Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Business Adaptability Through Deception Technology

Olaniyi Abiodun Ayeni, Adejumo Ibitola Elizabeth*, and Ovat Ejibha Victor
Department of Cyber Security, School of Computing, Federal University of Technology, Nigeria

Received 20 Aug. 2024; Accepted 10 Dec. 2024; Available Online 31 Dec. 2024

Abstract

This research introduces deception technology, an innovative cybersecurity strategy that involves the creation of deceptive assets within an organization's network. These assets, such as decoy servers and endpoints, closely mimic authentic resources, diverting potential attackers and facilitating crucial threat intelligence gathering. By engaging with adversaries and providing real-time insights, deception technology enables businesses to swiftly adapt to the evolving cyber threat landscape. This paper investigates phasor technology and its mathematical representation, alongside the implementation of FORTINET's FortiDeceptor and its integration into cybersecurity business operations. The objective is to enhance threat detection capabilities, detect insider threats early, and fortify overall security postures by deploying FortiDeceptor, a tool suitable for banking systems. In response to the escalating threat of cyberattacks, proactive measures have been taken to develop more adaptable and responsive cybersecurity protocols.

I. Introduction

Deception tactics mislead people into behaving against their best interests, whether they are employed by the military, cybercriminals, or cybersecurity experts [22]. Even though deception techniques and technology predate computers, they are today examined through the perspective of cybersecurity [22]. In the past, governments, armed forces, and intelligence services used deception technology to take advantage of the vulnerabilities of their opponents. Deception is said to be defined as "to delude by fabricating an appearance or statement," which is why the word itself has a negative implication [6]. In the past, using deceit to obtain a tactical edge was common practice.

While there is no creation of a fake military, deception technologies (DT), sometimes known as "false threat detection capabilities," can be employed to enhance comprehension of security breaches and enhance defense mechanisms [7]. These days, corporations basically use systems, deception, and fake lures to draw in and trap adversaries.

In [4], the spotlight was on the ways in which deception technologies can dramatically increase the ability of an organization to identify attackers with greater speed and accuracy while gathering adequate threat intelligence and attack attribution data to enhance the efficacy of response measures.

Keywords: adaptability, business, cybersecurity, deception technology, FortiDeceptor, Fortinet

Production and hosting by NAUSS

* Corresponding Author: Adejumo Ibitola Elizabeth
Email: ibitolaadejumo@gmail.com
doi: 10.26735/RMKH6846

Several research studies have explored different aspects related to this topic, including the need for adaptation in new technology-based businesses [8], the value creation from decentralized ledgers [1], the role of deception in earnings management [2], the detection of deception in electronic media [3], the overview of deception technology service adaptation in a business-to-business context [5], interoperability in the Enterprise Resource Planning (ERP) field [6], automated detection of deception in computer-mediated communication [7], the co-evolution model of business and IT for dynamic business process requirements [9], and the use of deception in business strategy [10]. A crucial point in the literature is that it is essential for businesses to adapt their initial models in response to changing conditions.

Types of Deception Technology

The primary types include honeypots, honeytokens, and deceptive user interfaces.

A. Honeypots

When it comes to use case, honeypots attract and engage attackers using decoy systems or networks. These mimic legitimate systems, applications, or services and serve as bait to lure malicious attacks. Honeypots detect and divert malicious activity, allowing organizations to monitor and analyze the tactics of potential attackers. Honeypots capture valuable information about attack methods, techniques, and vulnerabilities [11]. A honeypot can also record keystrokes made by an opponent trying to breach it; this gives extremely insightful information if the hacker utilizes the compromised computer's location as an Internet Relay Chat (IRC) chat server [19].

B. Honeytokens

Honeytokens can be said to be pieces of deceptive information or data strategically placed within a network. They appear as valuable or sensitive data but are entirely fake, honeytokens act as an intrusion tripwire, alerting security teams when an unauthorized entity accesses or interacts with them, very effective in identifying insider threats. Honeytokens produce few false alarms, making it easier to identify genuine security incidents [11].

C. Deceptive User Interfaces

This presents false information to potential attackers. They might mimic legitimate login screens, admin dashboards, or error messages. Misleading Attackers by providing false information, deceptive user interfaces can confuse attackers, delaying their progress and potentially discouraging them from continuing. They can engage with attackers in real-time, gathering valuable threat intelligence and potentially disrupting their activities [11].

Advantage and Disadvantage

The main benefit of deception technology is the ability to detect threats early. A dynamic and responsive security environment is created by companies through the use of a network of decoys that mimic real assets [21]. Complexity of implementation is one of the major challenges of deception technology [20].

II. Review of Related Paper

The authors in [12] presented a framework for evaluating business adaptability with deception technology in cybersecurity. The study aimed to develop a framework for evaluating the adaptability of businesses that have integrated deception technology into their cybersecurity strategies and contributed a practical framework for businesses to measure their adaptability improvements, contributing to the understanding of the benefits of deception technology. However, the framework's applicability might vary depending on the specific business context, it does not focus on the deception itself, and it is just a theoretical framework. Similarly, the research in [15] explored mitigating insider threats and enhancing business adaptability through the role of deception technology, aimed at exploring the role of deception technology in mitigating insider threats and enhancing business adaptability. The research highlighted how deception technology can proactively address insider threats and bolster business adaptability by reducing the time to detect and respond to such threats.

TABLEI
COMPARATIVE ANALYSIS OF DECEPTION TECHNOLOGY COMPONENTS AND THEIR OPERATIONAL IMPACT

Feature	Advantages	Disadvantages
Threat Detection	- Early Detection: Identifies threats early, often before they reach critical systems. -High-Fidelity Alerts: Produces fewer false positives, focusing security teams on genuine threats [23].	- Potential for Bypassing: Sophisticated attackers may learn to recognize and avoid decoys [23].
Threat Intelligence	Actionable Intelligence: Provides valuable insights into attacker tactics, techniques, and procedures (TTPs) [24], [25].	Maintenance and Management: Requires ongoing monitoring, updates, and management of decoys [24].
Insider Threats	Effective Detection: Particularly good at identifying malicious insiders who have legitimate network access [25].	Complexity of Implementation: Initial setup and configuration can be challenging, requiring careful planning and expertise [25].
Security Overhead	Proactive Approach: Shifts the security posture from reactive to proactive, allowing organizations to engage attackers [25].	Scalability: Deploying and managing decoys across large, complex networks can be difficult [25].
Resource Overhead	Potentially Low: Can have a relatively low resource overhead compared to some security solutions, especially after initial setup [26].	Cost: Initial investment in solutions and expertise can be significant [26].

However, the study focused on a specific aspect of deception technology's application and might not cover its broader utility, nor did it mention evaluation metrics. Furthermore, the work presented in [16] investigated adapting to emerging cyber threats: the influence of deception technology on business resilience. This study aimed to investigate the adaptability of organizations to emerging cyber threats when deception technology is employed as a proactive cybersecurity strategy using case studies of organizations that had experienced cyber threats, assessing their adaptability in response to these threats. The research contributed to highlighting the significance of adaptable cybersecurity strategies, such as deception technology, in maintaining business continuity. However, the case studies may not represent all industries and organizational sizes and are limited by their scope. Likewise, the authors in [17] presented practical implications of deception technology for business cybersecurity and adaptability. The study aimed to examine the practical implications of incorporating deception technology into business cybersecurity strategies. The research provided insights into the practical implications, benefits, and challenges of implementing deception technology for enhancing business adaptability. However, the study's scope did not cover the most recent advancements in deception technology, which is allowing security teams to install decoys on endpoints, nor did it address the potential drawbacks. Finally, the work conducted in [18] introduced an architectural style: distortions for deploying and managing deception technologies in software systems. The authors suggested a type of architecture that emphasizes the integration of DTs into software systems; this style will be referred to as style from upon arrival on. While the research introduced an architectural style that explains how software systems deploy and manage deceptions, it lacks validation of findings on the concerns and practices of developers who use deception technologies. The authors were also unable to ascertain whether this style is adopted in practice or how cybersecurity practitioners view the proposed style, and furthermore, the architecture may not be suitable for all software systems. The research focused on bridging the gap between the art of deception and the technical aspects of using a DT.

III. METHODOLOGY

This sections, shows the flowchart that presents a multi-stage methodology for leveraging deception technology in cybersecurity. The flowchart below presents key stages which include asset

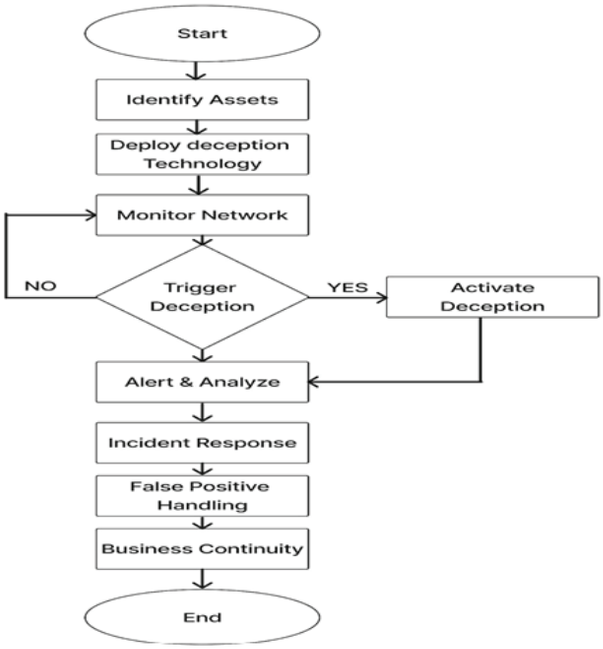

Fig. 1 Flowchart of the deception technology system

identification, deployment deception technology, network monitoring, threat detection and analysis, incident responses, false positive handling and business continuity.

