@CyberStatecraft

Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain

Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, June Lee, Simon Handler, Tianjiu Zuo, and Logan Wolff

Atlantic Council

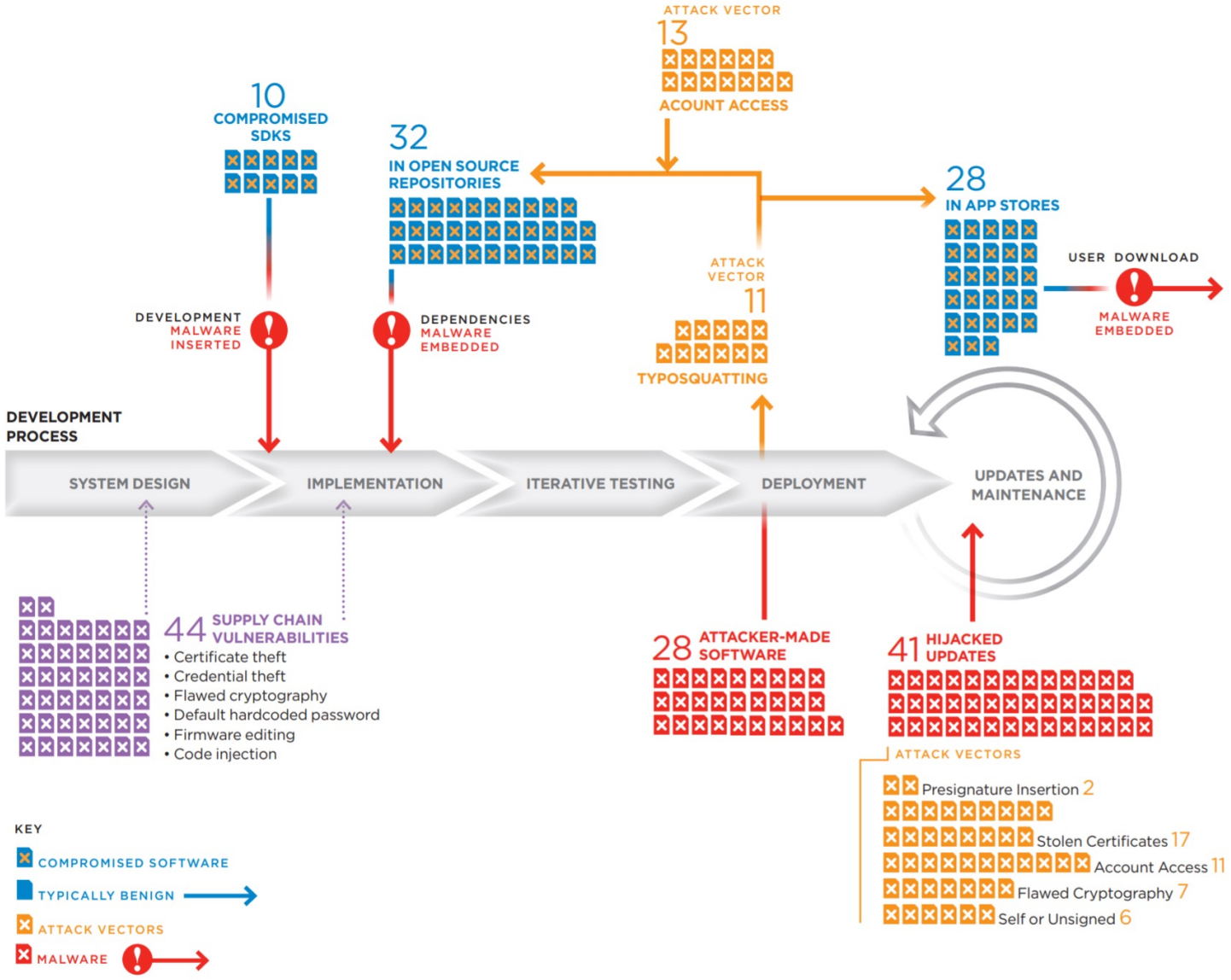
Why software supply chains?

