Cyber Resiliency and the Implementation of a Host-Based Intrusion Detection System in an Urban Air Mobility Environment

Terrence D Lewis[1]
NASA Ames Research Center, Moffett Field, CA 94035

Steve W. Garcia Jr.[2]
Science & Technology Corporation, Moffett Field, CA 94035

Ainaz Estiri[3]
University of California Riverside, Riverside, CA 92521

With the growth in Urban Air Mobility systems and the increasing reliance on interconnected technologies, ensuring the security of these complex components has become critical. As cities evolve into smart urban centers, the vulnerability to cyber threats escalates, possibly endangering citizens' safety and the efficiency of transportation networks. In response to these challenges, this paper presents a study on the need for cyber resilient techniques within future air traffic environments. It will pay specific attention to the implementation of a Host-Based Intrusion Detection System (HIDS) utilizing Atomic OSSEC software, tailored specifically to a NASA simulation of an Urban Air Mobility environments' unique demands. Further, this study seeks to outline the rational for NASA's recommendation for a HIDS in such environments. It explores the design, development, and deployment of the proposed HIDS, focusing on its adaptability to monitor the hybrid nature of the Urban Air Mobility environment. Leveraging machine learning algorithms and anomaly detection techniques, the HIDS is equipped to continuously monitor and analyze the behavior of individual host systems, vehicles, and devices, thereby providing a proactive approach to threat detection. Implementing a HIDS is a pivotal strategy for enhancing cyber resiliency, as it gives an organization granular visibility into internal system activities, enables rapid detection and response to anomalous behavior and cyber threats, and fortifies the organization's overall cybersecurity posture. Finally, this study aims to provide recommendations and include learned takeaways that the Urban Air Mobility industry should consider. In brief, this paper highlights the significance of host-based intrusion detection in Urban Air Mobility environments and underscores the necessity of tailored security solutions to safeguard against emerging cyber threats.

I. Introduction: Cybersecurity vs Cyber Resilience

In an era where digital transformation accelerates extraordinarily, the ever-evolving cyber threat landscape presents complex challenges to organizations. These threats bring technical challenges and can significantly impede business operations. Organizations need a strong, robust security system as these threats grow and become more sophisticated. This cybersecurity research within the emerging Urban Air Mobility environment, discussed in detail below, aims to test and suggest recommendations for multiple aspects of this. These features are practical and seek

[1] IT Specialist, Secure Airspace Technology Group, Aeronautics Projects Office, NASA Ames Research Center
[2] Senior Security Architect, Science & Technology Corporation
[3] Student Intern, University of California Riverside

to modify traditional processes and procedures within a simulation research environment at NASA. Considering that the risks associated with critical infrastructure are magnified in the digital age, in a break from traditional cybersecurity thinking, this research team aimed to adopt and approach the next generation of airspace cybersecurity concepts by implementing a cyber resilience approach. Given the integrated nature of networked systems, a breach in one area can have cascading impacts throughout an organization. As such, a robust cyber resilience strategy safeguards against such exposures, ensuring that crucial assets are protected, vulnerabilities are proactively identified, and breaches are rapidly contained.

Organizations and any new operating environments aiming to stay operational and competitive must acknowledge the principles of cybersecurity and cyber resilience while also understanding the crucial roles each plays in ensuring business continuity. Although these two concepts are closely related, they represent distinct ways of mitigating and managing cyber risks and attacks. Cybersecurity as a concept within an organization consists of protecting computer networks and systems from unauthorized access, modifications, disruptions, or destruction by implementing many security measures like firewalls, data encryption, intrusion prevention systems (IPS), and/or intrusion detection systems (IDS). On the other hand, cyber resilience is the ability of that same organization to withstand and recover from cyberattacks within a relatively short time [1]. It comprises of not only technical measures like technological crisis recovery plans but also less technical techniques like training employees to be more cyber aware and ensuring that they understand how to quickly respond to and follow procedures to report incidents in the first place. Cyber resiliency has four main principles: 1) Anticipate - organizations should anticipate potential threats and plan for these risks by regularly changing and evolving their IT systems. 2) Withstand - A system should withstand potential attacks and threats that cannot be detected. Cyber resiliency is accomplished through automatic repairs, deflecting attacks, tolerance to some damage, or replacing and removing compromised system components. 3) Recoverability – If there is a data breach, the system should be able to overcome the threat sophisticatedly and have the infrastructure to repurpose other system elements to support the targeted areas of the attack. 4) Adaptability - The system should adapt and correct itself to prevent future data breaches. This can be done by adding new elements and software to help identify weaknesses and vulnerabilities and removing or changing system design, architecture, operations, and requirements to help defend against future enormously evolved threats [1].

II. Background: Understanding the Need to Secure UAM

Through understanding cybersecurity and cyber resiliency, the threat landscape in an emerging market that aims to shake up how communities travel will be looked at – Urban Air Mobility (UAM). While this paper focuses on UAM and UAM vehicles, the security applications should not be isolated to solely the UAM environment but rather instead to the Advanced Air Mobility (AAM) ecosystem as a whole. To understand how cybersecurity and cyber resiliency should be looked at in UAM and AAM overall, it should first be defined in the broader sense. NASA is leading a project in air travel called Urban Air Mobility Airspace Integration.

