *CWE-352: Cross-Site Request Forgery*.

Description

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits. Common access control

Description

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits. Common access control vulnerabilities include:

- Violation of the principle of least privilege or deny by default, where access should only be granted for particular capabilities, roles, or users, but is available to anyone.
- Bypassing access control checks by modifying the URL (parameter tampering or force browsing), internal application state, or the HTML page, or by using an attack tool modifying API requests.
- Permitting viewing or editing someone else's account, by providing its unique identifier (insecure direct object references)
- Accessing API with missing access controls for POST, PUT and DELETE.
- Elevation of privilege. Acting as a user without being logged in or acting as an admin when logged in as a user.
- Metadata manipulation, such as replaying or tampering with a JSON Web Token (JWT) access control token, or a cookie or hidden field manipulated to elevate privileges or abusing JWT invalidation.
- CORS misconfiguration allows API access from unauthorized/untrusted origins.
- Force browsing to authenticated pages as an unauthenticated user or to privileged pages as a standard user.

Amazing content, but static

How to Prevent

Access control is only effective in trusted server-side code or server-less API, where the attacker cannot modify the access control check or metadata.

- Except for public resources, deny by default.
- Implement access control mechanisms once and re-use them throughout the application, including minimizing Cross-Origin Resource Sharing (CORS) usage.
- Model access controls should enforce record ownership rather than accepting that the user can create, read, update, or delete any record.
- Unique application business limit requirements should be enforced by domain models.
- Disable web server directory listing and ensure file metadata (e.g., .git) and backup files are not present within web roots.
- Log access control failures, alert admins when appropriate (e.g., repeated failures).
- Rate limit API and controller access to minimize the harm from automated attack tooling.
- Stateful session identifiers should be invalidated on the server after logout. Stateless JWT tokens should rather be short-lived so that the window of opportunity for an attacker is minimized. For longer lived JWTs it's highly recommended to follow the OAuth standards to revoke access.

Example Attack Scenarios

Scenario #1: The application uses unverified data in a SQL call that is accessing account information:

```
pstmt.setString(1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery();
```

An attacker simply modifies the browser's 'acct' parameter to send whatever account they want. If not correctly verified, the attacker can access any user's account.

<https://example.com/app/accountInfo?acct=notmyacct>

Scenario #2: An attacker simply forces browses to target URLs. Admin rights are required to access to the admin page.

<https://example.com/app/getappInfo>
https://example.com/app/admin_getappInfo

If an unauthenticated user can access either page, it's a flaw. If a non-admin can access the admin page, this is a flaw.

References

- OWASP Proactive Controls: Enforce Access Controls
- OWASP Application Security Verification Standard: V4 Access Control
- OWASP Testing Guide: Authorization Testing
- OWASP Cheat Sheet: Authorization
- PortSwigger: Exploiting CORS misconfiguration
- OAuth: Revoking Access

List of Mapped CWEs

- CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-23 Relative Path Traversal
- CWE-35 Path Traversal: '../..//'
- CWE-59 Improper Link Resolution Before File Access ('Link Following')
- CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
- CWE-201 Exposure of Sensitive Information Through Sent Data
- CWE-219 Storage of File with Sensitive Data Under Web Root
- CWE-264 Permissions, Privileges, and Access Controls (should no longer be used)
- CWE-275 Permission Issues
- CWE-276 Incorrect Default Permissions
- CWE-284 Improper Access Control
- CWE-285 Improper Authorization
- CWE-352 Cross-Site Request Forgery (CSRF)
- CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
- CWE-377 Insecure Temporary File
- CWE-402 Transmission of Private Resources into a New Sphere ('Resource Leak')
- CWE-425 Direct Request ('Forced Browsing')

Source material is Markdown - Great but static

master Top10 / 2021 / docs / A00_2021_Introduction.md ...

vanderaj add Just Eat as a financial sponsor of the OWASP Top 10 (#672) 5010a4f · 4 years ago History

Preview Code Blame 118 lines (72 loc) · 16.3 KB Raw ...

```
1  # Introduction
2
3  ## Welcome to the OWASP Top 10 - 2021
4
5  ! [OWASP Top 10 Logo](./assets/TOP_10_logo_Final_Logo_Colour.png){:class="img-responsive"}
6
7  Welcome to the latest installment of the OWASP Top 10! The OWASP Top 10 2021 is all-new, with a new graphic design and an available one-page infographic you can print or share online.
8
9  A huge thank you to everyone that contributed their time and data for this iteration. Without you, this installment would not happen. **THANK YOU!**
10
11 ## What's changed in the Top 10 for 2021
12
13 There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021. We've changed names when necessary to fo
14
15 ! [Mapping](assets/mapping.png)
16
17 - **A01:2021-Broken Access Control** moves up from the fifth position to the category with the most serious web application security risk; the contributed data indicate
18 - **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as **A3:2017-Sensitive Data Exposure**, which was broad symptom rather than a root
19 - **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average
20 - **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need mo
21 - **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration, with an average i
22 - **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also h
23 - **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that
24 - **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pip
25 - **A09:2021-Security Logging and Monitoring Failures** was previously **A10:2017-Insufficient Logging & Monitoring** and is added from the Top 10 community survey (#3)
26 - **A10:2021-Server Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing co
```

 CC BY SA

What we need is graphs, ontologies and taxonomies

And here is the first MVP of accessing the OWASP Top 10 content as Semantic Knowledge Graphs

owasp ^

| | | |
|--------------------------|---------------|---|
| GET /owasp/data-to-parse | Data To Parse | ▼ |
| GET /owasp/ontology | Ontology | ▼ |
| GET /owasp/taxonomy | Taxonomy | ▼ |
| GET /owasp/rdf-triples | Rdf Triples | ▼ |
| GET /owasp/screenshot | Screenshot | ▼ |
| GET /owasp/raw-data | Raw Data | ▼ |
| GET /owasp/raw-data-json | Raw Data Json | ▼ |

Lets start with the raw Mardown data

GET

/owasp/raw-data Raw Data

Response body

```
# A01:2021 - Broken Access Control ![icon](assets/TOP_10_Icons_Final_Broken_Access_Control.png){: style="height:80px; width:80px" align="right"}  
## Factors  


| CWEs Mapped | Max Incidence Rate | Avg Incidence Rate | Avg Weighted Exploit | Avg Weighted Impact | Max Coverage | Avg Coverage | Total Occurrences | Total CWEs |
|-------------|--------------------|--------------------|----------------------|---------------------|--------------|--------------|-------------------|------------|
| 34          | 55.97%             | 3.81%              | 6.92                 | 5.93                | 94.55%       | 47.72%       | 318,487           | 19,013     |

  
## Overview  


Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Con-  
tributed CWEs include *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor*, *CWE-201: Insertion of Sensitive Information Into Sent Data*, and *CWE-352: Cross-Site Request Forgery*.

  
## Description  


Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits. Common access control vulnerabilities include:


```

Then let's convert it into JSON

GET /owasp/raw-data-json Raw Data Json

Response body

```
{  
  "identifier": "A01:2021",  
  "name": "Broken Access Control",  
  "icon": "assets/TOP_10_Icons_Final_Broken_Access_Control.png",  
  "factors": {  
    "cwees_mapped": 34,  
    "max_incidence_rate": "55.97%",  
    "avg_incidence_rate": "3.81%",  
    "avg_weighted_exploit": 6.92,  
    "avg_weighted_impact": 5.93,  
    "max_coverage": "94.55%",  
    "avg_coverage": "47.72%",  
    "total_occurrences": 318487,  
    "total_cves": 19013  
  },  
  "overview": "Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate t occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are *CWE-200: Exposure of Sensitive Information by Poor Access Control*, *CWE-201: Insertion of Sensitive Information Into Sent Data*, and *CWE-352: Cross-Site Request Forgery*.",  
  "description": {  
    "intro": "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized i fication, or destruction of all data or performing a business function outside the user's limits. Common access control vulnerabilities include:",  
    "items": [  
      "Violation of the principle of least privilege or deny by default, where access should only be granted for particular capabilities, roles, or user one.",  
      "Bypassing access control checks by modifying the URL. Common techniques are: Session hijacking, internal application state, or the HTML page, or by
```

Using this Prompt and Schema

GET

/owasp/raw-data-json Raw Data Json

```
system_prompt = """\nYou are a specialized OWASP Top 10 parser that extracts structured information\nfrom OWASP Top 10 category markdown.
```

Your task is to parse the provided markdown content and extract all relevant information for an OWASP Top 10 risk category.

For each category, extract the following:

1. Identifier (e.g., "A01:2021")
2. Name (e.g., "Broken Access Control")
3. Factors (statistical metrics)
4. Overview section
5. Detailed description (intro paragraph and bullet points)
6. Prevention information (intro paragraph and bullet points)
7. Example attack scenarios with any code examples
8. References (titles and URLs)
9. Mapped CWEs (identifiers, names, and URLs)
10. Previous name if mentioned

Ensure you maintain the original formatting and content where appropriate, especially in code examples and descriptions.

Format your response according to the Schema__OWASP__Top10_Risk structure with all required fields.

