Table of Contents

li Purple Guide: All You leed to Know

May 10, 2024 Andrew DeVito

Listen to the article

Kali Purple promises to be your innovative cyber security distribution designed specifically for the defensive side of the cyber realm, offering you a comprehensive toolkit that caters to various aspects of network defense. This newly released platform is based on the NIST Cybersecurity Framework and provides you with a comprehensive suite of tools and features to bolster your security posture.

In this article, we will delve into the unique features and capabilities of Kali Purple, explore the differences between it and the traditional Kali Linux, and examine how it aligns with the NIST Cybersecurity Framework. We will also take a closer look at some of the new tools incorporated into Kali Purple, discuss the concept of SOC-in-a-box architecture, and provide guidance on obtaining and installing the distribution.

Join us as we take a first look at Kali Purple and explore the ins and outs of this impressive platform.

What Is Kali Purple?

Table of Contents

ddition to the Kali Linux ecosystem, creatively tailored for
l ethical hackers who focus on defensive security strategies. As
ali Linux platform, Kali Purple seems uniquely positioned to
audience by leveraging the **NIST Cybersecurity Framework**.

y Framework 1.1 comprises five core domains
vel, strategic approach to managing cyber

organization's assets, systems, and data, and understand
curity risks.

- **Protect**: Implement safeguards to ensure the delivery of critical infrastructure
ss control and data security.

ely detection of cyber security events through continuous
y reporting.

iate actions upon detecting a cyber security event involving
mmunication, and mitigation.

- **Recover**: Restore services and operations affected by a cyber security event, focusing on recovery planning and continuous improvement.

Unlike traditional Kali Linux, which you may know for its use in offensive security, Kali Purple expands the platform's capabilities by integrating an array of defensive tools and resources designed to equip you with the ability to proactively identify, respond to, and mitigate cyber security threats. This strategic approach should allow Kali Purple to function as a **complementary solution within the Kali Linux family** rather than replacing the existing platform.

Despite being in its early stages of development, Kali Purple has already garnered interest from the cyber security community, with anticipation building around future updates and enhancements that could further refine and expand its feature set and demonstrate clearer use cases. As the platform continues to evolve, Kali Purple could prove to become a valuable resource to help you strengthen your defensive posture.

How Is Kali Purple Different?

Kali Purple distinguishes itself from its Kali Linux counterpart by offering a distinct and
uts tailored to meet your specific demands as a defensive cyber
gence is evident not only in the tools and resources provided
l architecture and design philosophy.

nces between Kali Purple and traditional Kali Linux is the
ools specifically curated to bolster defensive security
will be explored in greater detail in subsequent sections,
e from the predominantly offensive-oriented toolset found in
s.

upon the latest Debian kernel, ensuring optimal performance,
modern hardware. It also incorporates the most up-to-date
r a more refined and user-friendly experience.

ncluded with Kali 2023.1:

nges to Thunar file management and panel management.
window tiling, widgets, and adding LTS for this version.
ajor update soon, but some tweaks have been made by Kali
s using F4 to open the terminal from the Nautilus file manager.

Another key differentiator is the introduction of the SOC-in-a-box architecture. This innovative design integrates a diverse suite of security operations center (SOC) components into a modular, connected platform, streamlining workflows and facilitating improved collaboration between security professionals.

The intent behind using Kali Purple as a SOC In-A-Box can be described as setting up multiple machines that monitor a network in various ways. Additionally, you could use them to connect as a **red team/blue team** exercise. One thing that seems to point to this is the way the tools are broken out during the installation process. **More on that later**.

Kali Purple also features **Kali Autopilot**, a powerful attack script-building capability that allows you to automate various tasks and processes, further enhancing the platform's versatility and adaptability.

Kali Purple Hub

> Also introduced is Kali Purple Hub, which is designed to allow the community to upload own custom Kali Autopilot scripts.

e latest Python release, ensuring compatibility with ols and libraries. The new Python 3.11.2 implements many e version. Here are a few of the changes in this version:

on in tracebacks.
een 10-60%.
odules (tomllib).
s.

> - New typing features.

Level Up in Cyber Security: thon Release Notes.

ge maintainers work on updating their packages to the latest behavior changes in Python. **Namely, installing older ways function properly.** Kali's recommended method during this time is to use `apt install python3-<package>`. When 2023.4 comes out towards the end of the year, this may be the only method supported.

By embracing these advancements and strategically expanding its focus to encompass both offensive and defensive security, Kali Purple has demonstrated a commitment to developing a formidable addition to the Kali Linux ecosystem, further solidifying its position as a comprehensive and versatile solution for cyber security professionals.

What New Tools Come With Kali Purple?