> UAM is the concept of expanding transportation networks to include short flights that transport people and goods around metropolitan areas. UAM is part of a more significant paradigm shift toward AAM. New technologies and business models enable transformational applications of aviation, allowing aviation to play an integral role in regional and local transportation. AAM is envisioned as a safe, sustainable, affordable, and accessible form of aviation for local and intra-regional missions. UAM describes air travel as a practical and cost-effective mobility alternative for the general public, primarily serving urban areas extending into the metropolitan periphery [sic]. UAM has the potential to revolutionize urban transportation networks and play an integral role in future smart cities. In this future paradigm, the general public widely uses urban air travel, enabling rapid movement between locations of high passenger demand as cities grow [2].

The critical item here is the goal of UAM - creating safe and efficient air transportation systems that operate above populated areas, which can be used for various purposes, including carrying passengers with air taxis over densely populated areas. “When fully mature, it ultimately enables thousands of people to use autonomous/semiautonomous air mobility services daily in major cities” [2]. Therefore, proactively monitoring and preventing cyberattacks and recovery on a project of this scale and value is crucial. As with many of current technologies, security has traditionally not been factored into the initial design and development of the product. However, since this is a burgeoning environment with these services being novel, industry leaders are given a unique opportunity to bake cyber resilient systems in at instantiation.

Flying people over densely populated areas is not a new concept, as helicopters and other rotorcraft have traditionally been used. These vehicles use a traditional flying model, aircraft technology, and communication: i.e., individual pilots working closely with air traffic controllers in a relatively open operating environment, with

standard and less connected components. UAM vehicles, conversely, will introduce novel, "smarter," and connected vehicles that provide safer, and more efficient flight while at the same time introducing new and various cybersecurity concerns to the environment. With UAM being flight-related, aviation cybersecurity is crucial to study, and understanding the threat landscape is imperative. Threats to these vehicles include, but are not limited to, A) in-flight Wi-Fi attacks where attackers can compromise sensitive information by gaining access to an unsecured network using wireless hacking technology [3]. Or, taking this concept further, if the vehicle manufacturer does not consider security during design and does not correctly segment the vehicle's network, attackers can disrupt flight operations by taking control of the aircraft's control system. B) GPS spoofing lets the attackers manipulate the GPS signal of the aircraft, causing the aircraft to fly off course into a different location or restricted airspace, possibly causing potential mishaps [3]. C) Distributed Denial-of-Service (DDoS) attacks bring down air traffic control systems and other critical aviation infrastructures by overwhelming them in a way that can lead to planes being delayed, grounded, or causing mishaps [3]. D) Further, given the possible novel and connected components to enable such a vehicle and also ensure passenger comfort - manufacturers are at risk of a supply chain attack. Here, the attacker targets the aviation suppliers to gain access to essential systems to install malware that could be used in the future to gain control of an aircraft. This leads to cyber-physical attacks because the attacker now has control of not only the software components but also the hardware. Malware-infected aircraft or drone can take control and do whatever they want [3]. Understanding that these are only some of the tactics used for attacking the UAM environment, the tools and tactics used for cyber-attacks are ever evolving, leading to ever-changing threats to UAM environments. Given this, the NASA cybersecurity research team wanted to extend previous research on a cyber threats and security controls analysis that was done for Urban Air Mobility Environments to look at the security controls needed to maintain the security posture of a UAM environment - specifically within the "identified" component in the analysis [4].

The UAM environment does not consist singularly of a company and their vehicles. Instead, it is more akin to an ecosystem of components and infrastructure providers, vehicles, service providers and operators that all work together to form a UAM *operating* environment. In its simplest form, this can be broken down into UAM operators, who work independently to manage aerial vehicles in the urban environment. Providers of Service (PSU), which are the primary service and data providers for UAM stakeholders and act as the primary connect through for operators and the interactive interface within the UAM ecosystem. Supplemental Data Service Providers (SDSP), which provide services to support flight operations within the UAM environment, e.g., radar services. Lastly, the Flight Information Management System (FIMS), which is used by the Federal Aviation Administration (FAA) so that they can coordinate flight information between the FAA-controlled National Airspace System (NAS) and the UAM environments [4]. These relations with each other are illustrated in the Notional UAM architecture below in figure 1 [2].

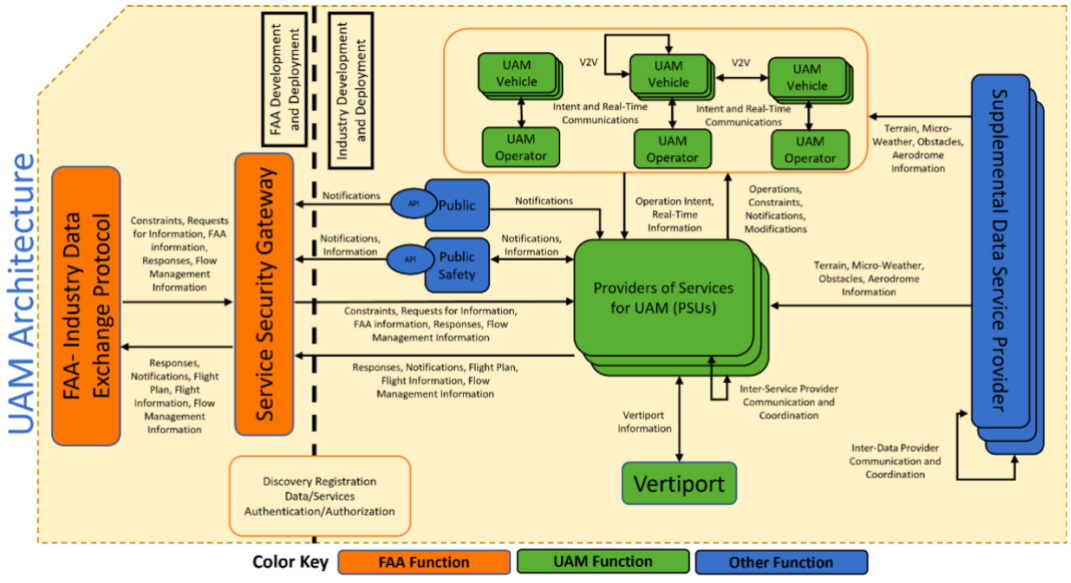

Fig. 1 Notional UAM Architecture.

