A Holistic Approach for Security Configuration

Patrick Stöckle

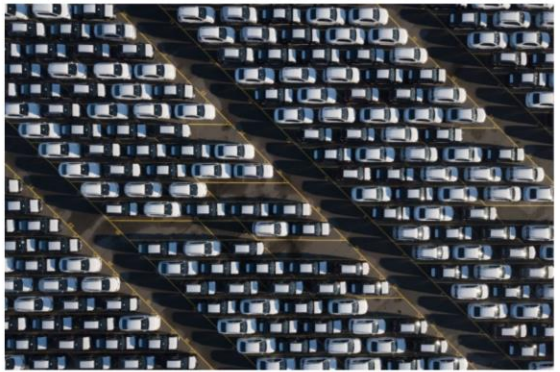
Garching, 28.06.2024

Recent Motivating Example

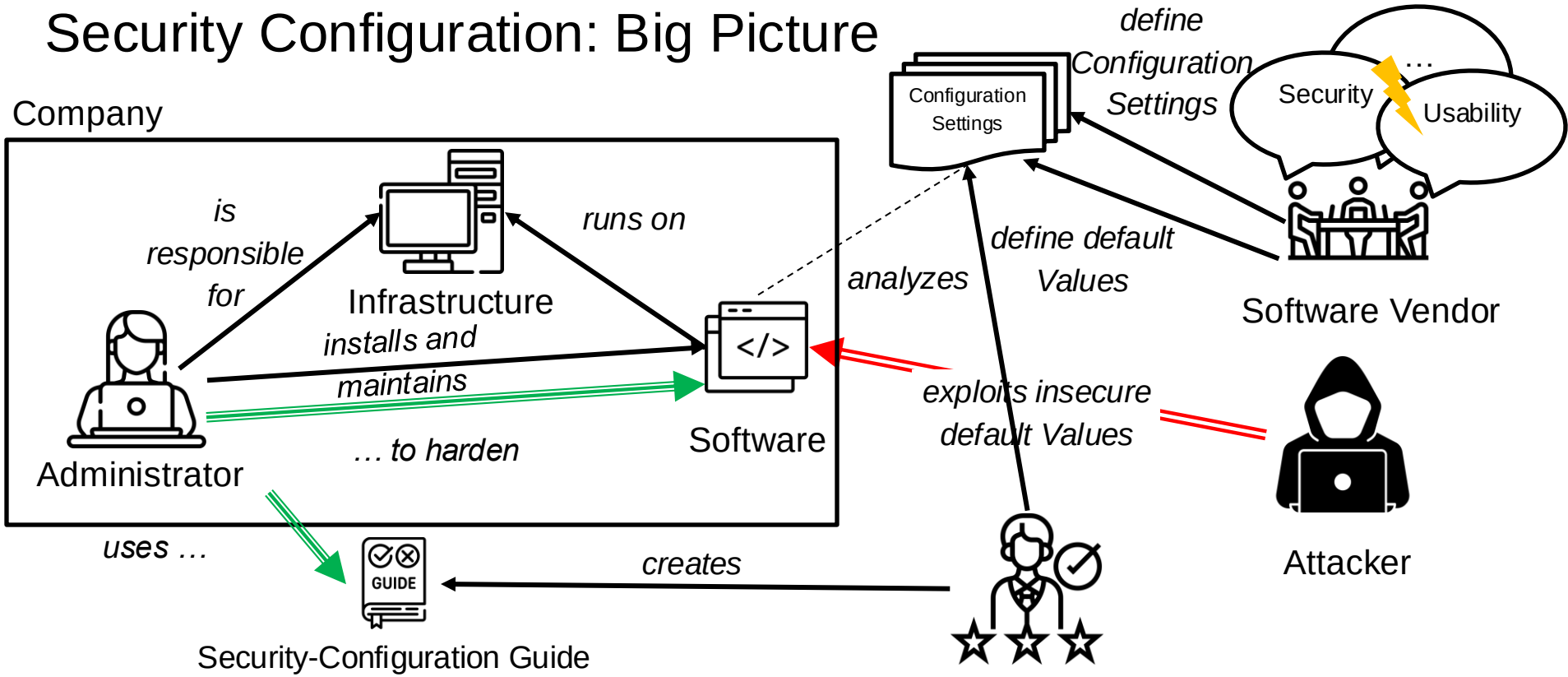
… about 2.15 million customers whose personal and vehicle information were left exposed to the internet after a “cloud misconfiguration” …