- Software Channels Scale
- We Don’t Build What We Use
- Supply Chain (in)Security

@CyberStatecraft

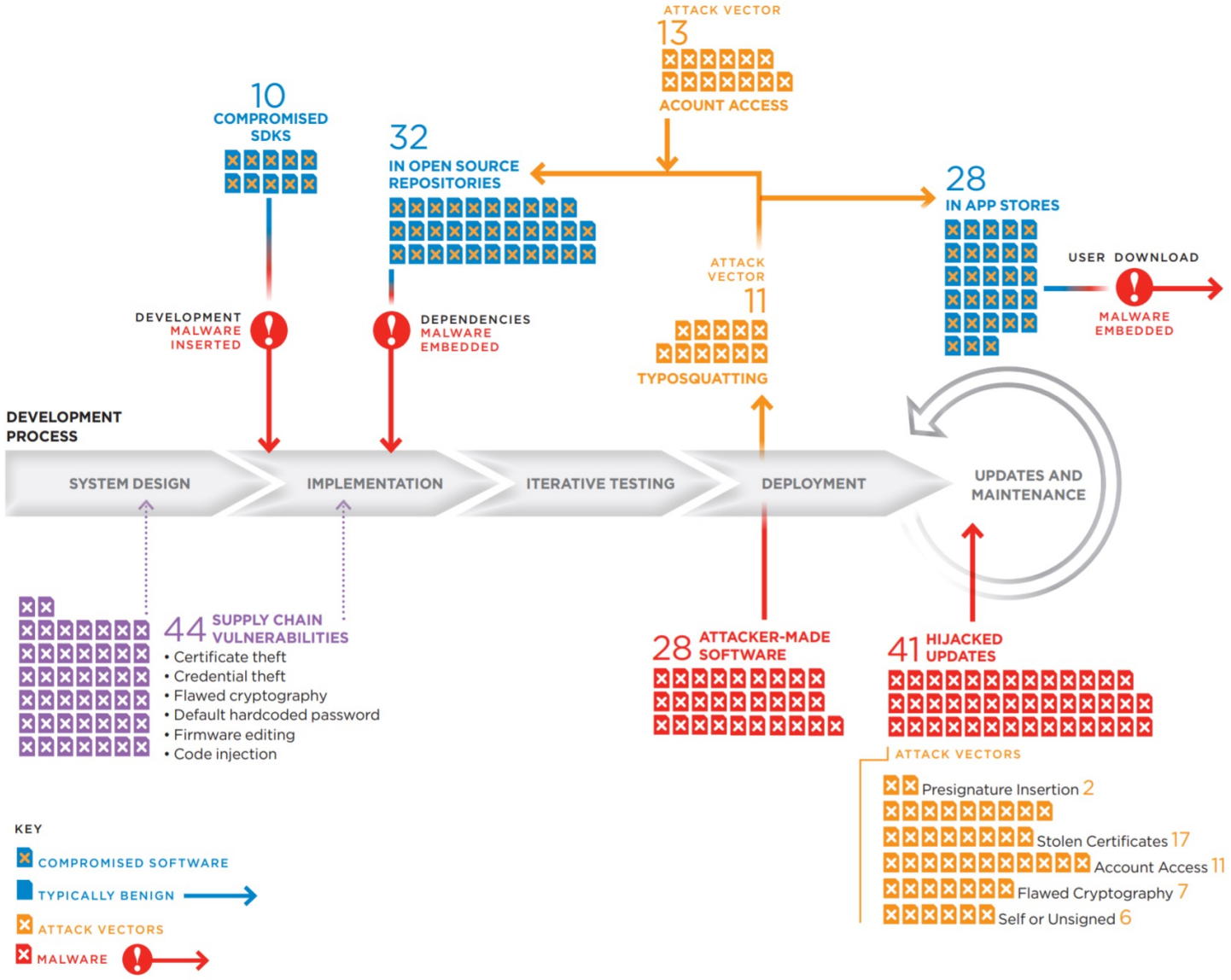
A decade of attacks and disclosures in the software supply chain