Against this backdrop, the various components of the UAM environment can be understood. Given the complex environment, and without insight into the systems to identify security concerns, i.e., understanding one's security posture - the possibility of increased security incidents skyrockets. Consequently, the research team identified an intrusion Detection System (IDS) as a vital tool to serve as an early warning system against potential threats. By continuously monitoring network traffic or host activities for suspicious patterns and known malicious signatures, an IDS can detect anomalies, unauthorized access, or breaches in their nascent stages, allowing for timely mitigation and reducing potential damage [5].

III. IDS: An Essential Component of a Comprehensive Security Framework

While preventive measures, such as firewalls and antivirus software, form the primary defense against cyber threats, they are not infallible. Cybercriminals continually devise novel tactics and techniques, seeking ways to bypass these first lines of defense. This is where the relevance of an IDS becomes paramount. It operates under the assumption that, at some point, initial defenses will be breached. By implementing an IDS, organizations adopt a proactive security stance, ensuring threats do not remain undetected should they penetrate the outer defenses. This multi-layered approach to security, where preventive measures are complemented by detection and response mechanisms, ensures a more robust defense against the multifaceted cyber threats of the modern era. Furthermore, in a regulatory and compliance-driven environment, where many industries are mandated to have stringent security measures, the integration of an IDS enhances security postures. It helps adhere to regulatory standards, thereby safeguarding both data, reputation and life.

Now with the understanding of the operating environment and the threat landscape, operators need to be able to implement one of the first steps to security – cyber situational awareness, e.g., detection. For the overarching objective of strengthening and improving the cybersecurity posture of the Urban Air Mobility experiment within the NASA research environment, the research team chose to implement a Host Based Intrusion Detection System (HIDS). Unlike an intrusion prevention system (IPS), a HIDS's operations are more passive and does not interfere with operations and thus do not impede the performance of the various services operating in the UAM environment. In the landscape of cybersecurity, a HIDS offers dual functionalities. First, it precisely examines the intricacies of network traffic, aiming to detect anomalies or malicious activities that might transgress predefined thresholds or patterns. Concurrently, it extends its surveillance to encompass individual machines within the network, providing an in-depth analysis of system behaviors and potential breaches. This granular-level monitoring is indispensable in identifying and countering threats that might bypass perimeter defenses. To demonstrate, HIDS functionality monitors system events, logs, file integrity, and network traffic on various hosts by comparing the information to known threat signatures and patterns. When an intrusion is detected, HIDS generates an alert for an admin to act. HIDS also provided the research team with deep visibility into what was happening across all the vital systems for this research demonstration. In this case, we could detect and respond to malicious and anomalous activities discovered in the simulated UAM environment.

A HIDS typically has two approaches to detecting intrusions: signature-based, which involves finding well-known attack patterns, and anomaly-based systems, which attempts to detect new unknown attacks by logging activities considered normal and looking for abnormal behavior patterns [5]. To illustrate, HIDS monitors computer systems and software for any potential signs of suspicious activities or anomalies like malware, unauthorized access, changes to files, failed login attempts, or user pattern changes. If an intrusion is detected, the host-based system generates alerts to be logged and sent to the administrators or the security team for further investigation. Both of these methods will be looked at later in this report.

While many cybersecurity steps and implementations can be taken to implement cyber resiliency in an operating environment like UAM, the research team decided to focus on a HIDS for our initial tests, specifically for its inherent passive nature. This was crucial as we were operating in a simulation-based environment with other key UAM concepts being researched. The goal was to limit as much computational overhead as possible, ensure minimal impact on overall simulation activities and research outcomes, and minimize the work for admins to implement within the environment.

A HIDS has advantages, but its use may not suit all environments as it has its limitations. Due to its passive nature, HIDS only monitors potential risks, which can be problematic as some environments would require it to be able to actively block attacks from happening. The HIDS must be frequently updated for new threats, which can be challenging to configure and maintain [6]. It can be especially slow at detecting some attacks at the start because HIDS needs to collect a good amount of data and then analyze it before it can even detect a potential attack [6]. This not only gives attackers a bit of an opportunity gap but also, HIDS is not at its optimal potential for detecting threats. While infrequent, HIDS may generate false positive alerts when no malicious activity exists, which can waste

resources. The security teams monitoring various segments in the UAM environment must investigate each alert to determine whether they are valid. As the UAM ecosystem consists of numerous varied parts, PSU, operator, etc., security teams must focus their time on real and pertinent security incidents as bad information and loss of time could have real world implications of actual flying vehicles. Further, too many false positives may lead to teams ignoring alerts should they become too erroneous. Another limitation of HIDS is that it can be costly because it requires specialized software and hardware and the initial lift of configuring and tuning it for each environment. Despite these limitations, a HIDS is still valuable for protecting against cybersecurity attacks and is a preliminary yet crucial step in the maturation of our cybersecurity architecture.

