BUFFERZONE

BUFFERZONE® Safe Workspace™ Prevention and Protection In MITRE® D3FEND™ Framework

In the ever-evolving landscape of cybersecurity, frameworks play a vital role in understanding and explaining how to defend against adversarial tactics and techniques. Two prominent frameworks, MITRE ATT&CK™ and MITRE D3FEND™, provide comprehensive insights into offensive and defensive cybersecurity strategies. This article will delve into what MITRE® D3FEND™ [1] (version 0.12.0-BETA-2) is and explore its relationship with the previously discussed MITRE ATT&CK framework [2] (BLOG). Organizations can develop more robust and effective cybersecurity strategies by understanding these frameworks and their interconnections.
This Whitepaper will focus on how BUFFERZONE® Safe Workspace™ prevention and protection capabilities are mapped in the MITRE D3FEND framework.

MITRE ATT&CK:

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a well-established framework focusing on offensive cybersecurity. It provides comprehensive information on the tactics, techniques, and procedures (TTPs) commonly used by adversaries to breach networks and compromise systems [2].

ATT&CK offers a knowledge base and a matrix that categorizes adversary behavior and maps it to various stages of an attack lifecycle [2]. The framework covers various platforms, including Windows, Linux, macOS, mobile devices, cloud-based systems, and industrial control systems [3]. It categorizes TTPs into tactics, techniques, sub-techniques, and documented adversary usage, providing a detailed taxonomy for offensive cybersecurity. The ATT&CK Matrix visualizes the relationships between tactics, techniques, and sub-techniques, enabling organizations to understand the different phases of an attack and associated tactics.
By utilizing ATT&CK, organizations can evaluate common adversary behavior, identify potential vulnerabilities in their systems, and enhance their cybersecurity strategies [2].

What is MITRE D3FEND?

MITRE D3FEND, which stands for "Defensive Cyber Framework," is a knowledge graph released by MITRE to establish a common language and framework for cybersecurity defenders [1]. It is a companion project to the well-known MITRE ATT&CK framework but with a distinct focus on defensive techniques and countermeasures. While MITRE ATT&CK provides a comprehensive understanding of adversarial tactics, techniques, and common knowledge, D3FEND aims to categorize and illuminate defensive methods employed by cybersecurity professionals [1].

Understanding the Relationship between MITRE ATT&CK and MITRE D3FEND:

MITRE ATT&CK focuses on offensive tactics and techniques adversaries use to breach networks, MITRE D3FEND concentrates on defensive strategies and countermeasures [1]. The D3FEND framework establishes terminology and vocabulary for defensive techniques, shedding light on the relationships between defensive and offensive methods [2].

By utilizing both frameworks together, cybersecurity professionals comprehensively understand the full spectrum of cyber threats and effective defensive strategies. The ATT&CK matrix visualizes the phases of an adversary's attack lifecycle. It provides insights into offensive tactics and techniques, while the D3FEND knowledge graph complements it by offering a vocabulary of defensive methods and countermeasures [3].

BUFFERZONE Safe Workspace D3FEND Protection Mapping:

The MITRE D3FEND framework organizes defensive cybersecurity techniques into six categories or stages of defense:

- **Harden**: This category focuses on hardening the security of applications, platforms, credentials, and messages. Techniques under this category include application hardening, platform hardening, credential hardening, and message hardening [1].
- Detect: The detect category involves techniques for detecting potential threats and malicious activities. It includes network traffic analysis, process analysis, file analysis, platform monitoring, identifier analysis, message analysis, and user behavior analysis.
- Isolate: Techniques under the Isolate category aim to isolate or contain threats within the network. This includes network isolation and execution isolation methods.
- Deceive: The deceive category involves techniques used to mislead or deceive adversaries. This can be achieved through the creation of decoy environments or decoy objects.
- Evict: The evict category focuses on techniques to evict or remove adversaries from the network. It includes credential eviction and process eviction methods.

D3FEND's defensive techniques are linked to MITRE ATT&CK techniques and the artifacts they produce, offering a comprehensive understanding of the connection between defensive and offensive methods [1]. BUFFERZONE® Safe Workspace™ is a suite of preventive tools that rely on application isolation technology. It includes Safe Browsing, SafeBridge® (with Content Disarm and Reconstruction (CDR) capabilities), and Safe Removable (for USB attack prevention), all equipped with clipboard security. The Safe Workspace™ virtual container is created by a kernel driver, which divides the operating system into two logical areas.