Toyota Japan exposed millions of vehicles’ location data for a decade

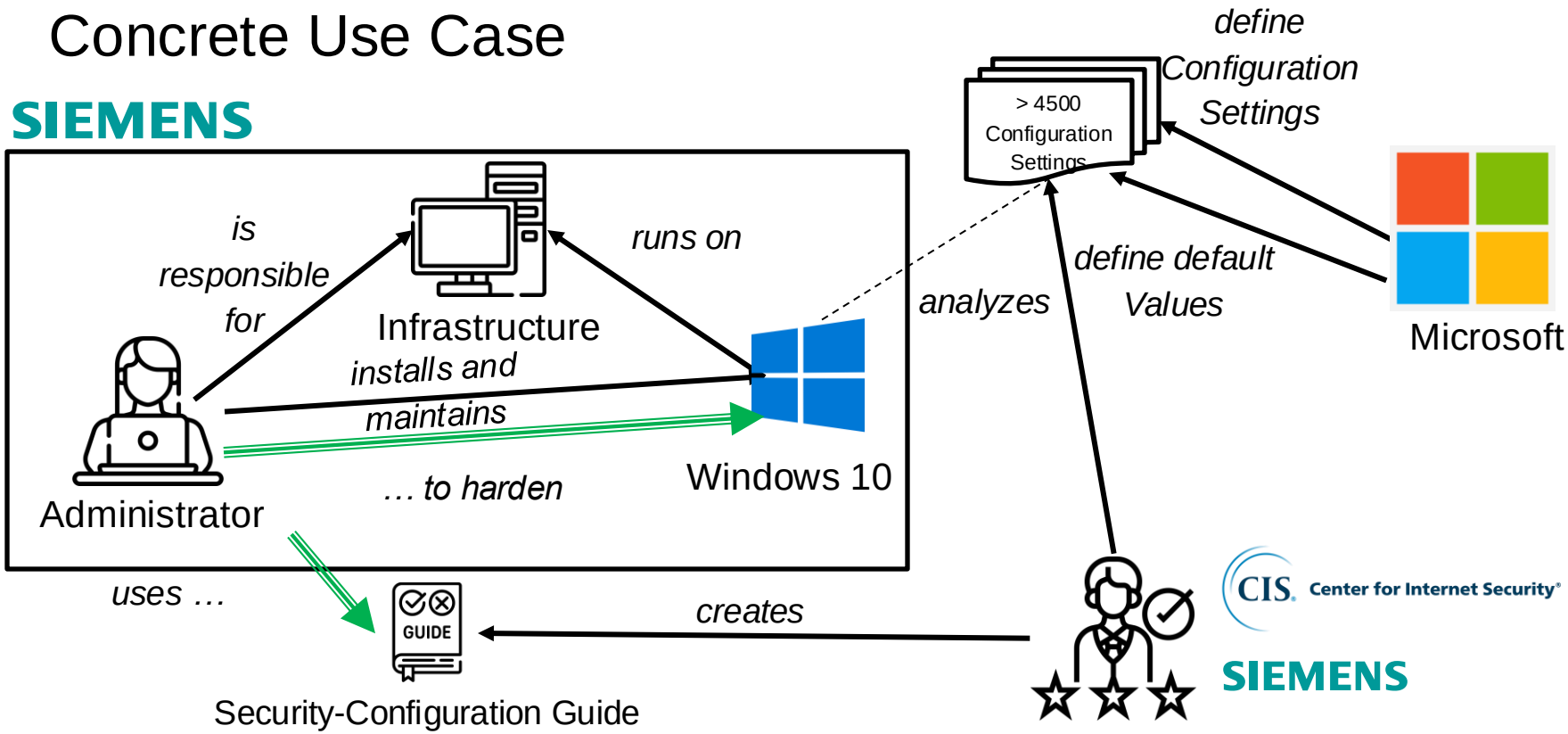
Zack Whittaker @zackwhittaker / 3 days



Security Configuration: Big Picture



Concrete Use Case



Problems

No efficient process

No automated implementation

Forgetting security-relevant settings

Underestimating the risk of default values

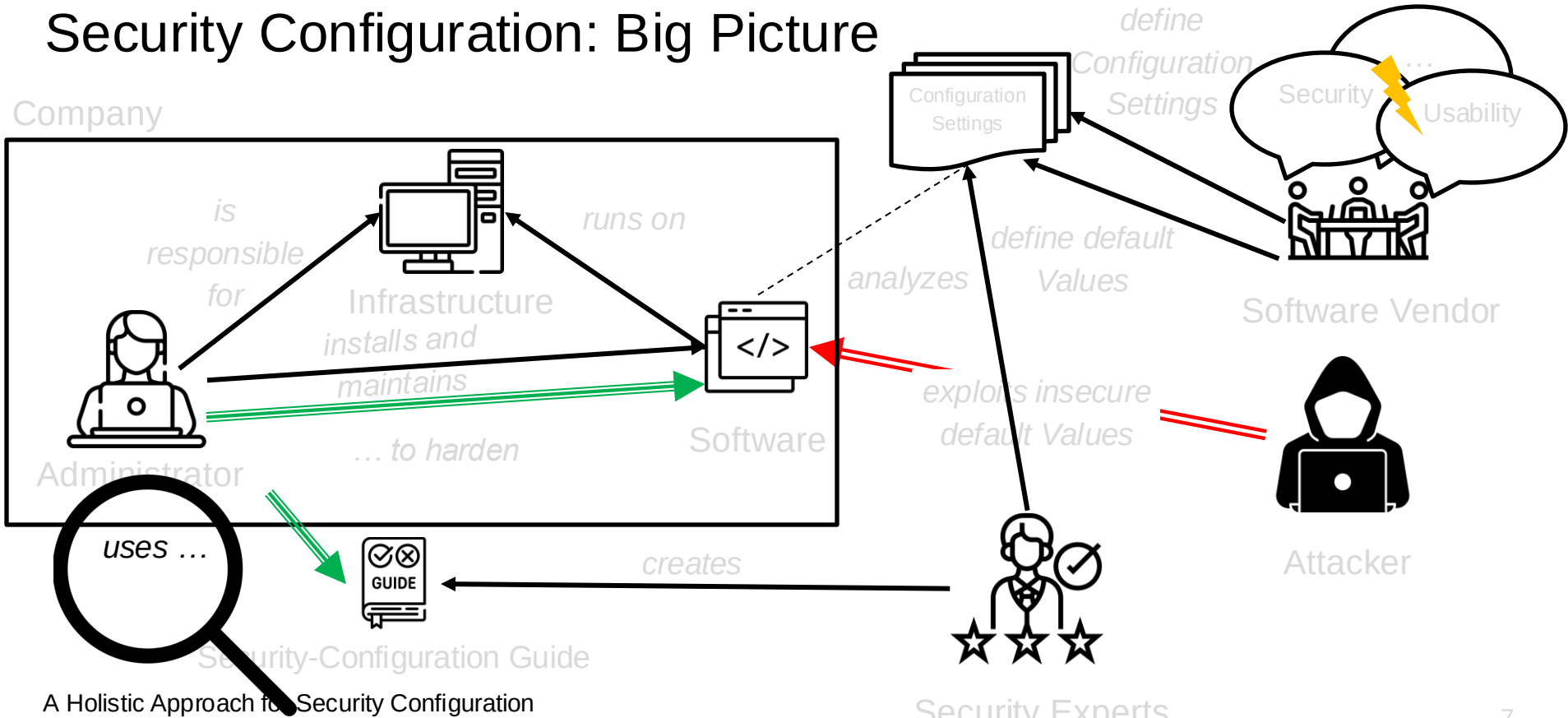
Breaking functionality

Solutions

- **Scapolite-Approach to ease security configuration**
- **Use NLP to implement guides automatically**
- **Use NLP to classify settings based on description**
- **Catalog of attacks exploiting insecure default values**
- **Use Covering Arrays & Decision Trees to find breaking rules**