IV. HIDS Breakdown

A. Rules Based HIDS

1. Understanding a Rules-Based Host-Based Intrusion Detection System (HIDS)

A Rules-Based Host-Based Intrusion Detection System (HIDS) is a security solution designed to monitor and analyze activities on individual computing hosts for signs of malicious or anomalous behavior. Some of these activities include unusual or unauthorized behaviors. The HIDS compares observed actions against predetermined rules or signatures crafted to identify known malicious patterns, policy violations, or suspicious behaviors [6]. These rules are essentially patterns of known malicious activities. When an action on the host matches one of these patterns, the HIDS triggers an alert. The alert could require a range of actions identified, from specific file modifications and unauthorized system calls to abnormal processes or unusual user behaviors. As cybersecurity threats evolve, the rules must be regularly updated and fine-tuned. This ensures that the HIDS remains proficient at spotting new attack vectors while minimizing the risk of false positives.

2. Deploying and Utilizing a Rules-Based HIDS

Deploying a Rules-Based Host-Based Intrusion Detection System (HIDS) requires a careful approach to ensure optimal protection and minimal system disruption. The initial phase involves selecting a HIDS solution that aligns with a UAM operating environment's security requirements and infrastructure. Once chosen, it's crucial to determine which systems or endpoints warrant monitoring, with priority often given to critical servers, databases, and workstations that house sensitive data. Installing the HIDS agent on these hosts is the next step, ensuring they can monitor system activities and relay information to a centralized management server. The configuration phase is perhaps the most critical, as it involves defining and fine-tuning the rules the HIDS will employ. UAM operating environments must ensure these rules are relevant to their environment, tailored to detect known threats, and regularly updated to remain effective against evolving cyber threats.

3. Challenges and Best Practices for Rules-Based HIDS

While Rules-Based Host-Based Intrusion Detection Systems (HIDS) offer invaluable insights into host activities, they are not without challenges. One significant hurdle is the management overhead, as each host requires agent installation and upkeep. There's also the risk of false positives, which can arise when rules aren't finely tuned, leading to unnecessary alarms and potential desensitization to genuine threats. Performance impact on monitored systems, especially if the HIDS is resource-intensive, is another concern. To address these challenges, several best practices are recommended. Regularly updating and fine-tuning the ruleset ensures that the HIDS stays relevant in detecting emerging threats and minimizes false alarms. Deploying the system in phases allows for initial testing and adjustments before a full-scale rollout. Integration with Security Information and Event Management (SIEM) tools which collect and combine logs and events that have produced monitoring information, threats, and responses to risk. These tools deployed across network, endpoint application, cloud environments and applications, can enhance data correlation and provide a holistic security view [7]. Lastly, continuous training of security personnel ensures they can effectively interpret alerts and respond promptly, maximizing the system's protective capabilities.

B. Anomaly Detection-Based HIDS

1. Introduction of AI or ML

Intrusion Detection Systems, when empowered by Artificial Intelligence (AI) or Machine Learning (ML), can elevate their detection capabilities beyond static rules. Instead of solely relying on predefined patterns, an AI or ML Anomaly Detection-Based HIDS learns the typical behavior of a system over time and identifies deviations from this norm as potential threats [8]. This dynamic approach is particularly adept at detecting previously unknown or zero-day attacks, as it's not limited to recognizing only known malicious signatures. By continuously learning from the system's operations and adjusting its baseline, the AI-enabled HIDS can adapt to evolving behaviors and environments. However, while this adaptability can significantly reduce false negatives, it might increase false positives initially until the system undergoes enough training [8]. Integrating AI or ML in HIDS represents a

significant leap in cybersecurity, offering a proactive approach to threat detection and allowing for faster and more informed response measures.

2. Deploying and Utilizing ML Anomaly Detection HIDS

A HIDS analyzes several areas to determine misuse (malicious or abusive activity inside the network) or intrusion (breaches from the outside). Further, detecting cyber-attacks with machine learning requires a large pool of attack examples or models. This will require the identification of as many examples as possible of most current cyber-attacks and constant updates to ensure an attack library stays up-to-date with the ever-growing cyber-attacks. It is essential to Periodically review models and datasets used and update them as the organizational IT environment changes.

3. Challenges and Best Practices for ML HIDS

While this paper won't go into the specifics of machine learning, as that is out of scope, we will provide a high-level overview. To be useful, machine learning requires a relatively large dataset or models to pull from and begin to "learn" moving forward. These ML models can require a significant time to train and a long time to classify a record out of sample as anomalous or normal, especially for complex models like an ensemble or neural network [8]. Because network data is dynamic and changes daily, the database of collected network flows would have to be updated daily with an ML-based approach. This would mean that the ML model must be re-trained every time.

Further, the time the model is online and can classify packets in real-time would be small - all yielding flaws with this ML-based IDS approach. As such, learning offline can fill the gaps, utilizing existing datasets for network activity, system events, and other host-based anomalies. If the data changes daily or a novel attack is found, fast incremental learning or other online methods can make ML-based IDS more viable [8]. However, even with this approach of using existing datasets, getting updated datasets is challenging for the newly developed attacks, and the training time for these systems also causes potential challenges with the effectiveness and quality of an ML-based approach [9]. Another challenge with this approach is the introduction of false positives. Anomaly-based methods detect abnormal behavior by comparing it against a model of normal behavior; while they have higher false positive rates, they can detect brand-new attacks [10]. In creating a practical ML-based approach for HIDS, admins should select their models based on their performance on reference datasets with a combination of known traditional datasets and a more modern system called datasets [10].