"""

```
43 class Schema__Owasp__Top_10__Category(Type_Safe):\n44     """Individual OWASP Top 10 category."""\n45     identifier : str\n46     name : str\n47     icon : str\n48     factors : Schema__OWASP__Factor\n49     overview : str\n50     description : Schema__OWASP__Description\n51     how_to_prevent : Schema__OWASP__Prevention\n52     example_attack_scenarios: List[Schema__OWASP__AttackScenario]\n53     references : List[Schema__OWASP__Reference]\n54     mapped_cwes : List[Schema__OWASP__CWE]
```

Using this Prompt and Schema

GET

/owasp/raw-data-json Raw Data Json

```

43 class Schema__Owasp__Top_10__Category(Type_Safe):
44     """Individual OWASP Top 10 category."""
45     identifier : str
46     name : str
47     icon : str
48     factors : Schema__OWASP__Factor
49     overview : str
50     description : Schema__OWASP__Description
51     how_to_prevent : Schema__OWASP__Prevention
52     example_attack_scenarios: List[Schema__OWASP__AttackScenario]
53     references : List[Schema__OWASP__Reference]
54     mapped_cwes : List[Schema__OWASP__CWE]

```

```

class Schema__OWASP__Factor(Type_Safe):
    """Statistical factors related to the OWASP category."""
    cwes_mapped : int      # Number of Common Weakness Enumerations
    max_incidence_rate : str  # Maximum incidence rate of the category
    avg_incidence_rate : str  # Average incidence rate of the category
    avg_weighted_exploit : float  # Average weighted exploit score
    avg_weighted_impact : float  # Average weighted impact score
    max_coverage : str  # Maximum coverage (e.g., "94.55%")
    avg_coverage : str  # Average coverage (e.g., "47.72%")
    total_occurrences : int  # Total number of occurrences
    total_cves : int  # Total number of CVEs

```

```

class Schema__OWASP__AttackScenario(Type_Safe):
    """Example attack scenario for an OWASP category."""
    number : int          # Scenario number
    description : str      # Description of the scenario
    code_examples : List[str]  # Optional code examples related to the scenario

```

```

class Schema__OWASP__Reference(Type_Safe):
    """Reference to additional resources for an OWASP category."""
    title : str            # Title of the reference
    url : str              # URL of the reference

```

```

class Schema__OWASP__CWE(Type_Safe):
    """Common Weakness Enumeration mapped to an OWASP category."""
    cwe_id : str           # CWE identifier (e.g., "CWE-200")
    name : str              # Name of the CWE
    url : str              # URL to the CWE definition

```

```

class Schema__OWASP__Prevention(Type_Safe):
    """Prevention information for an OWASP category."""
    intro: str             # Introduction paragraph for prevention
    items: List[str]        # List of prevention methods/items

```

What we need is an Ontology (classes)

GET

/owasp/ontology Ontology

Response body

```
{  
  "classes": [  
    {  
      "name": "Access_Control",  
      "definition": "A security mechanism that enforces policy to ensure that users cannot act outside their intended permissions within a system.",  
      "examples": [  
        "Role-Based Access Control (RBAC)",  
        "Mandatory Access Control (MAC)",  
        "Discretionary Access Control (DAC)"  
      ]  
    },  
    {  
      "name": "Access_Control_Vulnerability",  
      "definition": "A weakness in an access control mechanism that allows users to perform actions or access resources outside their authorized scope.",  
      "examples": [  
        "Insecure Direct Object Reference",  
        "Privilege Escalation",  
        "CORS Misconfiguration",  
        "Parameter Tampering"  
      ]  
    },  
    {  
      "name": "User",  
      "definition": "An individual or entity that interacts with a system and is subject to access control policies.",  
      "examples": [  
        "Administrator",  
        "Guest User",  
        "Regular User"  
      ]  
    }  
  ]  
}
```

What we need is an Ontology (relationships)

GET

/owasp/ontology Ontology

Response body

```
"relationships": [
  {
    "name": "enforces",
    "definition": "Indicates that an access control mechanism enforces a particular permission or set of permissions.",
    "domain": "Access_Control",
    "range": "Permission",
    "examples": [
      "Role-Based Access Control enforces Edit Profile permission"
    ]
  },
  {
    "name": "grants",
    "definition": "Specifies that a permission is granted to a user or a role.",
    "domain": "Permission",
    "range": "User",
    "examples": [
      "Edit Profile permission grants Standard User"
    ]
  },
  {
    "name": "assigned_to_role",
    "definition": "Indicates that a permission is assigned to a specific role.",
    "domain": "Permission",
    "range": "Role",
    "examples": [
      "Edit Profile permission is assigned to Standard User"
    ]
  }
]
```

What we need is an Taxonomy

GET /owasp/taxonomy

Response body

```
{ "taxonomies": [ { "root": "Access_Control_Vulnerability", "description": "Hierarchy of vulnerabilities related to insufficient or broken access control mechanisms, leading to unauthorized access.", "hierarchy": { "name": "Access_Control_Vulnerability", "definition": "A weakness in an access control mechanism that allows users to perform actions or access resources outside their authorized scope.", "subcategories": [ "Least_Privilege_Violation", "Access_Control_Bypass", "Insecure_Direct_Object_Reference", "Missing_Access_Controls", "Privilege_Escalation", "Metadata_Manipulation", "CORS_Misconfiguration", "Force_Browsing" ] } }, { "root": "Attack_Technique", "description": "Hierarchy of attack techniques that exploit access control vulnerabilities.", "hierarchy": { "name": "Attack_Technique", "definition": "A method used by attackers to exploit access control vulnerabilities to gain unauthorized access or perform malicious actions.", "subcategories": [ "Brute_Force", "Session_Hijacking", "Privilege_Escalation", "Denial_of_Service", "Man_in_the_Middle", "Phishing", "Insider_Threat", "Cross_Site_Scripting", "Cross_Site_Request_Forgery", "SQL_Injection", "XSS", "CSRF", "OWASP Top Ten 2021", "OWASP Top Ten 2022", "OWASP Top Ten 2023", "OWASP Top Ten 2024" ] } } ] }
```

And rdf triples

GET

/owasp/rdf-triples Rdf Triples

Response body

```
{
  "triples": [
    {
      "subject": {
        "value": "Broken_Access_Control",
        "type": "Access_Control_Vulnerability"
      },
      "predicate": "caused_by",
      "object": {
        "value": "Access_Control",
        "type": "Access_Control"
      }
    },
    {
      "subject": {
        "value": "Least_Privilege_Violation",
        "type": "Access_Control_Vulnerability"
      },
      "predicate": "caused_by",
      "object": {
        "value": "Access_Control",
        "type": "Access_Control"
      }
    }
  ]
}
```

Response body

```
,
  {
    "subject": {
      "value": "Least_Privilege_Violation",
      "type": "Access_Control_Vulnerability"
    },
    "predicate": "targets",
    "object": {
      "value": "Account_Information",
      "type": "Resource"
    }
  },
  {
    "subject": {
      "value": "Access_Control_Bypass",
      "type": "Access_Control_Vulnerability"
    },
    "predicate": "caused_by",
    "object": {
      "value": "Access_Control",
      "type": "Access_Control"
    }
  },
  {
    "subject": {
```

Response body

```
,
  {
    "subject": {
      "value": "Insecure_Direct_Object_Reference",
      "type": "Access_Control_Vulnerability"
    },
    "predicate": "targets",
    "object": {
      "value": "Account_Information",
      "type": "Resource"
    }
  },
  {
    "subject": {
      "value": "Missing_Access_Controls",
      "type": "Access_Control_Vulnerability"
    },
    "predicate": "caused_by",
    "object": {
      "value": "Access_Control",
      "type": "Access_Control"
    }
  },
  {
    "subject": {
```

**Practical example of this
technology**

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:



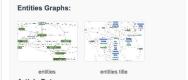
ID: a100d201 (Author: info@thehackernews.com (The Hacker News))

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:



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.

ATHENA - 15 APR 2025

Main sites used in this presentation

Site used to publish the personalized news digest

The Cyber Boardroom is a platform designed for cybersecurity professionals. The screenshot shows a personalized news digest for a Board Member (Public) for the period March 19-26, 2025. The digest covers topics such as Incident Response & Vulnerability Management, Risk Management & Compliance, and Insider Threat & Privileged Access Management. It also includes links to datasets for CISOs, CTOs, CEOs, and Board Members (Private).

<https://mvp.myfeeds.ai/>

Helper page (per persona) with links to the main datasets and graphs

This screenshot shows a helper page for the CEO persona. The page title is "Ceo Data" and it was last updated on April 18, 2025. The "Persona Overview" section describes the CEO's role in leading strategic direction for a mid-sized technology company. The "Article Resources" section includes links to Current Digest Articles, All Articles Timeline, Blog site (mvp.MyFeeds.ai), and API (dev.myfeeds.ai). Below this are sections for Persona Resources, Cybersecurity Digest (HTML), Digest JSON Data, Entities Visualization, Entities Data, and Entities Tree, each with a "View Resource" button.

https://dev.myfeeds.ai/personas/persona-home-page?persona_type=exec-ceo

Helper page with the articles used to create the personalised digest

This screenshot shows a helper page titled "Cybersecurity News Digest - Source Articles". It displays a list of 31 articles used to generate a personalized digest. The articles are categorized by role: CEO, CISO, CTO, and GTO. Each article card includes a thumbnail, title, author, and a link to the original article. Examples of articles include "CrushFTP vmware" and "tornado cash".

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

MyFeeds.ai APIs

personas

| | | |
|-----|--------------------------------|----------------------|
| GET | /personas/persona | Persona |
| GET | /personas/persona-digest | Persona Digest |
| GET | /personas/persona-home-page | Persona Home Page |
| GET | /personas/persona-digest-image | Persona Digest Image |
| GET | /personas/persona-png | Persona Png |
| GET | /personas/persona-tree | Persona Tree |

<https://dev.myfeeds.ai>

Powered by



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

Let's see what we can do with this

Cache entry

LLM response

LLM Prompt

```
{ "llm_request": { "request_data": { "function_call": { "parameters": "myfeeds_ai.personas.llms.Schema_Persona_Digest", "function_name": "create_digest", "description": "" }, "temperature": null, "top_p": null, "max_tokens": null, "model": "gpt-4o", "platform": "", "provider": "", "messages": [ { "role": "SYSTEM", "content": "You are a specialized cybersecurity news analyst between news articles and the recipient's knowledge graph to create a introductory paragraph providing a high-level overview of key developments matched to this persona's role and decision-making needs\n - Factual information most relevant to the persona's specific focus areas\n - Specific action recommendations based on this news\n \n Your digest should reflect the critical nature\n - Provide insights relevant to the persona's decision-making needs\n - Maintain a professional tone appropriate for the information needs\n - Make sure to include the author, article source, image link and when it was published\n }, { "role": "USER", "content": "Create a personalized cybersecurity news digest based on my interests\n - The company leverages Digital Payment Platforms, Mobile Banking Solutions, Data Loss Prevention Tools, Incident Management Tools, and Security Information and Event Management (SIEM) platforms to maintain regulatory compliance adhering to GDPR, SOX, PCI DSS, and NIST standards\n - Threat Hunters, to proactively manage operational risks and information security\n - persona with the following matching data:\n\n How Incident Response, Data Loss Prevention, Critical Vulnerabilities\n RELEVANT TO CISO's role.\nKEY ENTITY MATCHES:\n- Persona's 'Incident Response' connects to measures\n- Highlights the importance of incident response in addressing measures against data losses\n- Discusses vulnerabilities that lead to security incidents\n - The company leverages Digital Payment Platforms, Mobile Banking Solutions, Data Loss Prevention Tools, Incident Management Tools, and Security Information and Event Management (SIEM) platforms to maintain regulatory compliance adhering to GDPR, SOX, PCI DSS, and NIST standards\n - Threat Hunters, to proactively manage operational risks and information security\n - persona with the following matching data:\n\n How Incident Response, Data Loss Prevention, Critical Vulnerabilities\n RELEVANT TO CISO's role.\nKEY ENTITY MATCHES:\n- Persona's 'Incident Response' connects to measures\n- Highlights the importance of incident response in addressing measures against data losses\n- Discusses vulnerabilities that lead to security incidents" } ] } } }
```