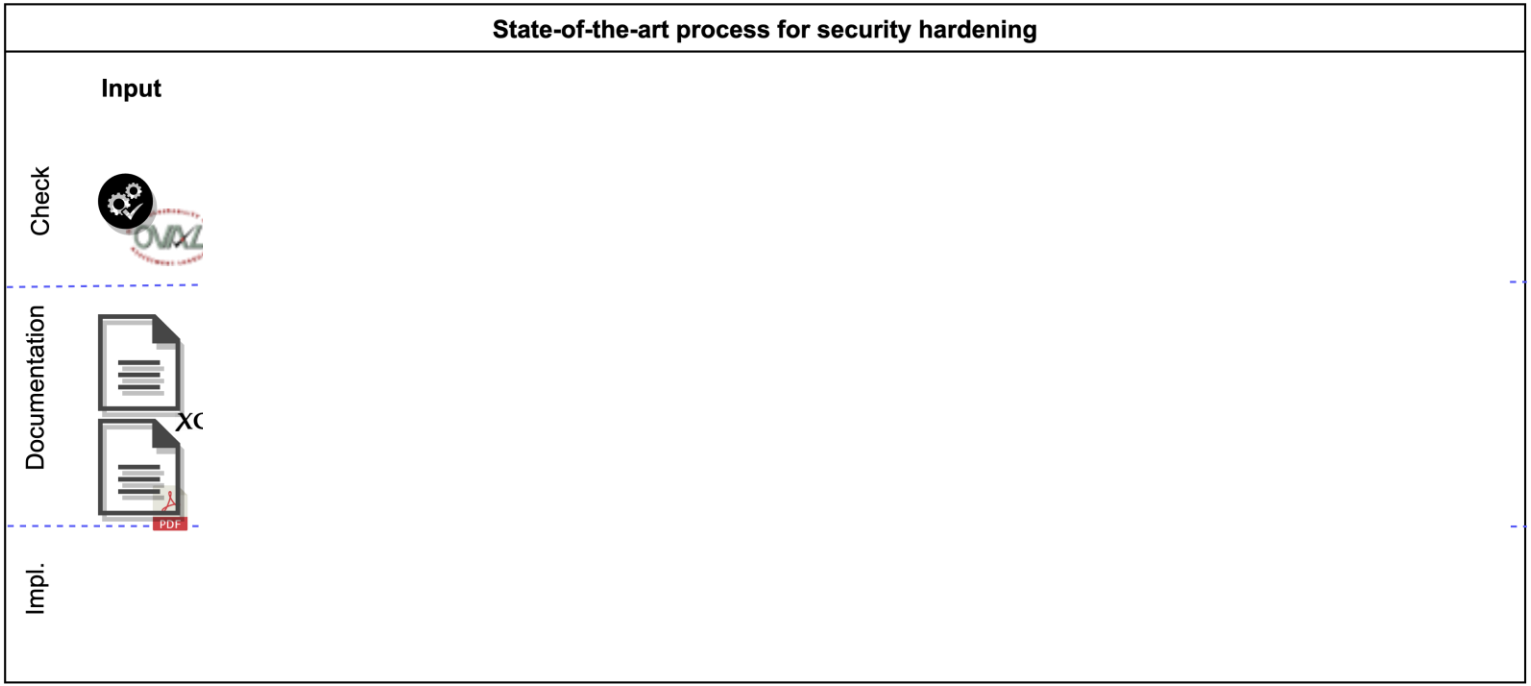
Stöckle et al.: *Hardening with Scapolite: A DevOps-based Approach for Improved Authoring and Testing of Security-Configuration Guides in Large-Scale Organizations*, CODASPY'22

Security Configuration: Big Picture



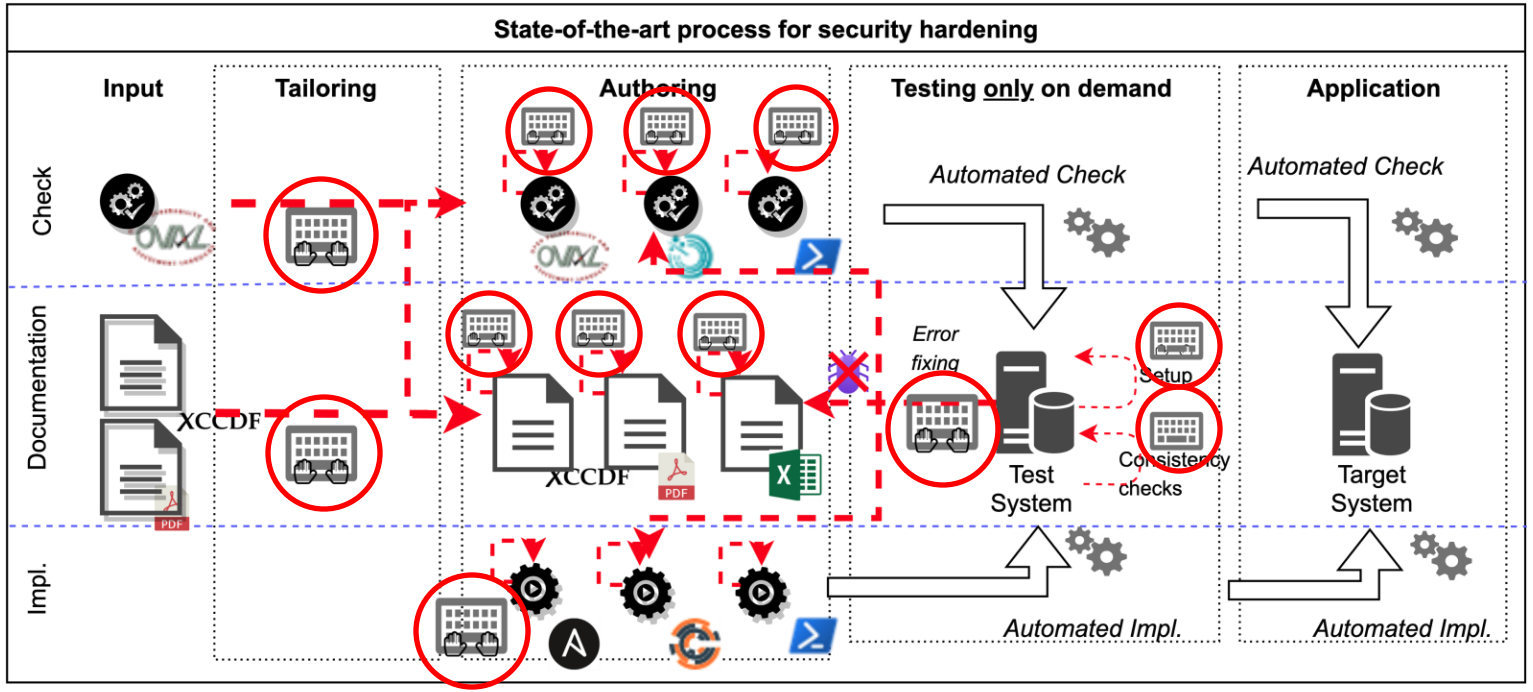
Stöckle et al.: *Hardening with Scapolite: A DevOps-based Approach for Improved Authoring and Testing of Security-Configuration Guides in Large-Scale Organizations*, CODASPY'22