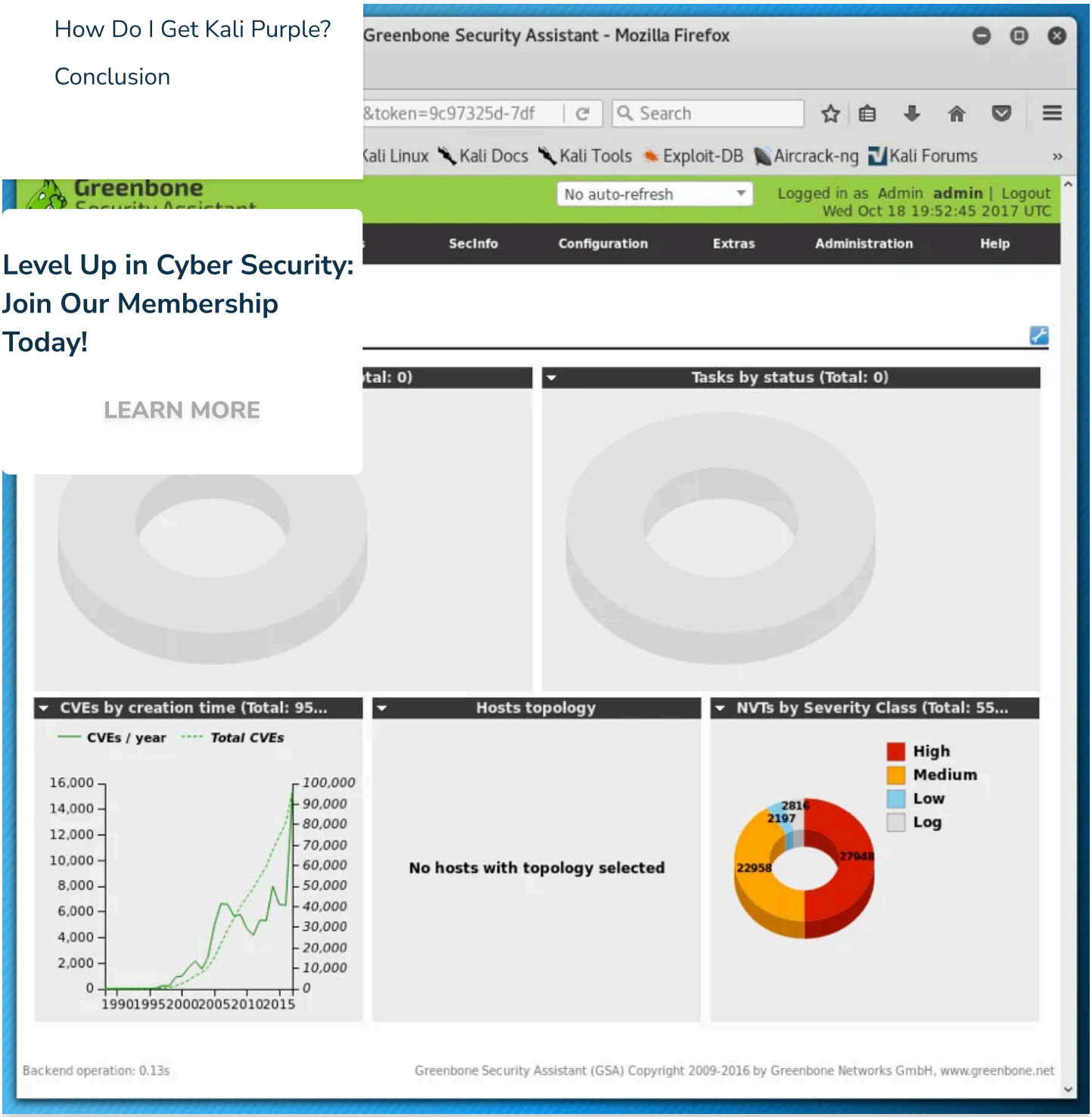
Kali Purple introduces a suite of new tools that align with the five domains of the NIST Cybersecurity Framework (CSF) 1.1: *Identify, Protect, Detect, Respond, and Recover*. This alignment ensures that the tools provided cater to a broad range of defensive cyber security tasks, further pointing to Kali Purple's future potential as a comprehensive solution for security professionals.

As a note, we found that many of these newly announced tools weren't available by default in this first release. Instead, many of them needed to be downloaded and installed by following the directions in the Community Wiki. Even more, at the time of writing, a few of the tools have

challenges with regard to executing them on the device. This is perhaps continued evidence that this is a rapidly distributed that will require regular updates.

Table of Contents

VM (Greenbone Vulnerability Management) are crucial in tial vulnerabilities within an organization's infrastructure. By and networks, GVM enables security teams to stay ahead of a strong security posture.