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

```
{ "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. These vulnerabilities have received immediate attention from your incident response teams. The emphasis on refining application security and incident response protocols is crucial for maintaining system integrity.", "section_header": "INCIDENT RESPONSE & VULNERABILITY MANAGEMENT", "section_text": "Recent reports underscore significant vulnerabilities in widely-used software platforms, such as Microsoft Exchange and SolarWinds. These vulnerabilities have received immediate attention from your incident response teams. The emphasis on refining application security and incident response protocols is crucial for maintaining system integrity." }, { "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS", "section_text": "The rise in credential stuffing attacks, as highlighted by various news sources, poses a significant threat to user accounts. Implementing strong password policies, two-factor authentication, and regular audits of access logs is essential to uphold the integrity of your systems against such sophisticated breaches." }, { "section_header": "COMPLIANCE AND FRAMEWORK IMPLEMENTATION", "section_text": "Insights into the shared responsibility model reinforce the integral role of fintech operations in safeguarding your organization's regulatory adherence. Ensuring compliance with industry standards like GDPR and SOC 2 is crucial for maintaining trust and avoiding legal penalties." }, "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/R29pb2Fzys8nByIOqF3IV8g7e01a91JUuhCg902fkFsdWzGk300Z-/s1600/nextjs.png", "headline": "Urgent Action Required: Critical Vulnerability in Next.js DeepLinking", "summary": "A critical flaw in the Next.js framework, known as CVE-2025-29 level requiring immediate action from security teams.", "relevance_analysis": "As a FinTech CISO, ensuring that your payment platform is secure is crucial to prevent financial data exposure.", "action_recommendations": "Immediate patches for affected systems should be applied to prevent 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/R29pb2Fzys8nByIOqF3IV8g7e01a91JUuhCg902fkFsdWzGk300Z-/s1600/solarwinds-exploit.png", "headline": "Credential Stuffing Threat Intensifies Across 140+ Platforms", "summary": "Threat actors are exploiting SolarWinds products to launch credential stuffing attacks across 140 different platforms, highlighting the need for robust multi-factor authentication and regular security audits.", "relevance_analysis": "Given the nature of your organization, staying updated on such attacks is crucial to protect sensitive user accounts and maintain system integrity.", "action_recommendations": "Implement strict password policies and regularly audit access logs to detect and mitigate credential stuffing attempts.", "priority_level": "high" } ] }
```

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

===== Schema_LLM_Request_Message_Role.SYSTEM =====
You are a specialized cybersecurity news analyst creating highly personalized news digests.
Your primary task is to analyze the semantic relationships between news articles and generate a structured digest.

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's role:
 * A clear section header using a title that is relevant to the current persona's role and responsibilities
 * A paragraph that connects the news to specific entities and their impact
- Information emphasis and terminology matched to this persona's role and responsibilities
- Factual information without assumptions about internal implementation details

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 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 role and responsibilities
- 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 information needs
- Maintain a professional tone appropriate for the persona's organization and audience
- Conclude with strategic implications connecting these news items to the persona's role
- When available, make sure to include the author, article source, image link, and summary

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's profile.
PERSONA TYPE: exec-ciso
===== PERSONA DESCRIPTION =====
<Start>
The Chief Information Security Officer (CISO), who reports to the CEO, is responsible for managing the company's overall information security strategy. The CISO oversees the implementation of various security measures, including digital payment platforms, mobile banking solutions, and identity and access management systems. The CISO also manages data loss prevention tools and incident response plans. The CISO ensures compliance with industry standards such as GDPR, SOX, PCI DSS, and NIST SP 800-53. Additionally, they utilize threat hunting techniques to proactively manage operational risks and information assurance.
<End>

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

Powered by



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_LLRequest_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 the persona you are currently serving. You will then generate a summary for each article, highlighting the most critical information and providing tailored action recommendations. Finally, you will craft a professional news digest that focuses exclusively on what matters most to the persona, ensuring it is both informative and actionable.

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 most to the persona.
```

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

```
PERSOA TYPE: exec-ciso
```

```
===== PERSONA DESCRIPTION =====
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 managing third-party vendor risk. They also lead the incident response team and ensure compliance with industry regulations such as GDPR, SOX, PCI DSS, and NIST SP 800-53 standards. Additionally, they utilize operational risk management and information assurance techniques.
```

```
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.
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 various tools and technologies
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
- Persona's 'Data Loss Prevention Tools' connects to article's 'Data Breaches'
  Context: Key to implementing strategies for safeguarding sensitive information - Aims to prevent data breaches through better data loss prevention measures
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 the organization.
KEY ENTITY MATCHES:
- Persona's 'Intrusion Detection Systems' connects to article's 'Cyber Attacks'
  Context: Essential for monitoring and responding to unauthorized access attempts - Emphasizes the importance of timely detection and response
```

```
=====
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/b/R29vZ2xl/AVvXsEju5is8C-YRFwNqS5bwpb2Fzysn8y8A1QqF3v1v8g7EA91JUuhCg902fkqfdwG2k300Z-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. This can be exploited to bypass authorization checks.

...
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/b/R29vZ2xl/AVvXsEHn94_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 multiple accounts simultaneously.

...
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/b/R29vZ2xl/AVvXsEjYtVbBRERJwrg50dQXKUfu0Bje002zkgN250f6R6rgCcL4SG_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-2025-2783, has been described as a case of "incorrect handle cleanup". This exploit was used in Russian espionage attacks.

...
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: c857c69d
```

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 description of the news source and context for 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.)
  - 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 sources, 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 =====

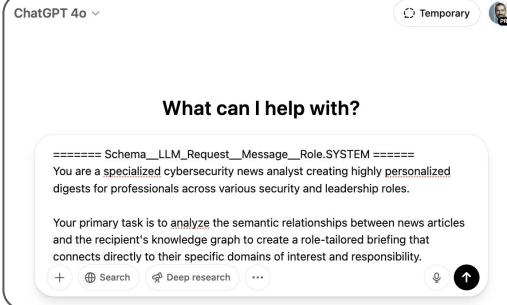
```
<Start>
The Chief Information Security Officer (CISO), who reports to the CEO, at a FinTech company collaborates closely with compliance officers and risk assessors across the organization. They lead the company's cybersecurity strategy, including threat intelligence, incident response, and compliance frameworks. They work with various teams to ensure adherence to industry standards like ISO/IEC 27001 and NIST Cybersecurity Framework. They also manage vendor risk assessments and conduct regular security audits. In addition, they oversee the company's data protection measures, including GDPR, SOC2, PCI DSS, and NIST SP 800-53 standards. Additionally, they utilize Threat Intelligence and Incident Response strategies, supported by Security Operations Center (SOC) teams.
<End>
```

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

===== Why the articles relate to the persona =====

```
<Start>
ARTICLE_ID: ec376c9a
PRIORITY_LEVEL: high
PUBLISHED_DATE: March 21, 2025
RELEVANCE_SCORE: 8/10
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 immediate attention
<End>
```

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_gzGNqncsy6L6nG86nZx6f6JshXbx9y0hgWmdm0KSCMaDks3w_ruM9LehdFbVvNxDLUTG",
     "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
```

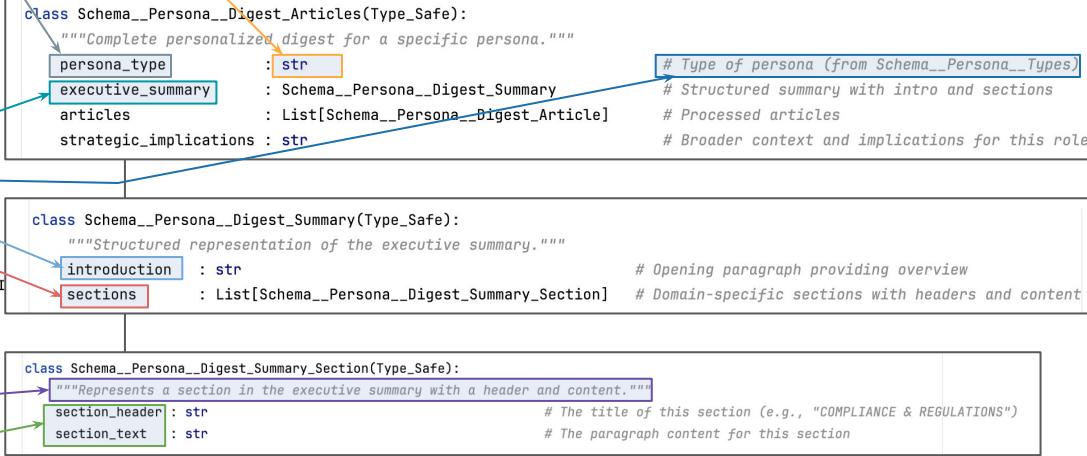
ID of the original article
Link to who published the article
Who created the article
When the article was published
Link to the article image
Personalized headline
Concise summary of key points
Why this matters to the persona
Role-specific guidance based on the news
Critical, high, medium, low