A. Algorithm of the deception technology process

Start: Starts the process here.

Identify Assets: Identify critical assets, systems, and the resources that need protection for business continuity.

Deploy Deception: Deploy Implementation deception technology, such as honeypots, honey tokens, or other deceptive skills, within network infrastructure.

Monitor Network: Continuously monitoring the network traffic, system activity, and the user behavior using intrusion detection systems (IDS) and other security tools.

Trigger Deception: Deception technology creates unverified elements inside an organization's network when it detects suspicious activity. This can be achieved by diverting attackers' attention from the organization's critical assets or information by utilizing decoy servers, data, or employees. Alert and Analyze: Assisting in the operation of the deception technology by keeping an eye on prudence and evaluating the data to identify the type of hazard caused.

Incident response: As soon as an organization recognizes a threat that is authentic, it should initiate an incident response strategy. This might include eliminating the threat and isolating systems that are been compromised while concentrating on business recovery.

False positive Handling: In order to avoid interfering with lawful business operations is to look into and fix any results that are negative that triggered the deception technology in the organization. Business continuity: Resolving security problems while ensuring that essential business operations continue without interruptions. End: End procedure.

B. Integration with AI and Machine Learning Algorithm

The integration of deception technologies with AI and machine learning (ML) enhances cybersecurity by making it harder for attackers to identify and bypass security systems [27].

Deception Technologies: Distract and track down cybercriminals by using fictitious digital assets (such as honeypots and decoy systems). AI and Machine Learning: modify systems instantly, forecast actions, and Utilize use of algorithms to spot trends [28].

When these two advantages are combined, deceptive assets become more genuine and potent, making it more difficult for attackers to locate them. The impacts of this integration are explored in this introduction is the major advantage to the organization. This integration has the capacity to fundamentally alter the adaptive cybersecurity landscape [28].

C. Adaptive Deception

One of the key benefits of Artificial Intelligence and Machine Learning integration with deception technology is adaptive deception. Deceptive assets can autonomously adjust their behaviors and characteristics in response to evolving attack strategies. By learning from past interactions and continuously analyzing threat data, deception sys-

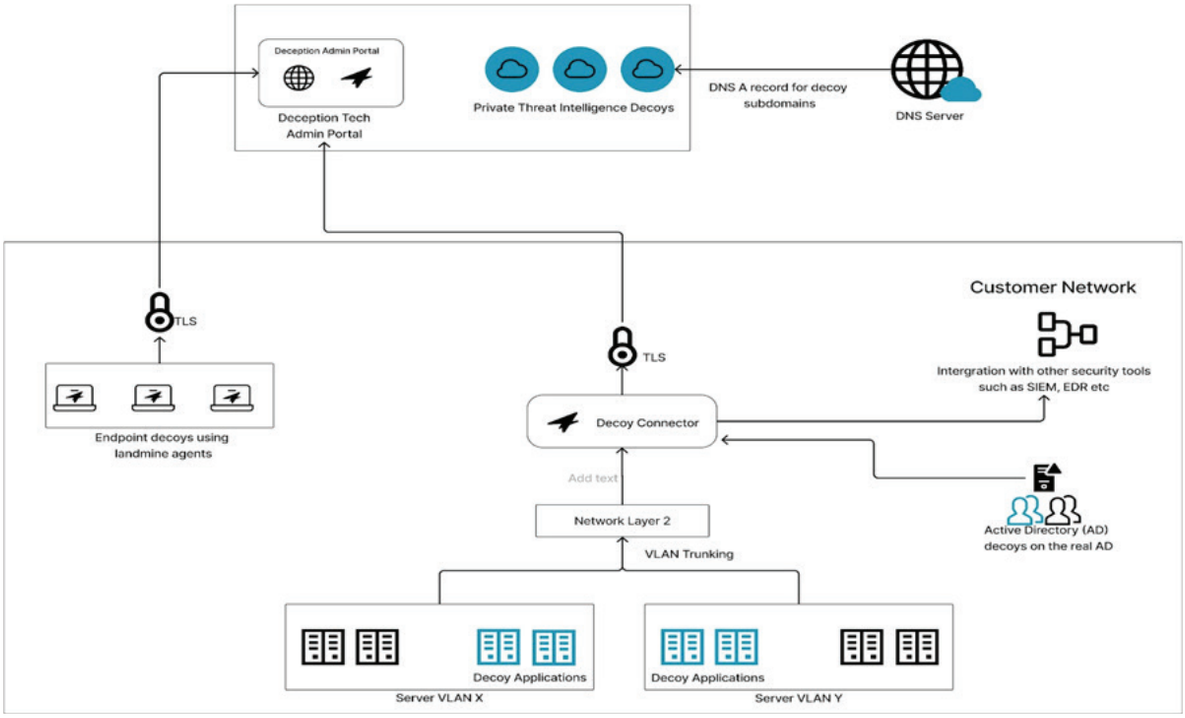

Fig. 2 Architecture of Deception Technology

tems become more challenging for attackers to detect [29].

D. Architecture of Deception Technology

Using a layered architecture, deception technology strengthens cybersecurity protections. Decoys and bait, which imitate actual network resources, are among the deceptive tools it uses, along with deception servers and services that provide the impression of legitimacy. As attackers approach these assets, predetermined policies, misleading triggers, and deception data direct them and cause alarms to sound when they come into contact [18]. Tools for continuous threat detection and analysis, known as real-time monitoring and analysis, offer important insights into the strategies employed by attackers. Through the generation of coordinated responses to threats and the facilitation of incident investigation, deception technology can be integrated into the larger security ecosystem. Proactively identifying and rerouting potential cyber threats is made possible by deception technology, which is scalable, comes with management tools, and requires continuous training for security professionals [11].

Fig. 2 shows an illustration of a cybersecurity deception platform's architecture that demonstrates the use of decoy systems and endpoints in a network to lure attackers into interacting with fictitious resources in order to identify possible threats. The architecture to provide an interactive trap for attackers to gather information about their strategies, and enhance network security in general.

1) Operation Mechanism of FortiDeceptor

FortiDeceptor creates multiple virtual machines across multiple segments of your network. The virtual machines are essentially advanced honeypots that can detect an attacker as soon as they interact with the machine's exposed services. In addition, Fortinet's deception technology deploys tokens to the network's actual endpoints these Tokens are breadcrumbs which direct to the deception machines [30].

Fig.3 shows a hybrid deployment of a deception platform, demonstrating how security management systems and decoys function in both on-premises and cloud settings to give insight into risks in hybrid networks, identify and evaluate malicious activity di-

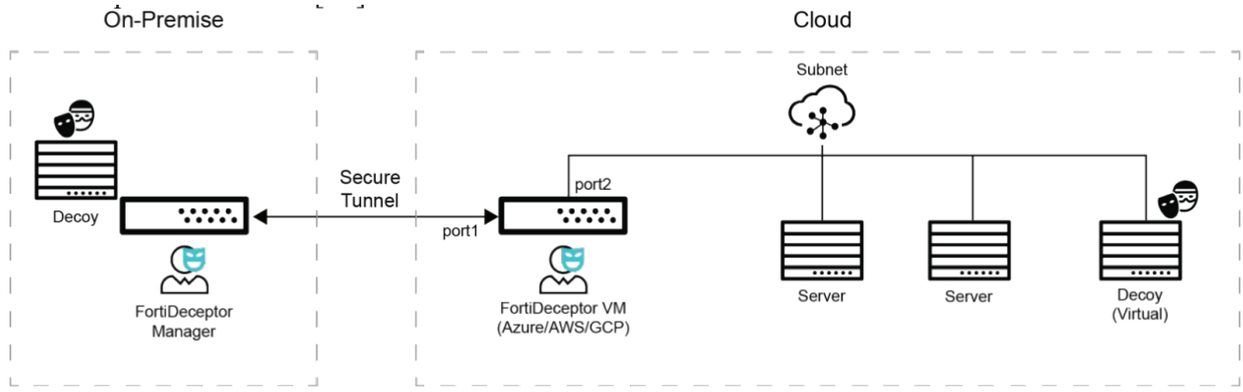

Fig. 3 FortiDeceptor cloud topology

rected at both cloud and on-premises systems, and provide seamless integration and security management independent of the deployment location.