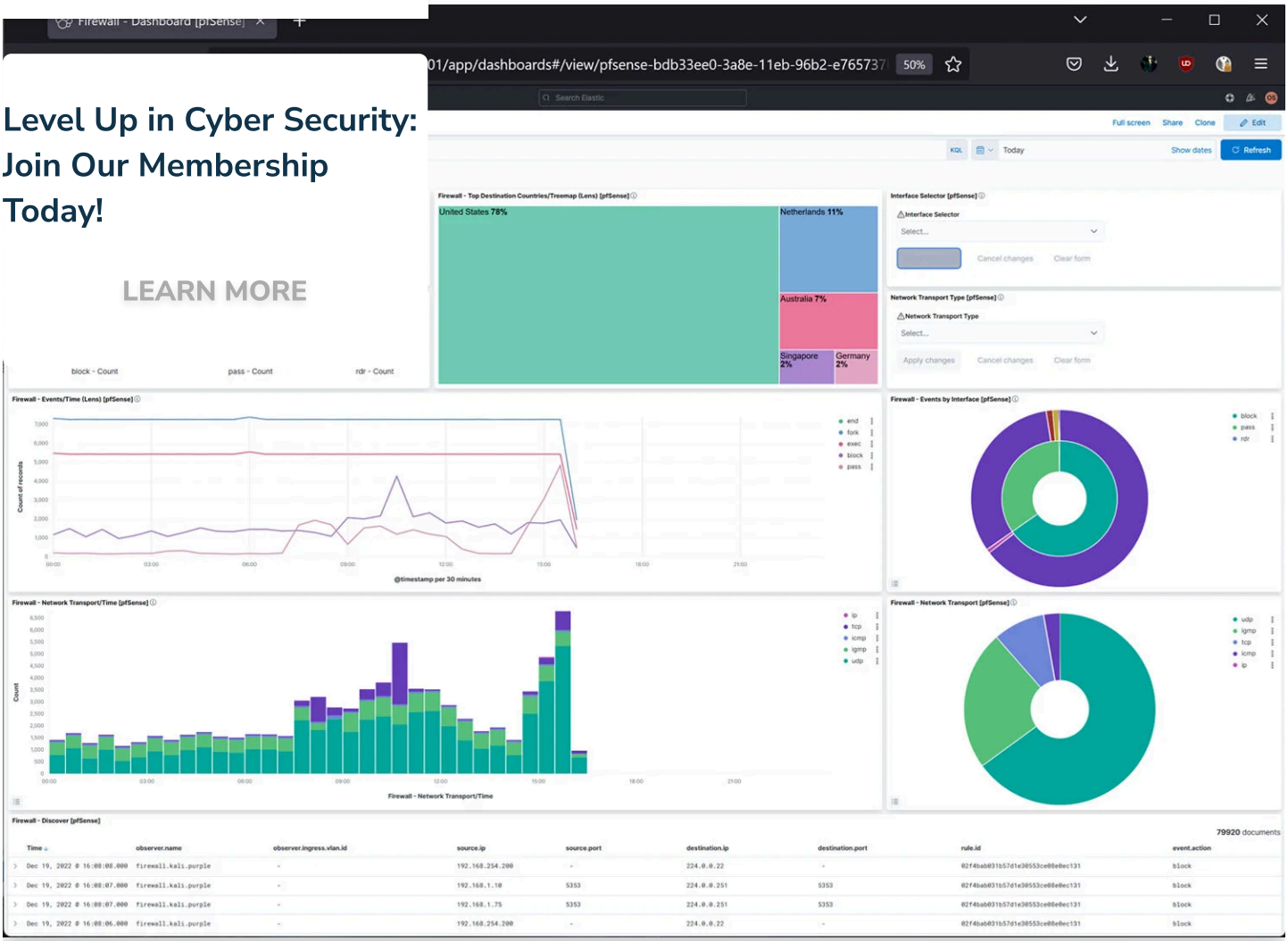


Greenbone Vulnerability Management from the Kali Wiki.

Needs to be installed

https://gitlab.com/kalilinux/kali-
-/wikis/101_30:-GVM

tools aimed at bolstering an organization's protective
Security, a powerful Security Information and Event
onsolidates and analyzes security data from various sources,
mitigation of potential threats. However, it's worth noting that
s with setting up Elastic Security in Kali Purple.



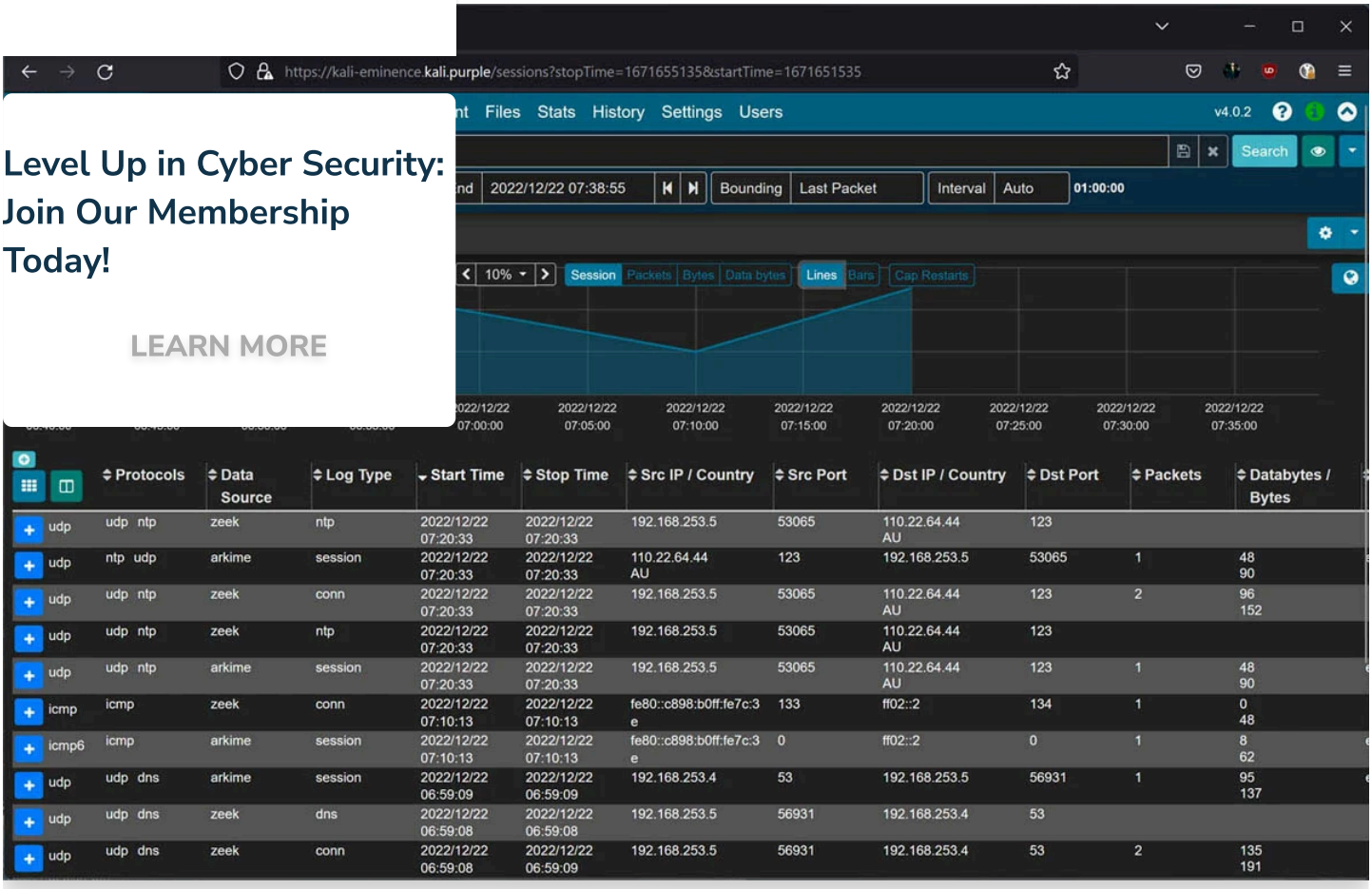
Elastic Security from the Kali Wiki.