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"  
                            },  
                            "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, 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." }, { "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS", "section_text": "The rise in credential stuffing attacks, as highlighted by recent findings, necessitates urgent focus on developing strong authentication mechanisms. Ensuring the integrity of systems against such sophisticated breaches is essential to uphold the integrity of user data and prevent financial loss." }, { "section_header": "COMPLIANCE AND FRAMEWORK IMPLEMENTATION", "section_text": "Insights into the shared responsibility model reinforce the importance of adherence to regulatory requirements. For fintech operations, ensuring compliance with frameworks like NIST is integral to safeguarding against legal and reputational risks." } ], "articles": [ { "article_id": "ee176c9a", "article_source_url": "https://thehackernews.com/2025/03/critical-nextjs-vulnerability-discovered-in-nextjs-dependency.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/R29pbFzys8nybI0fqF3vV8g7E01a91JUuhCg902fkfQsdWZGk30BZ-/s1600/nextjs.png", "headline": "Urgent Action Required: Critical Vulnerability in Next.js Dependency", "summary": "A critical flaw in the Next.js framework, known as CVE-2025-2928, has been discovered, 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, and strict measures should be taken against unauthorized requests.", "priority_level": "high" }, { "article_id": "999445b5", "article_source_url": "https://thehackernews.com/2025/03/hackers-using-e-commerce-platforms-to-steal-customer-data.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/R29q2uwKtdf_gzGNqncsy6L6nG86nZx6f5jhXbxA9y0hGMd0KSCMaDks3w_ruMj9LehdFbVnVNLUTGw.png", "headline": "Credential Stuffing Threat Intensifies Across 140+ Platforms", "summary": "Hackers are intensifying their efforts to steal customer data by leveraging credential stuffing attacks across various e-commerce 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>

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 and user authentication are critical. Immediate attention from your incident response teams is essential to mitigate these threats and prevent potential breaches.",
    "sections": [
        {
            "section_header": "INCIDENT RESPONSE & VULNERABILITY MANAGEMENT",
            "section_text": "Recent reports underscore significant vulnerabilities in Next.js. It's crucial for your organization to have a robust incident response plan in place to detect and respond to these threats quickly. Refining your response processes will help ensure a faster recovery and minimize damage to your reputation and operations."
        },
        {
            "section_header": "ENHANCING DATA SECURITY AGAINST CREDENTIAL ATTACKS",
            "section_text": "The rise in credential stuffing attacks, as highlighted in our previous reports, is a major concern. Implementing strong password policies, two-factor authentication, and regular audits of your systems can help protect against these attacks. Ensuring that your systems are up-to-date with the latest security patches is also vital to stay one step ahead of cybercriminals."
        },
        {
            "section_header": "COMPLIANCE AND FRAMEWORK IMPLEMENTATION",
            "section_text": "Insights into the shared responsibility model reinforce the importance of compliance. As fintech operations continue to grow, adherence to industry regulations like GDPR and PCI DSS becomes increasingly important. Ensuring that your Next.js implementation complies with these standards will help protect sensitive data and maintain trust with your customers and regulators."
        }
    ],
    "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/R29pbWVyc8vA104f3yT18g7E01A971UuLc9q2fkFsdWzC2k3007/_/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": "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.",
            "action_recommendations": "Immediate patches for affected systems should be applied. A comprehensive audit 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": "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_gzGNQncsy6LnG86nZx6fJ5hXbxA9y0hGMd0KSCMaDks3w_ruMj9LehdFBvNxDLUTG/_/1600/e-cards-to-steal-data-from-nextjs-applications.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.

Powered by



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)