117 attacks & 44 disclosures



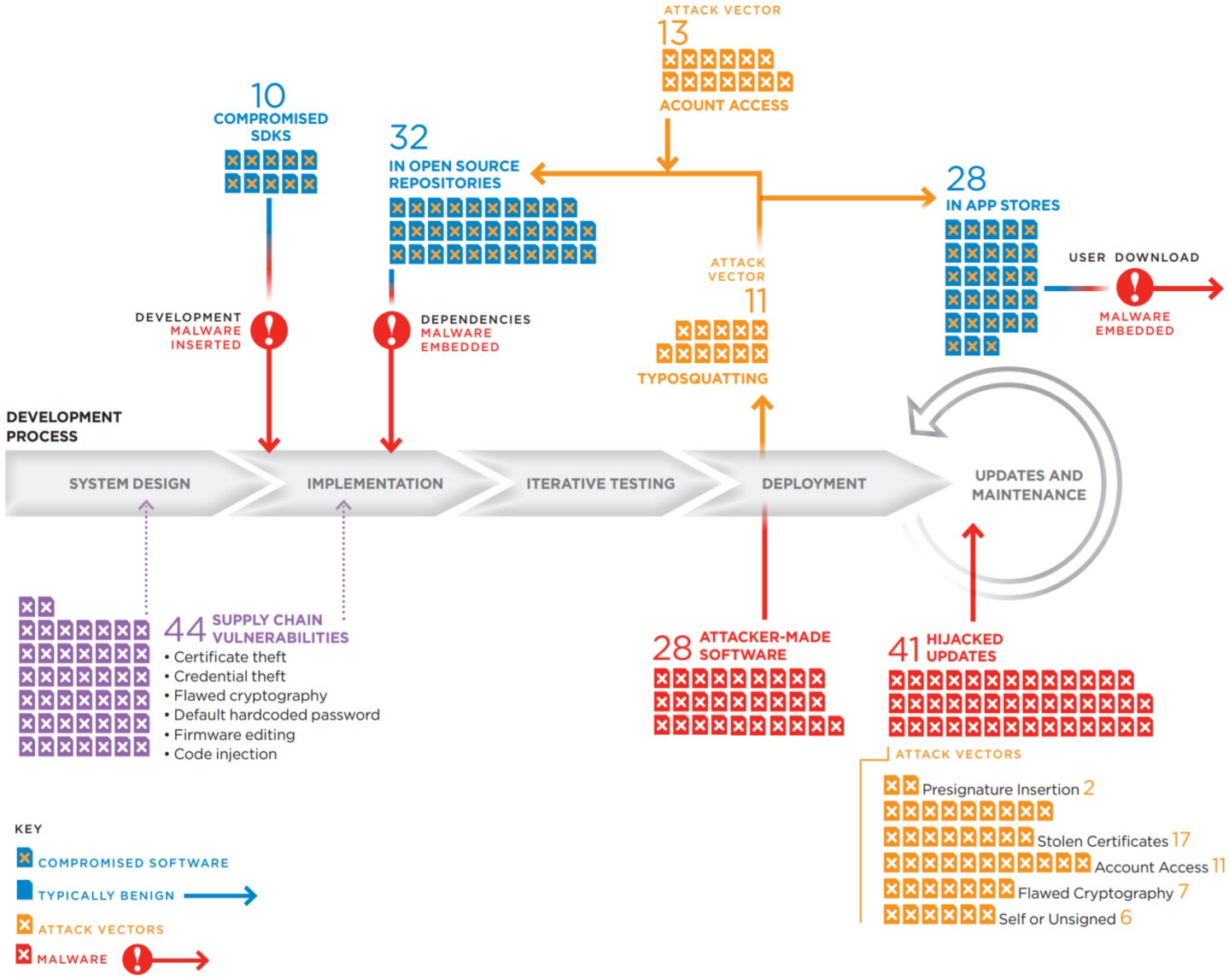
Atlantic Council

Attacks on open source with repeated targeting of NPM and PyPi



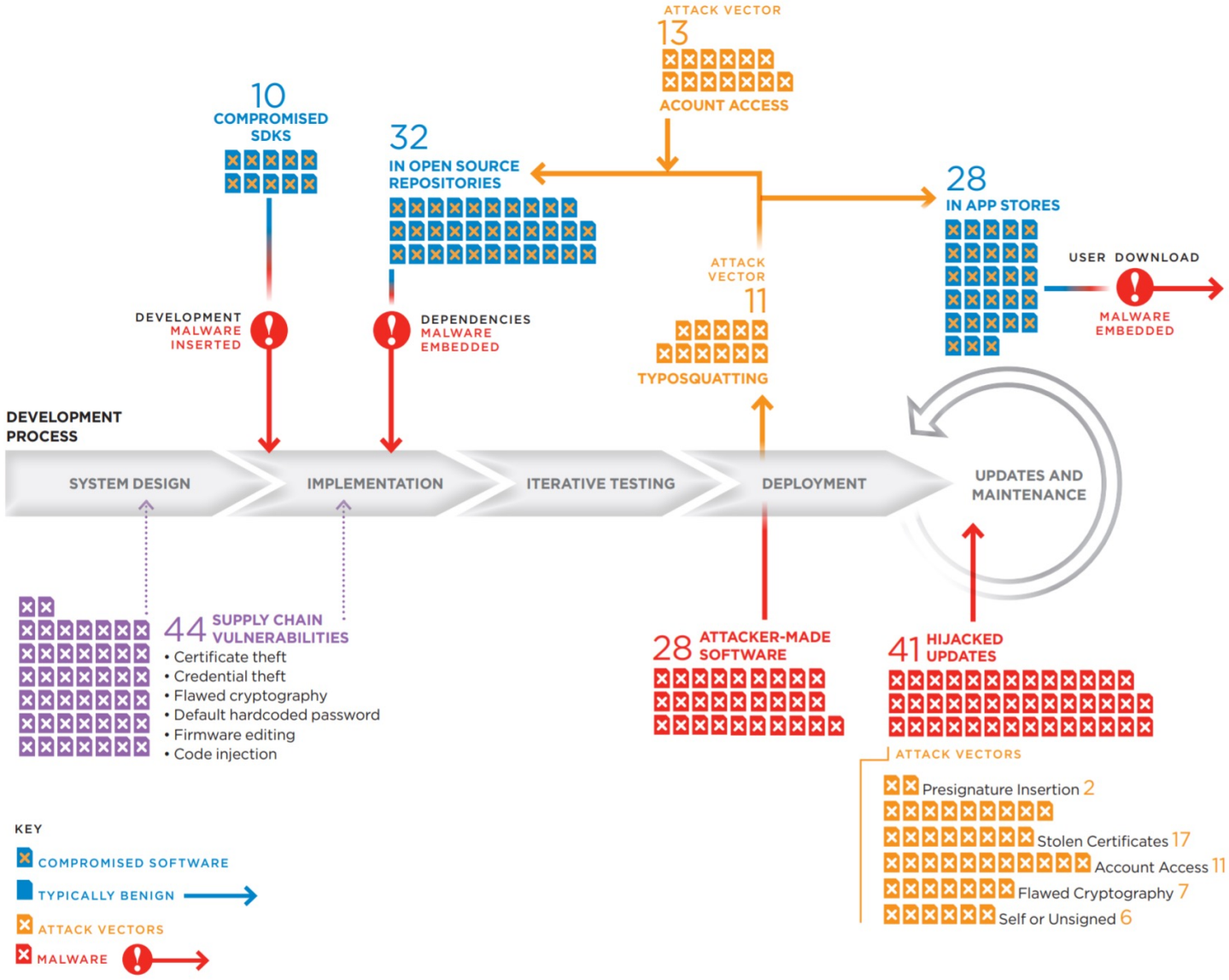