Needs to be installed

- Installation instructions: **https://gitlab.com/kalilinux/kali-**
  -/wikis/101_40:-Elastic-Agent

own issues with getting all the dependencies installed.

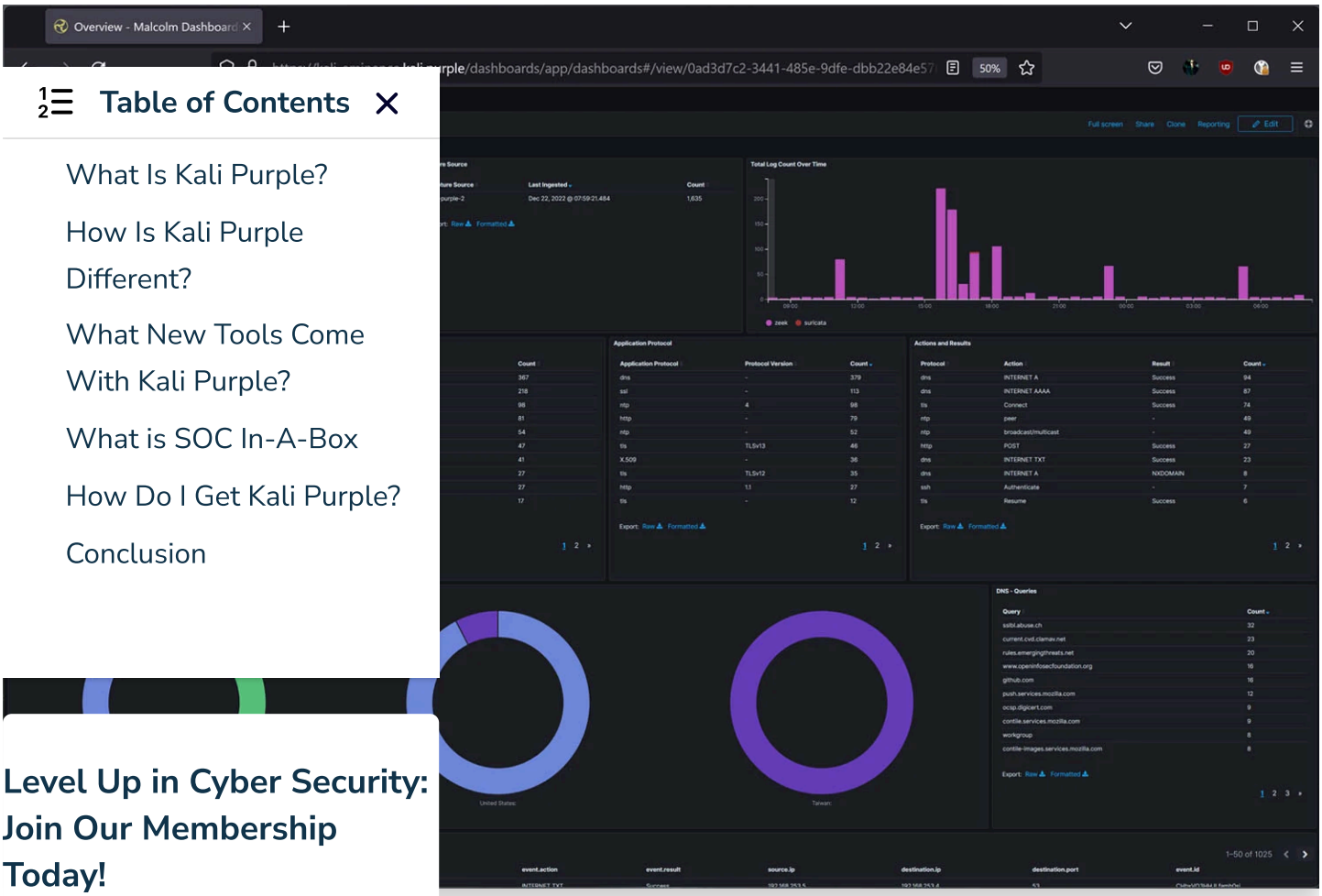
monitoring and analyzing network activity to identify potential
Arkime, a network forensics platform, excel in this area,
network traffic and enabling the early detection of malicious
ork monitoring and analysis tool, complements Arkime, though
in Kali Purple.



