IACD & FS ISAC Financial Pilot Results

Charlie Frick, JHU/APL

Integrated Cyber October 2018 Conference

TLP WHITE

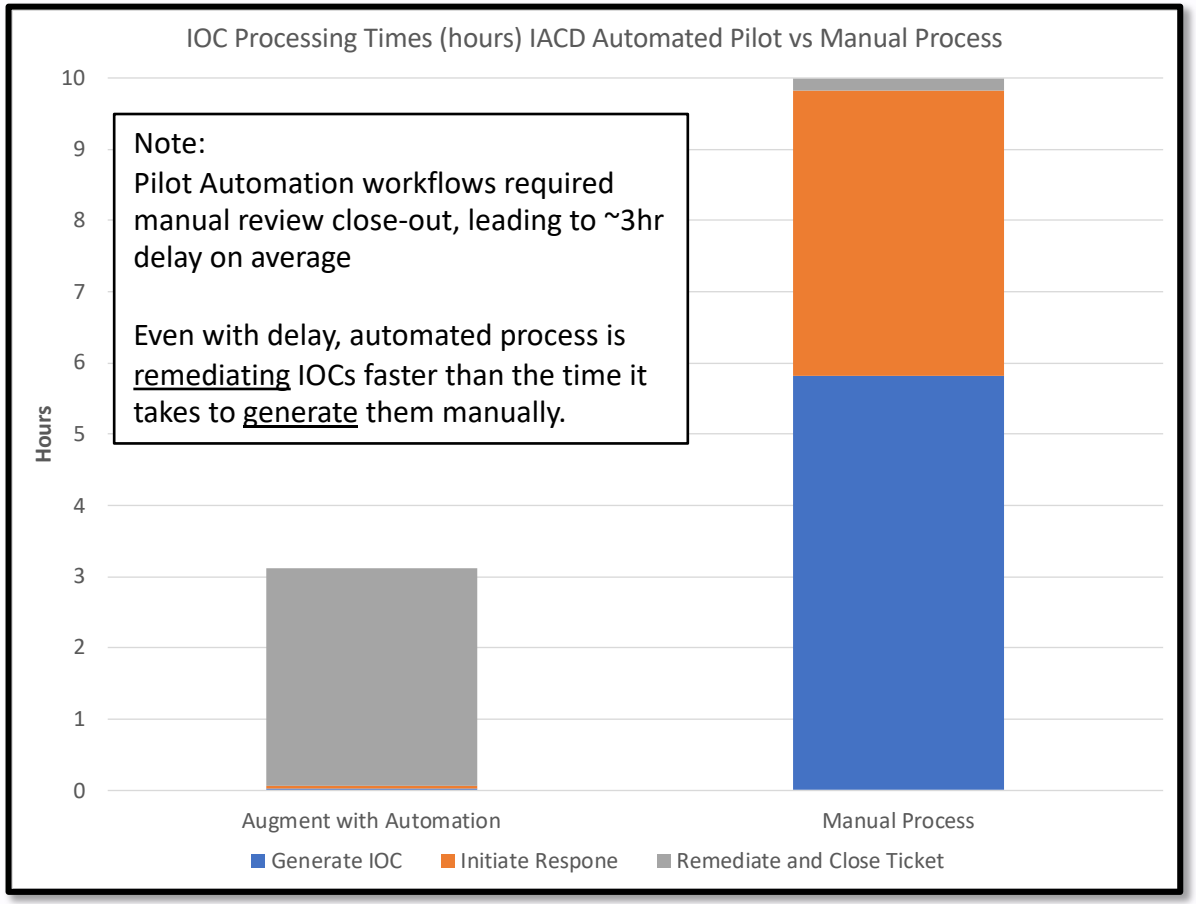
Agenda

- Executive Summary
- Pilot Scope and Design
- Pilot results
  - High Level Lessons Learned
  - Technical results – FS ISAC
  - Technical results – Financial Institutions
- Conclusions
- Discussion

FS Pilot - Executive Summary

- **Joint IACD and FS ISAC pilot for the Financial Sector**
- **Pilot focus was on the use of automation to enhance the use of threat Indicators of Compromise (IOCs)**
  - **Generation and Scoring of IOCs from FS ISAC**
  - **Receipt and response to IOCs at three Financial Institution**
- **The pilot has generated several valuable lessons learned for deploying Security Automation and Orchestration**
- **Pilot has also shown promising technical results from the use of automation and orchestration**
  - **Generation of threat IOCs ~6 hrs. faster than legacy process**
  - **Action upon indicators within ~3 min. of receipt**
  - **Remediation of indicators within ~3 hrs.* of receipt**

(* Pilot remediation had man in the loop approval leading to queue)



Pilot results show automation allowed remediation of IOCs ~3 hrs. *before* receipt times when using the manual process

Pilot Scope and Design

Integrated Pilot Process

Discovery Phase
(Oct. 2017 – Jan 2018)

