Cybersecurity Orchestration and Machine Speed Information Sharing to Defend State and Local Networks

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

MS-ISAC® Multi-State Information Sharing & Analysis Center®

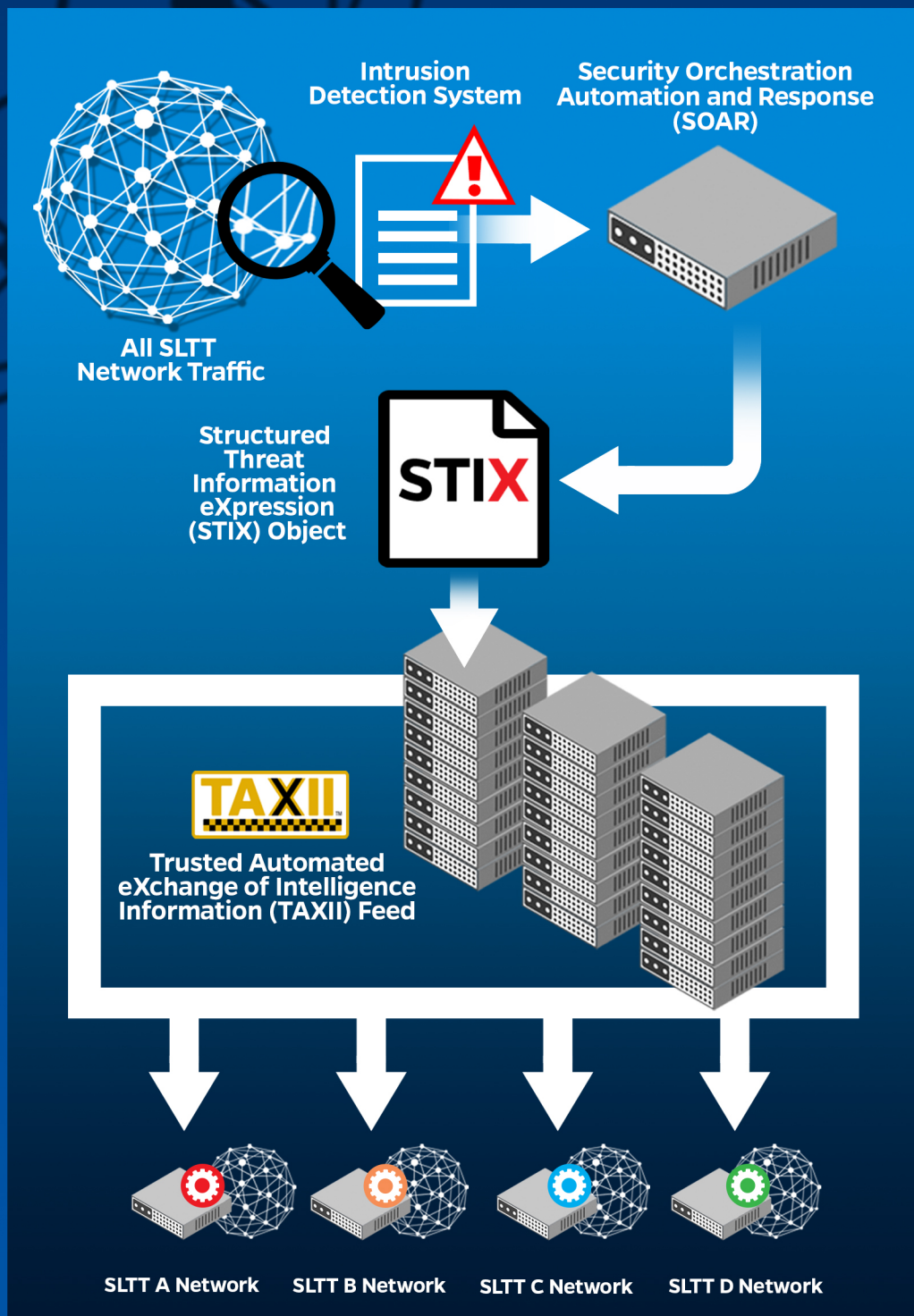
Pilot Design

Orchestration at MS-ISAC

- Extract indicators from intrusion detection systems
- Identify potential malicious indicators
- Filter on “low-regret” indicators
- Convert to STIX
- Submit to TAXII feed

Orchestration at State, Local, Tribal, and Territorial (SLTT) Partners

- Pull Indicators from TAXII feed
- Identify courses of action in accordance with SLTT policy
- Execute courses of action



