Repeated Deployment of Network Security Devices

This paper focuses on improving the accuracy, effectiveness and adaptability of honeypot deployment, and proposes an intelligently driven deception resources deployment method.

This site contains the Security Technical Implementation Guides and Security Requirements Guides for the Department of Defense (DOD) information technology systems as mandated by DODI 8500.01. ...

Organisations are encouraged to implement an event logging policy focused on capturing high-quality cyber security events to aid network defenders in correctly identifying cyber security incidents.

It highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices. The purpose of this report is to enhance incident response among ...

The deployment configuration detailed in this guide describes one way of configuring a FortiGate to provide security to small and medium businesses. The example is designed for a hypothetical ...

To begin, we introduce the concept of security burst (SEB) and security burst requirement (SeBR) as the ever-changing cyber-attacks and the periodic need for enhancing security services in ...

A Cisco firewall breach involving CVE-2025-20333 and FIRESTARTER malware shows how attackers can survive patching and regain network access.

A buffer overflow that delivers unauthenticated root-level code execution on a network security device is among the most severe possible vulnerability classes. With over 5,800 instances ...

This report presents best practices for overall network security and protection of individual network devices. It will assist administrators in preventing an adversary from exploiting their...

Consider the following best practices when preparing an Device Security deployment.

Repeated Deployment of Network Security Devices

Web: https://busydoniemiecwaldii.pl