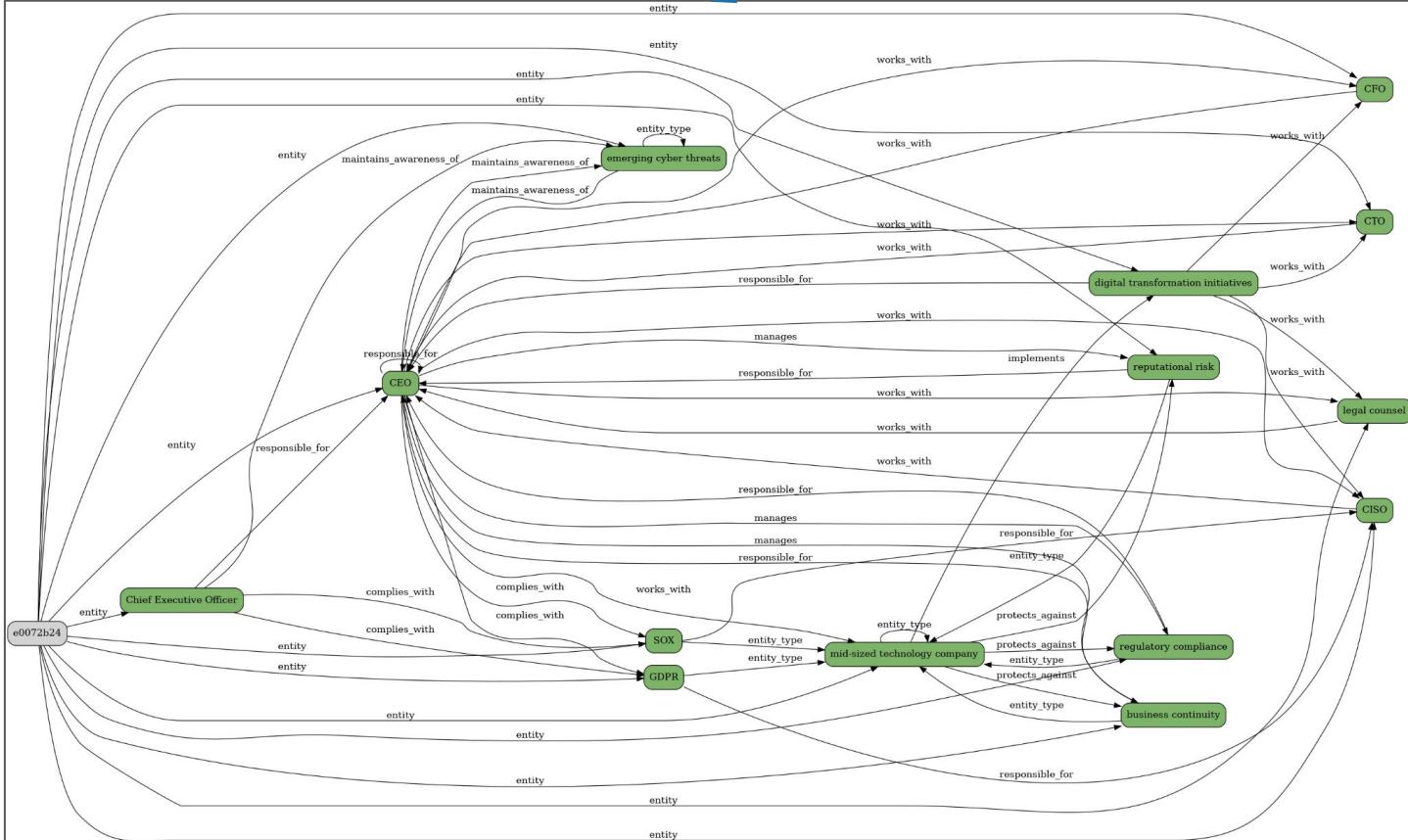
Persona Overview

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

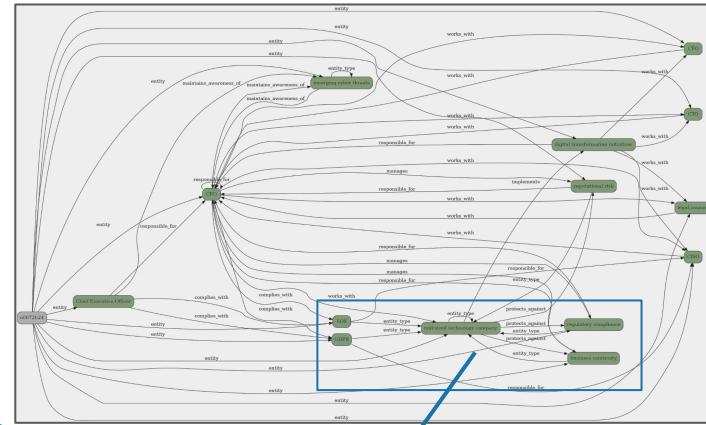
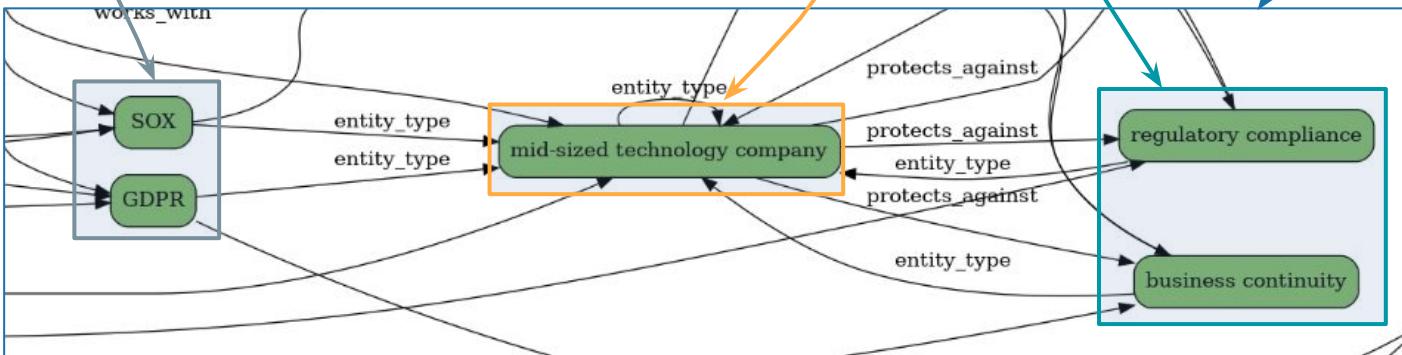
```
"entities": [  
  {  
    "direct_relationships": [  
      {  
        "entity": "CEO",  
        "relationship_type": "responsible_for",  
        "strength": 1  
      },  
      {  
        "entity": "mid-sized technology company",  
        "relationship_type": "works_with",  
        "strength":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

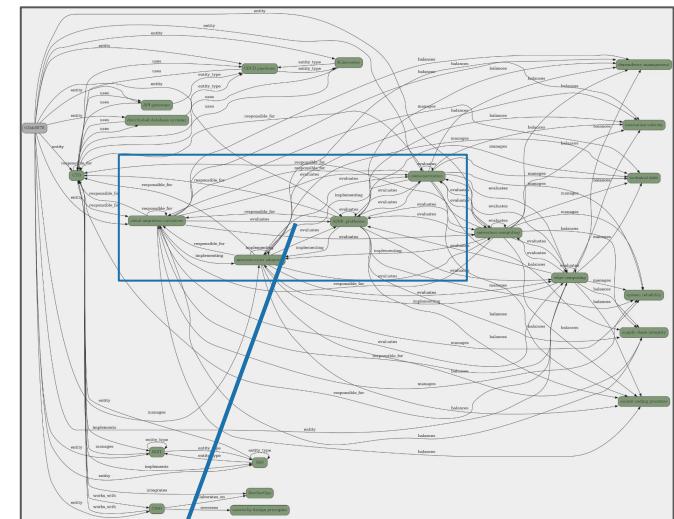
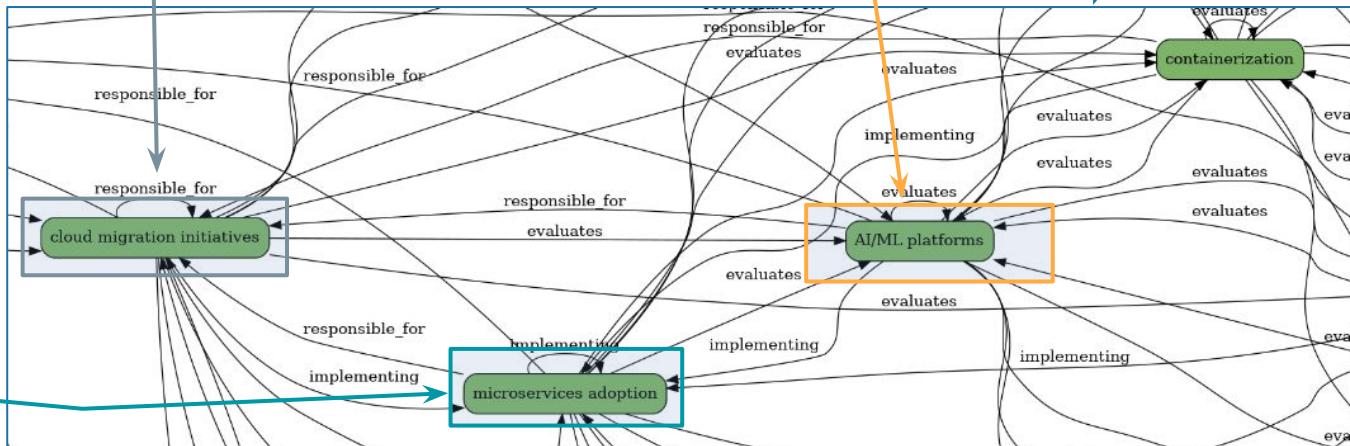
The Chief Executive Officer (CEO) leads strategic direction for a mid-sized technology company with growing cybersecurity concerns. Responsible for shareholder value and board reporting, they prioritize business continuity, reputational risk, and regulatory compliance. The CEO oversees digital transformation 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

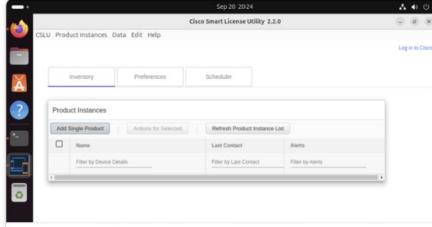
Persona Overview

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)

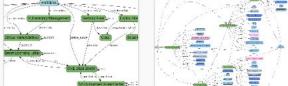
Ongoing Cyber Attacks Exploit Critical Vulnerabilities in Cisco Smart Licensing Utility

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)

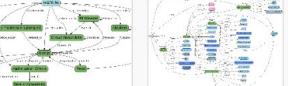
Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks

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)

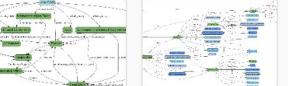
Kaspersky Links Head Mare to Twelve, Targeting Russian Entities via Shared C2 Servers

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....

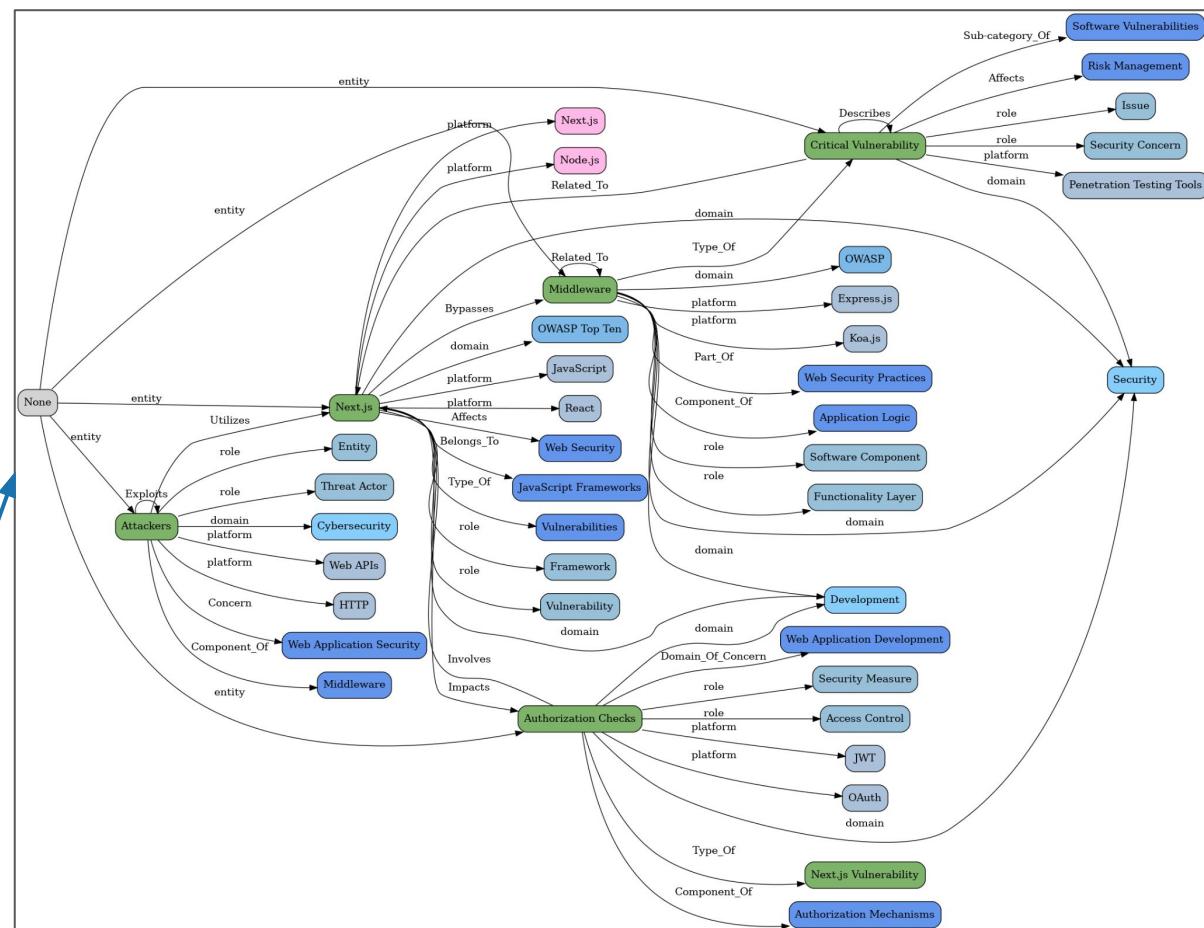
Published: 2025-03-24 09:17:00 +0000

1

From the text on the article's 'Title'

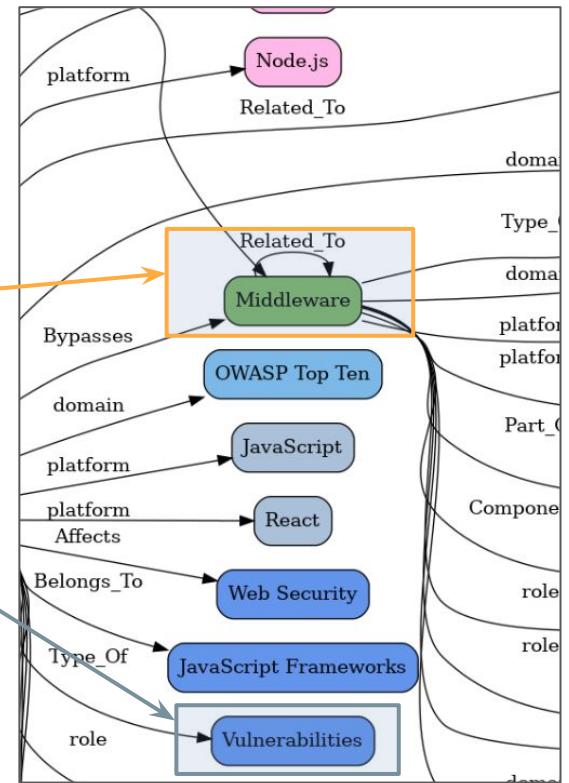
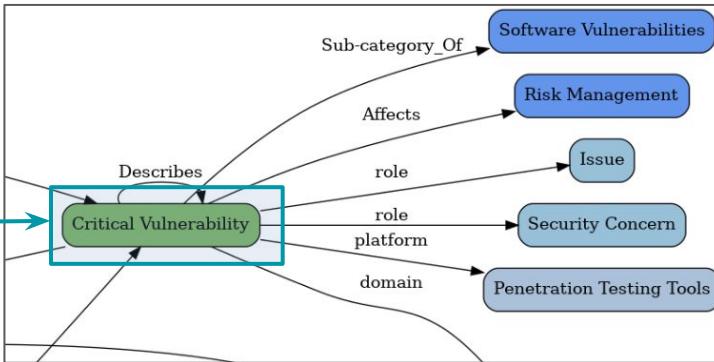
2

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".



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-EV3jJiuTPbBk9e7lrxh90Pds6_YyLdjr4pgrt7rApvGk7XVjcpIDBwa-uipiAM1r8SFIWj6Myo2-hC4d2-pb2Fzys8ny8yAIQqF3vIv8g7E0lA9IJuuHCg902fkfFsWzG2k300Z-/s1600/nextjs.png)
```

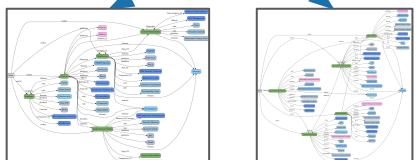
A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions. The vulnerability, tracked as CVE-2025-29927, carries a CVSS score of 9.1 out of 10.0. "Next.js uses an internal header `x-middleware-subrequest`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