- **Observe/Interview relevant staff for threat intel ingestion / processing at 3 member organizations and FS ISAC**
- **Identify and document potential areas for improvement via IACD**

Proof of Concept Design Phase
(Feb 2018 – April 2018)

- **JHU/APL, FS ISAC, and Members collaborate to draft plan for developing/piloting identified improvement capabilities**
- **Validate plan to ensure suitability of pilot options within member environments**

Proof of Concept Execution Phase
(April 2018 – Sept. 2018)

- **Execution of pilot plan within FS ISAC and Member networks**
- **Evaluation of metrics to assess improvement via IACD implementation**
- **Collaborative Design of follow-on Activities**

High Level Pilot Design

Automation based on IACD

Threat Intelligence converted to STIX / TAXII formats once published to the pilot Portal

Automation based on IACD Framework pulls and responds to intelligence at each Financial Institution based on their SOPs (Bring your own Enterprise)

Workflows A, B, C

Workflows B,D

Workflows A,C,E

TLP - WHITE

Demonstration Videos

We have created some demonstration videos on our YouTube channel to showcase the technical efforts in these pilots.

These show how automation can augment processing of Indicators of Compromise (IOCs) with respect to certain core functional capabilities:

Automated Processing

Human In the Loop Processing

Identification of Automation Errors

Monitoring Automation Engine Health

Generic Example for Response Workflow Detail

Indicator from pilot feed Arrives at TAXII Client

IOC: 1.2.3.4

STIX TAXII

Threat Feed Client

Orchestrator gathers additional Enrichment Reputation of IOC

IOC: 1.2.3.4

External Enrichment Feeds/Sources

Orchestration Services

Orchestrator checks IOC against organization whitelist/blacklists

Automatically ignored if whitelisted

IOC: 1.2.3.4

Verify block if blacklisted

Internal Data Repositories

Orchestrator creates ticket summarizing IOC, reputation scores, and prevalence within network

Ticket

Ticketing Server

SOC Analyst

COA

SOC analyst reviews ticket and sends Course of Action (COA) to Orchestrator

Orchestrator searches logs for network workstations/servers with connections to IOC in last 30 days