Arkime from the Kali Wiki.

Needs to be installed

- Installation instructions: **https://github.com/arkime/arkime**

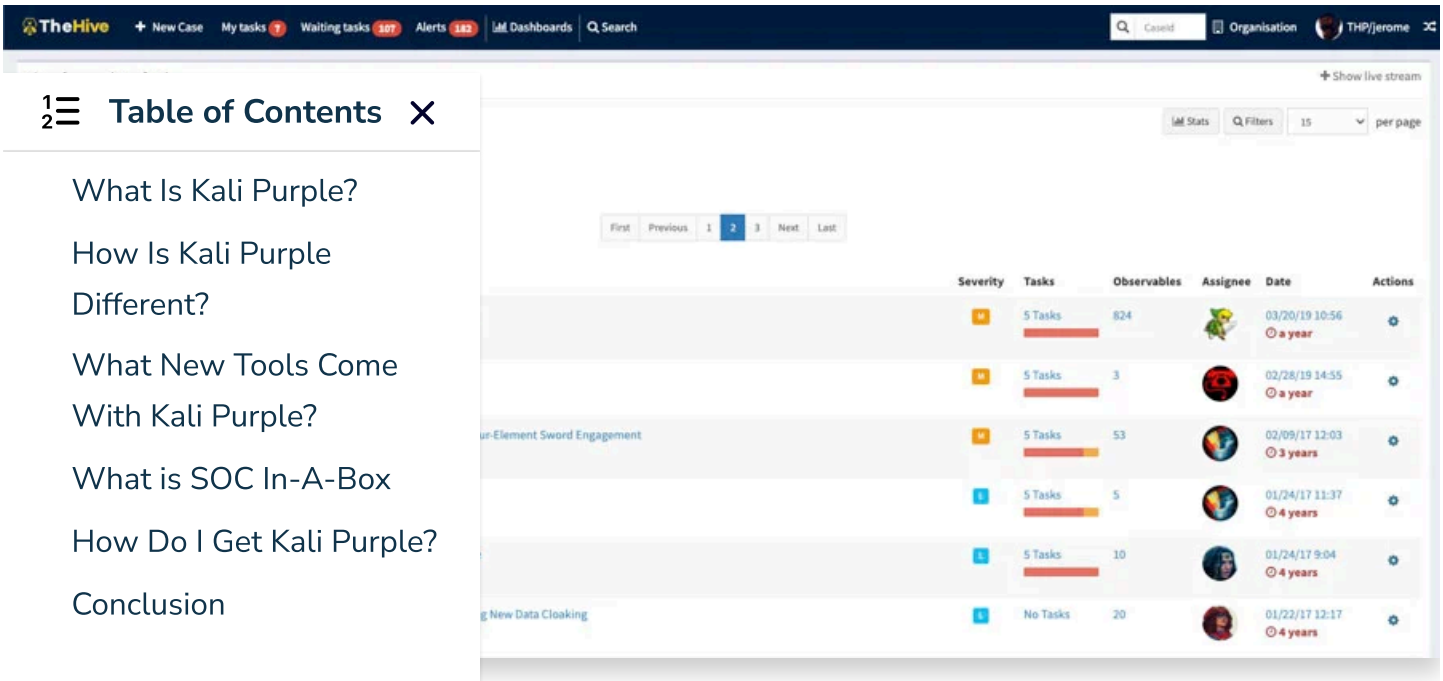


Malcolm from the Kali Wiki.

> ### Needs to be installed
>
> - Installation instructions: **https://gitlab.com/kalilinux/kali-purple/documentation/-/wikis/401_20:-Malcolm-Installation**
>
> As noted above, there are known issues with getting all the dependencies installed.

Respond

In the event of a security incident, efficient response is crucial. Kali Purple offers **TheHive**, an incident response and forensic tool, to aid security teams in managing and coordinating their response efforts. TheHive provides a collaborative environment where team members can share information, track progress, and streamline the incident response process.