V. Our Implementation

Shown below is an architectural network diagram showing the NASA UAM simulation environment. The simulation environment was designed after the Notional UAM Architecture in Figure 2. With UAM having billions of dollars already invested by industry, government, and academia; to achieve the high level of operational density and complexity desired by the UAM community, an airspace system that enables UAM operators to readily access and operate safely and efficiently in the National Airspace System (NAS) is needed. As such NASA developed a service-oriented architecture to enable a high level of operational density and complexity for UAM operations [11]. It was created to test various research concepts in collaboration with the FAA and industry partners. Aiming to make a robust HIDS, an open-source approach was utilized within the UAM simulation environment. The software solution OSSEC+ by Atomicorp was used [12]. Our HIDS provided several different functionalities but all with the goal of being able to detect anomalous behavior within the environment by providing network traffic analysis, security checks, and alerting.

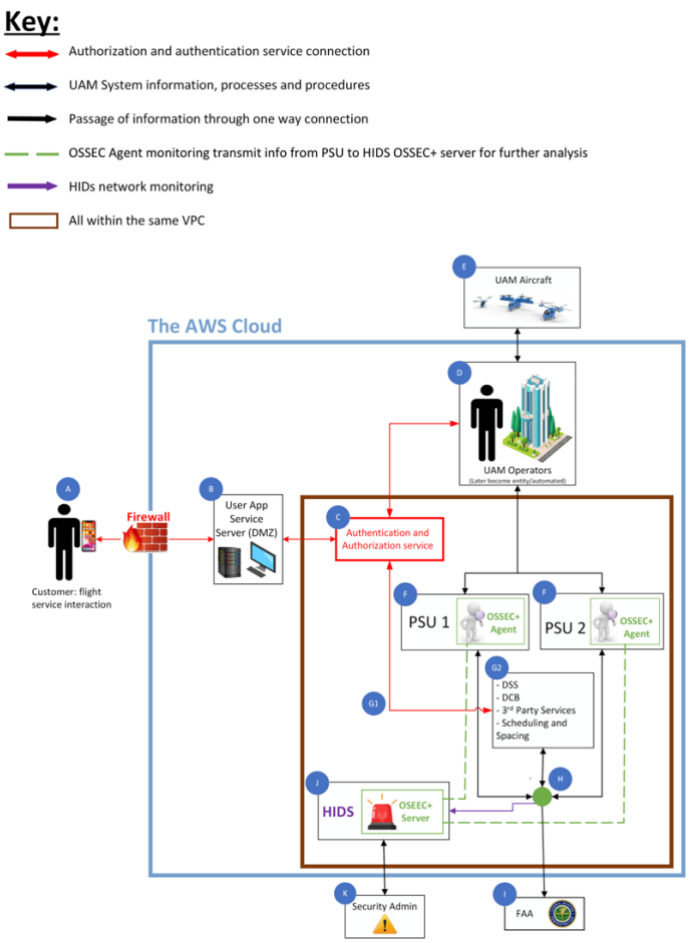

Fig. 2 UAM Simulation Environment Network Diagram.

Below are details of the steps of the UAM environment and how it interacts with different elements of the HIDS:

A. The user interacts with flight services. Must be authenticated before utilizing services
B. After passing through the firewall, the user is in the Amazon Web Services (AWS) cloud for UAM and can now request flight through the app
C. The users role must be verified before a UAM operator can book the aircraft for the request.
D. UAM operator receives flight requests after it is authenticated, utilizing system elements, PSUs, and 3rd party service information (G.) to contact the aircraft. UAM Operators also authenticate to use services
E. The UAM company reserves an aircraft for the specified request
F. The Provider of Service (PSU) will manage air traffic controls and blockchain. While the OSSEC+ Agents monitor the overall service for potential threats and anomalies to report back to the OSSEC+ Server
G1. After being verified and given authorization
G2. The information on 3rd party services, pilot-intended flight path data, spacing, scheduling, etc., are shared within the UAM system
H. "Central Hub" where all networking passes through, such that data are shared and components are connected. To be used as a network tap to monitor network traffic
I. FAA gets a copy of the flight request information
J. HIDS monitors all the events in the UAM system by accessing the data on the OSSEC+ server that was collected and received through the Agent transmission in the PSUs
K. Admin solely gets involved if and only if the HIDS finds threats and anomalies within the system or flight requests and are notified

Note that this was a simulation environment and nearly all the items of study are contained within the same virtual private cloud (VPC) – a private cloud instance environment containing computer resources on an isolated network on a public cloud environment. These various resources will be more distributed in actual UAM operating environments.

VI. Setup & Test Results

Once the build of the HIDS server was completed and initially validated, we "integrated" it into the rest of the simulation environment which was the testing environment shown in Figure 2. The original plan for integration was to do this in three parts: A) add agents to simulated PSU instances, B) ensure data forwarding to collect on a central server, and C) implement network tap ingress into HIDS. However, due to constraints of the operating environment, part C, network inspection via network taps, was not completed.

Much of the testing procedure in the simulation environment was done out of an abundance of caution to address the network and CPU utilization concern impeding the overall simulation. It was planned that when a simulation was run, HIDS agents, data collection, and log forwards would be disabled. There was to then be a secondary run with the HIDS components enabled. Data from the HIDS run and any possible associated performance deltas would be noted, and an assessment would be made for how simulations with the HIDS would be run in the future. This was later modified following a positive reception of the team's cyber research goals along with a better understanding of HIDS and limited timing for multiple runs for testing. As such, we were able to run the agents with active simulations. The following outline is an overview of the installation of the server, agent, and test results to confirm operability.