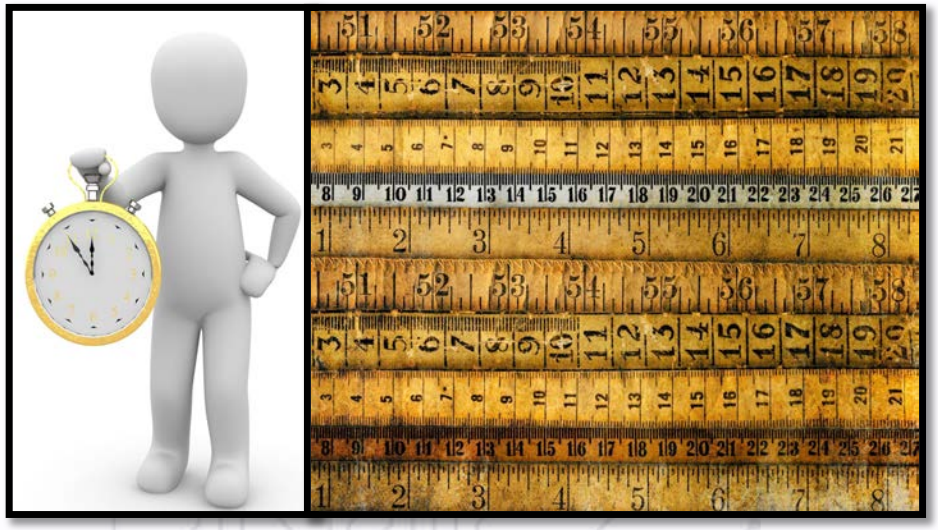
Defense Appliances / Services

Orchestrator executes COA, blocks IOC, and closes ticket

Closed

TLP - WHITE

Pilot Metrics



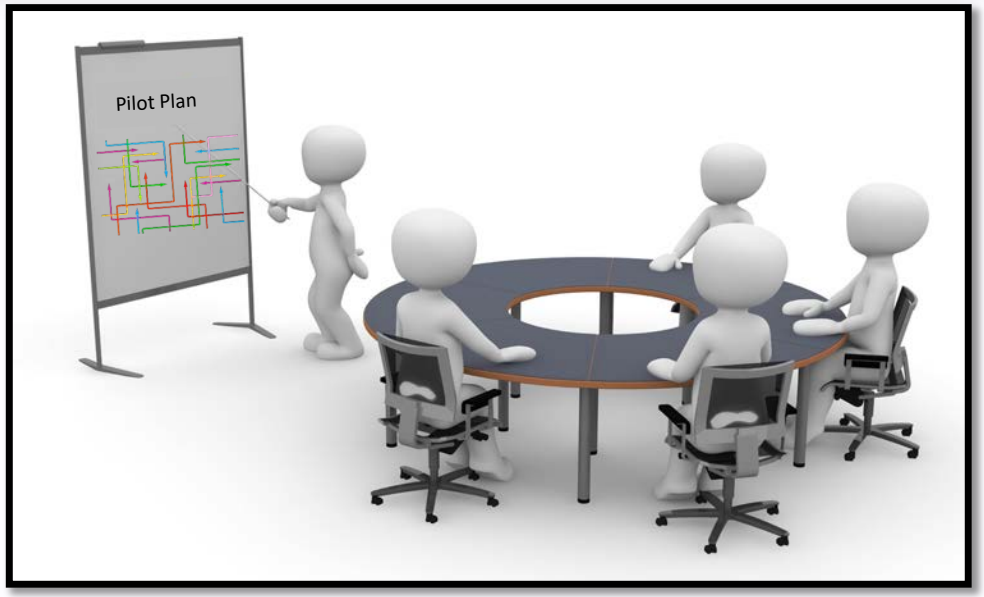
- The collect everything and figure out what metric you can calculate strategy doesn't work
- You have to have comparison numbers to show improvements
- Simple counts and time calculations can be powerful

Pilot Results – Lessons Learned

Organizational Culture

If the organization isn't ready, the opportunities are limited

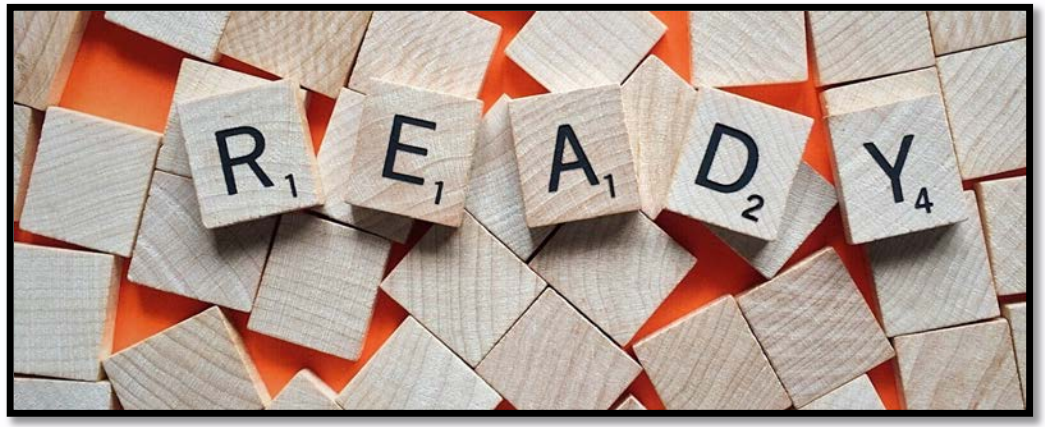
- **Common problems that prevent successful deployment:**
  - **The appearance of conflicting priorities**
  - **Processes are too complex or not agreed upon**
  - **The environments current products cannot be integrated in an automated manner**



Operational Readiness

Scaling and improvement require a different perspective

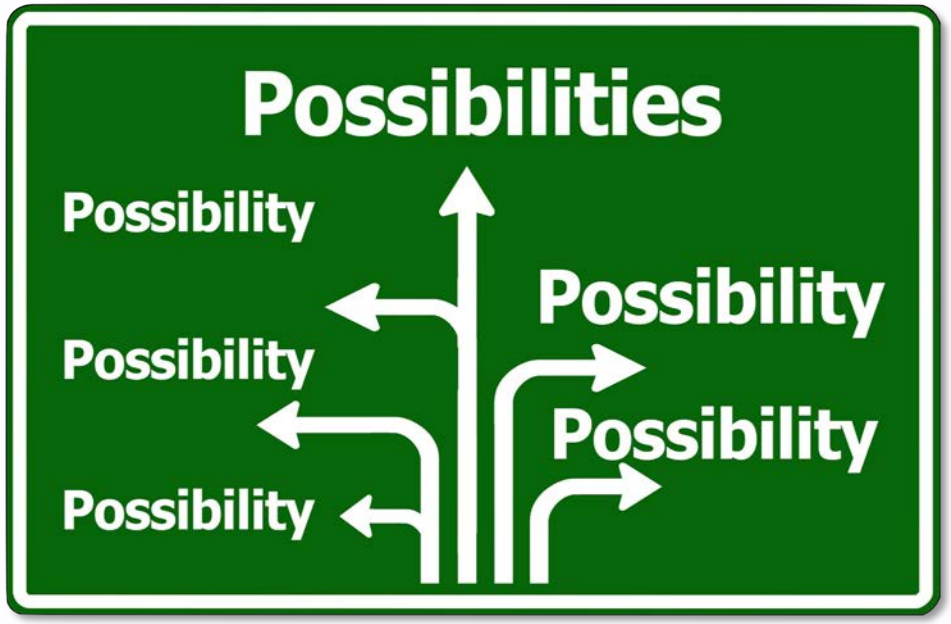
- **Scalable processes**
  - Humans in more loops and licensing limits are first break points
- **SAO skill sets**
  - Make sure you have the training and necessary SMEs available
- **Evolving SOPs**
  - Know ahead of time what the next priority is once the current priority is being handled



