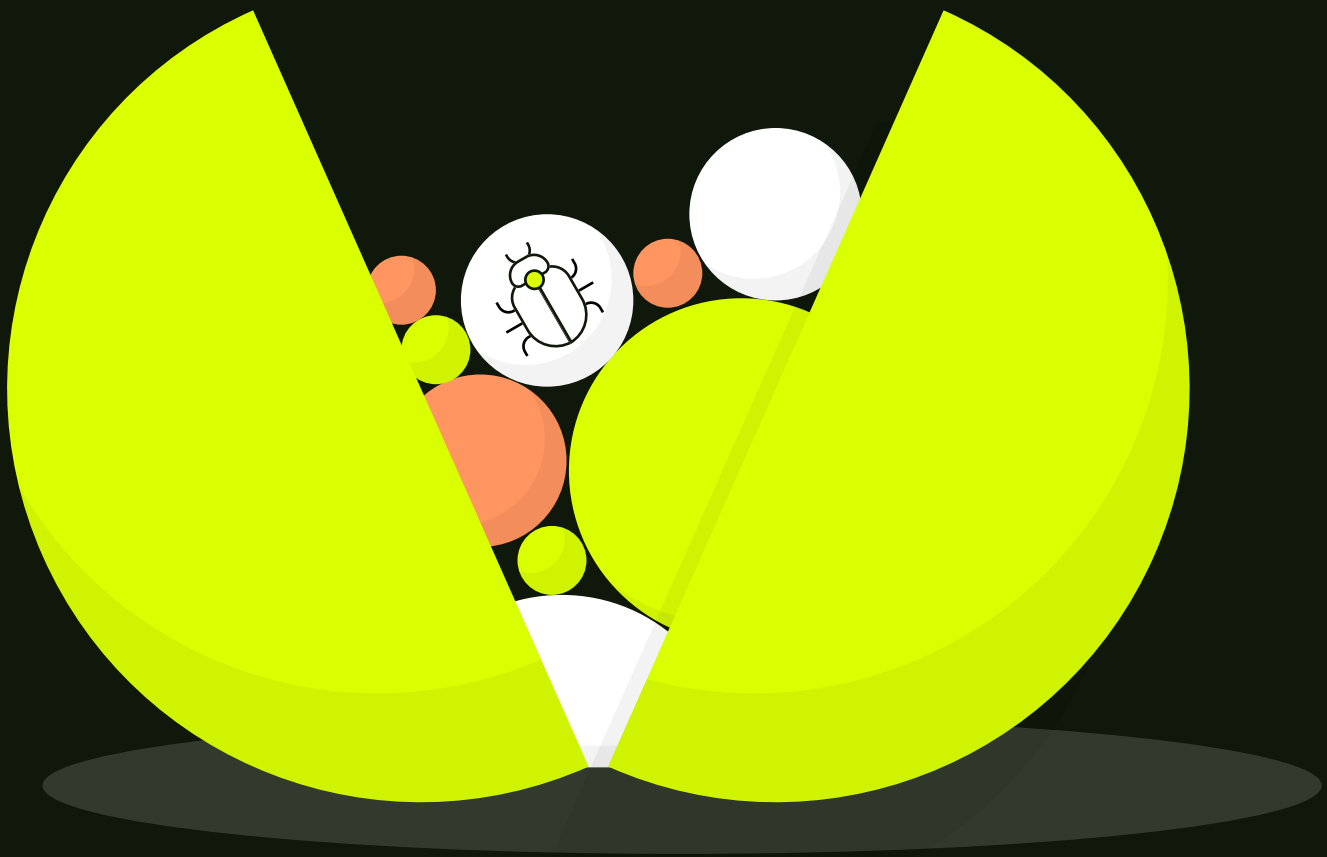
sweet.

Sweet Security
Runtime Vulnerability Management



www.sweet.security

Security teams receive an excessive number of vulnerability reports with no clear way to determine their actual risk. Many vulnerabilities lack prioritization, leading to wasted efforts on issues that may not be exploitable. Without runtime context, teams struggle to differentiate between theoretical risks and real threats, slowing down remediation efforts and diverting focus from meaningful security improvements.