A. HIDS Server/Web UI

The HIDS server was built on a Rocky Linux 8 instance, utilizing the OSSEC+ install script on the OSSEC website. During our initial setup, we utilized a rules-based HIDS. One of the first steps for setting up our HIDS instance was ensuring that the basic rule set worked out of the box. The initial rules were already configured, and we just needed to modify the configuration files to tell OSSEC where it should be monitoring. The ultimate goal was to utilize a ML approach. This was later accomplished once the HIDS servers' initial baseline with the PSU agents were set. Once OSSEC+ was installed and implemented within the simulation environment, it could take the data collected and use that as a training set for ML-based anomaly detection on its own. The setup for the HIDS includes this step as part of OSSEC+ and was validated once the proper configuration was confirmed.

B. Agents

The OSSEC+ software allowed for either an agent or agentless setup. An agent setup was chosen for our experiment to get richer data and near real-time alerts for anomalous behavior within simulation instances. Agents were installed on hosts and reported to the central OSSEC server via the OSSEC encrypted message protocol. An agent is a small program, or collection of programs, installed on the systems to be monitored. The agent collected information and forwarded it to the manager (HIDS server) for analysis and correlation. Some information is collected in real-time, others periodically. It has a small memory and CPU footprint by default, not affecting the system's usage. Understanding agent security: It runs with a low-privilege user (generally created during the installation) and inside a chroot jail isolated from the system [12].

Part of the capabilities that the HIDS and its agents provided, were security checks via looking at file modifications. This allowed us to confirm the file integrity of various security and system logs. To avoid possible security issues, it was critical that these agents were installed on multiple endpoints within the environment and that they reported back to the HIDS to ensure effective reporting. Due to the IT management structure of this simulated research environment our team did not have direct access to the PSUs. Given this, being able to easily get the admin to install the agents proved the value of have agents for data collection and giving us insight into what was happening on those machines

C. Test Results

Under our configuration, all of the HIDS operations were being performed by OSSEC+. This would include the initial baselining and ongoing monitoring of system events and critical monitoring. Once the system was configured, five major tests were done to ensure the successful functionality and alerting capabilities of the HIDS server. These included the validation of malware detection (TC001), Identifying and detecting unapproved file changes (TC002), Identifying, and detecting failed or unsuccessful login attempts (TC003), Identifying, and detecting new or deleted users and groups (TC004), and identifying and detecting user privilege escalation (TC005). While these suites of

tests were not comprehensive, they did allow us to understand the HIDS software and its capabilities and get a base knowledge for how we would like to continue in later research. For each of the following tests, it should also be noted again, that we did not have direct access to the PSUs to conduct any of the tests as they were actively being used for UAM research and under the administration of another team. As such, the following tests were done using an instance in the same environment as the PSUs with an agent installed on the same network but not a PSU. Tests were also conducted on the HIDS server to ensure its own monitoring. The following examples depict the alert(s) as that would presents themselves in the web UI.

TC001: Validate Malware Detection on Host-Based Intrusion Detection System Test
An EICAR file was placed on the HIDS server in the /dev/ directory. This type of file is a file that can safely be used that is non-viral but contains the signature of a viral file where anti-virus software should react to it as though it were a virus [13]. with a known signature to alert malware detection software was placed on. We were alerted to the file showing where the file was, which machine and when.

TC002: Identifying and detecting unapproved file changes on Host-Based Intrusion Detection System
A test file was created in one of the systems directories and time was allowed to elapse to enable the file to be scanned by OSSEC+. The file then had an arbitrary change made to it. Following this change, an alert was immediately generated and could be seen from the OSSEC+ online server console.

TC003: Identifying and detecting failed or unsuccessful login attempts on the Host-Based Intrusion Detection System
There were three tests done: 1) A username that did not exist was used to log into a system with OSSEC running on it (both the server and the agent). It was found that OSSEC+ created an alert in real-time of the failed login and the user trying to log in. 2) A username that existed, but the credentials to log in were not correct. 3) A user and username that did exist; upon successful or unsuccessful login, an alert would be generated in real-time. OSSEC also has the ability to visually display login attempts geographically.

TC004: Identifying and detecting new users and groups on Host-Based Intrusion Detection System
There were four tests that were done to test this functionality. 1) The creation of a user was done on both the server and a machine with an agent installed. Upon user creation, an alert was generated for the machine in question with the username created in real-time. 2) The same account was deleted, and upon user deletion, an alert was generated for the machine in question in real time with the username removed. 3) Creating a new group was done on both the server and a machine with an agent installed. Upon group creation, an alert was generated for the machine in question in real-time with the group name that was created. 4) The same group was deleted, and upon group deletion, an alert was generated for the machine in question in real-time with the username removed.

TC005: Identifying and detecting user privilege escalation
A user was added to the admin group utilized the elevated privileges command ‘sudo’ to become the admin user root. Upon becoming root, an alert was generated for the machine in question in real-time with the username.

One of the most significant drawbacks of utilizing the open-source version of OSSEC+ was the limited documentation of getting everything to work together. While it is understood this is not necessarily unique to OSSEC, this can pose a significant barrier to entry for admins. Understanding how critical cyber situational awareness is, resources must be devoted to organizations so that proper monitoring may be set up and configured correctly.

VII. Key Findings, Relevance & Recommendations

Host-based intrusion detection systems are a valuable tool for beginning to protect aviation systems by addressing the shortfall of cyber situational awareness and beginning the switch to a more proactive security stance opposed to reactive. This bar for cyber situational awareness is raised by monitoring each host’s activity in the network for any suspicious anomalies so that problems can be investigated and resolved in real-time. However, it is also vital to understand that a HIDS is not the only protection solution. Incorporating other security measures like IPS, firewalls, and cyber resilience training and other concepts are crucial to creating a comprehensive defense mechanism for protecting the emerging UAM environment and even broader AAM environment against

cybersecurity attacks. Discussed in Section II were just a few examples of what the threat landscape for aviation is like. Attackers have found other sophisticated ways to disrupt and take advantage of aviation systems. These cybersecurity issues can be especially threatening to the emerging UAM environment, with our goal in this UAM project of better understanding the environment and begin to see how to better implement cyber resiliency.