Old Process

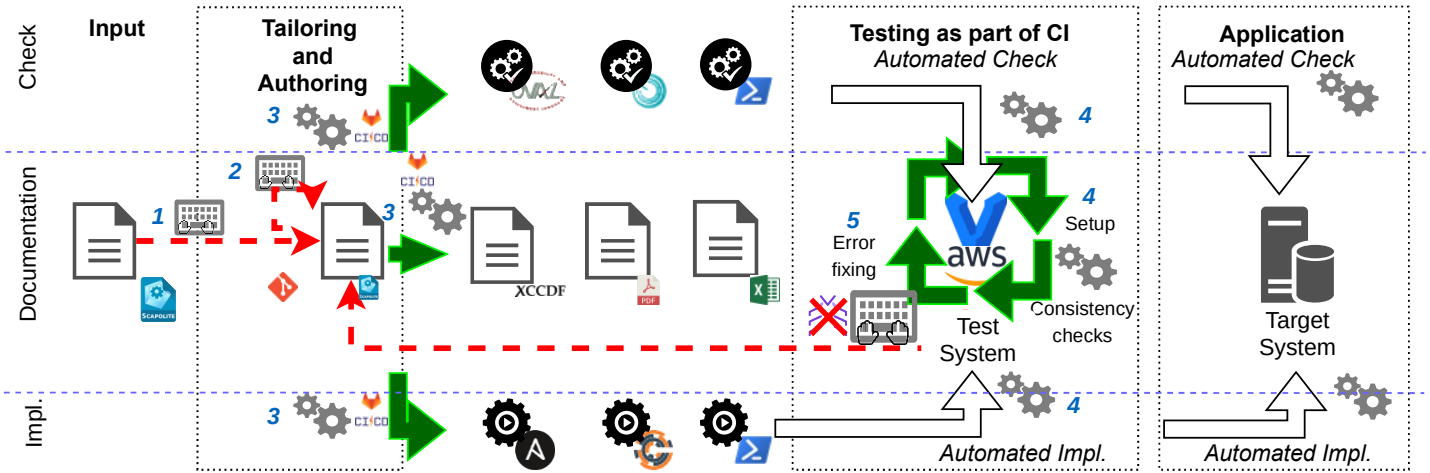


Stöckle et al.: *Hardening with Scapolite: A DevOps-based Approach for Improved Authoring and Testing of Security-Configuration Guides in Large-Scale Organizations*, CODASPY'22