2) Automatic Detection and Response to both external and Internal Threats

FortiDeceptor assists businesses in quickly establishing artificial deception networks, by automatically deploying deception virtual machines (VMs) and decoys that blend in with current infrastructures to fool attackers into disclosing their true identity [15].

FortiDeceptor serves as an early warning system by providing accurate detection of an attacker's activity details and movement which is fed to a broader threat campaign.

Deception technology is unique, it is the only zero false positive cyber-attack early warning system. Its aids in breach prevention by deflecting internal and external threats from important assets [15]. Multiple traps are set up on a network, using decoys that look like data assets and notify the organization when they are triggered. In order to enable forensic analysis to closely monitor patterns, behaviors, and tactics in real time to identify the compromised systems and dangers, FortiDeceptor entices cybercriminals away from the important data and reveals their existence, without their knowledge. The intelligence gathered from the attack can automatically be applied to in-line security controls to stop attacks before there is any significant damage [17].

Features:

- Actionable Visibility
- Automated Protection
- Deployment Ease

Key Characteristics of FortiDeceptor.

Deception OS: Decoy virtual machines (VMs) can be created using images of Windows, Linux, or SCADA OS. Decoy Virtual Machines (VMs): FortiDeceptor can be used to create VMs that mimic genuine endpoint behavior.

Lures: To replicate a genuine user environment, lures can be executed as users, services, or apps to a Decoy virtual machine.

FortiDeceptor Token Package: To set up breadcrumbs on genuine terminals and entice an attacker to a phony virtual machine, install the FortiDeceptor Token Package. To enhance the deception surface, tokens are typically dispersed among the actual endpoints and other IT assets on the network. Utilize tokens to sway the lateral actions and movements of attackers. Cache credentials, database connections, network shares, data files, and files for configuration are just a few instances of what can be used in a token.

Track the attacker's operations by keeping an eye on incidents, events, and campaigns as well.

- A situation, such as a login-logout event on a victim host, describes just one activity.
- Incidents is referred to as all actions on an individual host, such as system file changes,

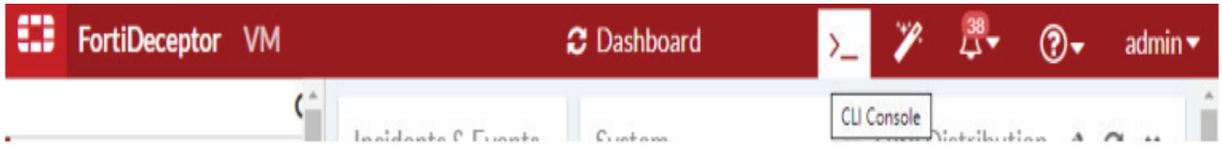

Fig. 4 FortiDeceptor

website visits, login-logouts, and registration alterations, are collectively referred to as

- A Campaign is the sideways movement of the hacker. Every associated incidence constitutes a campaign. An attacker might, for instance, use login information from another system to access a target.

3) Set up FortiDeceptor

This section describes how to set up FortiDeceptor initially. Establish a connection with the GUI To set up and maintain FortiDeceptor, the graphical user interface (GUI) can be used.

To connect to the FortiDeceptor GUI:

1. Use an Ethernet cable to link the device's port 1 (administration) interface to a management system.
2. Set up the management System to share a subnet with the FortiDeceptor units within the interface.
    - Change the IP address of the management system to 192.168.0.2.
    - Change the IP address of the network mask to 255.255.255.0.
3. Go to https://192.168.0.99.
4. Type admin in the Name field, leave the Password field blank, and click Login.

You can now proceed with configuring your FortiDeceptor unit.

4) Connect to the CLI

You can use CLI commands to configure and manage FortiDeceptor.

To connect to the FortiDeceptor CLI:

1. In the FortiDeceptor banner at the top, click the CLI Console icon

   The CLI Console pane opens
2. Click Connect and input your username and password if applicable.

   The CLI Console pane includes icons for opening the CLI console in a separate window, closing the console, clearing the console text, downloading the console text, and copying the console text.
3. Click the Close icon to end the CLI console.

5) Change the system hostname

The entire host's name is visible in the System Management widget. The host name of FortiDeceptor is modifiable.

To change the host name:

1. Select System Information from the Dashboard widget.
2. Next to Host Name, click Change.
3. Enter the new host name in the New Name box.

   A hyphen cannot come at the end of the hostname; it must begin with a letter or number. You can enter a hyphen, A-Z, a-z, or 0–9 (case-sensitive). Punctuation, white space, and other symbols are not permitted.
4. Press the Apply button

6) Change the administrator password

By default, you can access the GUI by logging in with admin and no password. Adding a password to the admin account is highly advised. Passwords for the admin account and any other accounts for administrators you add should be changed on a frequent basis for increased security.

To modify the administrator's password while they are logged in:

1. Select Change Password by clicking the username in the FortiDeceptor banner at the top.
2. After making a password change, click OK.

To modify the Administrators page's administrator password:

- Select Administrators under System.
- Click Edit after choosing an administrator.
- After making a password change, click OK.

7) Configure the system time

The Dashboard is where you may adjust the FortiDeceptor system time. The FortiDeceptor system time can be set manually or synchronized using a network time protocol (NTP) server. In order to set the system time:

1. Select the System Information widget on the dashboard.
2. Next to System Time, select Change.
3. Click Apply after adjusting the system time. You may have to log in once more.

8) Deploy Decoy Virtual Machine

Install Decoy virtual machines on your network by using the Deception webpage. It is possible to track the travels of a hacker who enters Decoy virtual machines without authorization in order to learn how they penetrate the network.

With an acquired subscription service, FortiDeceptor allows custom OS images in addition to the pre-installed decoy Windows, Linux, or SCADA images. You are able to install the FortiDeceptor Toolkit on your own ISO images by uploading them. Click the Help icon in the toolbar and choose Configuration to get instructions.

E. Networking Requirements for Deception Technology

Deception is said to be in a wide range of networks, including local area networks (LANs), wide area networks (WANs), and virtual networks in cloud environments, when it comes to networking, its most important factor is the ability to maintain the decoy or deception which can be virtual or not that can be positioned across board within the network. For example, a decoy could be put in a high traffic or out of control assets in a LAN setting where they likely to see an invaders or attackers. This decoy could be placed in various large location of Wide area network environment.

IV. Experiment Results

A. Deceptive Asset Deployment

In an organization, elements such as asset type believability, distribution across the area network dispersion must take account of all and optimize them all. Decoy technology maximize deceptive assets deployment in a basic component whereby taking honeypot with high interaction levels to be strategically used to engaged with invaders or attackers because they are almost lookalike like a real system and this can aid in early detection without requiring a large some of investment of resources in the organization.

B. Deception Technology Infrastructure

Docker and Kubernetes are two wonderful examples of containerization technologies that can be used for effectiveness asset deployment and management, where Segmentation and isolation are essential in preventing the compromised of legitimate assets, putting in place the systems and network architecture needed to enable deceptive assets is part of a strong deception technology infrastructure of the following:

1. Collection of data: This process is done by algorithm by collecting data about the network ad its assets. These collections will be based on the services running on each host, the IP addresses and Open ports.
2. Positioning of Decoy: this is where the algorithm would ascertain the best location for the decoys based on the data collected or the information gathered.
3. Configuration of Decoy: This process would be built up by the algorithm in a resemblance way.
4. Lure Generation: this is a kind of misleading components that could entails tricks or forging of emails, papers, or other appealing targets.
5. Monitoring and Alerting: This is where the process whereby a monitoring activity are

carried out after the lures and decoys are set up, the algorithm will then keep an eye out for any questionable activity. There can also be system that will give alarm on the event or activities that are carried out.

6. Adaptability: the is process to carry out the flexibility of the algorithm to adjust to network modifications and needed to be updated upon.

C. Threat Intelligence Integration

Deception technology have open-source intelligence, historical data attack and real time threat feed added to them, remaining ahead of some enemies that requires effective threat intelligence integrations, Security information and event management (SIEM) are responsible for centralized threat analysis that are made possible by integration.

D. Automation and Orchestration

Once it comes to managing fraudulent assets, orchestration and automation plays a very vital role, by enabling and automating the deployment of phony assets, security orchestration solution, this will require the need of human interaction or manual process when responding to the threat that are detected by the system in the organization.

E. Interaction and Engagement Strategies

Deception technology entice their victims to interact with fraudulent resources from foundation using various techniques like system levels, interaction at the application and the network. This interaction could bring challenges involving revealing the nature leading to the developments of custom interaction and that of the assets.

F. Threat Detection Algorithms

An effective deception technology relies on sophisticated algorithms for the detection of threat and with the help of machine language models, anomaly detection and behavioral analysis is able to differentiate between safter user interactions and harmful activity to the organization network. These algorithms or models are continually updated to accommodate new attack techniques. FortiDeceptors is the most difficult algorithm or techniques that lies its ability to constantly adjust to network changes.

This is may be achieved through the use of Phasor technology.