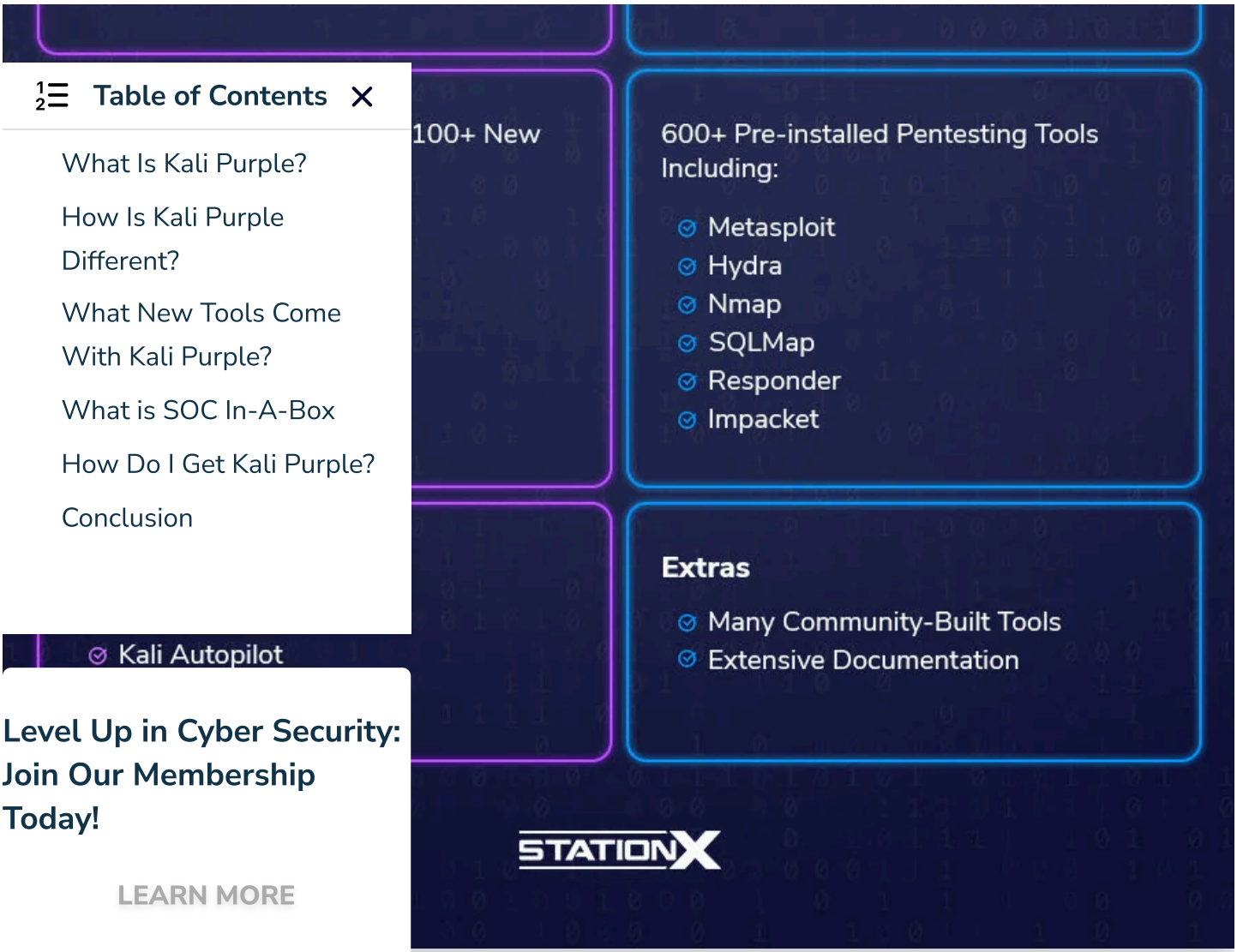
TheHive from The Hive Project.

https://github.com/TheHive-Project/TheHive

The final domain of the NIST CSF 1.1 involves restoring systems and services to normal operation after a security incident. While Kali Purple does not explicitly introduce tools focused on recovery, the integration of incident response and forensics tools, such as TheHive, can aid you in the development of effective recovery strategies and ensures a swift return to normal operations.

Kali Purple's new tools are intended to provide comprehensive coverage across the five domains of the NIST Cybersecurity Framework, enabling security professionals to effectively identify, protect against, detect, respond to, and recover from cyber threats. With its design to provide a powerful and specialized toolset, Kali Purple aims to enhance how you approach defensive cyber security.

If you want to learn about other tools that come with Kali Purple as part of the core Kali Linux suite, take a look at our article on the **25 Top Penetration Testing Tools for Kali Linux**.



What is SOC In-A-Box

00:00 00:00 1

Kali Purple, addresses this need by offering a streamlined, centralized solution for managing security operations and **incident response**.

SOC In-A-Box, or Security Operations Center In-A-Box, is an innovative architecture that aims to consolidate essential defensive cyber security tools and processes into a single, cohesive platform. This integrated approach allows you to efficiently monitor, analyze, and respond to threats, vulnerabilities, and incidents in real time.

By bringing together disparate tools and capabilities, SOC In-A-Box empowers you with a unified view of your security posture, thereby enabling you to make informed decisions and take swift, decisive action in response to emerging threats.