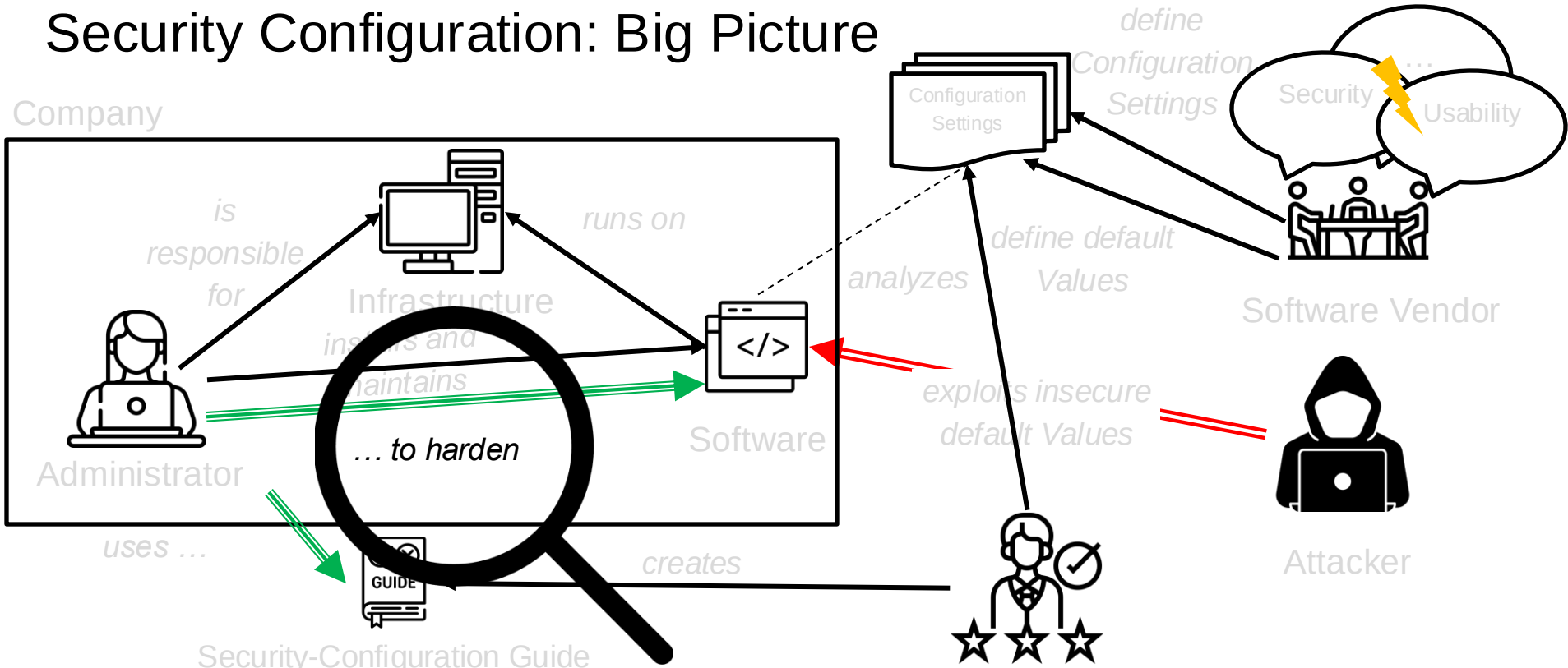
Problem: Manual Tasks



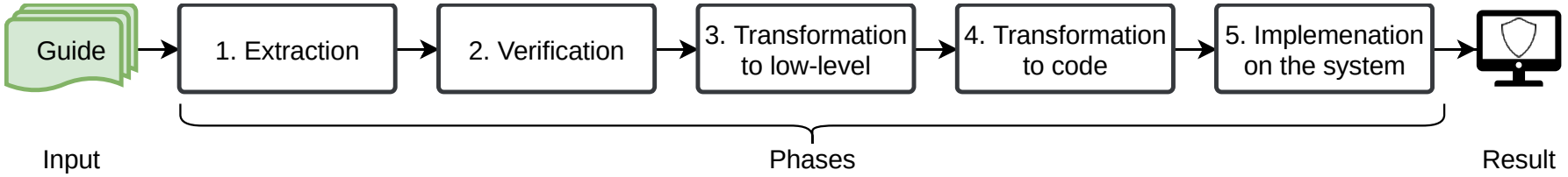
Scapolite Approach



Security Configuration: Big Picture



General Idea



Extraction with NLP

Example sentence

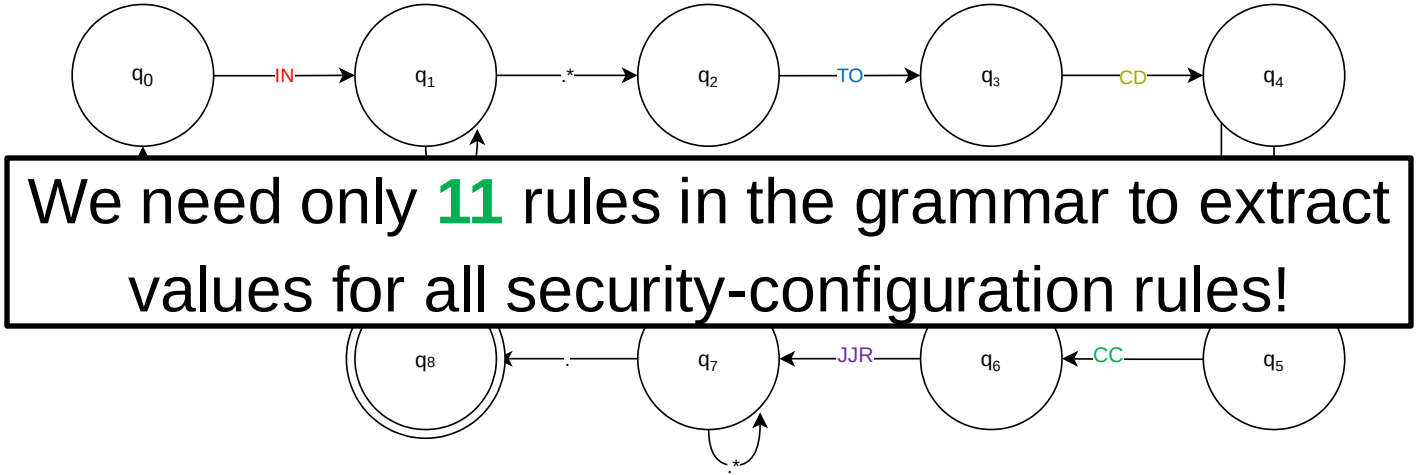
"Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> Account lockout duration to 15 minutes or greater."

After NLTK POS-tagging

(Configure, VB), (the, DT), (policy, NN), (value, NN), (for, IN), (Computer, NNP), (Configuration, NNP), (>, NNP), (>, NNP), (Windows, NNP), (Settings, NNP), (>, NNP), (>, NNP), (Security, NNP), (Settings, NNP), (>, NNP), (>, NNP), (Account, NNP), (Policies, NNP), (>, NNP), (>, NNP), (Account, NNP), (Lockout, NNP), (Policy, NNP), (>, NNP), (>, NNP), (Account, NNP), (lockout, NN), (duration, NN), (to, TO), (15, CD), (minutes, NNS), (or, CC), (greater, JJR), (., .)

CC:	coordinating conjunction
CD:	cardinal digit
IN:	preposition/subordinating conjunction
JJR:	adjective, comparative
NNS:	noun plural
TO:	infinite marker

Extraction with NLP

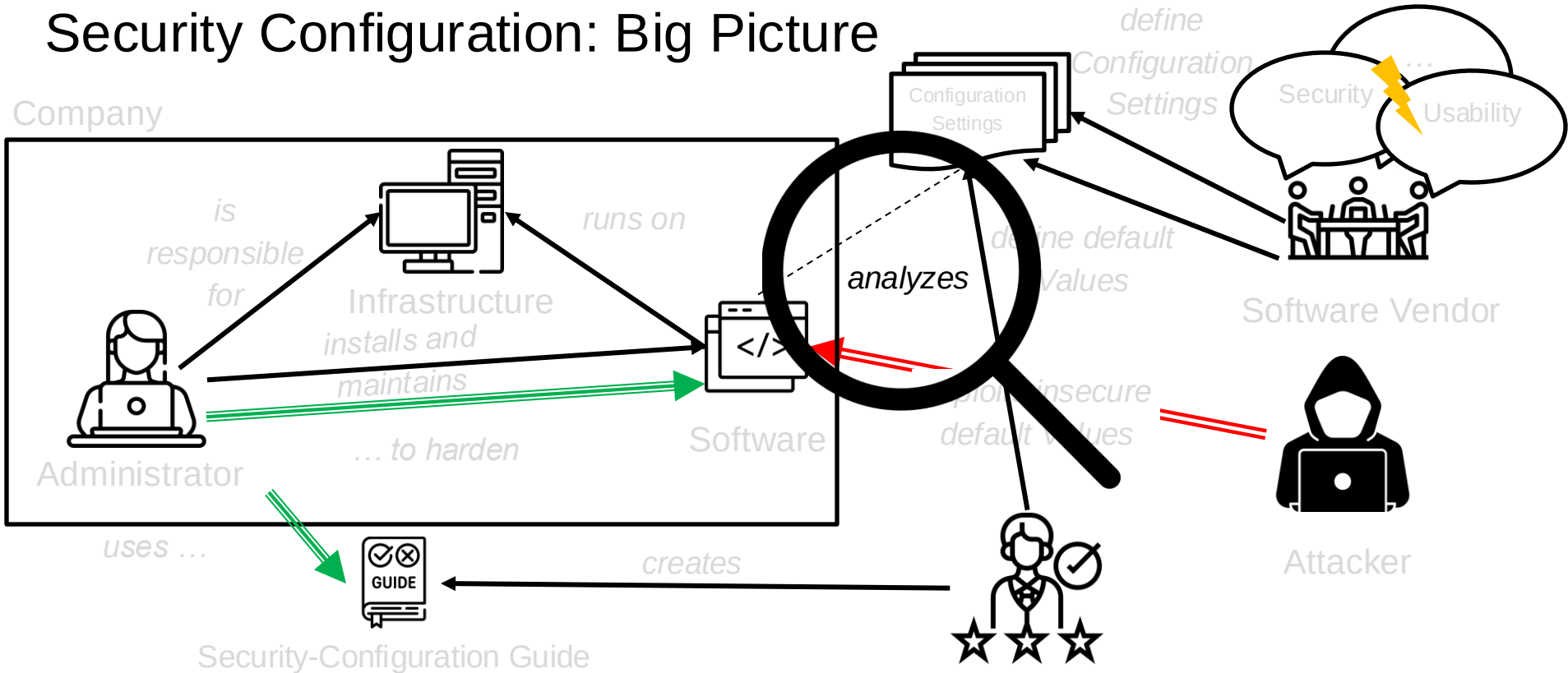


We need only **11** rules in the grammar to extract values for all security-configuration rules!