The deception algorithm used by FortiDeceptor heavily relies on phasor technology. Decoys and lures in the deception network will consistently match the network and services, even in the event of network alterations or application changes. The deception network's ability to adapt is essential to its continued efficacy. Attackers will be able to quickly identify phony decoys and lures as such, making the deception network ineffective, if they do not faithfully mimic the real network and services. Phasor technology does this by continuously scanning the network and its services, updating the decoys and lures to reflect the network's present condition. Because it is automated and doesn't need human intervention to achieve its aim, this procedure is scalable and effective.

The algorithm also takes into account the 'attractiveness' of the decoys and lures. This is a measure of how likely they are to be targeted by attackers. The more attractive a decoy or lure is, the more likely it is to be selected by the algorithm for deployment.

G. Real-time Monitoring and Analysis

Real-time monitoring is imperative to detect and respond to threats promptly. Security Operations Centers (SOCs) rely on real-time dashboards and alerts generated by the deception technology. Big data analytics and visualization tools are used to analyze the vast amount of generated data.

H. Adaptive Deception Technology

- A cybersecurity approach that uses AI and machine learning (ML) to create and manage fake assets and interactions.
- These assets evolve over time to stay effective against changing attacker tactics.

I. Architecture of FortiDeceptor

FortiDeceptor is designed to identify and isolate malicious actors by deploying lures that draw attackers to deception decoys looking at the FortiDe-

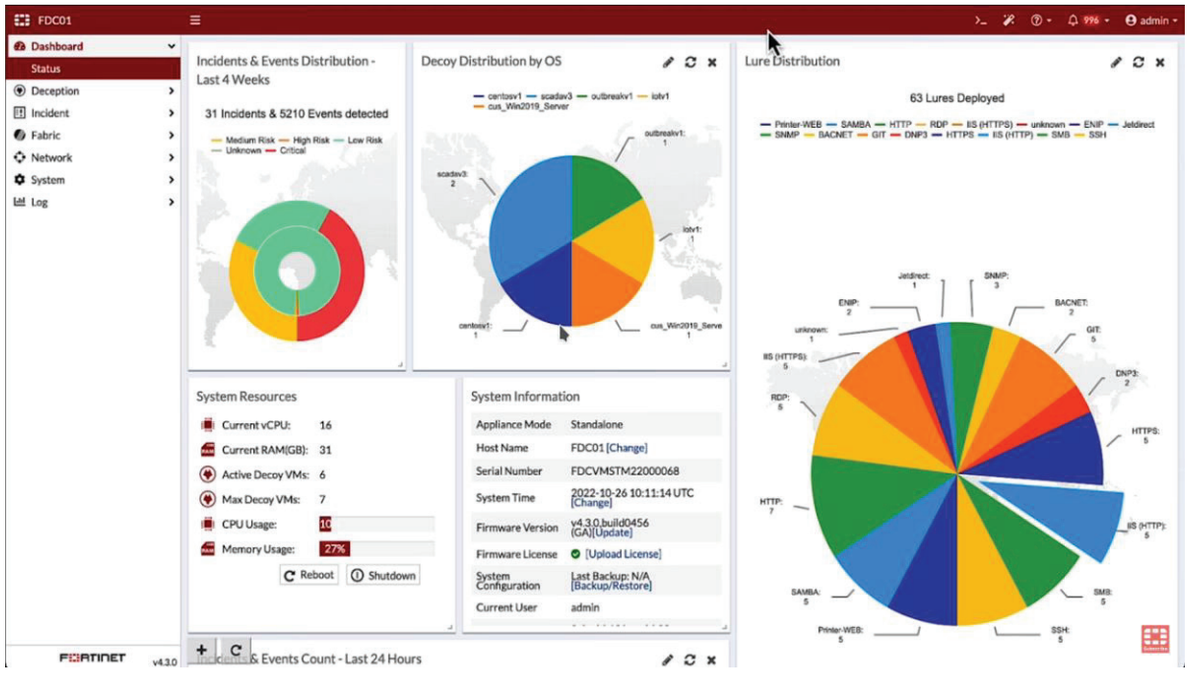

Fig. 5 Dashboard of the FortiDeceptor interface

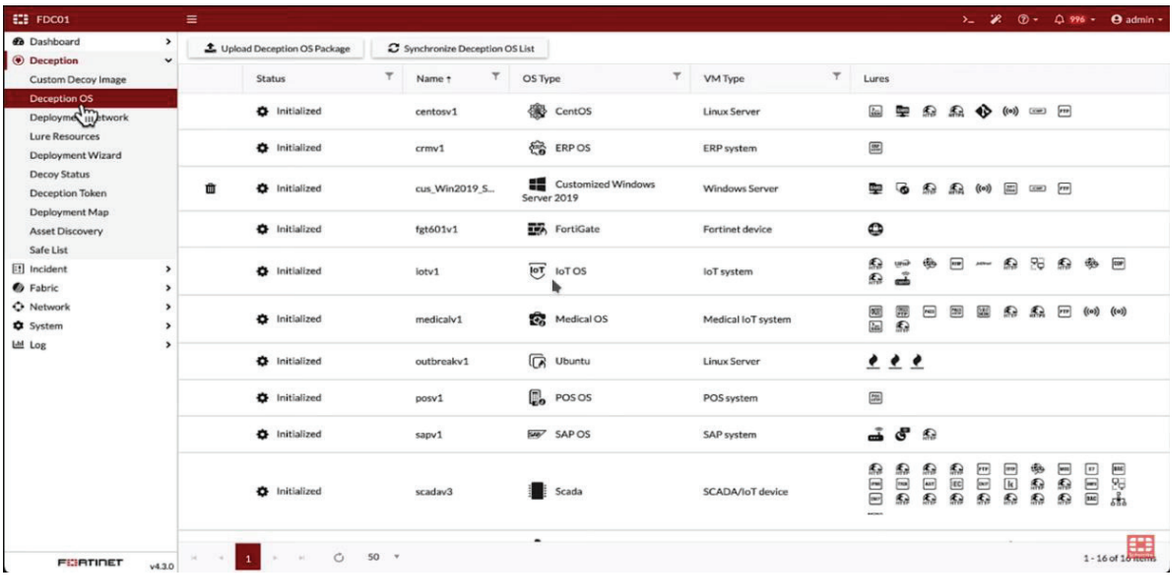

Fig. 6 Deception OS

ceptor dashboard, it is observed that the distribution of decoys by operating system in this environment we have several types of decoys including Linux windows and OT and we can also see the lowers that are deployed and visible to attackers on the network such as RDP SMB and http the dashboard also shows the incidents and events over the past four weeks and basic system health information.

Fig. 6 shows deception OS looking deeper into the decoys and lures the deception OS tab shows all the operating systems available for use in creating decoys this is an extensive and growing list of os types including voice-over-IP, IOT, multiple Linux OS's and windows workstations security analysts can also add custom OS images (like windows, ubuntu) to forward a deceptor for each deception