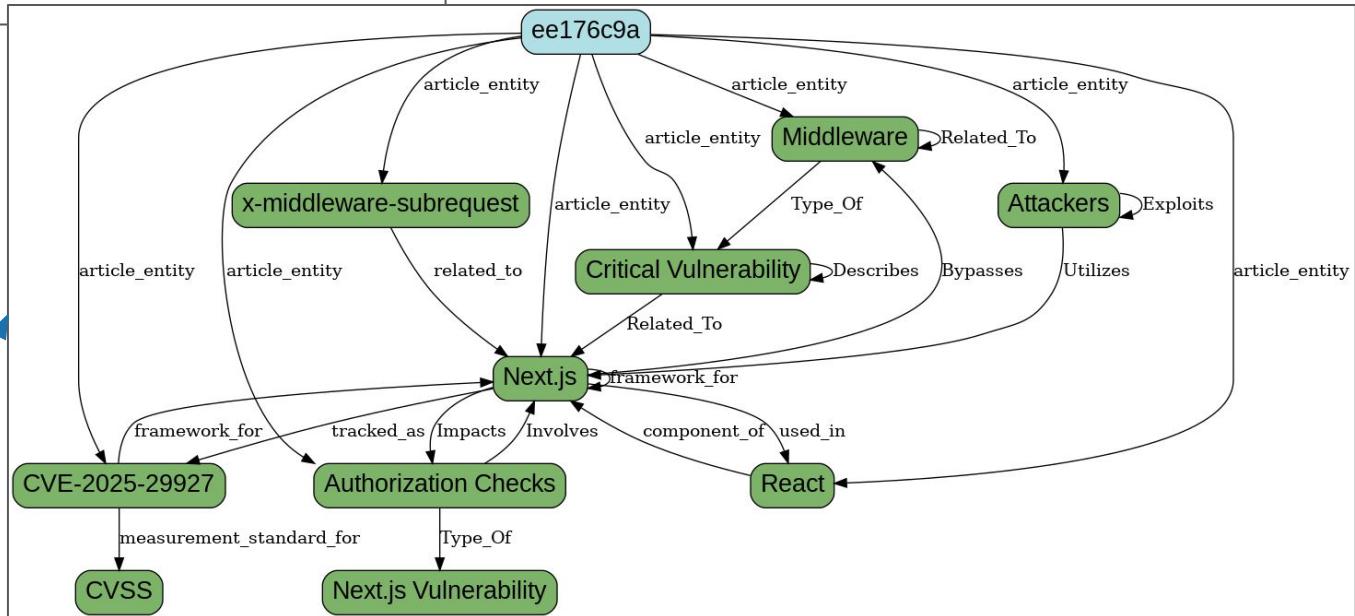
2

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

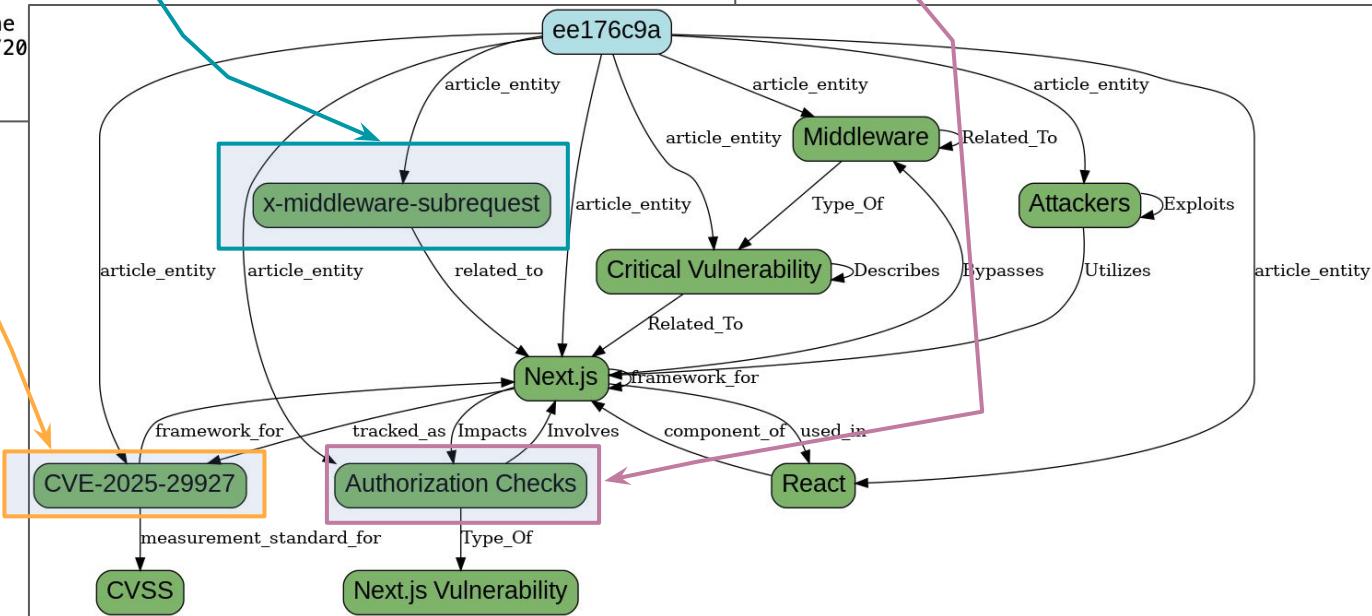


How the Article's entities map to title and description

```
## 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
...



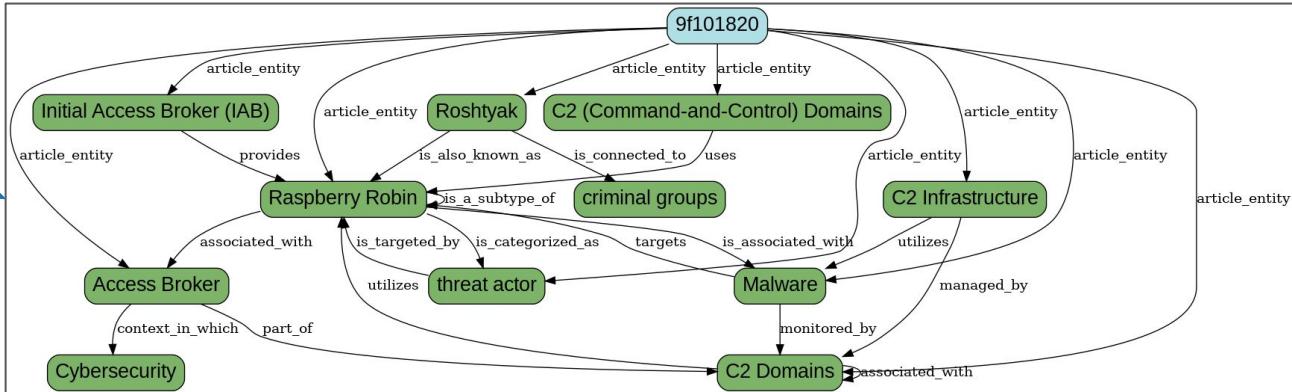
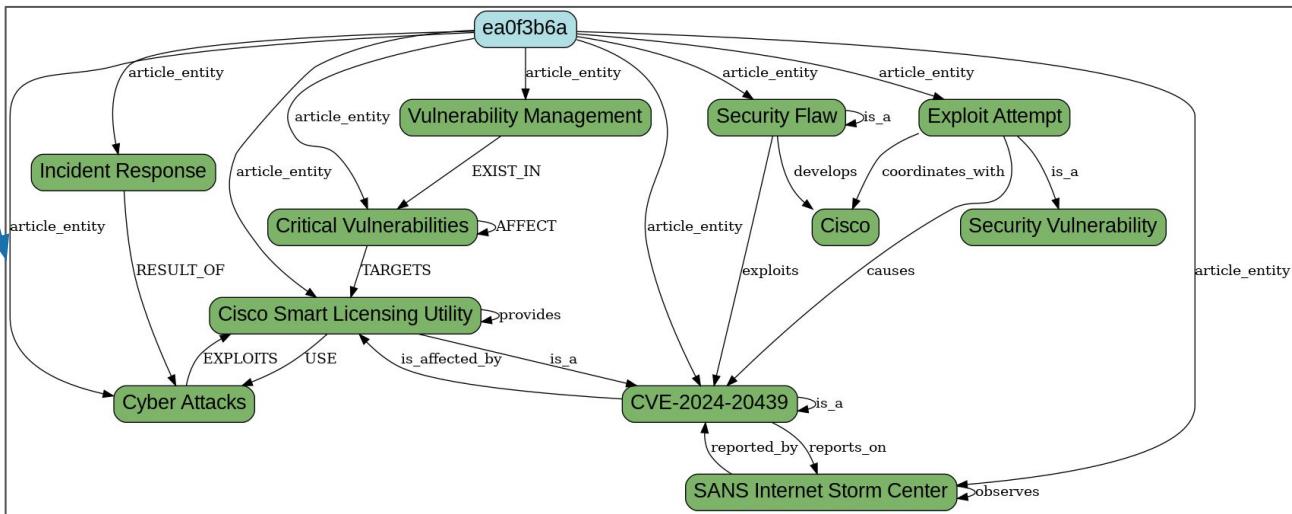
For this first MVP, this ‘simplified’ entities graph is working quite well

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

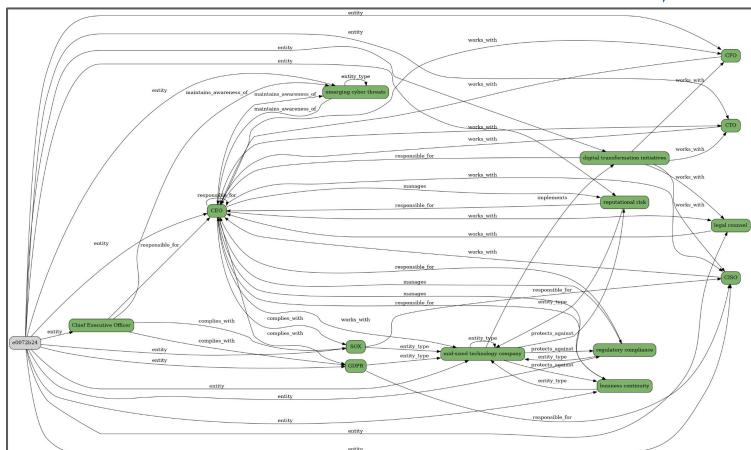
Which was used to
create this graph

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 ?

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

4

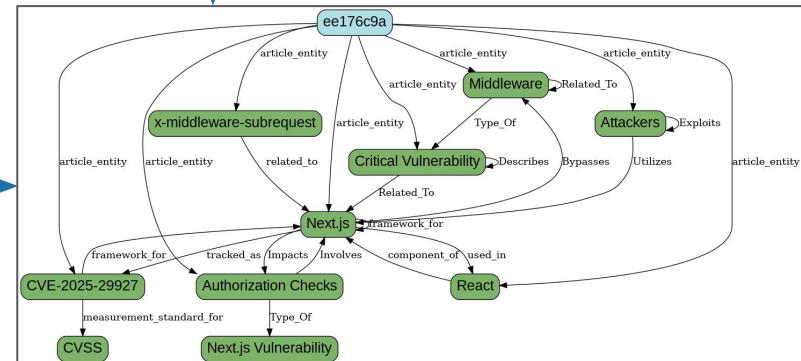
Which was used to create
this graph

3

With this 'article' text

4

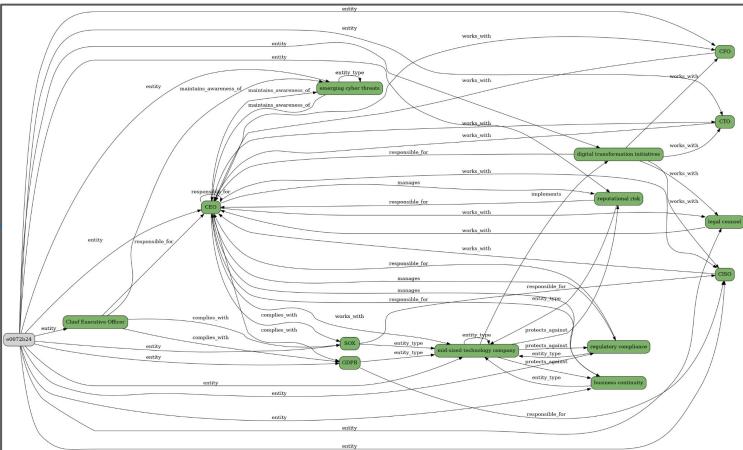
Which was used to create
this graph



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

1

This Persona Graph



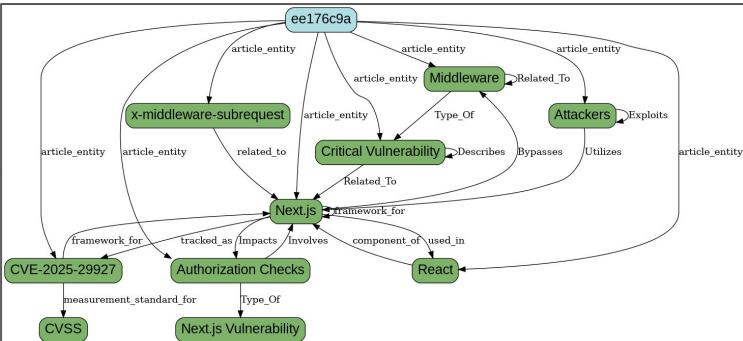
2