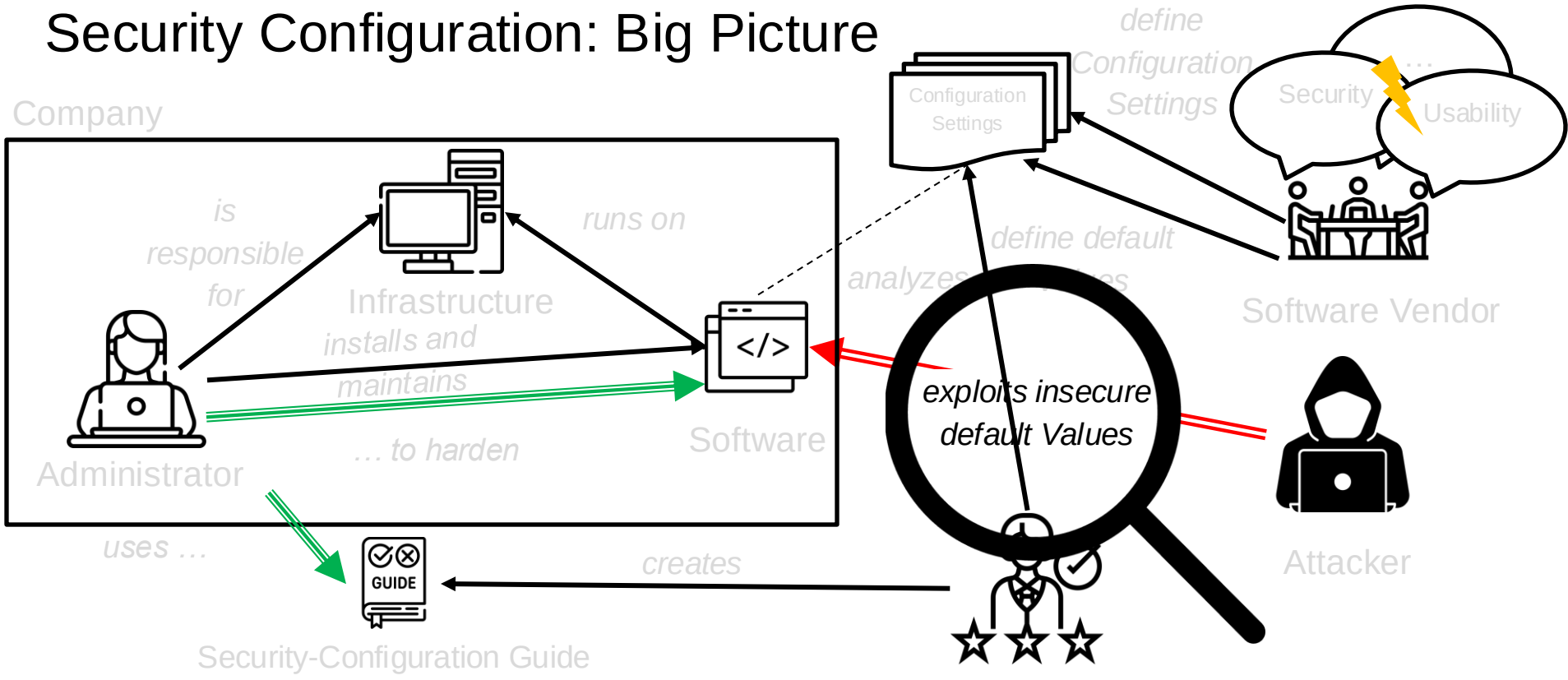
"Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> Account lockout duration to 15 minutes or greater."

CC:	coordinating conjunction
CD:	cardinal digit
IN:	preposition/subordinating conjunction
JJR:	adjective, comparative
NNS:	noun plural
TO:	infinite marker