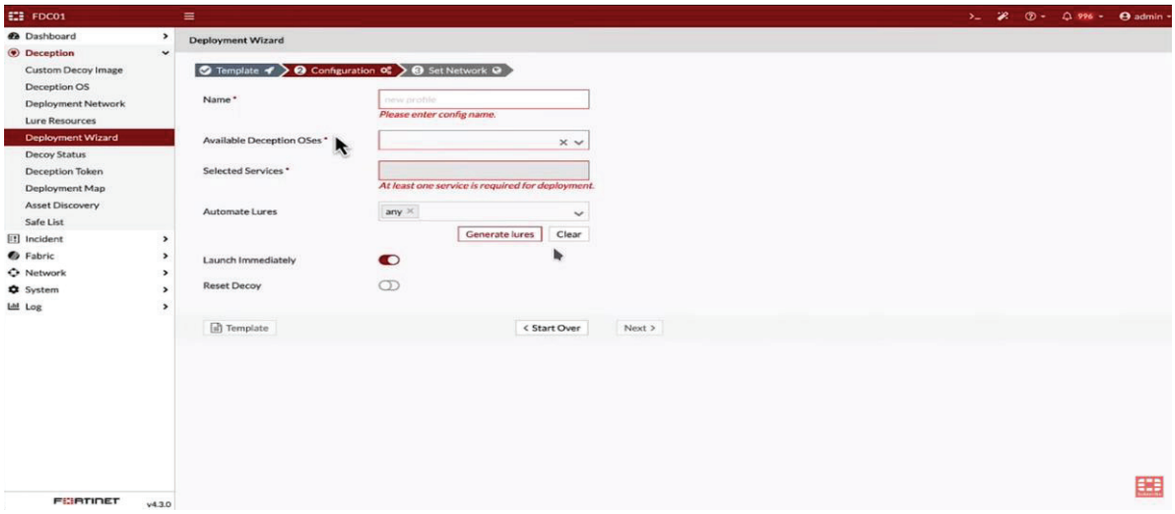

Fig. 7 Deployment Wizard

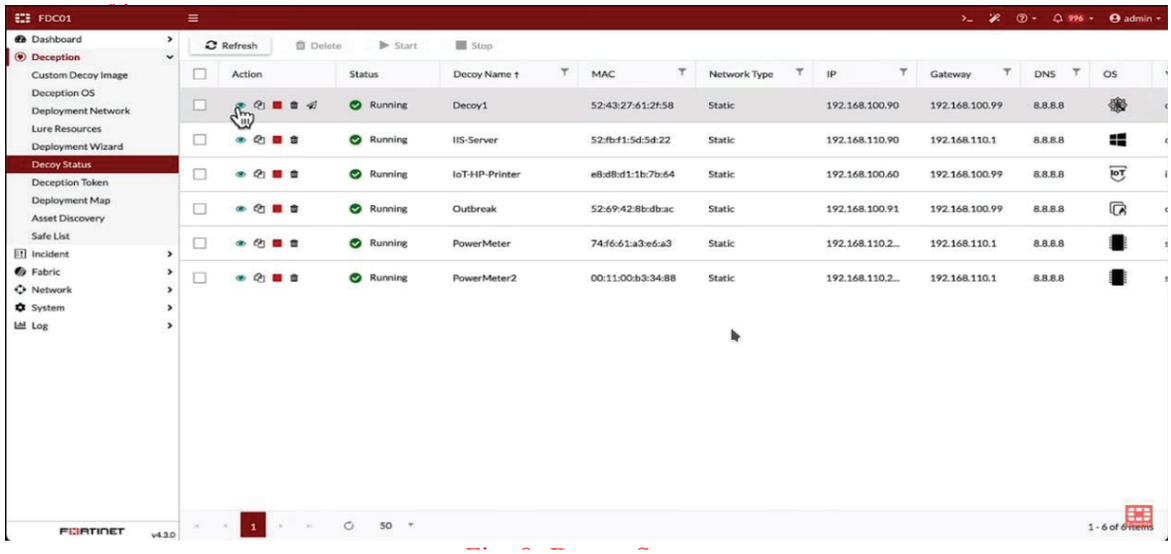

Fig. 8 Decoy Status

OS we can also see the lures that are deployed on the network for that OS type in the case of the OT deception OS we have lures such as HTTP tftp and modbus while in the Linux OS we have SSH, Samba and git among others in total for the deceptor supports more than a dozen deception os's and 29 different lures.

Fig.7 deployment Wizard deploying deception decoys is done through the deployment wizard on the deployment wizard screen we have the option to choose from a list of available deception os's choosing the scada deception OS we also have the option of choosing from a list of available decoys.

MAC Address this is a growing list of OT device types from manufacturers such as Schneider Rockwell GE and Siemens once a decoy is chosen, we can see the available lures that will be deployed for that device after selecting the deception OS and decoy FortiDeceptor will automatically generate a MAC address that matches the manufacturer and once the network settings are configured the decoy will start to Initialize Decoy Status looking at the decoy status.

Fig. 8 as seen above, it is seen that all decoys created on the FortiDeceptor looking at a Linux decoy in more detail we can see the configuration details and all the lures that have been deployed

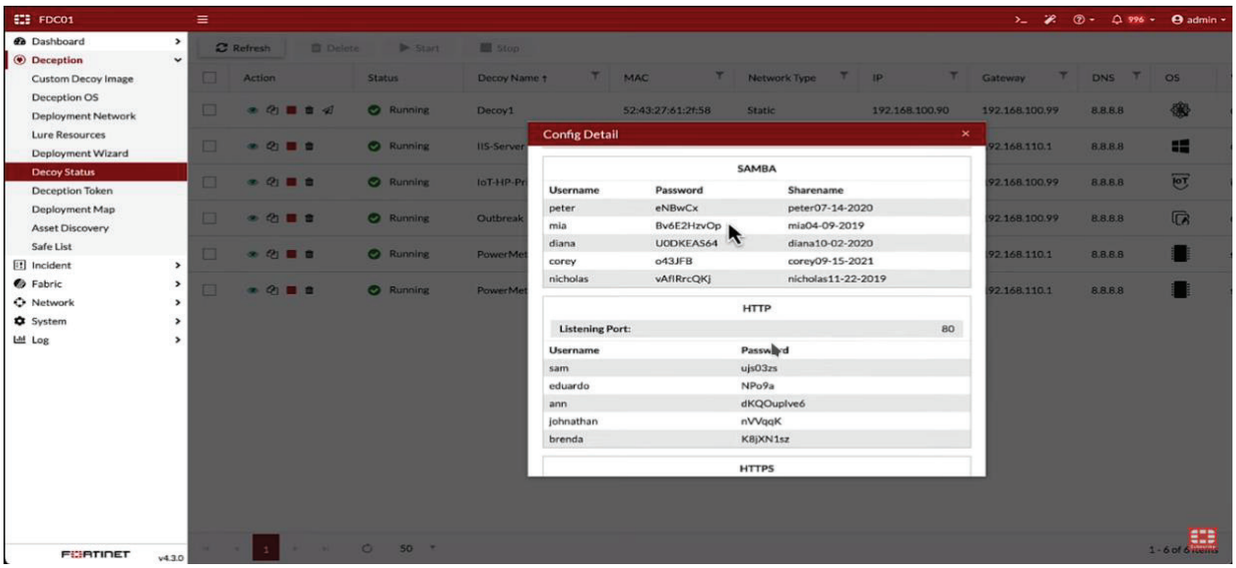

Fig. 9 Decoy Status-Configuration Details

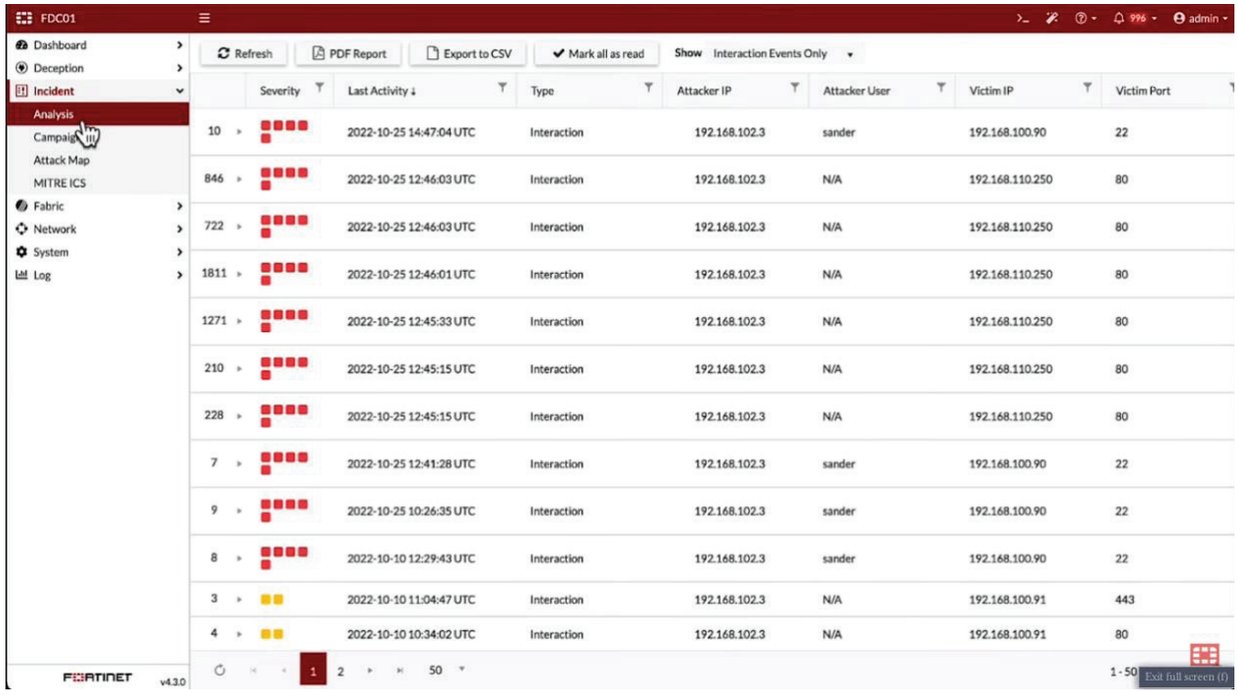

Fig. 10 Deception Analysis Interface

on the network we can also see credentials for SSH HTTP and https along with details.