Kali Purple's SOC In-A-Box offers you several advantages. It will simplify deployment and configuration, making it easier for you to get up and running with minimal effort. Additionally,

the platform's modular design facilitates the seamless integration of various tools and
tailor your security operations center to meet your unique
ıe next section.

n foster collaboration and information sharing among your team
ective and efficient approach to incident response and threat
u reduce reliance on multiple, disparate solutions, streamlining
reducing the complexity of managing a comprehensive cyber

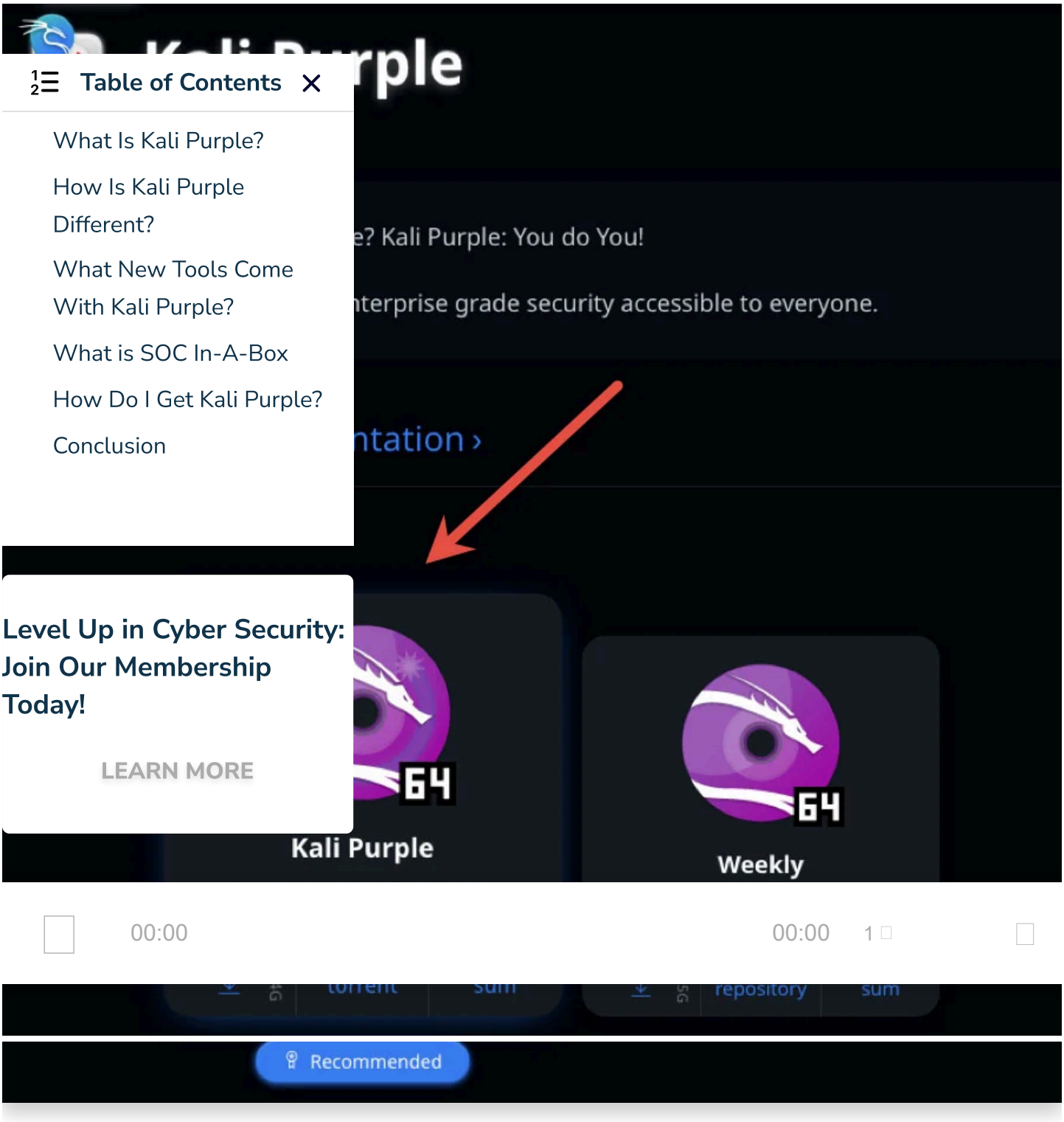
s may need to wait for the future development of Kali Purple.

urple?