Not All Vulnerabilities Are Created Equal

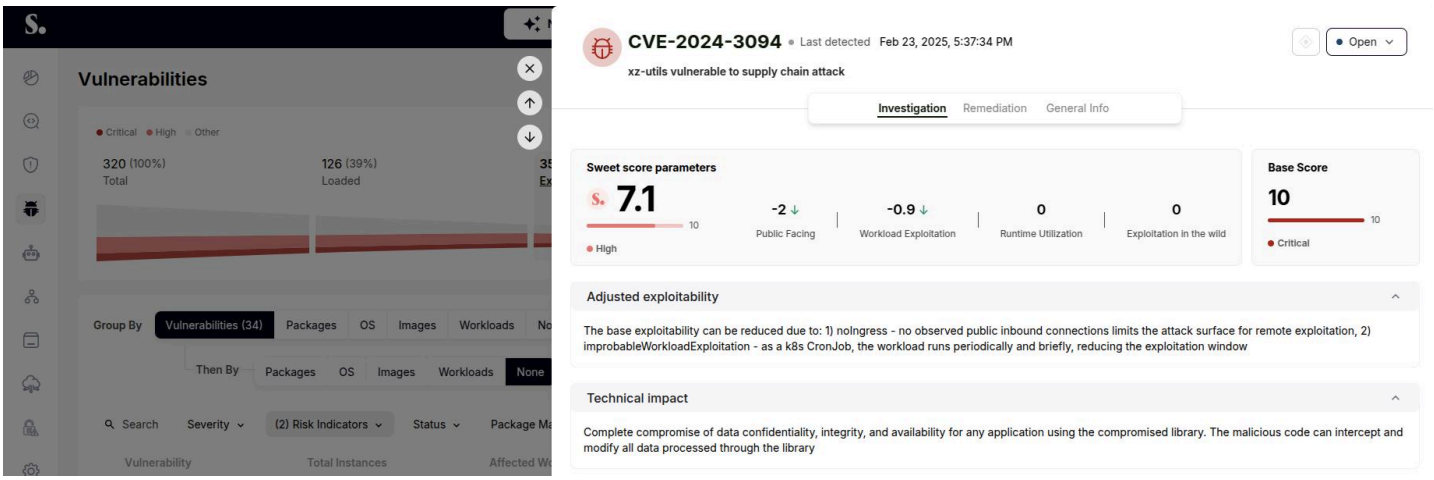
Even 2 public-facing vulnerabilities may not pose the same risk level. For example, a privilege escalation vulnerability with an inbound connection may not be as crucial as a RCE with an active inbound. Understanding the mechanism of the vulnerability and the exploitation requirements (beyond just the severity score) makes all the difference.

Vulnerability Management Lacks Context

Current vulnerability management solutions, primarily backed by scanners rather than runtime insights, generate overwhelming volumes of security issues. As application development continues daily, security teams must manually investigate new alerts to determine their actual risk.

Introducing Sweet Security's Runtime & LLM-Powered Vulnerability Management

Sweet Security revolutionizes vulnerability management by leveraging runtime insights and LLM-powered analysis to assess and prioritize vulnerabilities based on the behavior and knowledge of the vulnerability itself. By evaluating vulnerabilities in the context of the environment they reside in and the potential business impact, security teams can focus on what truly matters. This combination of runtime insights and LLM-powered analysis ensures that vulnerabilities are not only identified but are effectively prioritized based on their actual risk and impact to the business.