Atlantic Council

At least 32 attacks from state actors, most notably Russia and China



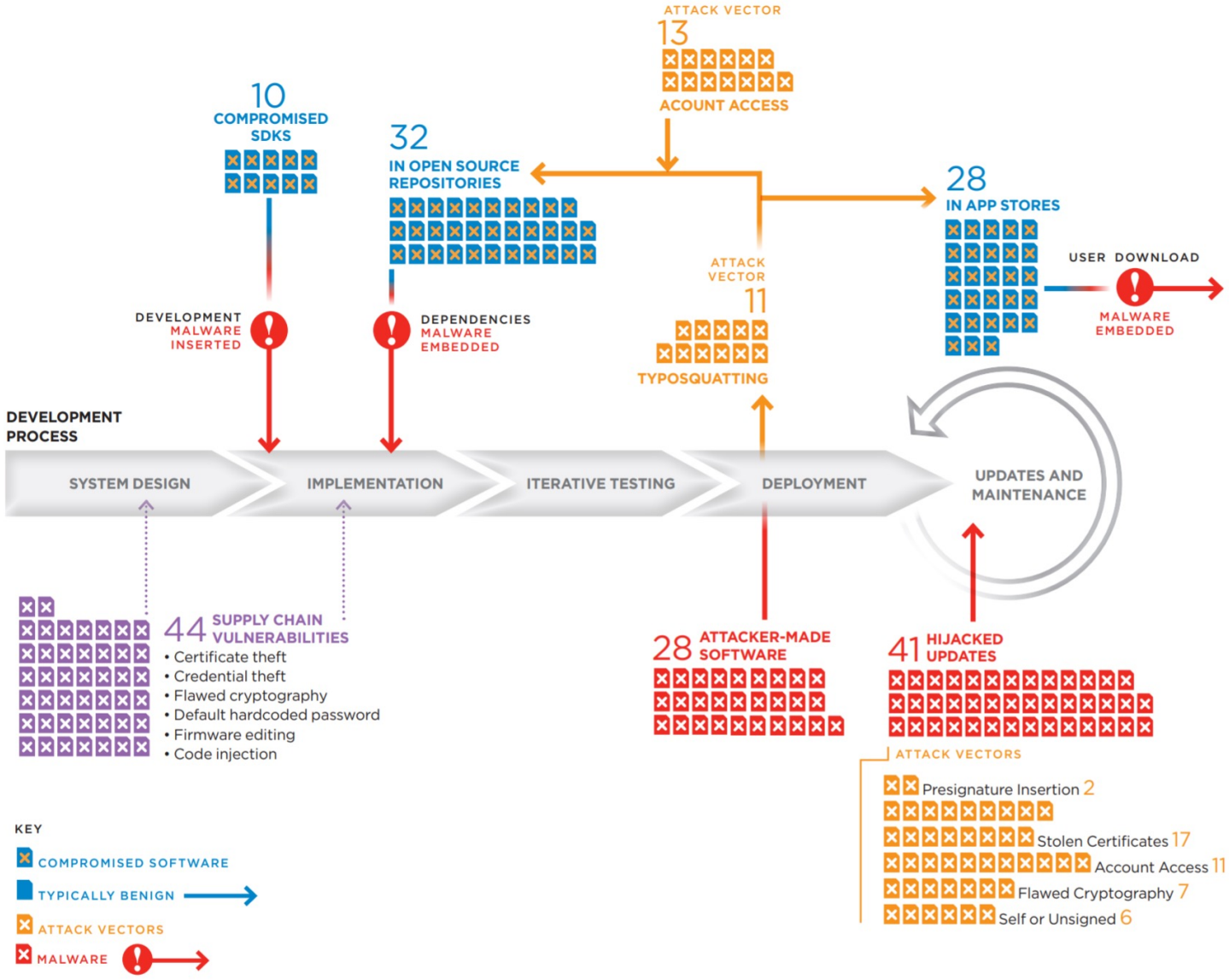
Atlantic Council

24% of attacks target app stores and developer tools



