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.

Key Benefits

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

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.
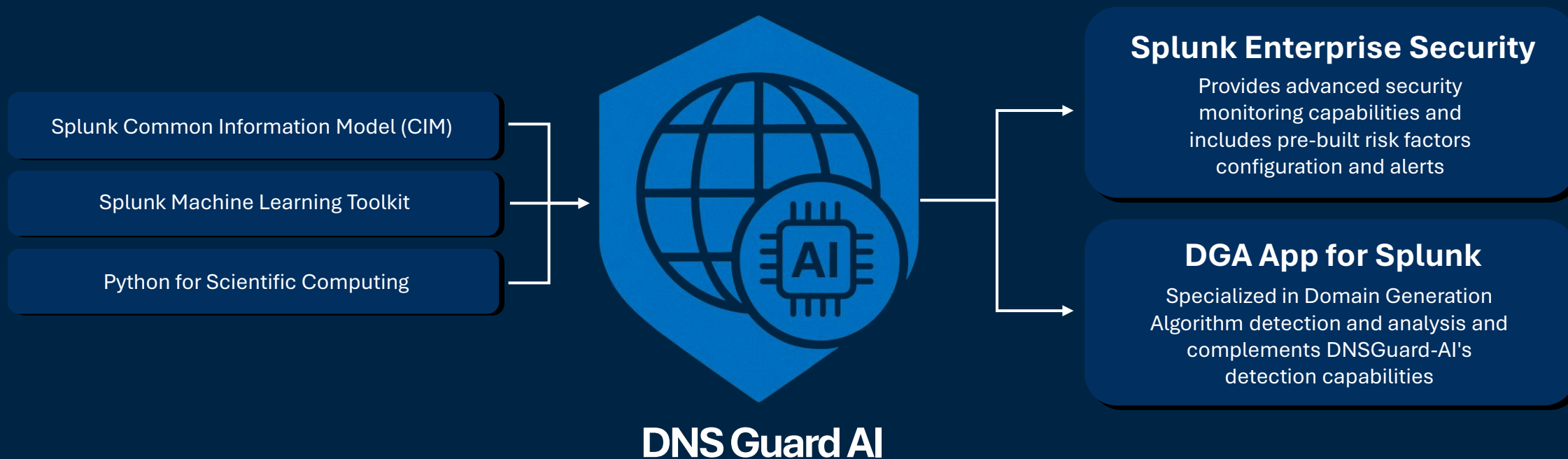
DNS Guard AI
AI-Powered DNS Threat Detection System
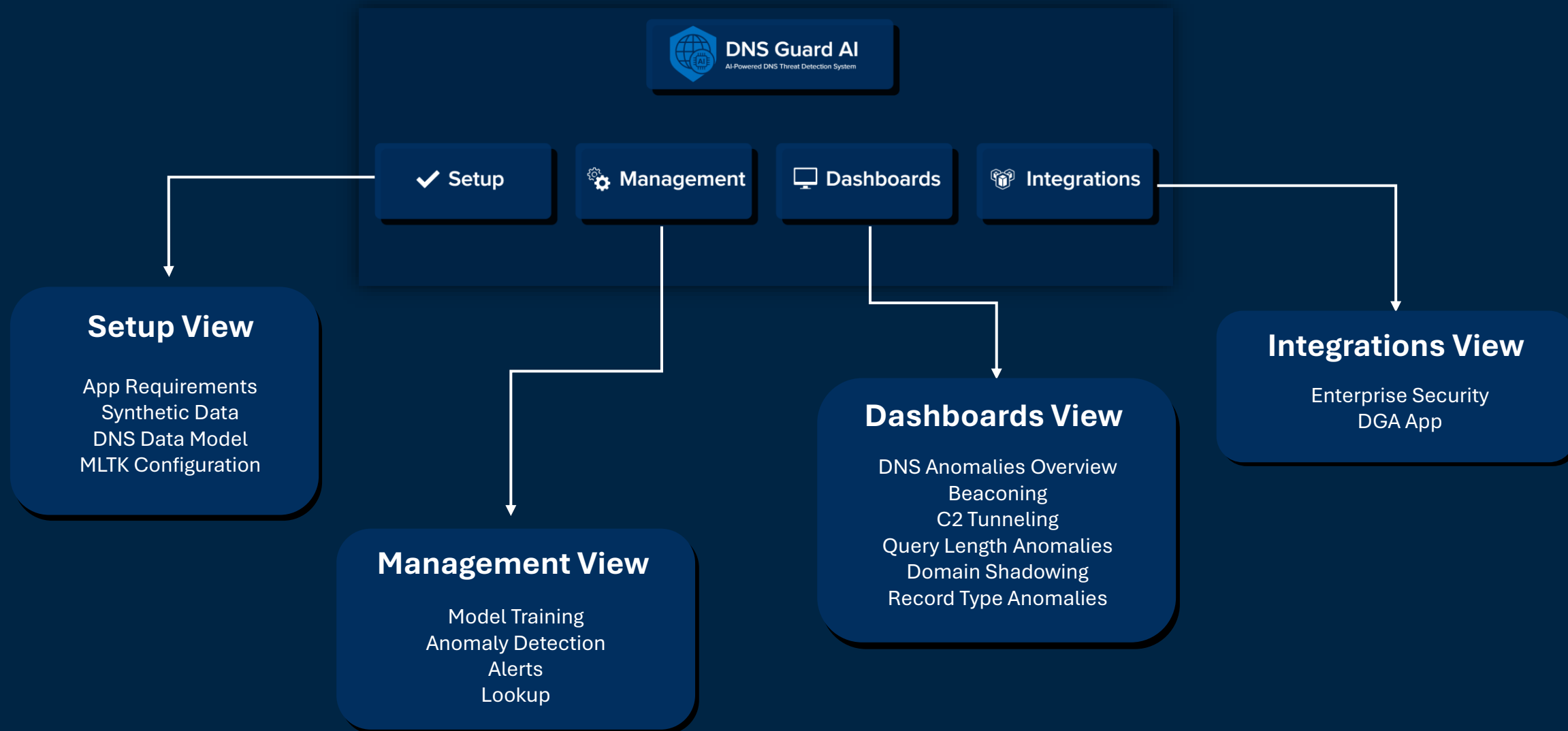
For testing and demonstration purposes, the application includes a custom Python script that generates synthetic DNS data specifically for the app's proof of concept.

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

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.