Deployment Scope

Be willing to underachieve in order to succeed

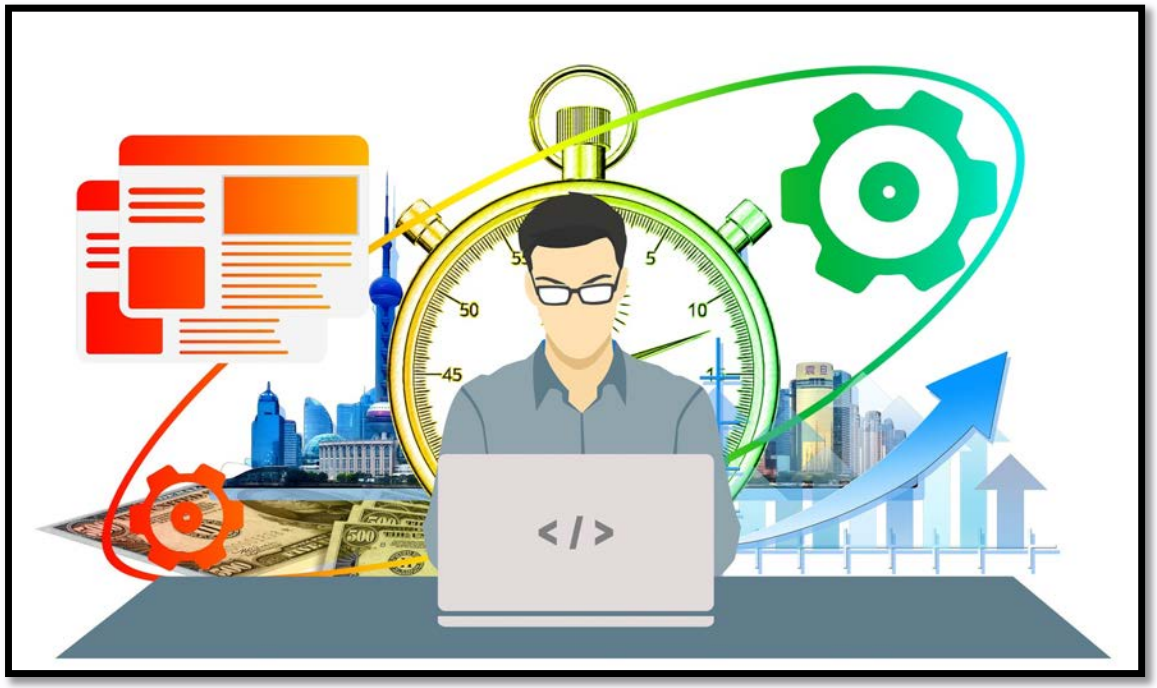
- **Define success and exit criteria**
  - Have a plan B, C, and D that can meet the intent
- **Identify key roles and responsibilities**
  - It takes more people and parts of your organization to be successful then you think
- **Manage risk through proper planning**
  - Build automation that can be easily modified to remove human interaction as comfort increases