One of the most significant drawbacks of utilizing the open-source version of OSSEC+ was the limited documentation of getting everything to work together. While it is understood this is not necessarily unique to OSSEC, this can pose a significant barrier to entry for admins. Understanding how critical cyber situational awareness is, resources must be devoted to organizations so that proper monitoring may be set up and configured correctly. It is understood that in a commercial environment, implementing a HIDS may be more straightforward. However, given the nature of the operating environment within NASA and the broader UAM research team's constraints and simulation environment, we considered this initial step a valuable and critical step (considering our software selection and approval challenges, configuration issues, customizations for our environment, and team's cyber adoption and reception). While the research team could implement one of the critical components of cyber resiliency – cyber situational awareness, we also aimed at working on the more holistic and practical components, which involved user education. We were able to get our colleagues, who were researching other UAM simulation aspects, to understand security better and our objectives therein. Their understanding of what we were doing, and the benefits of cybersecurity allowed them to gain a better appreciation for what we were doing with our research and allowed us to be more integrated with the broader team. Furthermore, with an understanding of our goals and being more receptive, they allowed us to install the agents on the PSU and have them run during active simulations as opposed to what was first proposed - running the simulation with the agents off and then turning on them on with less of a focus on having all of the simulation running.

In this experiment, we implemented a HIDS within a simulated UAM environment; the agents that reported to the host machine were on the PSUs - all within one AWS VPC environment. These agents then reported back findings to the central server, and should any anomalies be found, one of our researchers was notified. While this works in a research environment, this setup is not practical in practice. To begin with, the concept of a PSU can be considered a service where a company or companies can operate a single PSU or group of PSUs run by multiple companies rather than just one throughout different regions. As such, when this is commercialized, there will not be a single provider to aggregate security information – let alone a single person.

Given this, to have a robust cyber posture, multiple teams must be set up to monitor security events, both within a UAM operator's environment and the various PSU environments. As we project forward, the extensive cybersecurity oversight tasks for UAM will eventually need to be transitioned and consolidated under the aegis of a security operations center (SOC) for each company. Such centers would be dedicated to continuous surveillance, rapid incident response, and the iterative enhancement of defense mechanisms, ensuring that the UAM remains robust against evolving cyber threats. Understanding the seriousness of consideration of safety within the UAM operating environment, we realize the criticality of having cyber situational awareness. Where a cyber event could degrade, halt, or have catastrophic impacts on a company's UAM operations, the information one company has for a cyber incursion may benefit and prevent an attack on another company - all to ensure safety for all. Additionally, given the competitive nature and landscape of the market when potential cyber incursions are detected by company A's SOC, company A may not necessarily be incentivized to tell company B about the cyber incursion as having company B down for even a few hours recovering from a similar cyber-attack could generate additional business for company A. Given the stark reality of the competitive nature of the industry, we recommend that these entities be required to make threat sharing via an Information Sharing and Analysis Center (ISAC). ISACs collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency [14]. One such ISAC that UAM companies could join would be within the Aviation ISAC [15]. This would be mutually beneficial for all parties involved and help ensure the safety of customers and the surrounding urban environment in which UAM vehicles operate.

While valuable information was gathered, due to time and other project constraints, e.g., this being an active simulation environment - various tests were not able to be carried out. In future works, we would like to do more extensive testing, including penetration testing focusing on UAM scenarios to better assess the HIDS capabilities and offer additional recommendations for other tools. Part of these tests would include being able to utilize a network tap to study the network traffic throughout the simulation environment like the original network tap that was meant to analyze traffic between the PSUs, and third-party services, pilot-intended flight path data and spacing scheduling services. This would allow us to evaluate the incoming and outgoing traffic to compare the signatures found in the network traffic against a database of malicious signatures that the HIDS may have. More thorough testing would also like to be done using scripts that will look at complementing the capabilities of OSSEC and allow for further analysis. While ML was moderately used as part of the suite of features available from OSSEC+, better

tuning of the software's ML abilities should be looked at as well as testing out those capabilities. With the current implementation, there may have been a lack of a training set to detect non-rules-based anomalies accurately. From the dashboard, it was difficult to determine if alerts were triggered via set rule or ML so we would like to study this behavior further. For test TC005, further tests attempting privilege escalation through a means other than a user account would also like to be utilized to see if it is detected. We would also like to go more in-depth with the components of malware detection. Being able to test in a closed environment utilizing a better analogue for something malicious would aid in testing these capabilities. Lastly, while an emphasis was put on IDS in this study as a component of cyber resiliency for the UAM environment. As we move forward with technology and its ever-increasing capabilities a key focus of cyber resiliency in future work and one that would be an integral component that UAM organizations should focus on is the implementation of a zero-trust framework. With the ultimate goal minimizing the fall out of cyber incursions through the prevention of unauthorized access to services and data as while at the same time making access control enforcement as granular as possible [16].