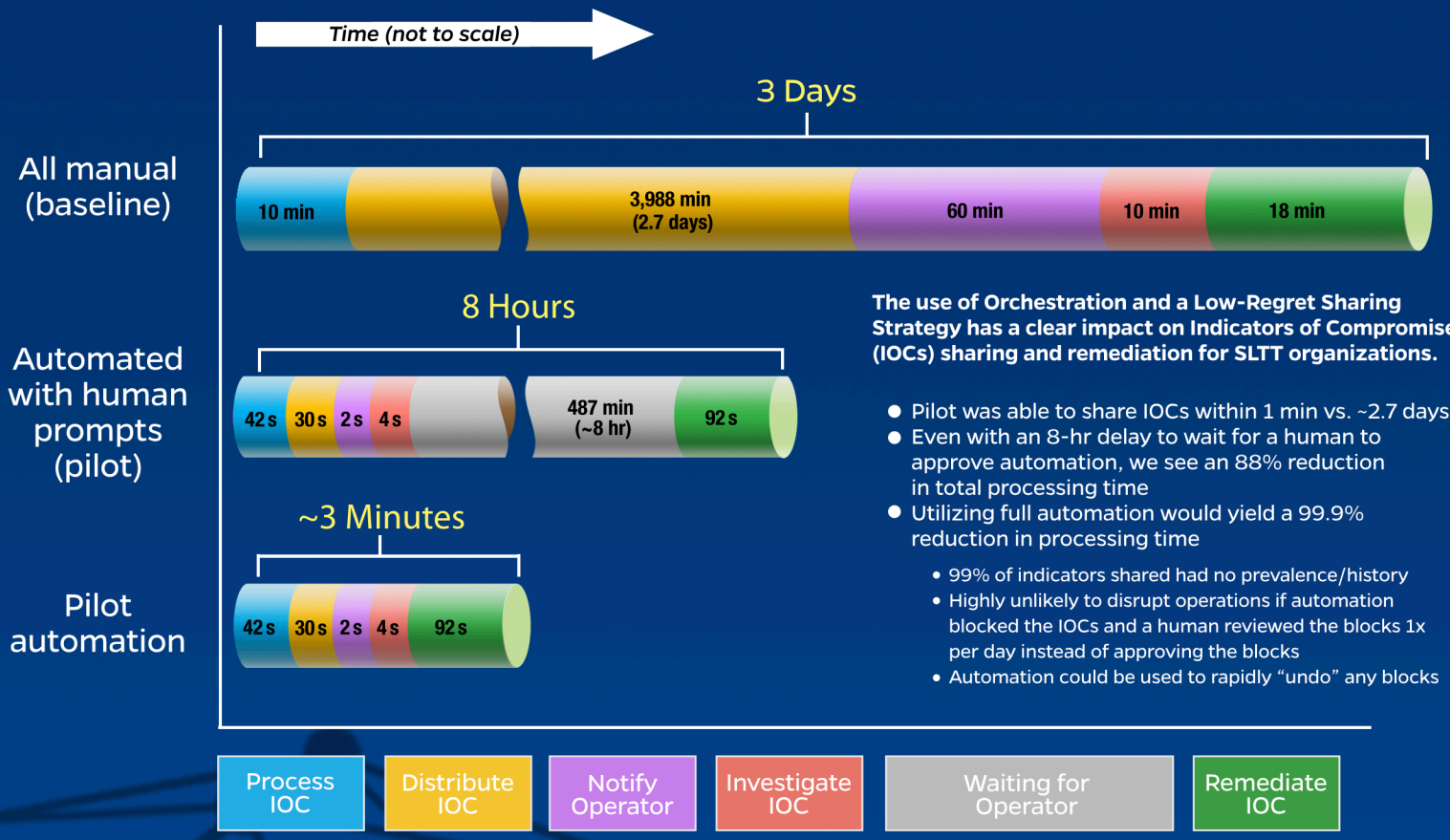
Acknowledgement:

This material is based upon work supported by the U.S. Department of Homeland Security/Cybersecurity and Infrastructure Security Agency under Grant Award Number DHS-19-CISA-128-SLT-001 (State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot).

Disclaimer:

The views and conclusions contained in in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security/Cybersecurity and Infrastructure Security Agency.

Pilot Performance Against Baseline



The use of Orchestration and a Low-Regret Sharing Strategy has a clear impact on Indicators of Compromise (IOCs) sharing and remediation for SLTT organizations.

- Pilot was able to share IOCs within 1 min vs. ~2.7 days
- Even with an 8-hr delay to wait for a human to approve automation, we see an 88% reduction in total processing time
- Utilizing full automation would yield a 99.9% reduction in processing time
  - 99% of indicators shared had no prevalence/history
  - Highly unlikely to disrupt operations if automation blocked the IOCs and a human reviewed the blocks 1x per day instead of approving the blocks
  - Automation could be used to rapidly "undo" any blocks

Attempted attacks from feed IOCs that were blocked (results from one SLTT partner)