Interoperability

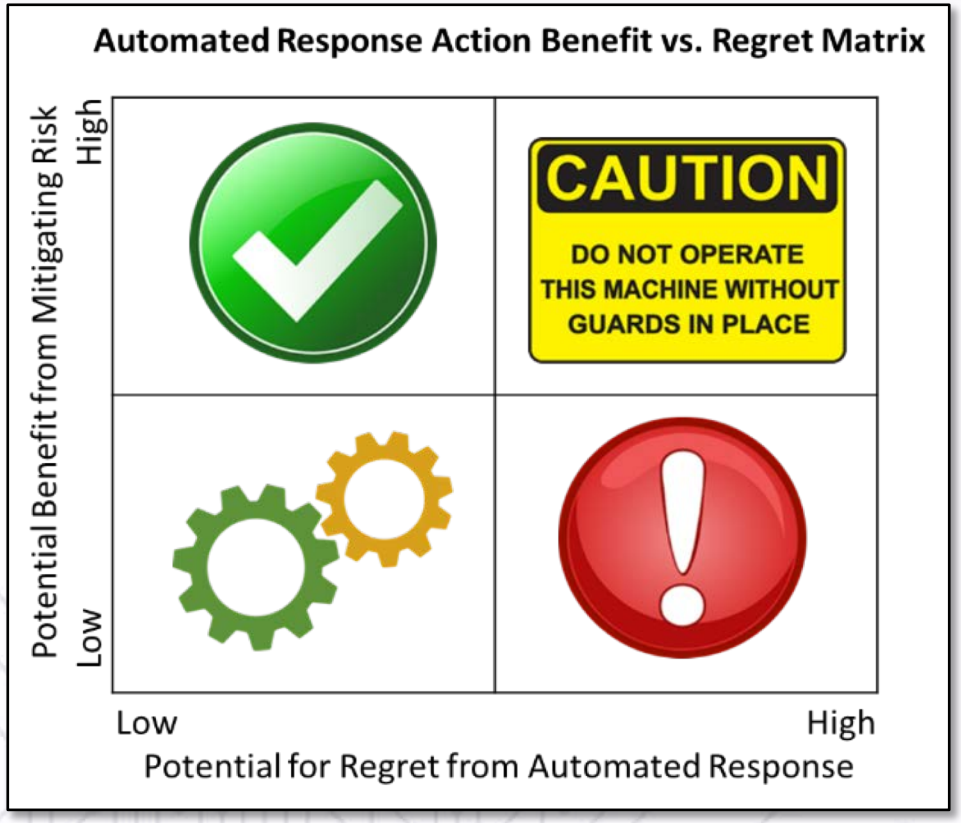
Invest in capabilities not products

- What capability is needed?
- What capability is missing?
- What cannot be integrated cannot be automated



Automated Response Actions

Knowing your environment can give you confidence



- What do you already allow your vendors to do? Why?
  - These are low regret actions
- Identify the information needed to determine low regret

Actionable Information

Consumers drive what is actionable

- You must consider how information is used to make it actionable
- The consumers determine value
  - Their views of timely, accurate, etc. are different than providers think

Sharing Models

Think of information sharing as standard sets of automated conversations

- Currently need to have clients and servers that are meant to talk to each other
- Triage and prioritization is purpose of initial exchange
- More advanced decisions on action or disposition only when required
- Query and respond model for on demand access

Trust

Lack of trust is an underlying assumption that impacts everything

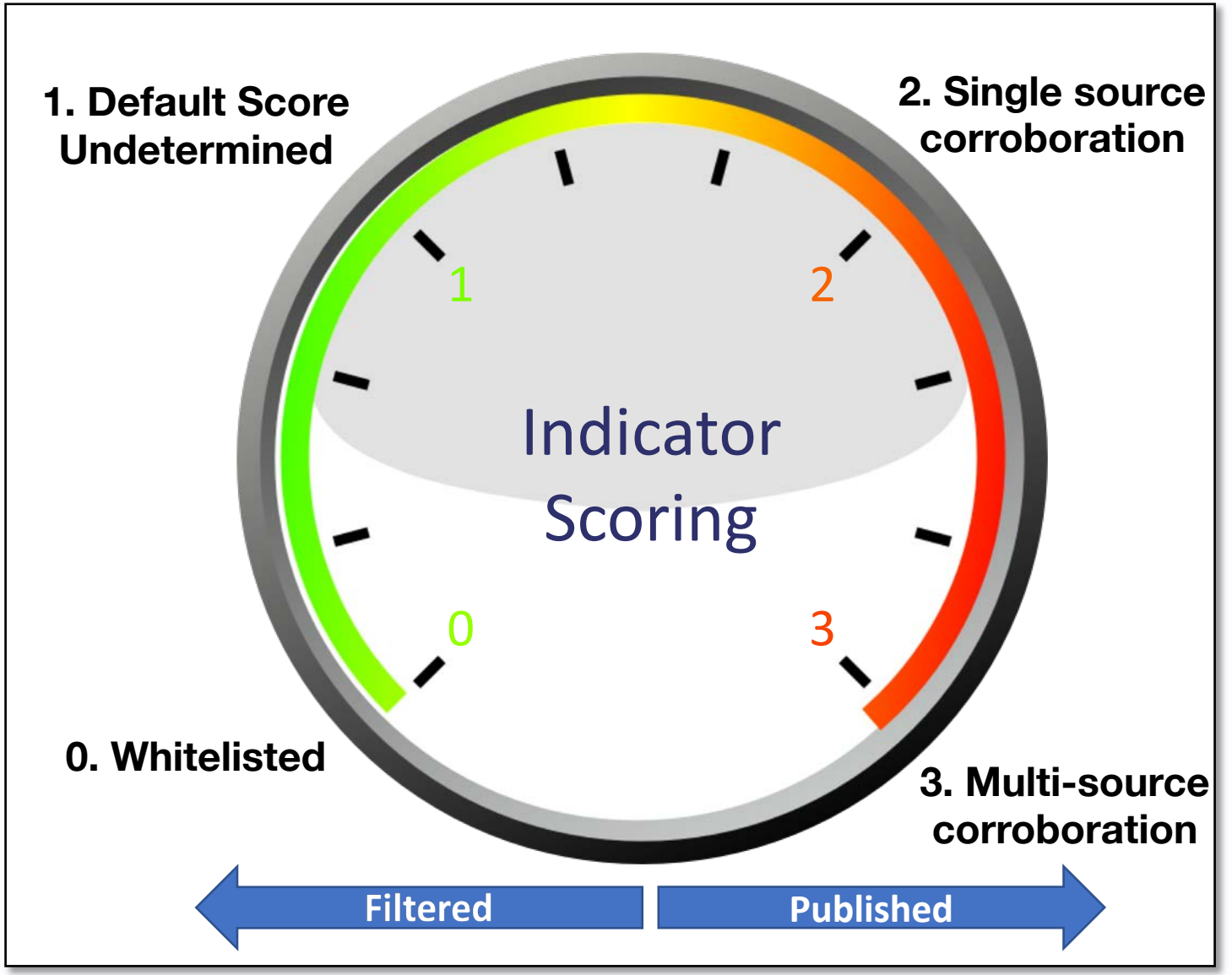
- Trust really is earned, even inside the organization
- Trust is easily lost – and usually results in me ignoring or replacing you