Security Configuration: Big Picture

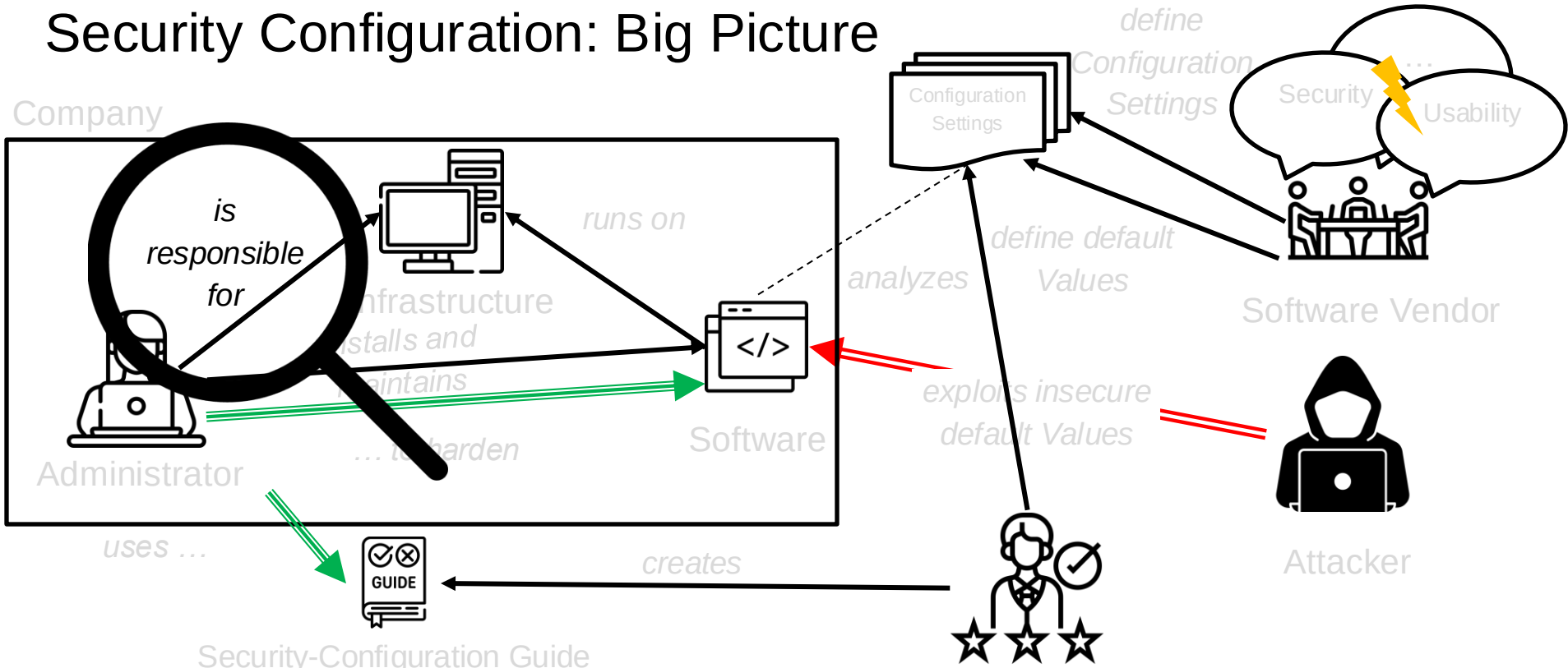


Security Configuration: Big Picture



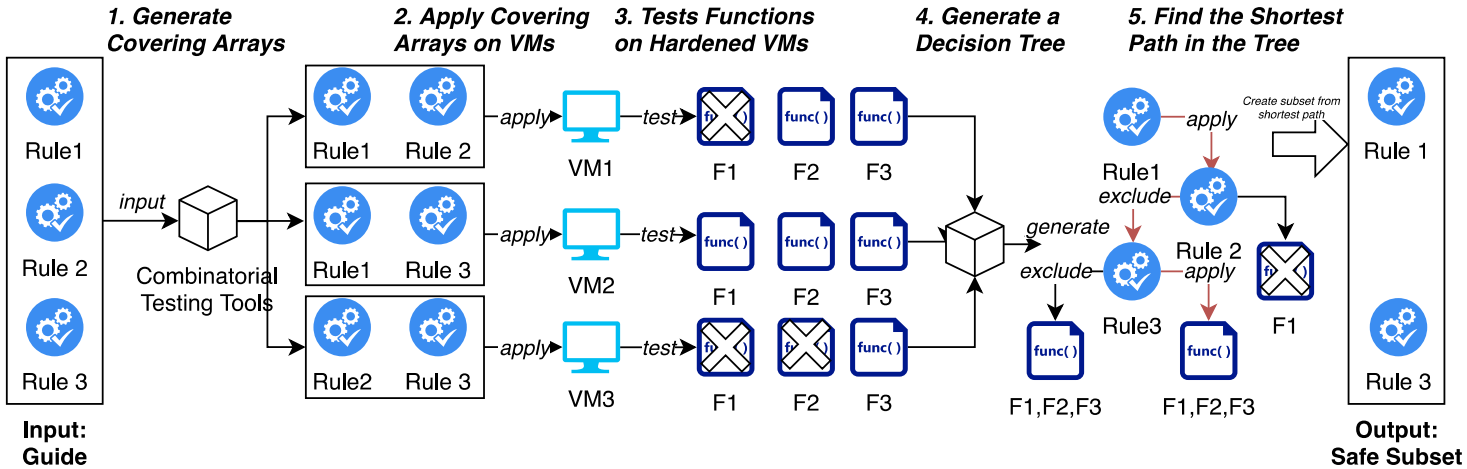
Stöckle et al. *Better Safe Than Sorry! Automated Identification of Functionality-Breaking Security-Configuration Rules*. AST'23

Security Configuration: Big Picture

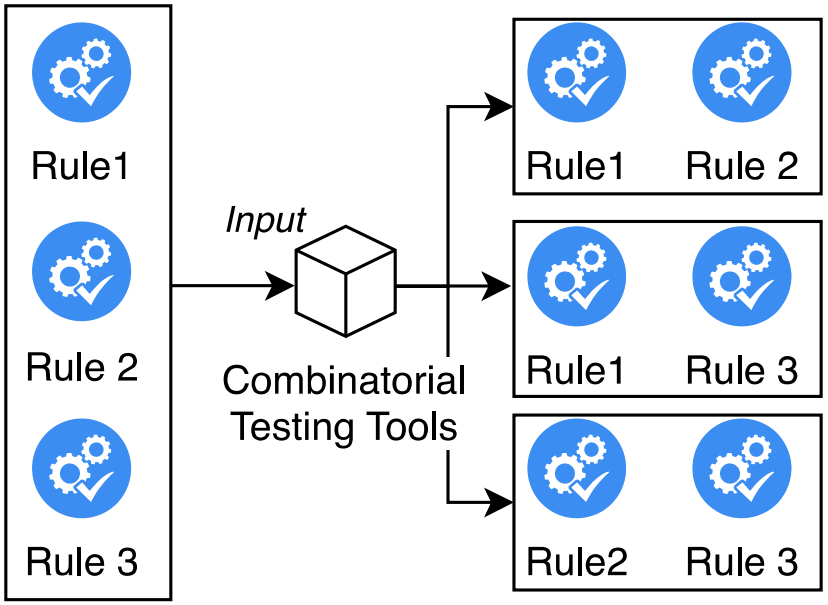


Stöckle et al. *Better Safe Than Sorry! Automated Identification of Functionality-Breaking Security-Configuration Rules*. AST'23