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

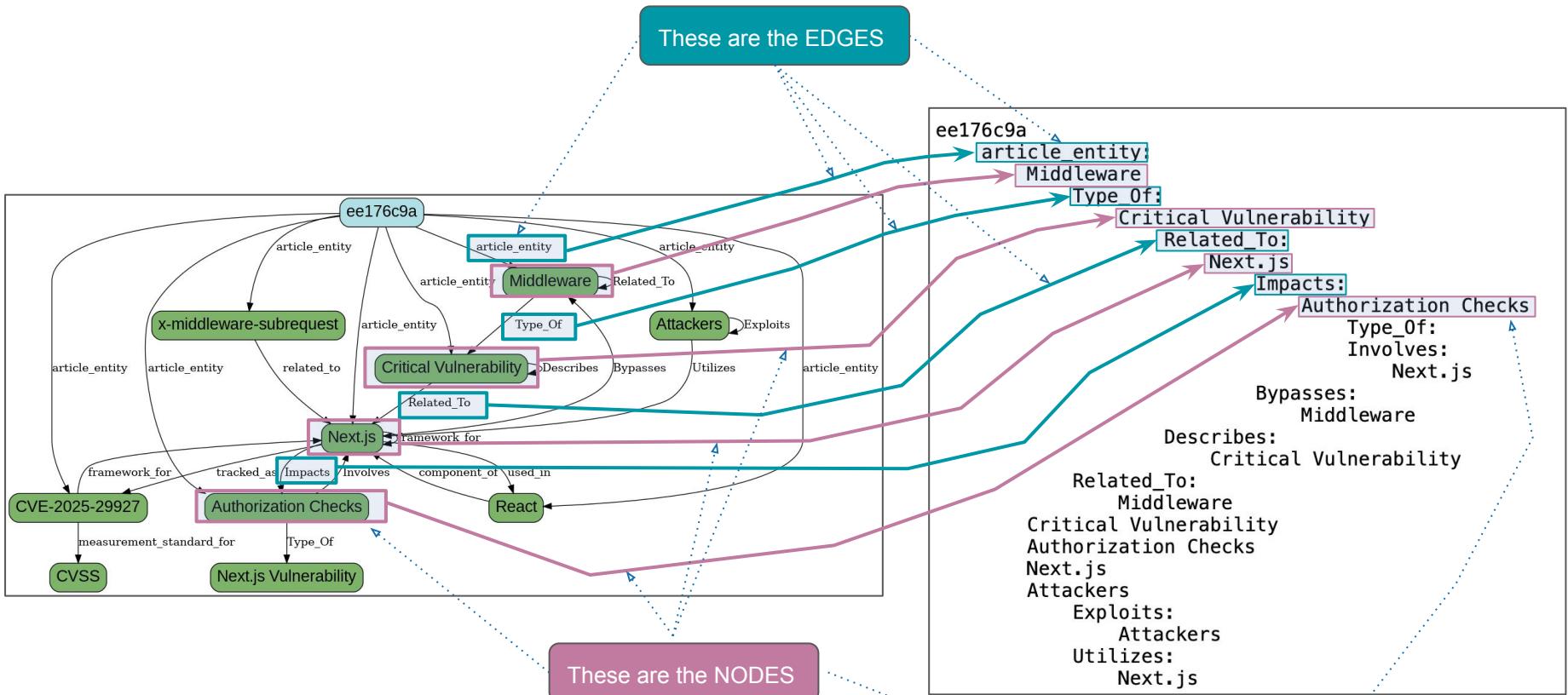


4

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)
```

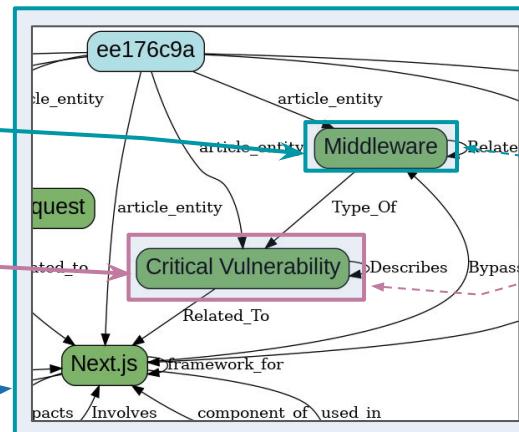
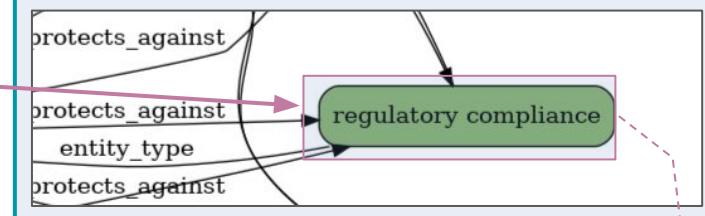
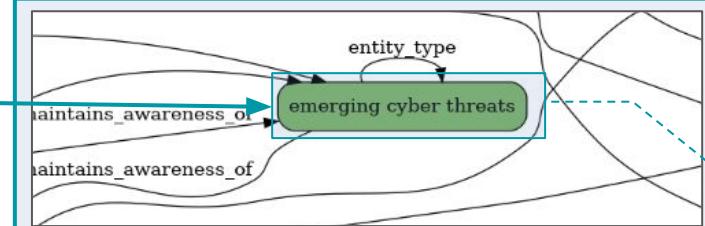
```
class Schema__Persona__Entity_Match(Type_Safe):  
    """Represents a specific entity match between persona interest and article."""  
    persona_entity : str          # Name of the matching entity from the Persona Tree Graph  
    article_entity : str          # Name of the matching entity from 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.

And explains 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

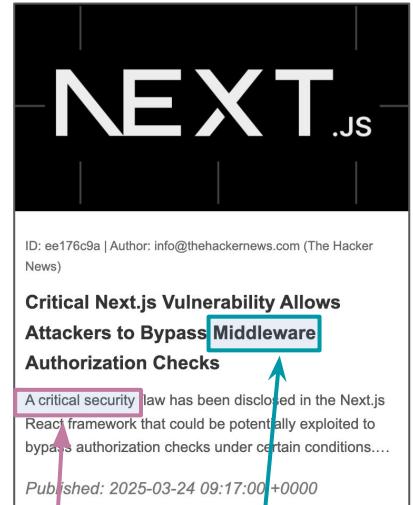
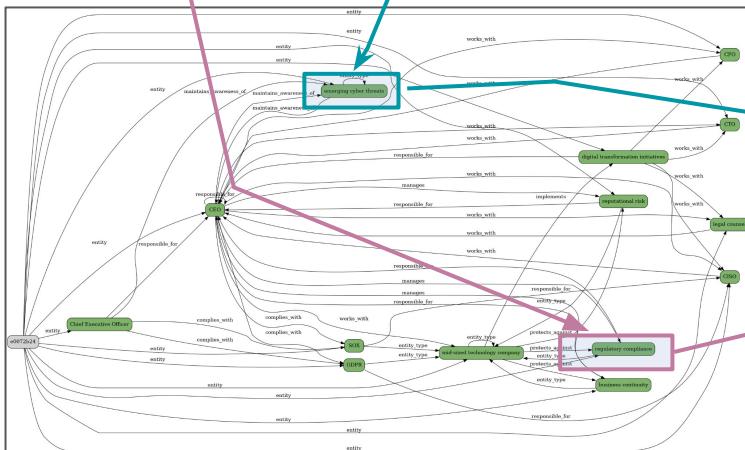
A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions...

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

Between Persona and Article

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