Atlantic Council

25% of attacks hit software updates



Atlantic Council

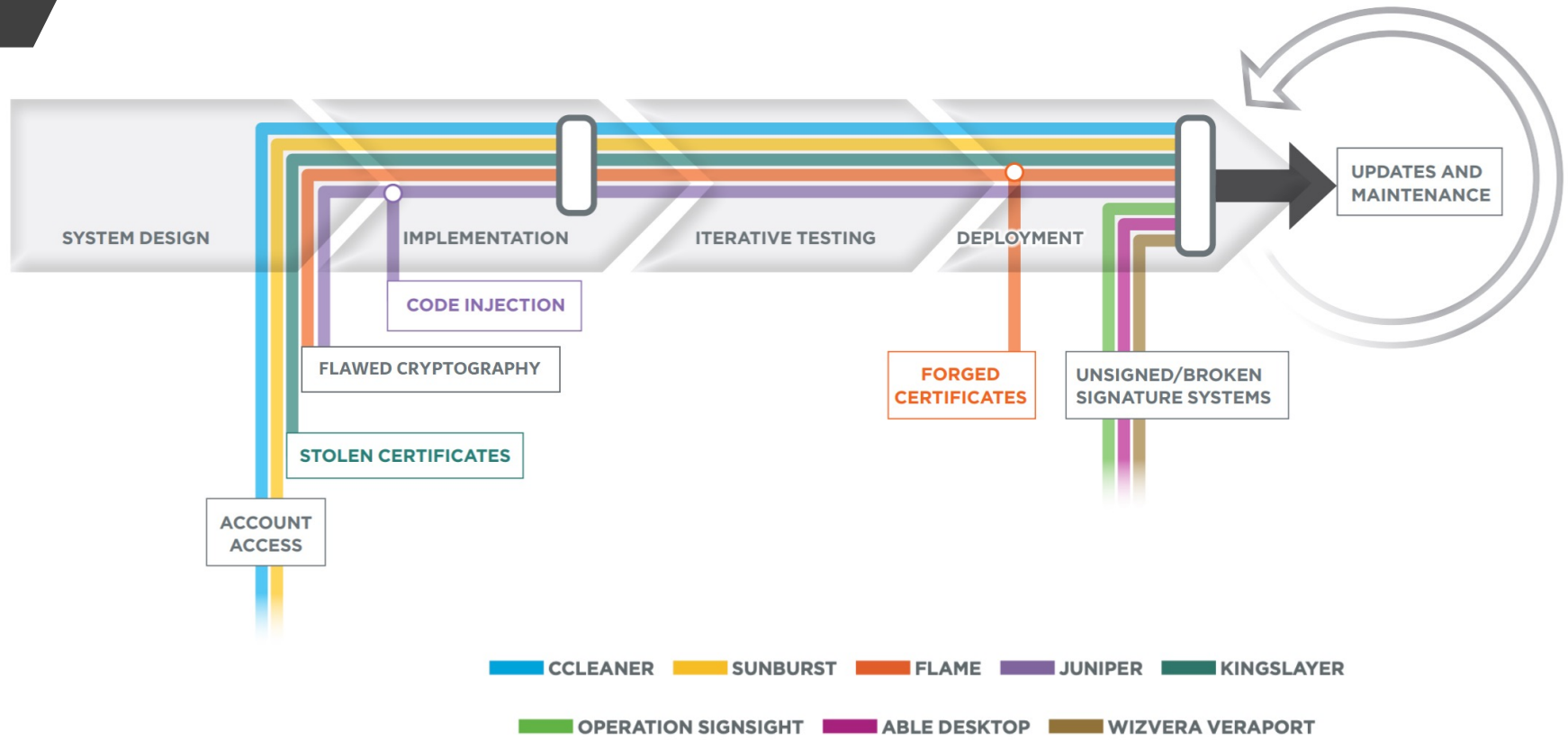
Key Trends

- Efficiency and Scale
- Path to Targeted Exploitation
- Subverting Vendor Code-Signing
- Targeting OSS Repositories

Sunburst


SYSTEM DESIGN
IMPLEMENTATION
ITERATIVE TESTING
DEPLOYMENT
UPDATES AND MAINTENANCE
ACCOUNT ACCESS

History Rhymes



What Comes Next?

