Project Title

Zero Trust Security Model Implementation using Lenel OnGuard and Amazon Policies

---

Project Overview

In this project, I focused on implementing the **Zero Trust Security Model** for Amazon's badge access system to take security to the next level. The idea was to ensure that every access request, even from authenticated employees, was verified and continuously monitored. By combining **Lenel OnGuard** with Amazon's internal security policies, we created a more robust and dynamic access control system where trust is never assumed and every action is validated. This model provided a higher level of security by making sure no one gets automatic access—everyone and everything is verified, every time.

Project Challenge

One of the biggest challenges I faced was shifting from a traditional perimeter-based security model to a Zero Trust approach. We had to ensure that all badge access—whether for employees, contractors, or visitors—was continuously verified, even after the person was initially authenticated. This shift involved a lot of coordination and technical setup to ensure that every access request was checked against real-time context, like time of day, location, and role.

My Objectives

- Seamlessly integrate **Lenel OnGuard** with Amazon's security policies to enforce the Zero Trust principles for badge access.
- Continuously monitor access requests in real-time to ensure they meet specific security criteria.
- Automate the monitoring process and generate alerts when unauthorized access attempts or unusual behaviors occur.
- Provide clear reports and documentation to help security teams quickly understand and act on access data.

What I Did

1. **Zero Trust Integration**
    - The first step was integrating **Lenel OnGuard** with Amazon's internal identity and security policies. This was a critical piece of the project because it ensured that all access requests were verified before being granted—no assumptions were made about who could access what and when.
    - I worked on defining specific user roles and permissions, making sure each access request was evaluated based on the person's context, such as where they were, what time it was, and what area they were trying to access.
2. **Contextual Access Control**
    - I developed policies for **Lenel OnGuard** that took context into account for every access request. For example, employees could only access certain areas during their assigned hours, and access to high-security areas was strictly controlled.
    - To help with this, I also set up **real-time alerts** for the security team, notifying them whenever access requests didn't align with the established rules.
3. **Monitoring and Risk Analysis**
    - One of the more interesting aspects of this project was integrating real-time monitoring. I helped set up a system where badge access requests were continuously evaluated for risk—each one was checked to ensure it was safe and legitimate.
    - I also incorporated **behavioral analytics** to detect abnormal access patterns, such as someone trying to enter a restricted area at unusual times or with a badge they shouldn't be using.
4. **Training and Documentation**
    - I made sure that all the security teams had clear documentation on how to use the new system, what to look out for, and how to respond to alerts. I also conducted training sessions to walk them through the new procedures and tools.

Results

- **Improved Security**: With the Zero Trust model in place, no one could gain access without being continuously validated. We significantly reduced the risk of unauthorized access, even from internal personnel.
- **Faster Response Times**: The real-time monitoring and alert system gave security teams a quicker way to detect potential security threats, allowing for faster responses.
- **Better Data Insights**: The automated reports and alerts helped the security team spot trends and understand access patterns more clearly. It also allowed us to identify areas where we needed to strengthen security.

What I Learned

- I gained hands-on experience in applying the **Zero Trust Security Model** to a physical security system, which was fascinating. It taught me a lot about balancing convenience and security, ensuring the system is efficient yet tight on security.
- I also learned how to work with **Lenel OnGuard** and integrate it with other Amazon systems, which was challenging but incredibly rewarding.
- The project gave me valuable experience in real-time data analysis and monitoring, skills that I can apply to both physical and cybersecurity tasks.

Challenges

- One of the biggest hurdles was integrating the various systems and ensuring the data was consistent and accurate across platforms. It took a lot of time to get everything connected and working seamlessly.
- Another challenge was figuring out how to manage false positives. The alert system needed to be sensitive enough to catch real threats but not so sensitive that it flooded the security team with unnecessary notifications.
- Finally, ensuring that the system was scalable and could handle a large number of users without impacting performance was another significant challenge.

Competencies Gained

- **Tools & Technologies**: Lenel OnGuard, Amazon's internal security policies, real-time monitoring tools, and behavioral analytics systems.
- **Skills**: Zero Trust Security Model implementation, system integration, data analysis, risk management, and security alerting.
- **Problem Solving**: Overcame challenges in system integration, managing real-time access requests, and handling false positives in alerts.