



Le Club TDSI et la Communauté Linux Sénégal avec le soutien de l'École nationale de Cybersécurité à vocation régionale et le Département mathématiques et informatique

Présentent

Journée Linux Sénégal - 3ème Édition

LA SÉCURITÉ DANS L'OPEN SOURCE

 18 Décembre 2021

 Grand Amphithéâtre UCAD 2 - UCAD

 09h00 - 18h30



Sponsors & Partenaires :





Sommaire

Introduction

Cybersécurité / Sécurité Informatique

C'est quoi le SOC?

C'est quoi le SIEM?

Démo Security Onion

Conclusion





Introduction

« Qui veut la paix, prépare la guerre. » , Jules CESAR

La sécurité Informatique / Cybersecurité



Le SOC, c'est quoi?



Le SIEM, c'est quoi?



A decorative header element consisting of a network diagram with blue nodes and connecting lines, spanning the top of the slide.

Présentation SIEM Security Onion



Démo: Security Onion

The screenshot shows a web browser window displaying the Security Onion Downloads page. The browser's address bar shows the URL `https://192.168.1.2/#/downloads`. The page header includes the Security Onion logo and a user profile icon. A blue notification box contains the text: "When installing packages such as osquery or beats onto remote systems be sure to run `so-allow` on the Security Onion Manager node to allow network access through the firewall." Below this, the page is organized into sections: "Elasticsearch Utilities (7.15.2)" with links for Winlogbeat, Filebeat (DEB/RPM), Metricbeat (DEB/RPM), and Auditbeat (DEB/RPM); "Wazuh Agents (3.13.1-1)" with links for MSI, DEB, RPM, and PKG; and "osquery Packages and Configs". The footer of the page displays "VERSION: 2.3.90", "© 2021 SECURITY ONION SOLUTIONS, LLC", and "TERMS AND CONDITIONS". The Windows taskbar at the bottom shows the system tray with the date and time set to 10/12/2021 at 20:39.

Security Onion

Downloads

When installing packages such as osquery or beats onto remote systems be sure to run `so-allow` on the Security Onion Manager node to allow network access through the firewall.

Elasticsearch Utilities (7.15.2)

- [Winlogbeat](#) (Windows)
- [Filebeat DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [Filebeat RPM](#) (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- [Metricbeat DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [Metricbeat RPM](#) (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- [Auditbeat DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [Auditbeat RPM](#) (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)

Wazuh Agents (3.13.1-1)

- [MSI](#) (Windows)
- [DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [RPM](#) (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- [PKG](#) (MacOS)

osquery Packages and Configs

VERSION: 2.3.90 © 2021 SECURITY ONION SOLUTIONS, LLC [TERMS AND CONDITIONS](#)

A decorative graphic at the top of the page consisting of a series of interconnected blue dots and thin lines, resembling a network or a stylized molecular structure.

Conclusion