Pilot Results – Technical Findings

Automated Threat Feed Scoring

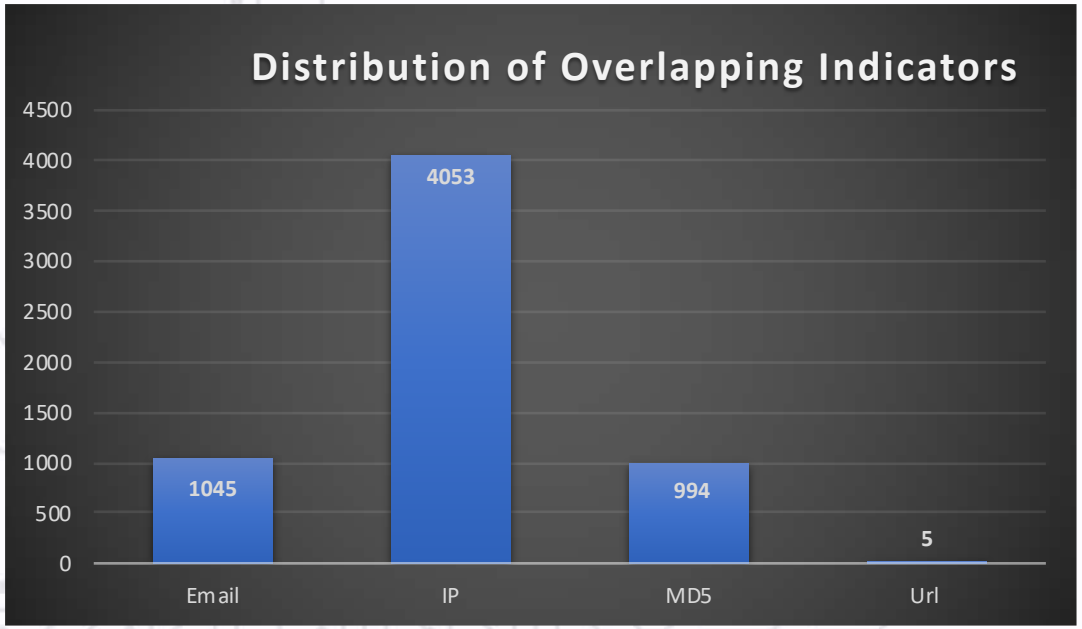
- Automation at FS ISAC received email IOC submissions

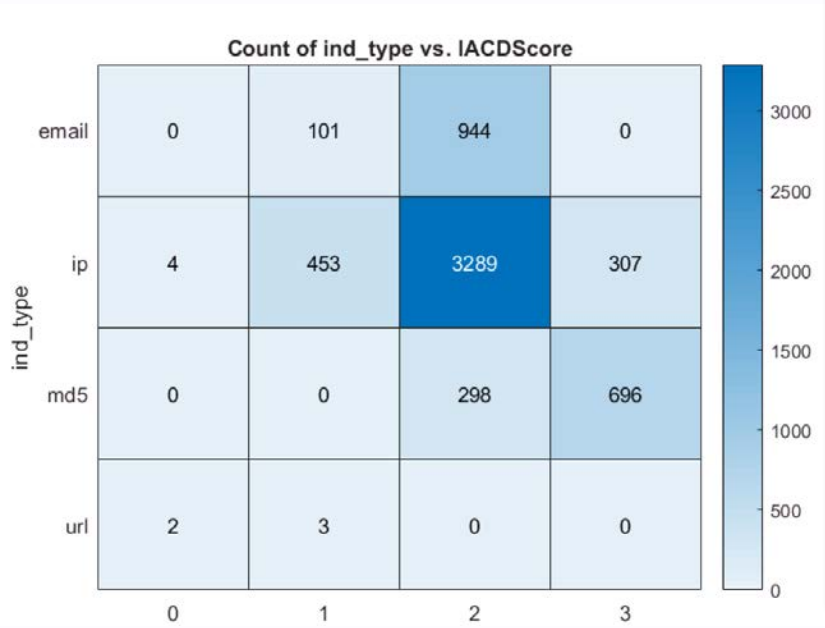
- Automated scoring and publish process followed three criteria
  - Default must do no harm
  - Different scores must result in different actions
  - Must be 100% automated to ensure consistency