The first area, referred to as the trusted zone, is connected to all the organization's networks and files within the operating system. The untrusted zone, the second area, acts as a buffer where various applications can securely operate, isolated from the trusted zone's memory, files, registry, and processes.

This approach has numerous benefits, including minimal CPU and memory usage, a high-quality user experience, and the ability to work seamlessly within the virtual container while remaining unaware of

the protective shield against browsing and USB threats. The following sections will explain how each suite product prevents various attack risks.
The following table summarizes our support per model while we removed the tactics we do not support for simplicity and readability. For further reading, we suggest visiting the MITRE D3FEND website.

Harden:

Credential Hardening	Message Hardening	Platform Hardening
Certificate-Based Authentication	Message Encryption	Driver Load Integrity Check
Multifactor Authentication	Transfer Agent Authentication	Local File Permissions
Domain Trust Policy		Software Updates

Credential Hardening:

- Certificate Based Authentication- BUFFERZONE Passport zone management option lets configure endpoint browsing sessions to be identified to the organizational proxy as originating from contained applications. This enables the proxy to block all outbound communications that are not from contained browsers. When passport enforcement is enabled, browser communications include an encrypted shared secret. The organizational proxy can check for this header and act accordingly. When users attempt to connect to untrusted sites (the internet) from an uncontained browsing session, the BUFFERZONE agent identifies the proxy block and switches to a contained session.
- Multi-Factor Authentication (MFA) – Users can securely log in to Microsoft Windows through Azure MFA by utilizing Bufferzone kernel agent enforcement. The agent manages the Windows OS User Login process. We do not provide any other authentication mechanism for other applications at this stage.
- Domain Trust Policy - When using BUFFERZONE Safe browsing, a zone switch function determines whether a website should be accessed within the secure virtual container (untrusted zone) or the secure zone (trusted). This decision is based on the organizations and domain trust policies.

Message Hardening:

- Message Encryption – BUFFERZONE Anti-phishing extension alerts against the use of insecure browsing protocols. (From version 2.0)
- Transfer Agent Authentication - BUFFERZONE Anti-phishing extension alerts against the use of insecure browsing protocols. (From version 2.0).

Platform Hardening:

- Driver Load Integrity Checking – When it comes to file installation, BUFFERZONE, based on administrator policy, can define which application can be installed. For example, it ensures that only authentic Microsoft certificates can be installed.
- Local File Permissions – BUFFERZONE meticulously categorizes local files, discerning their operational capacity within trusted or untrusted zones. To facilitate file transfers from the untrusted to the trusted zone, a Content Disarm and Reconstruction (CDR) process is obligatory. This measure ensures that no potential threats infiltrate the trusted zone. However, file transfers from the trusted zone to the untrusted zone are blocked to further enhance security.
- Software updates – BUFFERZONE's Safe Workspace fortifies the Operating System (OS) by implementing two key strategies. Firstly, it ensures that the OS is confirmed, fully supported, and meticulously patched. Following this, Safe Workspace keeps a vigilant eye for any latest updates relevant to the software installed within the virtual container. Should an update arrive, it promptly notifies the user.

Detect:

BUFFERZONE Safe Workspace is a zero-trust prevention based on application isolation and Content Disarm and Reconstruction (CDR). Recently we added anti-phishing detection for the Chrome browser.
The following describes our contribution to the Detect category.

File Analysis	Identifier Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis
Dynamic Analysis	Homoglyphs Detection	Certificate Analysis	Operating System Monitoring	Process Spawn Analysis
File Content Rules	URL Analysis	Administrative Network Analysis	Endpoint Beacon	Script Execution Analysis
		Blocking based on Policy		System Call Analysis
		RPC Traffic Analysis		File Creation Analysis

File Analysis:
BUFFERZONE SafeBridge™ is a sophisticated file analysis tool with two key features. Firstly, it boasts a local Content Disarm and Reconstruction (CDR) engine that functions without any internet connection. It is a file connector to different third-party detection engines and sandboxing solutions. By utilizing a central management system to set file policies and configurations, it analyzes files obtained from removable storage, web browsing, and downloads.

- Dynamic Analysis and static analysis – SafeBridge enables third-party detection connectors to various vendors' dynamic analysis and static analysis engines.
- File Content Rules – based on the file type BUFFERZONE enforce different file handling policies as part of SafeBridge.

Identifier Analysis:
BUFFERZONE's advanced Artificial Intelligence (AI) and Threat Intelligence engines are powered by our security measures for user browsing activity. These engines utilize various techniques such as URL analysis, homoglyphs, domain, host, and IP dynamic analysis based on URL sandbox and threat reputation to ensure our users' highest level of security.

