Detailed Design – Tool Selection

1. **Log Management & Visualization**
   • **ELK Stack** – Scales efficiently with large security data, integrates seamlessly with cloud environments, and delivers unmatched search performance. Chosen for its flexibility in handling both structured and unstructured logs.

2. **Backend Development**
   • **Flask** – Minimal overhead, easy API development, and fast deployment. Preferred for its simplicity, making security integration and maintenance easier than with heavier frameworks.

3. **Frontend Development**
   • **React** – Highly responsive, modular, and easy to maintain. Chosen for its fast rendering, dynamic UI capabilities, and long-term support in modern web apps.

4. **Cloud Integration**
   • **AWS (Boto3)** – Official AWS SDK, ensuring full compatibility, security, and stability. Chosen for deep integration and consistent support over generic libraries.
   • **Azure (Azure SDK for Python)** – Provides robust security features and role-based access. Preferred for its reliability, authentication handling, and enterprise-grade support over REST API calls.

5. **Log Collection – Cloud-Specific**
   • **AWS: Invictus AWS** – Purpose-built for AWS logs, optimized for performance and ensuring comprehensive log coverage. Avoids inefficiencies found in generic log collectors.
   • **Azure: Invictus Azure** – Designed specifically for Azure logs, ensuring completeness and compliance. Outperforms generic collectors with cloud-native optimizations.

6. **Multi-Cloud Security Auditing**
   • **ScoutSuite** – A comprehensive multi-cloud security auditing tool that supports AWS and Azure. It is ideal for auditing across different cloud environments and provides a unified view for all three major cloud providers, making it a perfect fit for projects requiring insights across multiple clouds. It minimizes the need for separate tools or custom integrations for each cloud provider and benefits from community contributions aimed at keeping it relevant across platforms.

7. **Cloud Storage Integration**
   • **AWS S3** – For cloud storage, S3 provides reliable, scalable, and cost-effective storage. Integrating S3 will allow the system to efficiently store and retrieve data across multiple cloud environments. Using S3 ensures compatibility with various cloud services, making it a flexible option for long-term scalability.

Anomaly Detection (for identifying security gaps or misconfigurations):

- **Algorithms:** K-Means Clustering
- **How It Works:** K-Means analyzes cloud logs and configurations to detect patterns of activity that deviate from normal behavior, signaling potential security gaps or misconfigurations. By grouping similar data points, it highlights unusual clusters that may indicate areas requiring security attention, such as unauthorized changes or abnormal usage.

Classification (for classifying resources or users based on security):

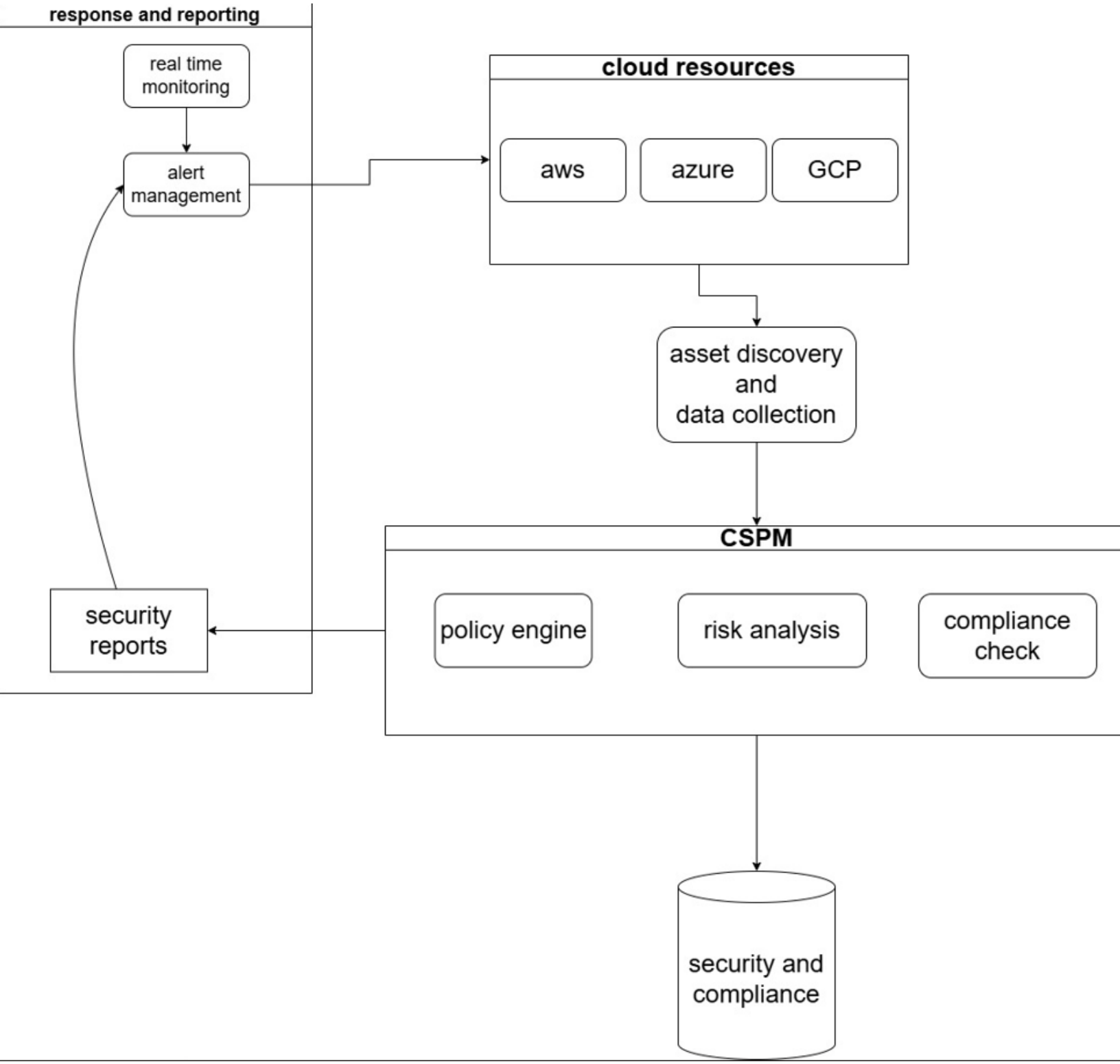
- **Algorithms:** Random Forest
- **How It Works:** Random Forest uses decision trees to classify resources and users based on various security features, such as access permissions, usage history, and behavior patterns. It effectively categorizes entities as secure or insecure, enabling proactive management of cloud resources and identifying potential vulnerabilities before they are exploited.

Log Analysis and Pattern Recognition:

- **Algorithms:** KNN
- **How It Works:** KNN analyzes historical cloud log data to detect patterns and classify activity as either normal or suspicious. By examining past behavior and comparing it to new log entries, it can predict potential security incidents, such as unauthorized access attempts or unusual resource consumption spikes.

Clustering (for grouping resources or users based on security patterns):

- **Algorithms:** K-Means
- **How It Works:** K-Means groups resources or users with similar access patterns or security behavior into clusters, helping to identify high-risk groups. This clustering can reveal patterns such as users with excessive permissions or resources with unusually high levels of exposure, allowing security teams to target specific areas for remediation.



Hadar nino – 314712464 Maor Hadad Levy – 212708077 Almog Asia – 325553543