Feed Comparisons

- **Number of Overlapping Indicators: 6097**
- **Number of Unique Overlapping Indictors: 1645 (31%)**
  - **Unique overlap based on 5275 FS-ISAC Portal Entries**
- **Score of overlapping on average IACD Scores: 2.0711**
- **Median Time to automatically score and publish : 1 minute**
- **Median time to manually score and publish : 5 hours, 49 minutes**





Automated Feed scores consistent with manual process

Automated scores published approximately 6 hours faster than manual process

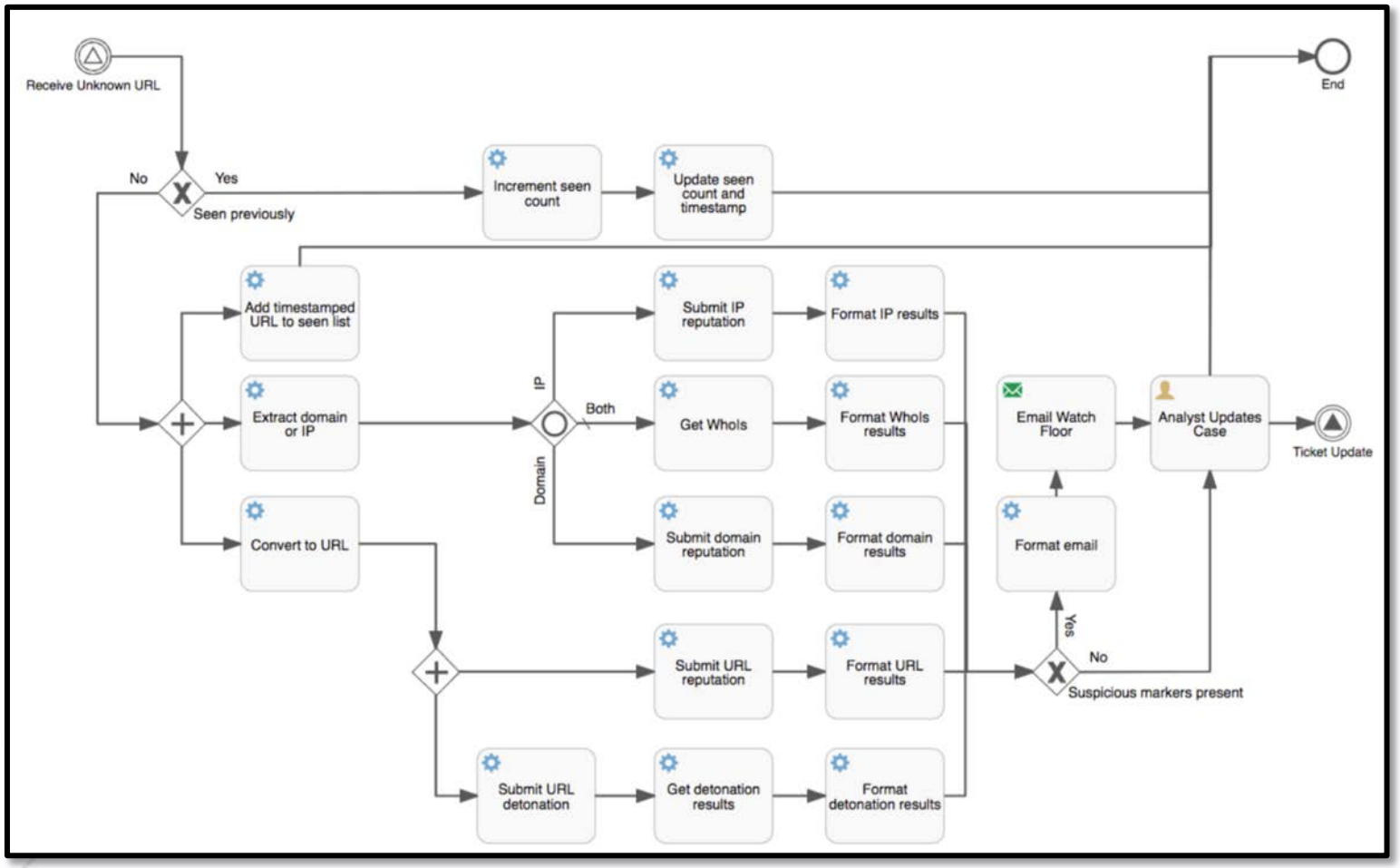
Analyst time freed to focus on threat reports to provide deeper context and adversary TTP knowledge

