Track 4: AI/ML

DNS Guard AI

AI-Powered DNS Threat Detection System

Team «Lone Splunker»

Riccardo Alesci

DNS Guard AI
AI-Powered DNS Threat Detection System

What is DNS Guard AI ?

DNS Guard AI is a Splunk App designed to detect various types of **DNS anomalies** that could indicate malicious activity such as **command and control (C2) communication**, **data exfiltration**, or **reconnaissance**.

The system uses Splunk's powerful search capabilities combined with **machine learning** techniques to identify patterns that deviate from normal DNS behavior.

DNS Guard AI
AI-Powered DNS Threat Detection System

Key Features

The system offers a comprehensive defense mechanism that goes beyond traditional signature-based detection by analyzing behavior, timing patterns, and statistical anomalies in DNS queries across the organization.

Real-time Detection

Continuous monitoring of DNS traffic for immediate threat identification

Comprehensive Analysis

Multiple detection methods working in concert to identify various types of threats

Splunk MLTK Integration

Advanced algorithms for pattern recognition and anomaly detection

DNS Guard AI

Enterprise-Ready

Scalable solution designed for large network environments

CIM Compliance

Fully compatible with Splunk's Common Information Model

Dashboard System

Specialized dashboards for each detection method and an overview dashboard for high-level threat monitoring.

DNS Guard AI
AI-Powered DNS Threat Detection System

Detection Methods

DNSGuard AI incorporates the following detection methods, each targeting a specific type of DNS-based attack vector.

Density Function Algorithm

Beaconing

Detects regular, periodic DNS queries at consistent intervals—a hallmark of malware communicating with command and control servers. Analyzes consistency of time gaps between queries to the same domain.

Anomaly Detection Algorithm

Record Type Anomalies

Detects abnormal usage of specific DNS record types often associated with reconnaissance or data exfiltration. Identifies outliers in the usage of TXT (data exfiltration), ANY (broad queries), HINFO (host info leakage), and AXFR (zone transfer attempts) records by host.

Anomaly Detection Algorithm

C2 Tunneling Detection

Identifies hosts making an unusually high number of DNS queries, which could indicate command and control communication or data exfiltration through DNS tunneling. Uses density function to find hourly query count outliers by source.

K Means Algorithm

Behavioral Clustering

Groups hosts with similar abnormal DNS behavior, which can reveal coordinated attacks or infected host groups across the enterprise. Uses KMeans clustering on multiple DNS behavior features.

Anomaly Detection Algorithm

Query Length Anomalies

Detects unusually long DNS queries that may represent data exfiltration channels where sensitive information is encoded in the query itself. Identifies outliers in query string length by host.

Anomaly Detection Algorithm

Domain Shadowing

Identifies patterns where many unique subdomains are requested for a legitimate domain, which may indicate an attacker using compromised DNS accounts to create malicious subdomains. Measures distinct subdomain count by parent domain and identifies outliers.

DNS Guard AI
AI-Powered DNS Threat Detection System

Prerequisites & Integrations

- Splunk Common Information Model (CIM)
- Splunk Machine Learning Toolkit
- Python for Scientific Computing

DNS Guard AI

- Real-time Detection
- Comprehensive Analysis
- Splunk MLTK Integration
- Enterprise-Ready
- CIM Compliance
- Dashboard System

Splunk Enterprise Security

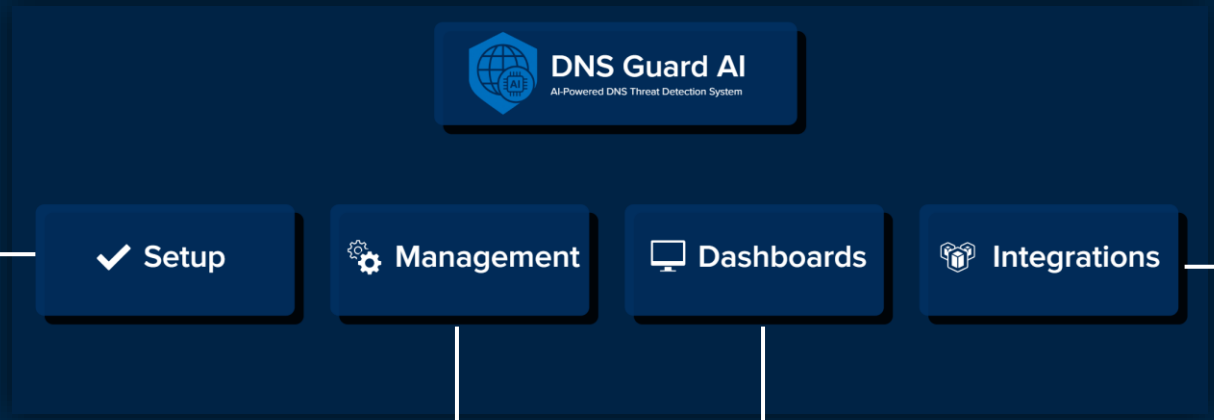
Provides advanced security monitoring capabilities and includes pre-built risk factors configuration and alerts

DGA App for Splunk

Specialized in Domain Generation Algorithm detection and analysis and complements DNSGuard-AI's detection capabilities

DNS Guard AI
AI-Powered DNS Threat Detection System

Dashboard System



Setup View

App Requirements
Synthetic Data
DNS Data Model
MLTK Configuration

Management View

Model Training
Anomaly Detection
Alerts
Lookup

Dashboards View

DNS Anomalies Overview
Beaconing
C2 Tunneling
Query Length Anomalies
Domain Shadowing
Record Type Anomalies
Behavioral Clustering

Integrations View

Enterprise Security
DGA App

DNS Guard AI
AI-Powered DNS Threat Detection System

Synthetic Data Testing

For testing and demonstration purposes, the application includes a custom Python script that generates synthetic DNS data specifically for the app's proof of concept.

The generated events adhere to the **Common Information Model (CIM)**, particularly the **Network Resolution** data model, ensuring compatibility with Splunk's detection and enrichment features. The synthetic dataset simulates a wide range of DNS anomalies

DNS Guard AI
AI-Powered DNS Threat Detection System

Practical Applications

DNS Guard AI

- Early detection of malware infections
- Unconver data exfiltration attempts
- Improves DNS-level threat visibility
- Expose coordinated or persistent threats
- Identify reconnaissance behavior

Track 4: AI/ML

DNS Guard AI

AI-Powered DNS Threat Detection System

Team «Lone Splunker»

Riccardo Alesci

Check out the **Github** repository for updates and development progress.