Improving The Nation's Cybersecurity Takes the Right Tools and Partners

THE CHALLENGE

Security vulnerabilities in critical applications in every industry from financial institutions to manufacturing, have been a problem for years and are now being thrust into the spotlight as a result of Executive Order 14028, Improving the Nation's Cybersecurity. Improving national security and the security of critical infrastructure starts with understanding exactly what's running in these applications and minimizing the exploitable attack surface.

Network-connected applications are exposed to significant vulnerabilities that can be exploited to cause significant interruption to essential services and even affect public safety. While targeted attacks on virtual institutions such as retail and banking, have been going on for decades, they have been largely focused on stealing information. Newer attacks focused on America's essential physical infrastructure and third party ecosystems offer attackers a better return on investment as they cause severe disruption of essential services and have outsized downstream impacts. These targets include applications supporting manufacturing, energy, surface transportation, logistics, agriculture, food and beverage.

Decades ago, W. Edwards Deming taught automobile manufacturers the critical importance of building quality into their products by more effectively managing suppliers, sourcing parts, and tracking the precise location of every part assembled in every vehicle. Today, these same lessons are being applied to optimize the security of modern software supply chains.

Executive Order 14028 states that by February 6, 2022, companies will be required to:

- Produce a software bill of materials (SBOM)
- Ensure Integrity of code via automated tools
- Check for and remediate potential vulnerabilities via an automated tool
- Maintain an up-to-date provenance of all 3rd party and proprietary code running in an application

As essential services use a complex web of interconnected systems and applications it is critical that America's essential organizations figure out a way to leverage Deming's insights and apply them to the quality and safety of their applications.

Amid the many challenges for America's critical infrastructure is managing escalating costs without compromising reliability of services and risks to public services and safety.

THE SOLUTION

NCC Group and Rezilion have partnered to help America quickly identify and prioritize mitigation of the risks that pose the greatest threat to essential services and public safety.

By doing so, we help organizations meet Executive Order 14028 which forms the foundation upon which organizations' necessary security activities are built. The two leading and key requirements revolve around risk analysis and risk management processes that become the baseline for America to effectively source and track code that composes their key applications.

RISK ANALYSIS

NCC Group and Rezilion provide an accurate assessment of the potential risks and vulnerabilities associated with applications currently in use. We determine which vulnerabilities associated with the application and its infrastructure present a legitimate risk based on their exploitability. Rezilion highlights which vulnerabilities are exploitable and which are not.

RISK MANAGEMENT

NCC Group and Rezilion help to minimize attack surface by prioritizing which vulnerabilities need to be addressed to make the biggest impact on risk reduction and identifying which resources that present risk, can be removed without impact to the underlying service functionality. Creating a smaller attack surface and prioritizing mitigation efforts based on risk helps IT resources efficiently and securely deliver services to their customers.

REMEDIATION

NCC Group and Rezilion provide key services to remediate the vulnerabilities that need to be addressed to make the biggest impact on risk reduction. Rezilion provides package level details that include the number and average severity of exploitable vulnerabilities present, allowing teams to focus their efforts on the highest impact patches.

