The MITRE SAF Cyber Security at Mission Speed

The Security Challenge

Today's faster deployments of software can also lead to faster deployments of vulnerable applications, leading to higher risk of unauthorized access to sensitive data. Given the speed of change in today's technology landscape and the resulting increased security threats, how can organizations keep up with the security requirements while deploying apps at speed?

The Solution: The MITRE Security Automation Framework (MITRE SAF)

The MITRE SAF helps teams implement security, visualize security status, drill down to identify root cause, and mitigate security risks. The MITRE SAF enables organizations to:

- Access a complete set of tools from a common platform
- Leverage shared solutions using an open-source continuous collaboration agreement
- Build automation into existing workflows to achieve security goals such as



How does the MITRE SAF help?

The MITRE SAF helps organizations develop and programmatically automate security in their current internal planning, development, assessment, and operational activities.

PLANNING

DEVELOPMENT

ASSESSMENT

OPERATIONS

During PLANNING an organization can use SAF to:

- 1. Identify applicable security requirements
- 2. Assess development best practice guidance
- 3. Identify SAF tools to support development, assessment, & operations
- 4. Participate in SAF through the Continuous Collaboration Agreement

During ASSESSMENT an organization can use SAF to:

- 1. Aggregate all security data for assessment
- 2. Visualize security status to prioritize assessment activities
- 3. Run validation checks on prioritized areas
- 4. Visualize security data to identify root cause and inform risk assessment

During DEVELOPMENT an organization can use SAF to:

- 1. Implement security hardening scripts
- 2. Validate/Aggregate security data at each build
- 3. Visualize security data to detect root cause and mitigations
- 4. Set security testing results thresholds
- 5. Store or export evidence for assessors

During OPERATIONS an organization can use SAF to:

- 1. Routinely monitor security of operational systems
- 2. Aggregate normalized security data to visualize, drill-down, and analyze root causes
- 3. Assign remediation actions for identified risks

For more information, contact the team at saf@groups.mitre.org or visit us at https://saf.mitre.org.