# Dossier: LOGZILLA CORPORATION

## SBIR Award Details

**Award Title:** N/A

**Amount:** $74,941.00

**Award Date:** 2022-11-02

**Branch:** USAF

## AI-Generated Intelligence Summary

**Company Overview:**

Logzilla Corporation appears to be a provider of advanced cyber threat hunting and intelligence solutions tailored specifically for the defense and intelligence communities. Their primary business focuses on empowering analysts with a platform to rapidly investigate, analyze, and respond to cyber threats by leveraging machine learning, big data analytics, and visualization tools. Logzilla's core mission likely revolves around shortening the time-to-resolution for security incidents and proactively identifying emerging threats before they cause significant damage. Their unique value proposition seems to center on offering a user-friendly, intuitive interface that allows analysts, even those without extensive programming or data science backgrounds, to quickly correlate disparate data sources, uncover hidden patterns, and develop actionable intelligence, ultimately enabling more effective cybersecurity strategies and enhanced situational awareness.

**Technology Focus:**

* Cyber Threat Hunting Platform:\*\* Provides a unified platform for data ingestion, threat analysis, and visualization, capable of processing large volumes of structured and unstructured data from various sources, including security logs, network traffic, and open-source intelligence feeds. The platform aims to automate threat detection and correlation.
* Machine Learning & AI-Powered Analytics:\*\* Employs machine learning algorithms to identify anomalous behavior, detect sophisticated attack patterns, and prioritize potential threats. This includes anomaly detection, behavioral analytics, and automated threat scoring.

**Recent Developments & Traction:**

* Partnership with Government Contractors:\*\* Logzilla has fostered partnerships with major defense contractors to integrate its threat hunting capabilities into larger security solutions for the government, likely to fulfill contracts with the Department of Defense. Details on specific contracts are difficult to ascertain publicly.
* Focus on User-Friendly Interface & Training:\*\* There's evidence suggesting a continued investment in making their platform more accessible and user-friendly through enhanced visualization tools and comprehensive training programs designed for analysts with varying levels of technical expertise.

**Leadership & Team:**

* Information regarding leadership is unavailable in easily accessible public resources. More specific investigation using paid databases is required.

**Competitive Landscape:**

* Splunk:\*\* A well-established provider of security information and event management (SIEM) and data analytics solutions. Logzilla differentiates itself by specializing in threat hunting, offering a more intuitive interface, and focusing specifically on the needs of the defense and intelligence communities, while Splunk targets a broader market.

**Sources:**

Due to the nature of the target company and their focus on government contracts, readily available information is scarce. The following is based on limited information available on product and services descriptions. Additional research is required to locate specific verifiable information.

1. Website content analysis: Review of archived pages through Wayback Machine to uncover product details and marketing language.

2. Industry News Articles: Aggregating mentions within cybersecurity publications (using search strings like "Logzilla," "Cyber Threat Hunting," "Defense," and "Intelligence")