SECURITY IS AMI'S TOP PRIORITY

AMI CEO takes security very seriously and prioritizes its cybersecurity program by structuring the CISO role as executive management with a direct reporting line to the CEO and the Board of Directors. At AMI, the CISO also manages the CIO organization. This solves the never-ending conflict that a mis-aligned CISO has with the CIO and other IT operational priorities.

AMI is a proud, early adopter of this unique zero-trust model that puts security as # 1 priority in our products and our global company processes.

AN INDEPENDENT SECURITY PROGRAM

The global CISO program is managed completely outside of engineering and development to enforce strong governance and independence over security monitoring and reporting. Separation of Duties (SoD) is a priority and independence within the AMI organization is key.

EXECUTIVE TRANSPARENCY

Our program includes key metrics, NIST CSF maturity planning, and roadmaps with frequent updates to executive management including the Board of Directors. Metrics are used to trend product security posture and focus on internal controls that continuously maintain and improve our cybersecurity posture.

Strategic cybersecurity roadmaps are managed and communicated that cover both product security and corporate security initiatives. The roadmaps are top-down sponsored and executive funded by the Board of Directors and the CEO.

PRODUCT SECURITY

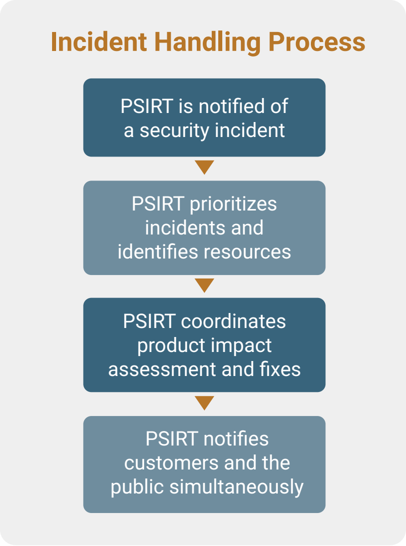
AMI not only maintains independent CISO security functions, but we have also formed an internal security engineering team with a mission to eliminate vulnerabilities in our products. This dedicated team is equipped to respond quickly and efficiently to any identified vulnerabilities and provide remediations to our OEM/ODM customers, as well as the industry at large, through releases, AMI Security Advisories, and other communication channels. We are committed to ensuring the security of our products.

— PROACTIVE SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC)

AMI has a dedicated product Independent SSDLC function that governs each product SSDLC process and leverages a shift-left security control framework. Our engineers implement our SSDLC processes which include training, security scans and remediation activities throughout the release management lifecycle.

— PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT)

Our PSIRT process is implemented with a modern Vulnerability Management System (VMS) equipped with scanners that are part of each product's SSDLC process. This integration enables automatic ingestion of new sightings into the vulnerability management system, triggering an immediate investigation process, and reducing critical remediation responsiveness times. We have developed custom tools to verify that remediations have been implemented into released products with secure code.


Incident Handling Process

PSIRT is notified of a security incident

PSIRT prioritizes incidents and identifies resources

PSIRT coordinates product impact assessment and fixes

PSIRT notifies customers and the public simultaneously

— SECURITY ADVISORIES

AMI believes in transparency when it comes to security issues. That's why we publish security advisories to provide our customers with timely and accurate information about vulnerabilities that may affect our products. We also provide our customers with access to our customer support team, who can answer any questions.

— OUR ROLE IN THE SUPPLY CHAIN

AMI plays a critical role in the firmware supply chain, situated between silicon vendors and downstream partners such as ODMs, OEMs, and CSPs. This gives AMI significant visibility and influence over the code that makes up the final firmware binaries programmed into devices. AMI recognizes the responsibility that comes with this position and is committed to ensuring the highest level of security for its code. To this end, AMI provides a comprehensive SSDLC integrated into every product's development workflow, a modern and responsive PSIRT, and tools that enable downstream partners to incorporate AMI's latest security fixes into their own firmware binaries.

RESILIENCY

Our focus on resiliency includes people, process, and technology and the ability to recover and continue operations including air gap data strategy, data recovery, ransomware protection, code integrity, recovery table tops, breach response plan, and much more.

COMPLIANCE

AMI adheres to ISO27001 and NIST CSF controls as well as local data protection acts such as GDPR. AMI is in the final stages of obtaining its first global ISO 27001 certificate for all global locations and product lines in 2023.

PROTECTING CUSTOMER INFORMATION

AMI takes protecting customer information and IP very seriously. Global dedicated people, process, and technology solutions are in place to deliver advanced Data Leakage Prevention (DLP) capabilities across our organization.

The office of CISO works closely with business leaders, the CEO, Legal Counsel, and internal functions to ensure data protection is embedded in our internal controls. ISO-based audit activities take place to every data protection capabilities.

Least access privileged management (RBAC) controls as well as dedicated 24/7 security monitoring is in place to ensure timely detection of access activities and response to any type of potentially suspicious activities.

SECURITY IS ALWAYS EVOLVING

AMI understands that the threat landscape is always evolving therefore driving constant evolution within the AMI security program. This concept is baked into our strategy which results in a very agile and ever-improving cybersecurity organization, program, and control framework.