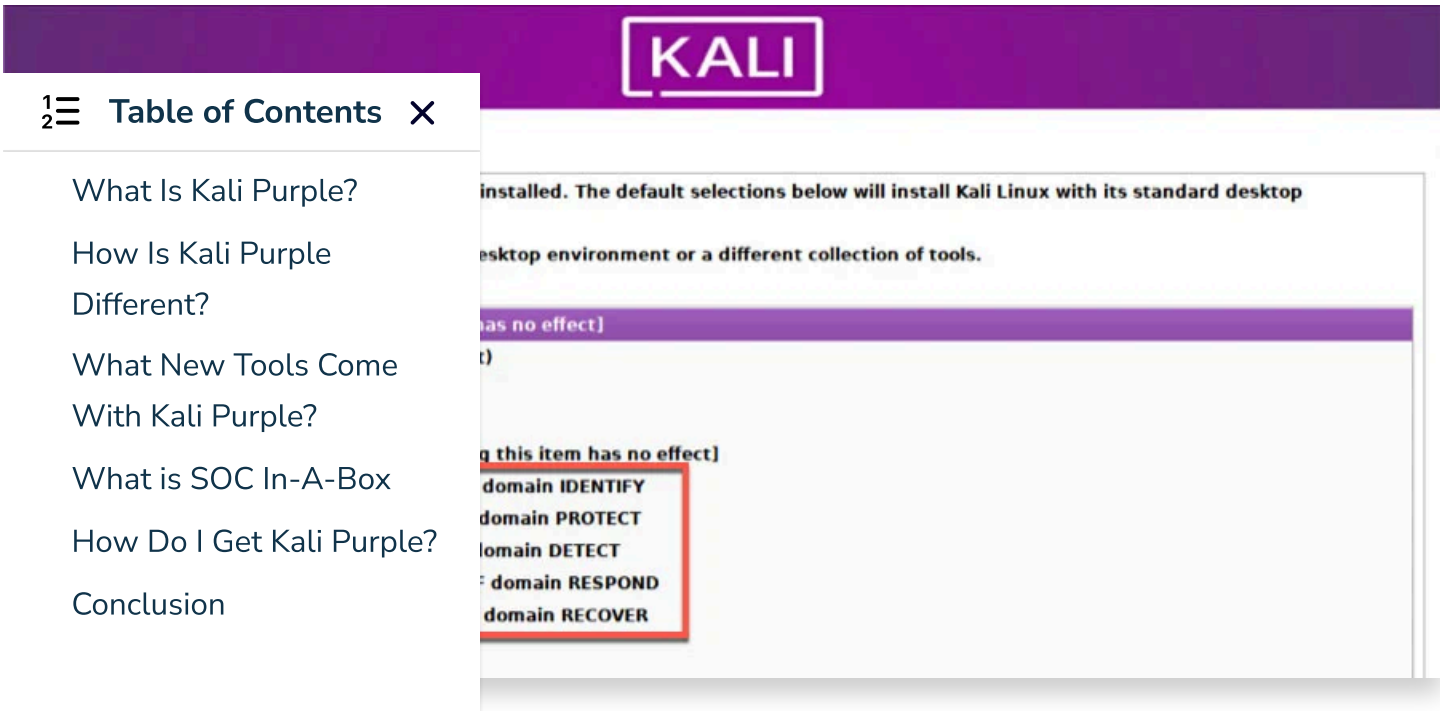
Getting your hands on Kali Purple is pretty much like getting any other Kali distro. Head over
nloads.

ay is the limited options compared to what we're used to
-built VM images, no ARM images, nor any of the rest. While it
lo come out, we believe that the presence of only the ISO file indicates what we've mentioned earlier in this article.

00:00 00:00 1



Let's speed through the installation for an example. While everything else appears exactly like any other Kali or Linux install, our first sense of the changes in Kali Purple occurs on the page where desktop environment selections are made.



Here you can see the options for the categories of tools that we discussed above. All are aligned with the NIST Cybersecurity Framework domains. While at first, it may not seem like a lot, remember that you could mix and match these tools in various ways.

Kali has tools for various defense tasks, including network monitoring, threat response, and forensics, so the possibilities for device configuration are endless. Currently Kali hasn't released the VM images yet, and it's unclear if

Start Hacking Now.

Conclusion

Kali Purple represents a significant leap forward for defensive cyber security, offering a powerful and versatile suite of tools that cater to each of the five domains of the NIST Cybersecurity Framework. By addressing the diverse needs of security professionals, Kali Purple equips you with the means to effectively identify potential threats, implement robust protection measures, detect malicious activity, respond swiftly to security incidents, and recover from cyber attacks.

Kali Purple's holistic approach to cyber security, in combination with its continued commitment to incorporating cutting-edge tools and features, makes it an indispensable asset for security professionals and organizations seeking to bolster their security posture.

As the landscape of cyber security threats continues to evolve, Kali Purple's focus on defensive
he NIST CSF 1.1 should allow it to remain at the forefront of
the tools and resources necessary to navigate the increasingly

skills yourself, take a look at the below courses available in our

Table of Contents

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

t Camp: Defending Against Hackers

STATIONX

00:00 00:00 1

Snort Intrusion Detection, Rule Writing, and PCAP Analysis

4.9 ★★★★★

STATIONX

thical Hacking: Develop Pentesting Tools

STATIONX

Table of Contents

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

n Cyber Security: Join Our embership Today!

00:00 00:00 1

Table of Contents

Andrew is a Content Writer at StationX. He comes from a multi-discipline professional background xperience in healthcare compliance, financial cyber security ecurity, and threat modeling. He is dedicated to translating complex nderstandable language to help you successfully navigate the ever-ts.

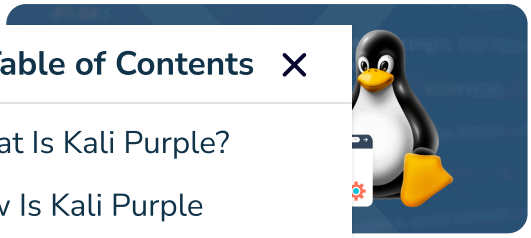
Related Articles

How to Use Ligolo-ng (Easy to Follow Pivoting Tutorial)

Read More »

Top 15+ Cyber Security Tools (2024 Ultimate Guide)

Read More »



...calation ...cking

OWASP ZAP Tutorial: Complete 2024 Guide

Read More »

Table of Contents

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

Table of Contents