- Homoglyphs Detection – AI-based Homoglyphs detection.
- URL Analysis – We provide dynamic, static, and AI-based detection suites for URL analysis. Our AI contains URL analysis, threat Intelligence, Object Detection, and website fingerprinting.

Network Traffic Analysis:

- Certificate Analysis – Based on BUFFERZONE PASSPORT.
- Administrative Network Traffic Analysis- The BUFFERZONE proprietary firewall, based on administrator policies, can be configured to block various protocols, including TeamViewer. However, it should be noted that BUFFERZONE does not perform any network traffic heuristic analysis.
- Blocking Based on Policy – BUFFERZONE central management enables network protocol blocking.
- RPC Traffic Analysis – BUFFERZONE effectively manages and monitors RPC traffic within the virtual container. As RPC is a challenging attack vector to prevent, the BUFFERZONE kernel driver takes charge of the untrusted virtual machine, effectively preventing any attempts at exploitation via RPC within the container and attempts for virtual container escapes.

Platform Monitoring:

- Operating System Monitoring – The BUFFERZONE agent oversees the process of virtual containers, keeps track of file usage, and sends the resulting data to a syslog server for monitoring by SIEM/SOC.
- Endpoint Health Monitoring- We collaborate with Absolute® to implement Application Persistence-as-a-Service (APaaS). This firmware-level solution ensures that endpoint health is continuously monitored, and that application persistency is automatically managed.

Process Analysis:

- Process Spawn Analysis- BUFFERZONE restricts any unauthorized processes that may be used for malicious attacks, such as DDE, RPC, SVCHOST, shell, and script, from operating within the virtual container. Only authorized processes are permitted to run inside the container. Furthermore, BUFFERZONE monitors the processing activity and exports it to syslog for advanced analysis.
- Script Execution Analysis- BUFFERZONE prevents running scripts inside the virtual container and logs the attempts.
- System Call Analysis – The BUFFERZONE agent analyzes the different system calls and processes and isolates system calls that belong to the untrusted zone (isolated zone).
- File creation analysis –BUFFERZONE agent monitors all file creations, reports them to Syslog, and ensures full isolation between trusted to untrusted zones.

Isolate:

BUFFERZONE Safe Workspace core is application isolation MITRE D3FEND defines two categories: Network and Execution isolation.

Network Isolation	Execution Isolation
Network Traffic Filtering	Executables Allowlist
Homoglyphs denylisting	Executables Blocklist
	Kernel-Based Isolation
	Mandatory Access Control
	System Call Filtering

Execution Isolation:

- Executables Allowlist- Safe Workspace controls the execution, and based on policy-driven configuration, can enable installation of executables based on defined application or executable certification.
- Executables Blocklist- Safe Workspace controls the execution, and based on policy-driven configuration, can disable the installation of executables based on defined application or executable certification.
- Kernel-Based Isolation- The core technology of BUFFERZONE is based on six patents focused on application and network isolation.
- Mandatory Access Control- BUFFERZONE kernel agent defines the access control for the application, network, and files based.
- System Call Filtering- The BUFFERZONE agent controls the system call and isolates system calls between the trusted and untrusted environment.
- Network Isolation-
- Network Traffic Filtering – Safe Workspace enables control of the inbound and outbound traffic based on a proprietary policy-driven Firewall.
- Homoglyphs Denylisting – BUFFEROZNE anti-phishing enables to detect homoglyphs. We do that on the URL level.

Evict:

Account Locking:
BUFFERZONE MFA is integrated with Active Directory and can lock the user from accessing the device. Also, isolating the device from the network is possible by blocking incoming and outgoing network traffic.

Process Eviction:
Process Termination – With BUFFERZONE, regulating the processes that run within the virtual container and effectively managing them according to the established policies is possible.

Summary:

In conclusion, companies should integrate the MITRE D3FEND and MITRE ATT&CK frameworks into their cybersecurity plans to gain a thorough understanding of both offensive and defensive tactics. By utilizing MITRE D3FEND, organizations can identify their safeguarded attack vectors and take necessary measures to enhance protection. BUFFERZONE Safe Workspace provides a comprehensive application isolation solution for secure

browsing and protection against evasive files from removable media and online activities, making it the perfect choice for companies serious about cybersecurity.

References:

[1] MITRE® D3FEND™ Knowledge Graph, https://d3fend.mitre.org/ .
[2] MITRE® ATT&CK™, https://attack.mitre.org/