Fig. 9 Samba and git Analysis is used to monitor all interactions with the decoys in the analysis section of the FortiDeceptor admin interface looking deeper into an event reveals details about the interaction between the attacker and the decoy here we can see the user account used by the attacker and their IP address FortiDeceptor also Maps the attack techniques to the mitre ICS framework clicking on one of the ICS techniques opens a new tab with additional details in this case more information about the lateral tool transfer technique Example continuing through the interaction details we can download

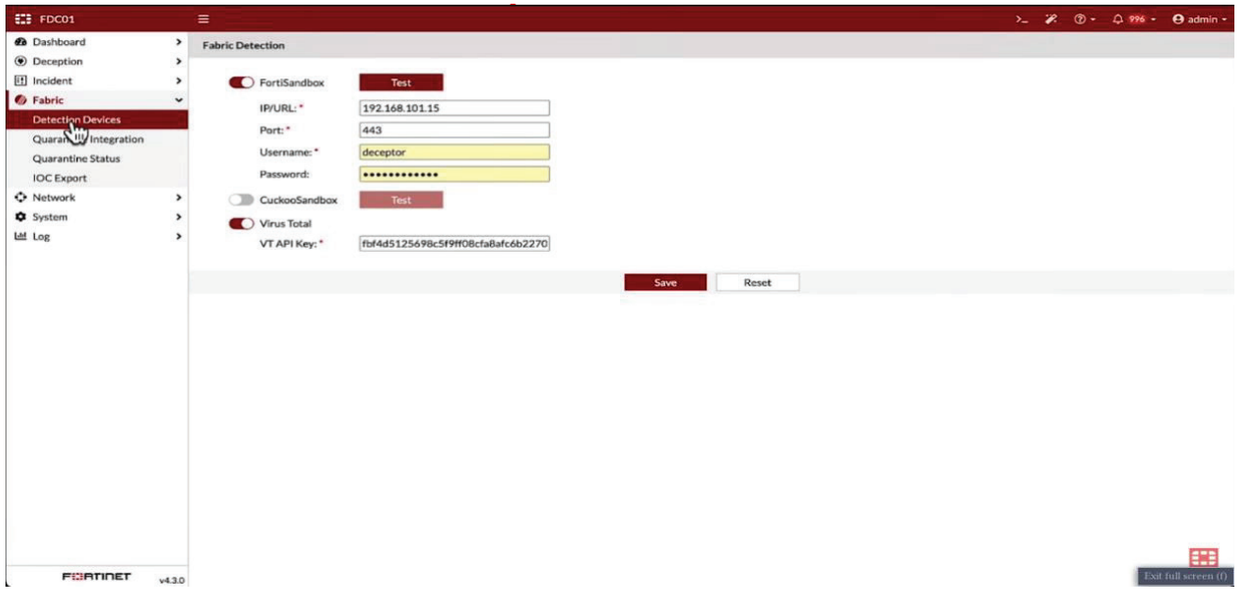

Fig. 11 Detection Devices Interface

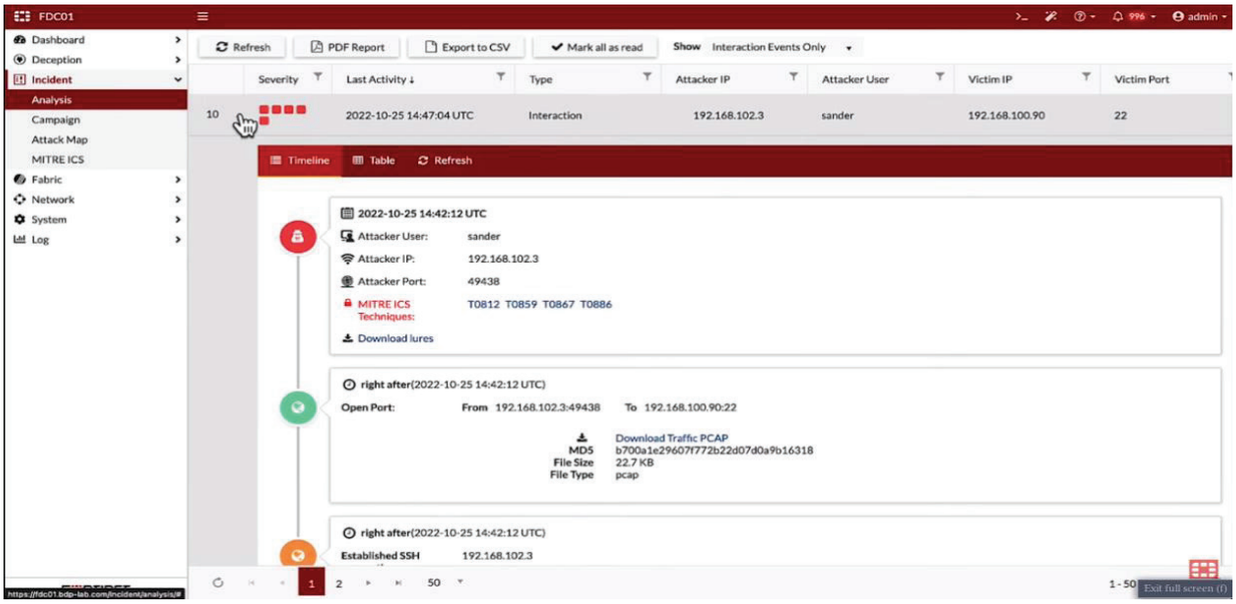

Fig. 12a Detailed Report on Detected Devices

a copy of the pcapp file and see the login detail and commands executed on the decoy in this example we have an attacker who connected via SSH. This attacker can be said to use a normal connection which can be:

- Verified interactions with actual network resources devoid of curious data requests, lateral movements, or indications of reconnaissance.
- Appropriate user actions that fit the normative patterns and conduct anticipated within the community.
- The ability for authorized individuals or systems to access real organizational assets without setting off ruses or lures.
- Traffic patterns that are anticipated and fit the organization's predetermined parameters.

Normal connection is different from assaults connection, which can be seen as:

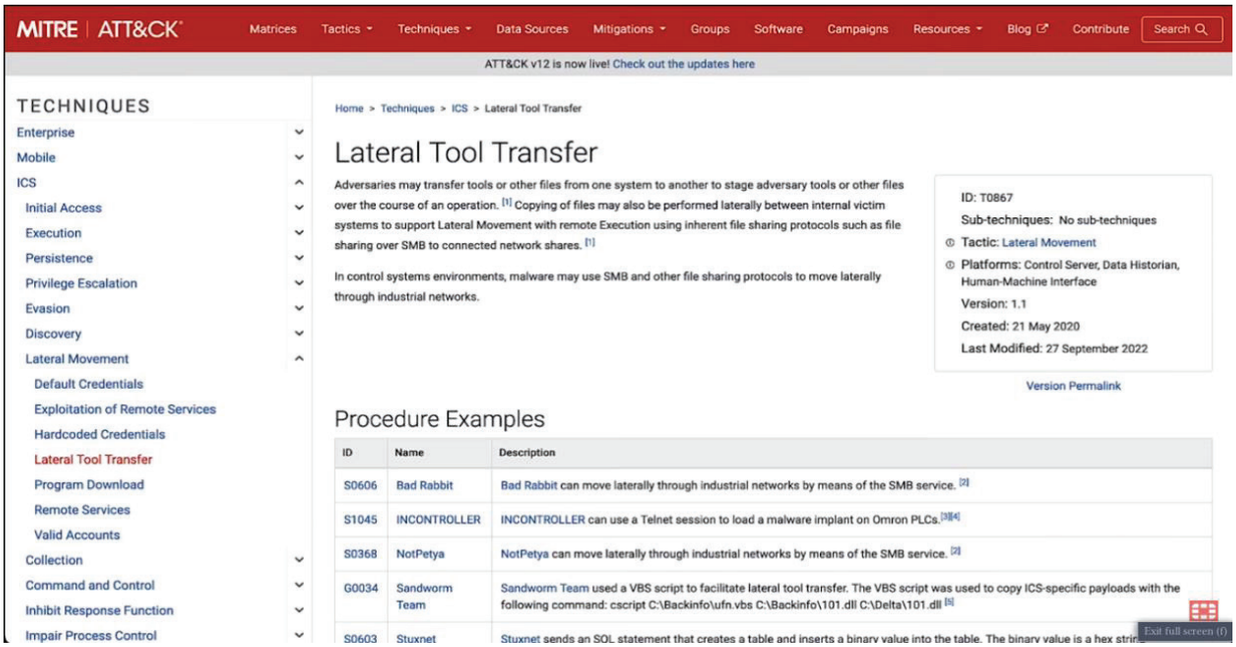

Fig. 12b: Detailed Report on Detected Devices

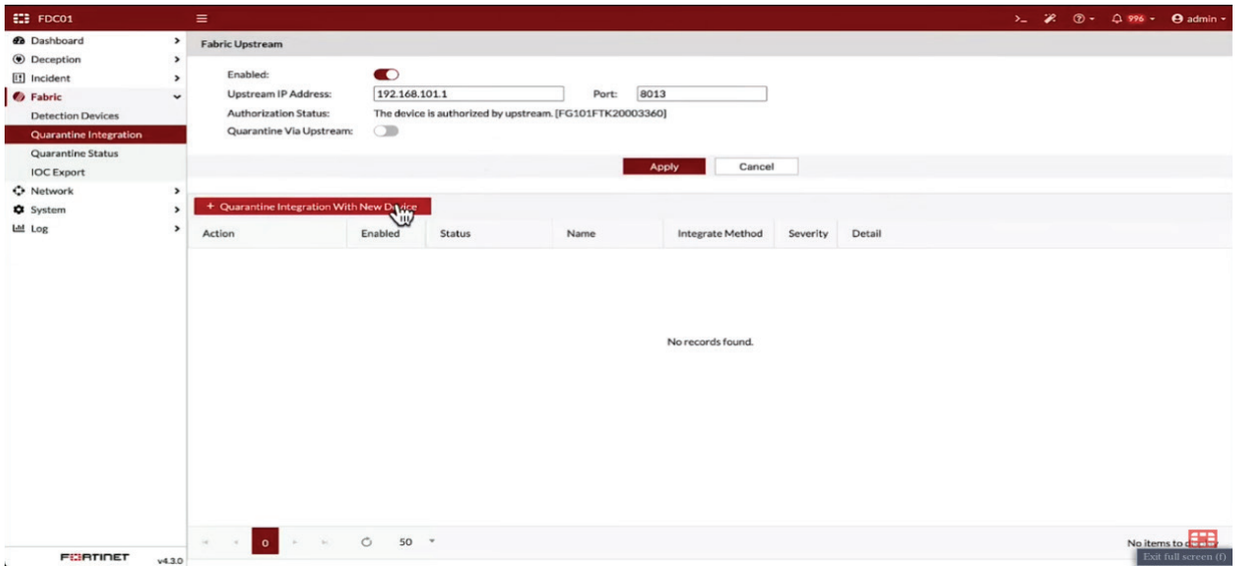

Fig. 13a: Quarantine Integration with other devices

- Interactions with misleading assets that are set up by deception technology without authorization, such as decoy virtual machines, honeypots, or honeytokens.
- Questionable practices, such as spying, probing, or attempts to take advantage of fictitious assets.
- Unusual user activity, like trying lateral moves based on lures or accessing decoy credentials. Decoy endpoints are used to monitor and trap intruders by imitating genuine systems.
- Malicious activity identified by threat detection systems, such as repeated unsuccessful attempts to log in or odd commands run on dummies.

This shows an example of the interaction details

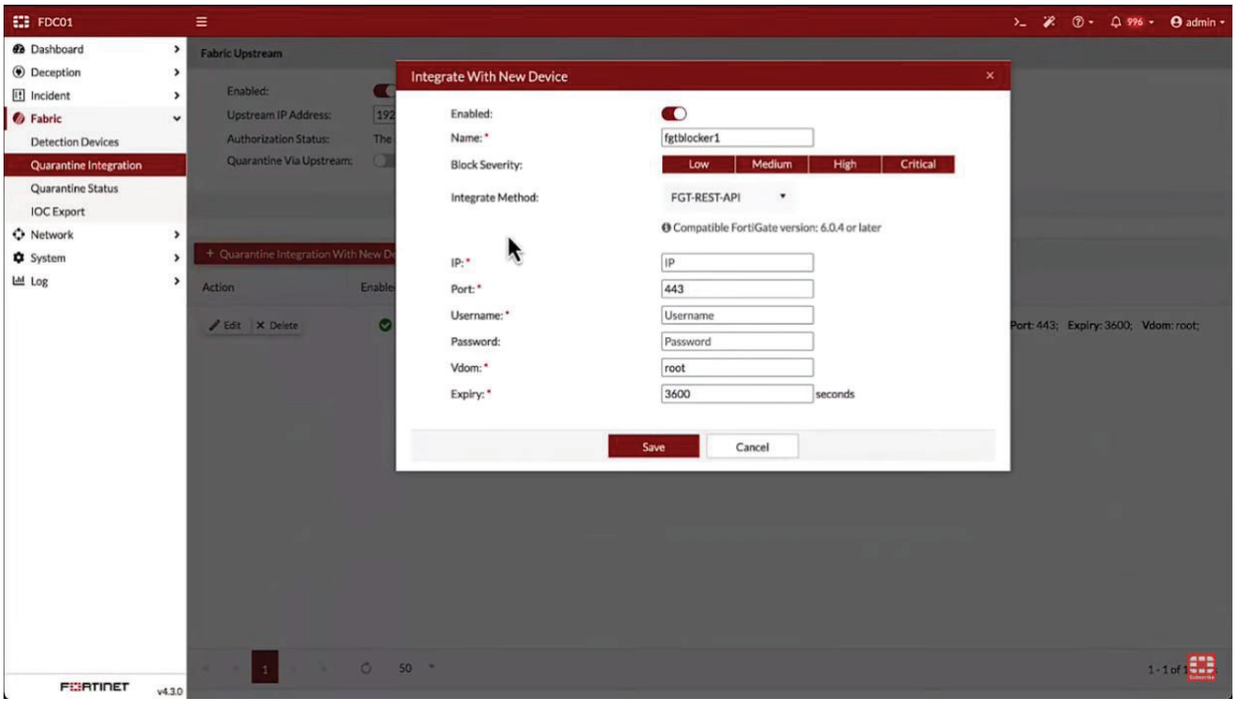

Fig. 13b Quarantine Integration with other devices

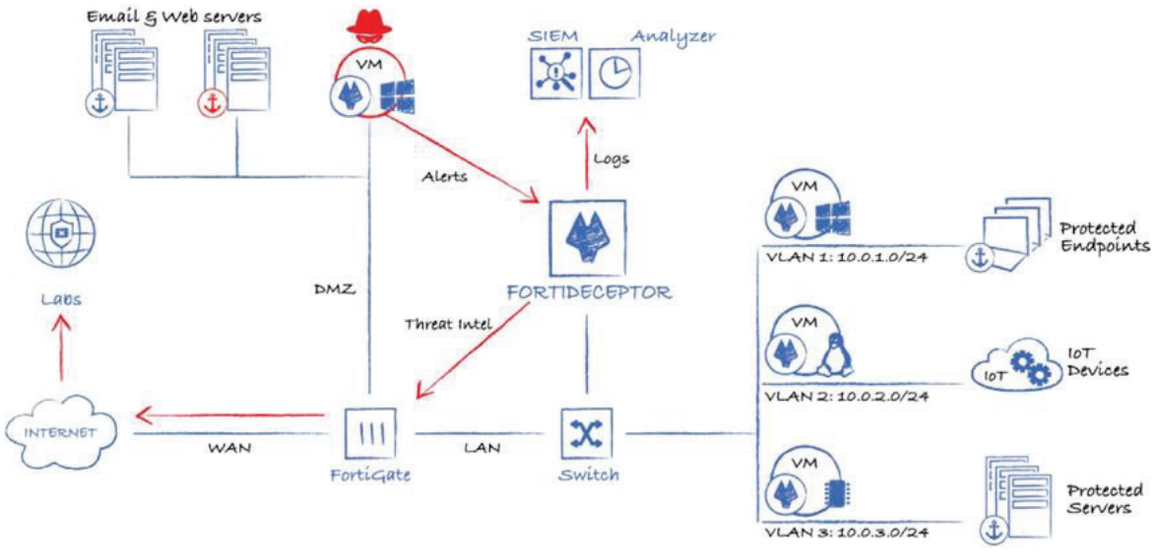

Fig. 14: FortiDeceptor Architecture

between the attacker and the decoy here we can see the user account used by the attacker and their IP address, the last activity, victim IP and their victim port.

Fig. 11 shows the detection device interface containing the Fortisandbox which are sub divided into IP/URL, port, username, password and UTAPI key which you can either save or reset.

Integrations as we saw in the interaction details for the deceptor can integrate with the Fortinet security fabric as well as third-party services and platforms for the deceptor supports sandbox integration with Fortisandbox and cuckoo sandbox and API integration with virustotal in addition to detection device integration FortiDeceptor also has a number of built-in quarantines.

This shows an integration to isolate a compromised endpoint when an incident is detected as part of the security fabric for the deceptor integrates with fortigate for The Knack and 40 EDR and also has built-in Integrations with Palo Alto and Cisco ise Microsoft ATP checkpoint firewall and crowdstrike. Below is an overview of the architecture and components of FortiDeceptor.

Fig. 14 shows the following:

1. Deception Fabric: FortiDeceptor is built on a Deception Fabric, which is a distributed network of deceptive assets. These deceptive assets include decoy servers, endpoints, and services. They are strategically placed within the organization's network, imitating real systems and applications.
2. Deception Engines: The Deception Fabric is powered by Deception Engines, which are responsible for managing and controlling the deceptive assets. These engines monitor the interactions with the deceptive assets and generate alerts when suspicious activities are detected. The engines use various detection techniques, including analyzing network traffic, user behavior, and attacker engagement with the deceptive assets.
3. Centralized Management: FortiDeceptor provides a centralized management console that allows security administrators to configure and manage the deceptive assets. The management console offers a user-friendly interface for defining deception policies, creating deceptive assets, and monitoring the network's security posture.
4. Threat Intelligence Integration: FortiDeceptor integrates with threat intelligence feeds and databases to enhance the authenticity of the deceptive assets. By incorporating up-to-date threat intelligence, the solution can mimic the latest attacker tactics and vulnerabilities, making it more convincing to potential threats.
5. Automation and Adaptation: One of the key features of FortiDeceptor is its ability to automate the deployment and adaptation of deceptive assets. The solution can dynamically create and adjust deceptive elements based on observed attacker behaviors. This dynamic adaptation ensures that attackers are continually misled and that the deception remains realistic.
6. Alerts and Incident Response: When suspicious activities are detected, FortiDeceptor generates alerts that are sent to the organization's Security Information and Event Management (SIEM) system or Security Operations Center (SOC). These alerts contain valuable information about the attacker's tactics, techniques, and procedures, enabling security teams to respond effectively.
7. Integration with Fortinet Security Fabric: It is possible to connect FortiDeceptor with the wider Fortinet Security Fabric with ease. In doing so, a wide-ranging and flexible security ecosystem is established, enabling synchronized attack response across many Fortinet security solutions.
8. Scalability and Customization: FortiDeceptor's design is adaptable and scalable to meet the unique requirements of the organization. Depending on their computer system environment and the kinds of attacks they expect, organizations can use a range of deceiving assets.
9. Reporting and Analytics: Security teams can look at data on attacker contacts, false positives, and the overall security posture to make well-informed decisions. FortiDeceptor's tracking and analytics features provide insight into how successful the deception scheme was. The core of FortiDeceptor's design is a Deception Fabric, which is built up of a network of misleading resources under the command of Deception Engines. This architecture provides a robust and adaptable cybersecurity solution by enhancing threat detection, automating flexibility responses, and facilitating seamless integration with Fortinet's broader Security Fabric.