VIII. Wrap up & Business Justifications:

Urban Air Mobility has emerged as a revolutionary concept for future smart cities aiming to ease traffic congestion, reduce commute times, and enhance the overall transportation infrastructure. Given the autonomous and interconnected nature of UAM systems, cybersecurity is not just a matter of protecting data; it directly correlates with public safety. In such an intricate environment, adopting an Intrusion Detection System becomes essential to ensure the integrity, availability, and confidentiality of the UAM ecosystem. At the same time, the main principle of UAM is citizens' transportation through urban landscapes. Cyber intrusion can compromise flight controls, navigation, or communication, directly threatening human lives. Implementing an IDS ensures that any abnormal behavior at the host level, whether in flight controls or ground stations, is promptly detected and addressed. Smart cities will rely on a complex web of interconnected systems. A compromise in the UAM infrastructure could have cascading effects, disrupting other critical services. HIDS offers an added layer of protection, identifying threats that might exploit specific vulnerabilities of individual hosts within the UAM ecosystem.

Further, UAM systems will generate vast amounts of data, from flight paths to passenger information. Protecting this data is paramount, both for operational efficacy and privacy concerns. HIDS provides a mechanism to detect unauthorized data access or manipulation at the source. Urban Air Mobility represents a cross-section of innovation, convenience, and efficiency in the futuristic landscape of smart cities. However, its success relies on its reliability and security. Implementing a Host-Based Intrusion Detection System in this environment is not merely a technical measure but a strategic approach. It strengthens the foundations of safety, trust, and operational integrity critical for UAM's integration into the urban fabric of smart cities.

Failing to incorporate cybersecurity and cyber resilience from the beginning can have stark consequences. Beyond cyber incidents' immediate technical and operational repercussions, the financial ramifications can be staggering. The economic toll of a cyber incident can be long-lasting, from direct costs associated with incident response and remediation to indirect costs like lost business. The enterprise focus on resiliency at a very high level is a competitive advantage and vital for business sustainability and growth. The holistic approach requires more substantial alignment and convergence of previously "siloed" activities, leading to the evolution and convergence of respective models and standards [17]. Additionally, in a world where reputation is pivotal in an organization's valuation and customer trust, cyber incidents can erode stakeholder confidence, leading to longer-term reputational damage. Showing an assurance of cybersecurity is critical for public acceptance. The growth in the development of UAM systems and the associated data exchange and service interactions will be at risk due to numerous cybersecurity attacks. The UAM cybersecurity and cyber resilience capabilities must adapt as these threats evolve.

Accordingly, as UAM becomes more mainstream, regulatory bodies must mandate stringent cybersecurity measures to ensure public safety. One such position of cyber resiliency that we have proposed would involve the early adoption and implementation of HIDS, which positions the UAM initiative of a smart city in line with current and future compliance requirements. We believe that investing in HIDS for the foundation of a broader schema of a UAM organization's cybersecurity cache is a forward-looking decision, securing not just the present but the future of urban air transportation.

References

[1] PNNL, "Cyber Resilience," [Online]. Available: https://www.pnnl.gov/explainer-articles/cyber-resilience.

[2] Federal Aviation Administration, "Urban Air Mobility (UAM) Version 2.0 Concept of Operations," 26 April 2023. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/Urban%20Air%20Mobility%20%28UAM%29%20Concept%20of%20Operations%202.0_0.pdf. [Accessed August 2023].

[3] E. Ukwandu, M. Amine Ben Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis and X. Bellekens, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," 10 July 2021. [Online]. Available: https://arxiv.org/pdf/2107.04910.pdf . [Accessed 2023].

[4] K. Freeman and S. Garcia, "A Survey of Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments," January 2021. [Online]. Available: https://doi.org/10.2514/6.2021-0660.

[5] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis and I. Kompatsiaris, "Host-based Intrusion Detection Using Signature-based and AI-driven Anomaly Detection Methods," *Information & Security: An International Journal*, vol. 50, no. 1, pp. 37-48, 2021.

[6] M. M. V. N. E. A. a. M. K. A. Damien, "Implementation of a Host-Based Intrusion Detection System for Avionic Applications," 2019.

[7] elastic, "What is SIEM (Security Information and Event Management)?," [Online]. Available: https://www.elastic.co/what-is/siem.

[8] A. Naik, "Issues and Recent Advances in Machine Learning Techniques for Intrusion Detection Systems," 12 December 2019. [Online]. Available: https://www.cse.wustl.edu/~jain/cse570-19/ftp/ml_ids.pdf. [Accessed October 2023].

[9] M. A. S. a. A. M. B.-E. K. Soliman, "Survey of Machine Learning HIDS Techniques," 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9686138. [Accessed October 2023].

[10] J. H. Ring, C. M. Van Oort, S. Durst, V. White, J. P. Near and C. Skalka, "Methods for Host-based Intrusion Detection with Deep Learning," 15 October 2021. [Online]. Available: https://doi.org/10.1145/3461462. [Accessed October 2023].

[11] NASA, "UAM Sub-Project," NASA, Moffett Field, 2021.

[12] "OSSEC -World's Most Widely Used Host Intrusion Detection System," Atomicorp, [Online]. Available: https://www.ossec.net/.

[13] European Institute for Computer Anti-Virus Research, "eicar - European Expert Group For IT Security," [Online]. Available: https://www.eicar.org/download-anti-malware-testfile/.

[14] "National Council of ISACs," [Online]. Available: https://www.nationalisacs.org/.

[15] "Aviation ISAC," [Online]. Available: https://www.a-isac.com/.

[16] CISA, "Zero Trust Maturity Model," [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model. [Accessed June 2024].

[17] G. Sharkov, "From cybersecurity to collaborative resiliency. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense," 2016. [Online]. Available: doi-org.library.capella.edu/10.1145/2994475.2994484.