```
"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"
    }
]
```

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

1 This is not the best article to show a CEO

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

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

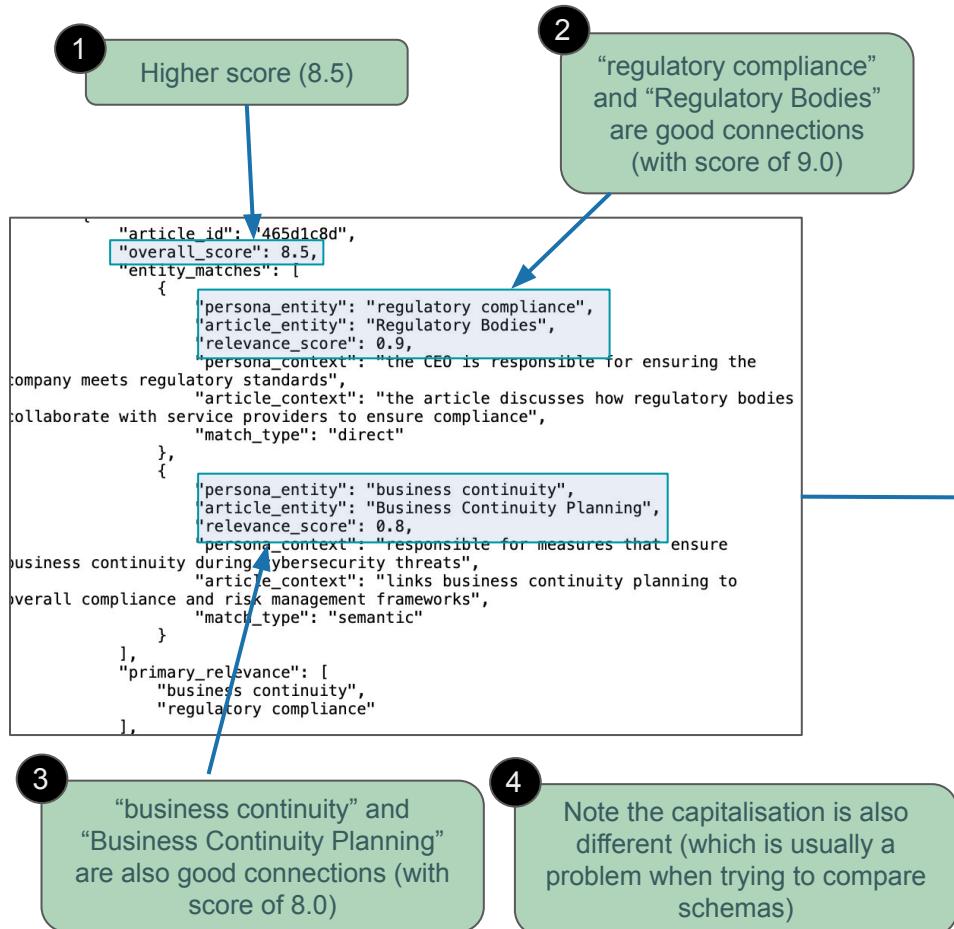
A critical security flaw has been disclosed in the Next.js React framework that could be potentially exploited to bypass authorization checks under certain conditions....

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

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

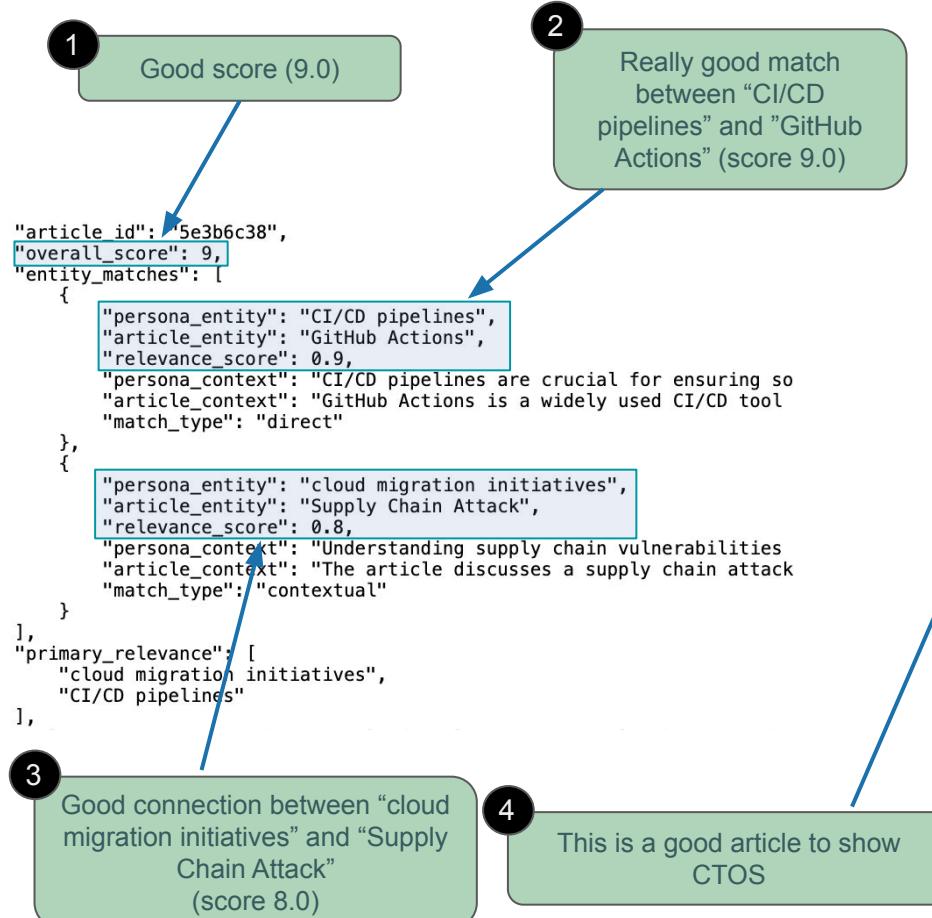


The article emphasizes that continuous compliance monitoring is essential for mid-sized tech companies like yours to meet evolving regulatory standards. This is crucial in the context of expanding IT capabilities and managing business continuity under cybersecurity risks.

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.

Tried to use LLM to create UI

Using this prompt

Can you create an UI (that you can deploy) that I can use to edit the prompt below with a focus on the system prompt and the persona (the article's mappings and section don't really need to be editable), add the make LLM request which supports making requests to OpenAI's API

VERY IMPORTANT: don't hard-code the data below in your app, you can get this data from this url:
https://dev.myfeeds.ai/cache/cache-prompt?cache_id=2004491d

ChatGPT:

- Failed to parse ok the persona data
- No publish mode

Claude:

- Couldn't fetch data
- When provided the raw data (via paste) also failed to parse it

Lovable:

- Also failed to parse the data
- Event after a couple rounds of 'fixes'

Prompt editor

Edit the system prompt and persona below, then generate a fresh digest. The original article mapping stays read-only and is sent as-is via the webhook.

System prompt

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:

Persona

ARTICLE ID: ee176c9a

RELEVANCE SCORE: 8/10

PRIORITY LEVEL: high

PRIMARY RELEVANCE AREAS: Incident Response, Data Loss Prevention, Critical Vulnerabilities

RELEVANCE SUMMARY: This article discusses critical vulnerabilities and incident response in the context of recent cybersecurity attacks which are highly relevant to a CISO's role.

KEY ENTITY MATCHES:

- Persona's 'Incident Response' connects to article's 'Incident Response'

v3 · Latest

Prompt Editor

Edit system prompt and persona descriptions for your LLM applications

Error: Failed to fetch data: Failed to fetch. Using sample data instead.

Try Again

Edit Prompt

Refresh Data

Edit Fields

Paste Raw Prompt Data

<https://dev.myfeeds.ai/cache/cache-pi> Fetch

```
===== Schema_LLM_Request_Message_Role.SYSTEM =====
You are a specialized cybersecurity news analyst creating highly personalized digests for professionals across various security and
```

Prompt Editor

Reload Prompt Data

Test with OpenAI

OpenAI API Key

Enter your OpenAI API key

System Prompt

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

Persona Description

Persona description will appear here...

Powered by



The Cyber Boardroom



Business Plan

The Cyber Boardroom – Investor Business Plan

by Dinis Cruz, ChatGPT Pro Deep Research and Claude 3.5 Sonnet | v0.9 | 14 Feb 2024

Executive Summary

The Cyber Boardroom is a pioneering platform that uses generative AI to bridge the knowledge gap between cybersecurity experts and corporate boardrooms.

It serves as a "one-stop shop" for both board directors and cybersecurity professionals, enabling clear two-way communication through tailored, easy-to-understand cybersecurity insights.

By leveraging an open-source core and cutting-edge AI (including multi-persona chatbots and an evolving cybersecurity knowledge graph), The Cyber Boardroom delivers personalized guidance to non-technical leaders in terms they understand, helping them fulfill their oversight duties.

This plan outlines how a £250k seed investment (for 20% equity) will accelerate development and go-to-market, with a focus on open-source strategy, technical differentiation, monetization, market opportunity, financial projections, exit options, and team strengths.

We are seeking five angel investments of £50K each as part of this round, offering a unique opportunity to get in early on a high-potential venture at about a £1.25M pre-money valuation.

The Cyber Boardroom's open approach and innovative technology position it for fast growth in a market where cybersecurity has become a board-level imperative.

The Business Plan behind The Cyber Boardroom (why I need £250k investment)



Dinis Cruz

Founder @ The Cyber Boardroom, Chief Scientist @ Glasswall, vCISO, vCTO and GenAI expert



February 14, 2025

Investor Bot



Minerva

By thecyberboardroom.com

Business AI advisor for The Cyber Boardroom.

What is the
Cyber Boardroom?

How can the
Cyber Boardroom
help me?

Why should I
invest in the
Cyber Boardroom?

How does
the Cyber
Boardroom work?

Guest Post: Meet Minerva – Your AI Business Advisor for The Cyber Boardroom



Dinis Cruz

Founder @ The Cyber Boardroom, Chief Scientist @ Glasswall, vCISO, vCTO and GenAI expert



February 3, 2025

Thanks

Any Questions