- Better Defense of OSS
- Risk Assessment on New Data
- Don’t Forget About Architecture

Thank you

For more on this project visit:
https://www.atlanticcouncil.org/breaking-trust/

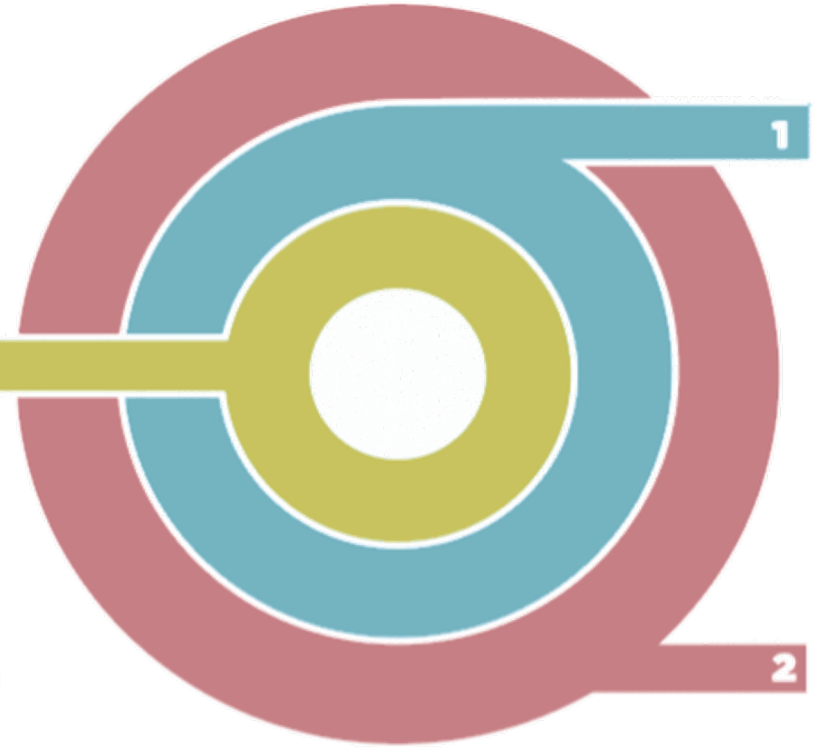
Recommendations

Atlantic Council

Ready for Work

These recommendations build on existing authorities, functions, or programs but may require new funding.

1. **Hunt for Blast Radius**
2. **FASC Sets the Process**
4. **Shift the Landscape for Adversaries**
6. **Give SBOM a Glide Path to Success**
8. **Do Not Leave Open Source Behind**
10. **Create a Trusted Traveler Program for FedRAMP**
11. **Evolve and Default to Secure**



Some assembly required

These ideas pair an action with an outcome or actor but may have a critical dependency that keeps them from being shovel ready.

5. **Develop a Lifecycle Security Overlay**
7. **Apply the Overlay**
12. **Govern Through the Cloud**

Step Carefully

Ideas to push outside the box a bit farther while still being rooted in critical needs

3. **Breach Response Hunger Games**
9. **Change an Architecture, Change the World**

Selected Recommendations

Atlantic Council

Ruthlessly Prioritize Risk

1. Hunt for blast radius

Improve the Defensibility of Linchpin Technologies

5. Develop a lifecycle security overlay

8. Do not leave open source behind

9. Change the architecture, change the world

Enhance the Adaptability of Federal Cyber Risk Management

12. Govern through the cloud