J. Integration with Business Processes

The success of deception technology depends on how well it is integrated into current business

procedures. Plans for incident response and business continuity should consider the capabilities of the technology. By proactively engaging with potential attackers, giving real-time information about developing dangers, and facilitating early intervention, deceptive technology improves organizational agility. Organizations can develop a dynamic security layer that disorients, confuses, and gathers threat intelligence from potential attackers by deploying assets that are intended to look and behave like genuine resources. With the use of this data, security teams can react quickly to changing cyberthreats and ensure business continuity through informed decision-making that enhances threat detection capabilities.

In order to facilitate coordinated reactions and incident management, deception technology can be simple to integrate with the current security architecture to transmit threat intelligence. This integration helps the company become resilient overall in the face of dynamic and complex cyber threats by ensuring that the deception strategy is in line with the larger cybersecurity environment.

V. Conclusion

Deception technology offered most crucial insights into new dangers by adding a typical security or preventive measures to the network across board today and integrating deceptive elements within their cybersecurity strategies, organizations have achieved proactive threat detection. Utilizing deception technology, cybersecurity has advanced into a revolutionary developmental level, this is an advantage that can make businesses more flexible. The consequences for organizations agility are significant, continuously developing and offers more exciting opportunities, this also has the potential or ability to change the cybersecurity landscape for good in an organization. Because deception technology is so inventive and flexible, cybersecurity has a bright future ahead of it.

The accuracy of this research findings can be verified by real-time monitoring of the network dashboard and continuous scanning. The ability of a system or technology to attract or lure attackers is what deception technology is all about. The IP address, URL and port number of the attackers can be verified to prove that it is illegitimate. An online service like virus total can also be used to analyse suspicious files and the URL . Figures 8, 9 and 10 has clearly demonstrated how the findings can be verified.

VI. Recommendations

For an organization to be able to detect threat and increase greatly in productivity, there should be an integration of deception technology into their cybersecurity plan taking into consideration optimizing the benefits. In order to pinpoint high value assets and probable attack routes requires doing a thorough risk assessment and threat modeling. Incorporating deception technology can be used to much greater effect in our organization can significantly boost the cybersecurity strategy. Organizations should also update and improve misleading assets on a regular basis to make sure they stay credible and in line with newly developed attack strategies.

Finally, organizations should try and spend more on training their staffs on cybersecurity when it comes to dealing with customers and many more and the development of well-defined incident response procedures. Effective detection and response are integral to business adaptability.

Conflict of Interest

Authors declare that they have no conflict of interest.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Bauer, L. Zavolokina, F. Leisibach, and G. Schwabe, "The value creation from decentralized ledgers," *Frontiers in Blockchain*, pp. 1-9, Jan. 2020.

[2] L. M. Dille, "Deception in earnings management," Ph.D. dissertation, School of Business and Management, Dept. of Accounting and Finance, Morgan State University, 2019.

[3] J. F. George, M. Gupta, G. Giordano, and A. M. Mills, "The detection of deception in electronic media," pp. 1-6, June 2014.

[4] K. Dickinson, "Measuring the impact of deception technology on reducing dwell time in cyber incidents," pp. 1-6, 2020.

[5] X. Zhu and J. Zolkiewski, "Exploring service adaptation in a business-to-business context," *Journal of Service Theory and Practice,* vol. 26, no. 3, pp. 319-330, 2016, doi: 10.1108/JSTP-02-2014-0039.

[6] A. Boza, L. Cuenca, and R. Poler, "Interoperability in the ERP field," *Journal of Informa UK Limited,* 2015, doi: 10.1080/17517575.2013.866697. [Online]. Available: https://e-space.mmu.ac.uk/625947/.

[7] S. Ludwig, T. Van Laer, K. De Ruyter, and M. Friedman, "Exploring automated detection of deception in computer-mediated communication," *Journal of Management Information Systems*, vol. 33, no. 2, pp. 512–534, Oct. 2016, doi: 10.1080/07421222.2016.1205927.

[8] P. Andries and K. Debackere, "The need for adaptation in new technology-based businesses," *International Journal of Management,* pp. 91-106, June 2016.

[9] M. A. Khan, "The co-evolution model of business and IT for dynamic business process requirements," *International Journal of Advanced Computer Science and Applications,* vol. 7, no. 2, pp. 348-351, 2016.

[10] J. Chelliah and Y. Swamy, "Deception and lies in business strategy," *Journal of Business Strategy,* Oct. 2018, doi: 10.1108/JBS-09-2017-0135.

[11] Sharif, "Deception technology in healthcare: Protecting patient data and medical devices," 2019.

[12] D. Chang, "Deception technology and its role in mitigating insider threats in business," 2017.

[13] S. Patel, "Adaptable cybersecurity solutions for modern businesses," 2016.

[14] D. S. Chen, "A framework for evaluating business adaptability with deception technology in cybersecurity," 2017.

[15] S. L. Kim, "Mitigating insider threats and enhancing business adaptability: The role of deception technology," 2019.

[16] M. P. Lee, "Adapting to emerging cyber threats: The influence of deception technology on business resilience," 2020.

[17] R. W. Grant, "Practical implications of deception technology for business cybersecurity and adaptability," 2015.

[18] E. Cantella, "Architectural style: Distortions for deploying and managing deception technologies in software systems," M.S. thesis, Dept. of Software Engineering, Golisano College of Computing and Information Sciences, Rochester Institute of Technology, Rochester, NY, 2021.

[19] O. A. Ayeni, B. K. Alese, and L. O. Omotosho, "Design and implementation of a medium interaction honeypot," *International Journal of Computer Applications*, vol. 70, no. 22, pp. 5, May 2013.

[20] "The rise of deception technology: Luring cybercriminals into traps to disrupt attacks," [Online]. Available: https://akitra.com/the-rise-of-deception-technology/. Accessed: Nov. 22, 2024.

[21] "What is deception technology? Benefits & use cases," [Online]. Available: https://www.thundercattech.com/tcat_blog/deception-technology/. Accessed: Nov. 22, 2024.

[22] S. Sarkadi, A. Rutherford, P. McBurney, S. Parsons, and I. Rahwan, "The evolution of deception," *R. Soc. open sci.,* vol. 8, pp. 1-5, Aug. 2021.

[23] D. Kalla, S. Kuraku, and F. Samaah, "Advantages, disadvantages and risks associated with ChatGPT and AI on cybersecurity," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 10, no. 10, pp. h84-h93, Oct. 2023.

[24] C. Krasznay and G. Gyebnár, "Possibilities and limitations of cyber threat intelligence in energy systems," *13th International Conference on Cyber Conflict Going Viral,* pp. 171-186, 2021. [Online]. Available: https://ccdcoe.org/uploads/2021/05/CyCon_2021_Krasznay_Gyebnar.pdf.

[25] G. Cascavillaa, D. A. Tamburri, and V. D. Willem-Jan, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Journal of Computer and Security,* pp. 1-26, Mar. 2021. [Online]. Available: www.sciencedirect.com.

[26] T. D. Wagnera, K. Mahbuba, E. Palomara, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Journal of Computer and Security,* pp. 1-22, Jan. 2019.

[27] H. Rehan, "Artificial intelligence and machine learning: The impact of machine learning on predictive analytics in healthcare," *Innovative Computer Science Journal*, vol. 9, no. 1, pp. 1-18, 2023.

[28] M. Paramesha, N. L. Rane, and J. Rane, "Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence," *Partners Universal Multidisciplinary Research Journal (PUMRJ),* vol. 1, no. 2, pp. 110-129, June-July 2024.

[29] T. Yin and G. Zhou, "Security control for adaptive event-triggered networked control systems under deception attacks," *IEEE Access*, vol. 8, pp. 10789-10795, 2020, doi: 10.1109/ACCESS.2020.3043238.

[30] [Online]. Available: https://www.fortinet.com/products/fortideceptor. Accessed: Nov. 22, 2024.