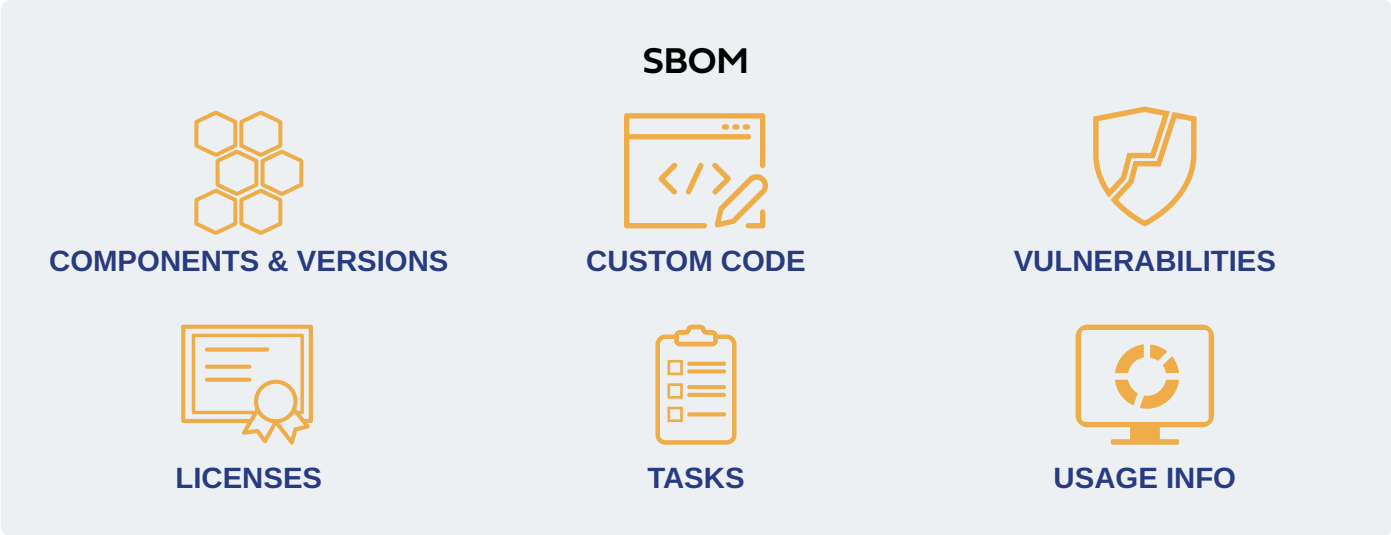
BUSINESS BENEFITS

NCC Group and Rezilion enable effortlessly secure delivery of mission-critical applications with minimal risk — improving organizational security posture while allowing America's critical infrastructure operators to focus on keeping America running smoothly.

With Rezilion, the volume and associated cost of vulnerabilities that must be mitigated in every release are dramatically reduced, and the ones that need to be addressed are remediated.

A vulnerability is only as dangerous as the threat exploiting it. The cyber security industry has been unnecessarily exaggerating the number of vulnerabilities security teams must address, which has significant ramifications to the cloud security landscape. By partnering with NCC Group and Rezilion, critical infrastructure operators receive a significant return on their investment by automating away time consuming manual processes and also benefiting from trusted advisors with years of experience in remediating exploitable vulnerabilities.

Rezilion also applies the philosophy of automating away time consuming manual processes to the creation of the SBOM that is the foundation of Executive Order 14028's security requirements. Tools such as Software Composition Analysis (SCA) are useful in populating a static OSS BOM, but they lack visibility into homegrown code, host-operating-systems and commercial 3rd party products deployed in production. Rezilion leverages patented Workload



Composition Analysis to automatically yield a comprehensive model of the host, container, and application that updates every time new code is pushed.

Workload Composition Analysis is akin to genome mapping for code. In the world of Genomics, Genome mapping is a detailed analysis of where each piece of your genetic code came from, what its function is, what it depends on, and whether it's in use or not.

Genome Mapping allows geneticists to understand the risk and impact of every mutation in your DNA. In the world of security, Workload Composition Analysis provides the same benefits, utilizing the SBOM as its genome map. The SBOM shows:

- **Inventory** - What code is deployed and where it's deployed
- **Provenance** - Where every artifact originated
- **Impact** - Is a piece of code loaded to memory and executed or unused, bloated code
- **Exposure** - Which components have network access and whether they are communicating
- **Interdependencies** - How artifacts and code interact

The ability to reliably and efficiently generate a software bill of materials for applications is essential to understanding the pedigree of all parts of your application. It can also be a daunting task without the right tools and advisors. With NCC Group and Rezilion, creating and maintaining this key artifact happens automatically, and remediating the exploitable vulnerabilities contained within critical applications happens efficiently. This combination of expertise and tailor-made tools lets critical infrastructure operators focus on providing maintainable and safe services to the public and supply chain partners while effortlessly complying with Executive Order 14028.

With NCC Group and Rezilion, creating and maintaining a SBOM happens automatically, and remediating the exploitable vulnerabilities contained within critical applications happens efficiently.