Process

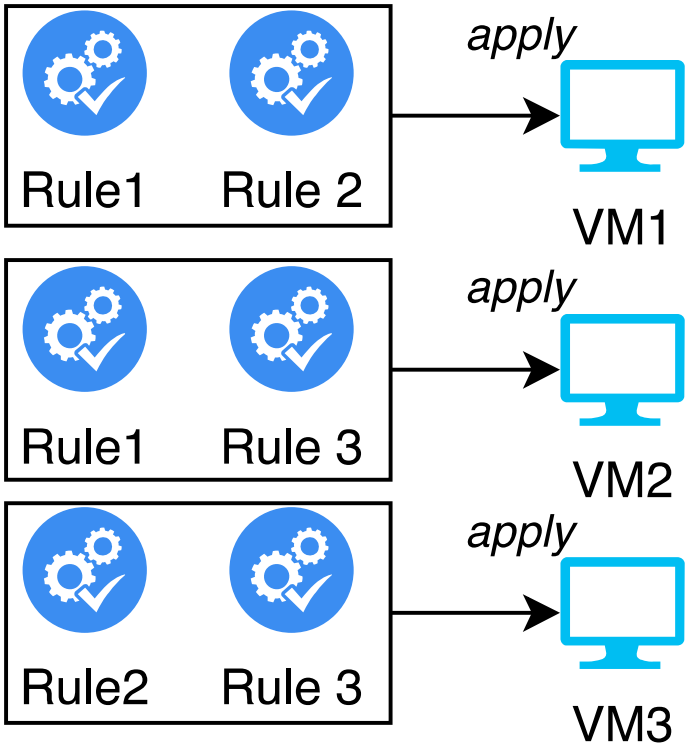


Generate Covering Arrays

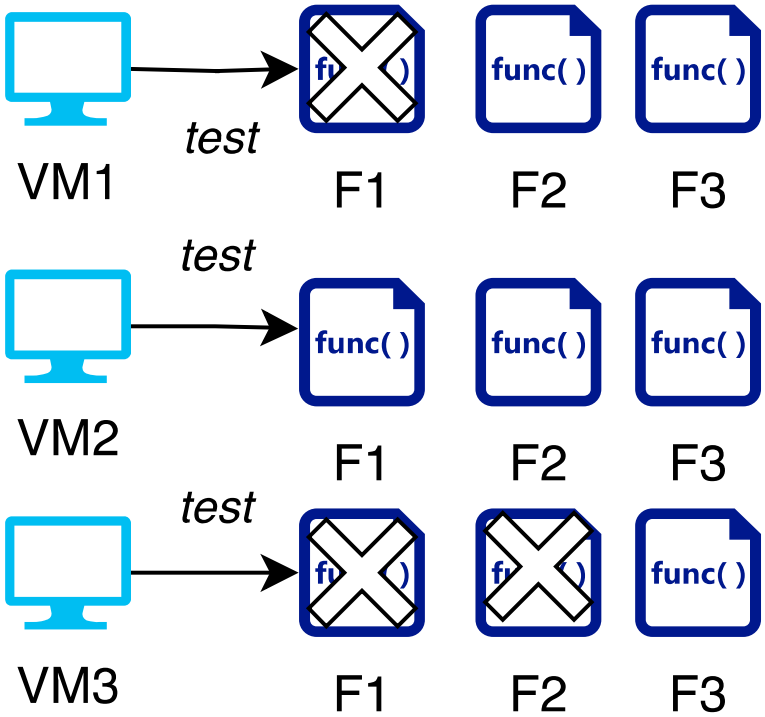


Input:
Guide

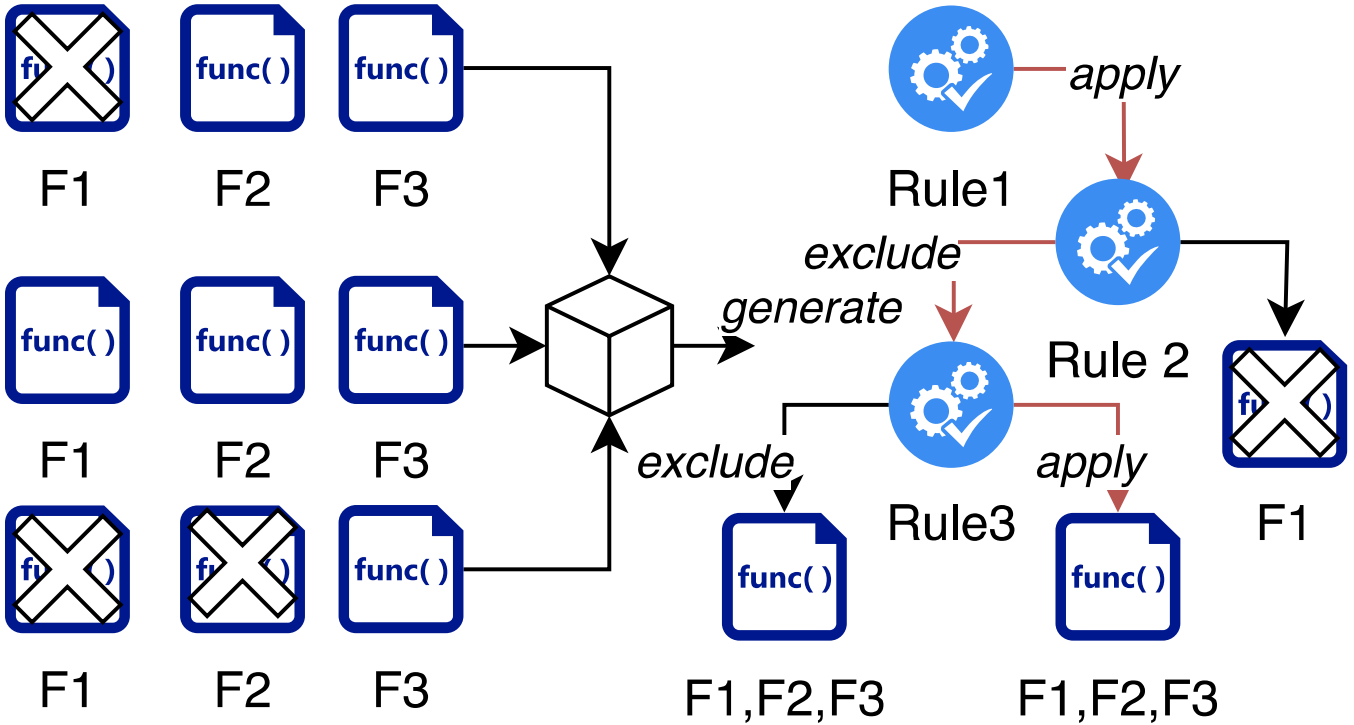
Apply Covering Arrays on VMs



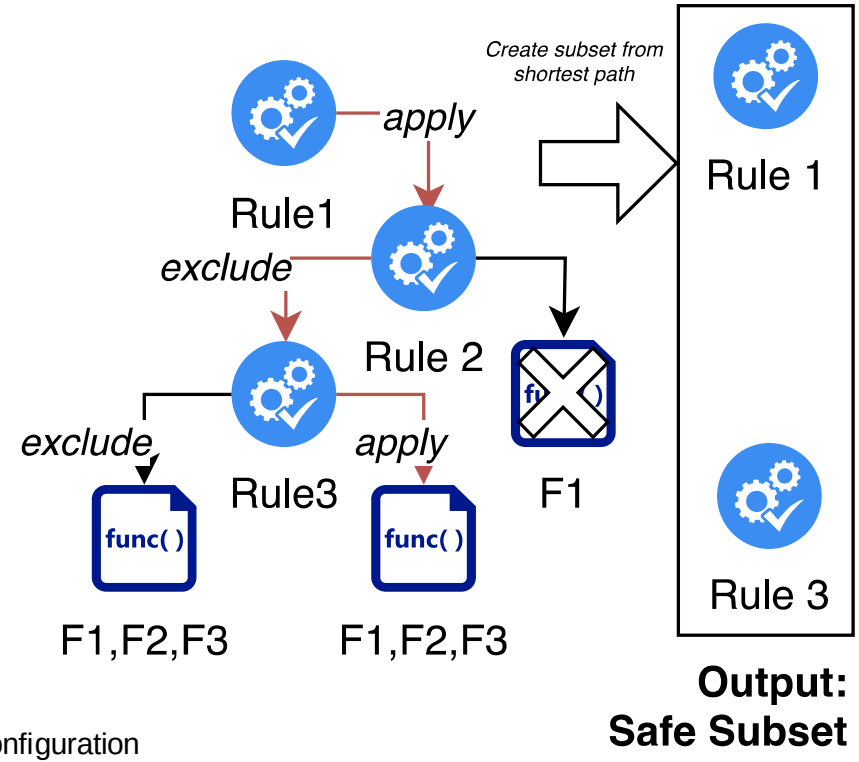
Test Functions on Hardened VMs



Generate a Decision Tree



Find the Shortest Path in the Tree



Conclusion

Opportunities

- More empirical studies on the impact of security configuration in practice
- Security configuration baked in by vendors
- Use better NLP models to implement settings automatically/classy settings

Impact

- Actively used at Siemens
- 8332 security-configuration rules in 49 different security-configuration guides (September 2023)
- Case study with 5 teams: tools saved > 2500h of manual hardening

Contributions

- Apply NLP to problems to harden systems
- Apply software engineering/DevOps techniques to make security configuration a first-class citizen
- Empirical data in the context of security configuration