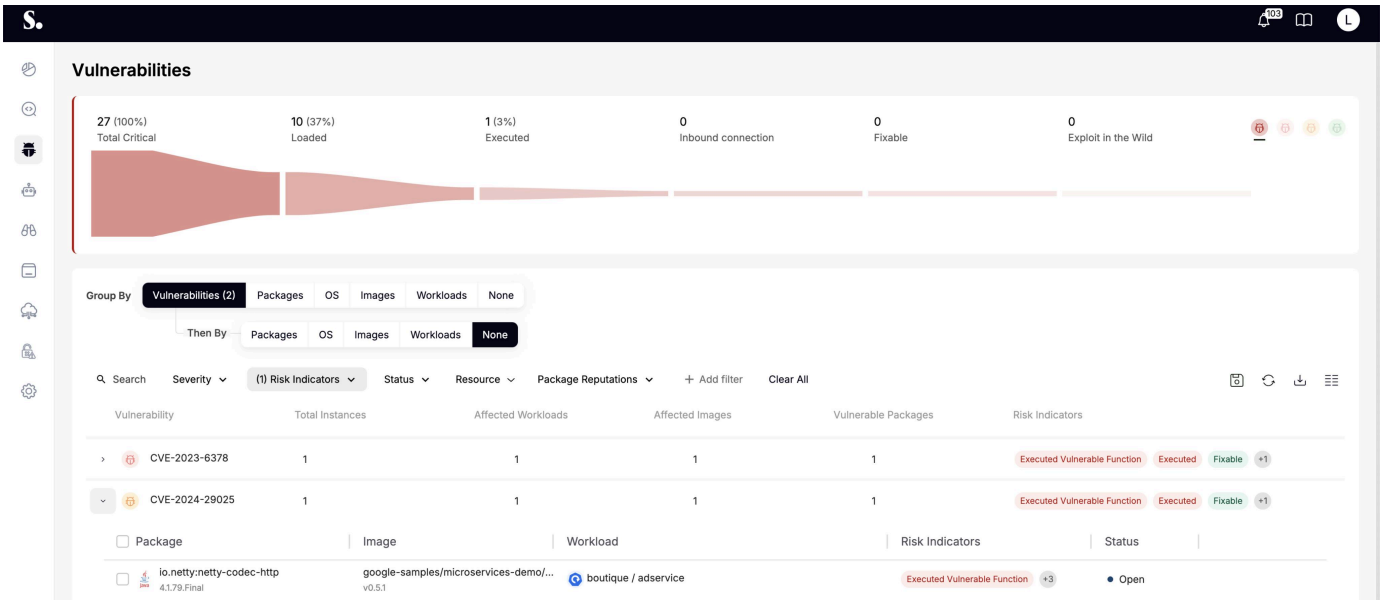
How Sweet's LLM Enhances Vulnerability Management:

- **External Knowledge Integration** – Incorporates additional data sources for enhanced analysis, enabling a more comprehensive view of potential risks.
- **Reasoning & Risk Assessment** – Uses domain expertise to evaluate the true risk of vulnerabilities, factoring in runtime behaviors and the potential impact on the environment.
- **Automated Prioritization** – Reduces manual effort by streamlining risk evaluation, ensuring security teams focus on the vulnerabilities that present the highest real-world risk.

Key Features of Sweet Security's Vulnerability Management

1. Prioritize CVEs Based on Runtime Insights & LLM Analysis

Attackers can only exploit vulnerabilities that are reachable. Without runtime-driven reachability analysis, security teams waste time addressing issues that pose no real risk. With Sweet, you can evaluate vulnerabilities based on runtime factors, including whether the vulnerability is loaded into memory, actively executed, its exploitability potential, and whether it is public-facing. In addition, the LLM will take the behavior of the vulnerability and its implications within the specific environment into consideration.



2. Proactively Identify and Mitigate Harmful Packages

Sweet's Package Reputation Analysis enables security teams to identify and mitigate risks associated with third-party dependencies before exploitation. It also strengthens defenses against supply chain attacks—even before a CVE is published.

3. Pinpoint Executed Vulnerable Functions

Sweet's advanced AI-powered detection identifies specific vulnerable functions that are actually executed in runtime. Unlike traditional scanners, which flag all vulnerabilities, Sweet pinpoints those that truly matter by analyzing runtime behavior.

4. List Vulnerabilities as a SBOM

Sweet provides a comprehensive package inventory that includes both vulnerable and non-vulnerable components. This lets teams view associated vulnerabilities, risk indicators, and package reputation, and ensures compliance with a detailed SBOM export.

5. Identify Vulnerabilities in Images

Sweet's image ad-hoc scanning extends vulnerability management from the runtime phase to the registry phases. Sweet supports multiple registries, including ECR, GCR, ACR, Docker.io, and more. With this feature, teams can identify vulnerabilities in an images before it enters the CI/CD pipeline. In addition, they can verify that patched images are free of known vulnerabilities before pushing them to production.

The Sweet Security Advantage

Sweet Security's vulnerability management solution is powered by runtime insights and LLM-driven intelligence—ensuring security teams can focus on the vulnerabilities that truly matter while reducing false positives and improving remediation efficiency. With Sweet, organizations can move beyond scanner-driven overload and adopt a proactive, risk-based approach to vulnerability management.

About Sweet Security

Sweet Security is a Runtime-Powered CNAPP designed to ensure comprehensive security across cloud environments. Utilizing lightweight eBPF-based sensors, Sweet specializes in real-time security that spans cloud infrastructure, workloads, and applications. Built to minimize overhead, streamline investigations, and deliver high accuracy with low false positives, Sweet provides comprehensive runtime context that empowers security teams to respond to threats faster and more effectively.