Nomura Research Institute Group

NEWS RELEASE

NRI Secure Launches Japan's First IT Security Assessment Service for Container Orchestration

TOKYO, November 21, 2019 - NRI SecureTechnologies, Ltd. (NRI Secure) today launched Japan's first[1] IT security assessment service for systems with container orchestration[2], that uses the leading container orchestration tool "Kubernetes."[3]

This service provides IT security assessment for a system using container orchestration technology from the viewpoints of both "static analysis" by interpreting configuration files, and "dynamic analysis" by attempting simulated attacks. The assessment consists of manual inspection by engineers of NRI Secure who have expert knowledge of container orchestration as well as several tests using auxiliary inspection tools. This service detects security issues by checking the validity of the information on the configuration file, and the architecture configuration generated by container orchestration.

In addition to the independent inspection of each configuration file, a comprehensive and highly accurate assessment is performed to check whether the configuration state is appropriate or not by looking at the entire architecture. This enables us to detect security issues at the design phase that are often overlooked by the inspection tool alone.

Followed by Kubernetes, NRI Secure plan to add more container orchestration tools to the scope of this IT security assessment service.

In recent years, as DX (digital transformation) has become more widespread, the need for greater flexibility and speed in system development has increased, and the design concepts and infrastructure technologies that support these requirements have been rapidly evolving. In particular, microservice[4], which develops applications by splitting them into services and functions, and other system development that presuppose deployment of cloud-native[5] and serverless[6] architectures are becoming more common.

One of the technologies that underpin these architectures is an application execution environment called a container. The emergence of container orchestration tools that automatically deploy, scale, and so on has

increased the adoption of containers when building systems.

On the other hand, since containers are a new technology area, there is a high possibility that the system is operating with a weak configuration since security measures are not yet fully in place. To deal with increasingly intense cyber threats and attacks, it is necessary to take appropriate security measures, such as access and privilege management, with a view to the entire system architecture, as well as vulnerability measures for the container itself.

NRI Secure will continue to provide various products and services in response to trends and threats of the times for supporting companies and organizations in their information security measures, contributing to promoting digital transformation for a safe and secure society.

---

[1] Japan's first:

This service is the first IT security assessment service for container orchestration provided by leading security vendors in Japan. (According to verification as of November 21, 2019, by NRI Secure)

[2] container orchestration:

A container is an application execution environment built on an operating system to provide virtualization with fewer computer resources. Docker is one of the leading tools for creating container-based virtual environments. Container orchestration means automatically deploying, scaling, and so on.

[3] Kubernetes:

An open-source platform for managing containerized workloads and services. It is a typical container orchestration tool with a large share of the market. In case Kubernetes users are not familiar with the tool-specific architecture and features, such as the components in the master nodes (manages the entire cluster) and worker nodes (manage containers according to the instructions of the master node), as well as the configuration of the Pods (one or more containers with shared storage or networks, or a specification of container execution methodology.), systems can be susceptible to security vulnerabilities.

[4] Microservice:

A software architecture that divides applications into multiple small services (microservices) according to business functions. It is characterized by greater flexibility in deploying and scaling services.

[5] cloud-native:

A system development and operation method that assumes the use of cloud services.

[6] serverless:

In a system on the cloud, a cloud service provider can assign resources to arbitrary events as a trigger and execute code without assigning server resources in advance. For the system owners, it helps lower the cost of infrastructure management.

Media inquiries:

Public Relations, NRI SecureTechnologies, Ltd.

TEL: +81-3-6706-0622

E-mail: info@nri-secure.co.jp

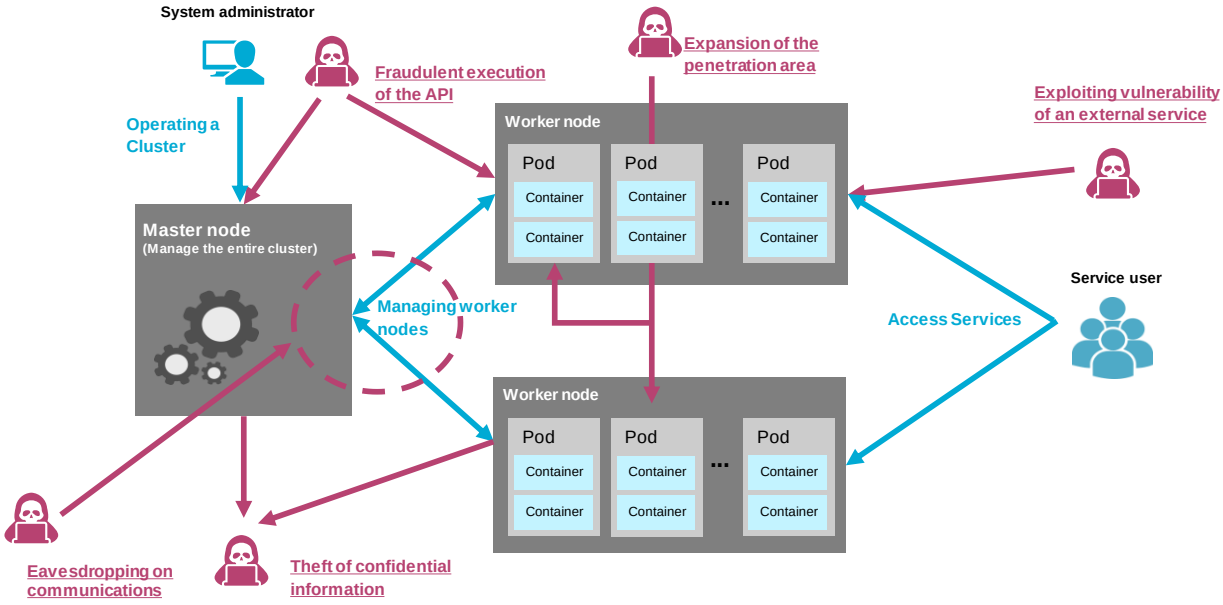
Inquiries about the solution:

Teruhiro Tagomori, North America Regional Headquarters, NRI SecureTechnologies, Ltd.

E-mail: info@nri-secure.co.jp

【References】

■ Common cybersecurity threats and conceptual diagram of container orchestration using Kubernetes



*This is a simplified representation of a typical Kubernetes architecture.

*Cyber threats are underlined in red. The threats shown in this diagram are examples only.

■ About NRI SecureTechnologies

NRI SecureTechnologies is a subsidiary of Nomura Research Institute (NRI) specializing in cybersecurity, and a leading global provider of next-generation managed security services and security consulting. Established in 2000, NRI Secure is focused on delivering high-value security outcomes for our clients with the precision and efficiency that define Japanese quality. For more details, visit us at https://www.nri-secure.com.