Secure System Engineering Practices

Overview

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts. Lumetric AI is committed to building security and privacy into every aspect of our system design and development process.

Secure-by-Design Principles

At a minimum, the following secure-by-design principles shall be applied to all system implementation efforts:

1. **Minimize attack surface area:** Every feature and component increases the potential attack surface. We actively work to reduce unnecessary functionality and limit exposure points.
2. **Establish secure defaults:** Systems are configured with security-first default settings. Users must explicitly choose to reduce security rather than having to add it.
3. **The principle of least privilege:** Users, processes, and systems are granted only the minimum levels of access necessary to perform their functions.
4. **The principle of defense in depth:** Multiple layers of security controls are implemented throughout the system to ensure that if one control fails, others continue to provide protection.
5. **Fail securely:** When systems encounter errors or failures, they default to a secure state rather than an open or vulnerable one.
6. **Don't trust services:** All external services, third-party integrations, and even internal services are treated as potentially untrusted and are validated accordingly.
7. **Separation of duties:** Critical operations require multiple parties or steps to complete, preventing any single individual from compromising system security.

8. **Avoid security by obscurity:** Security mechanisms do not rely on secrecy of implementation. Systems remain secure even when their design is known.
9. **Keep security simple:** Security mechanisms are designed to be straightforward and understandable, avoiding unnecessary complexity that can introduce vulnerabilities.
10. **Fix security issues correctly:** When security issues are identified, they are thoroughly analyzed, properly fixed at the root cause, and tested to prevent recurrence.

Privacy-by-Design Principles

The following privacy-by-design principles are embedded into all system development and operational processes:

1. **Proactive not Reactive; Preventative not Remedial:** Privacy risks are anticipated and prevented before they materialize, rather than addressed after the fact.
2. **Privacy as the Default Setting:** Maximum privacy protection is built into systems automatically, requiring no action from users to benefit from privacy protections.
3. **Privacy Embedded into Design:** Privacy is integrated into the architecture and functionality of systems from the earliest stages, not added as an afterthought.
4. **Full Functionality – Positive-Sum, not Zero-Sum:** Privacy and functionality coexist without unnecessary trade-offs. Systems are designed to achieve both objectives simultaneously.
5. **End-to-End Security – Full Lifecycle Protection:** Privacy protections extend throughout the entire data lifecycle, from collection through deletion, with secure handling at every stage.
6. **Visibility and Transparency – Keep it Open:** System operations remain transparent and open to verification. Users and stakeholders can understand how their data is handled.
7. **Respect for User Privacy – Keep it User-Centric:** User interests are prioritized in all privacy decisions. Systems are designed with the user's privacy needs at the center.

Development Standards and Documentation

Software developers are expected to adhere to Lumetric AI's coding standards throughout the development cycle, including standards for quality, commenting, and security. All engineering

practices are regularly reviewed and updated to reflect emerging security threats, privacy regulations, and industry best practices.