TLP - WHITE

Automated Response variation

- **Different organizations will implement response via automation or augmented by automation in different ways**
  - **Auto block all IOCs with zero prevalence**
  - **Human in the loop for each critical decision**
- **Pilot participants implemented multiple variants of these approaches in their workflows**
- **Workflows were also run in IACD laboratory performance for testing and baseline performance**

Generic workflow Example



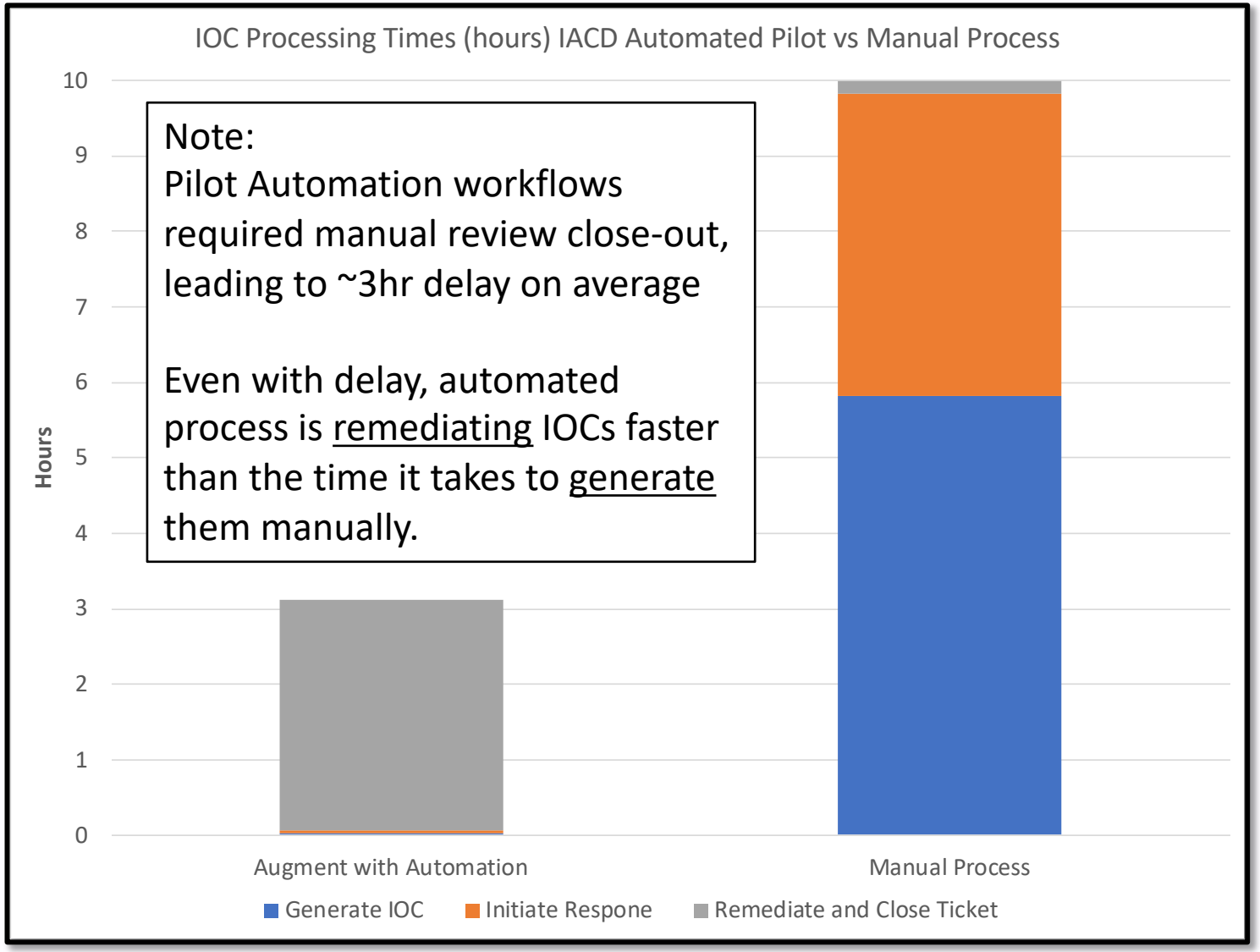
TLP - WHITE

Integrated Pilot Performance

Timeline	Pilot Process (Avg. per IOC)	Manual Process (Avg. per IOC)
Generate IOC	1 min.	5 hrs. ,49 min.
Initiate Response	3.03 min.	4 hrs.
Remediate & Close Ticket	3 hrs., 3 .3 minutes	10 min.
Total Time	3 hrs., 7.3 min.	9 hrs., ,59 min.

- Pilot remediation process required man in the loop for approval and closeout per IOC
  - Lead to ~3hr time in queue on average
- Automation significantly improved response time

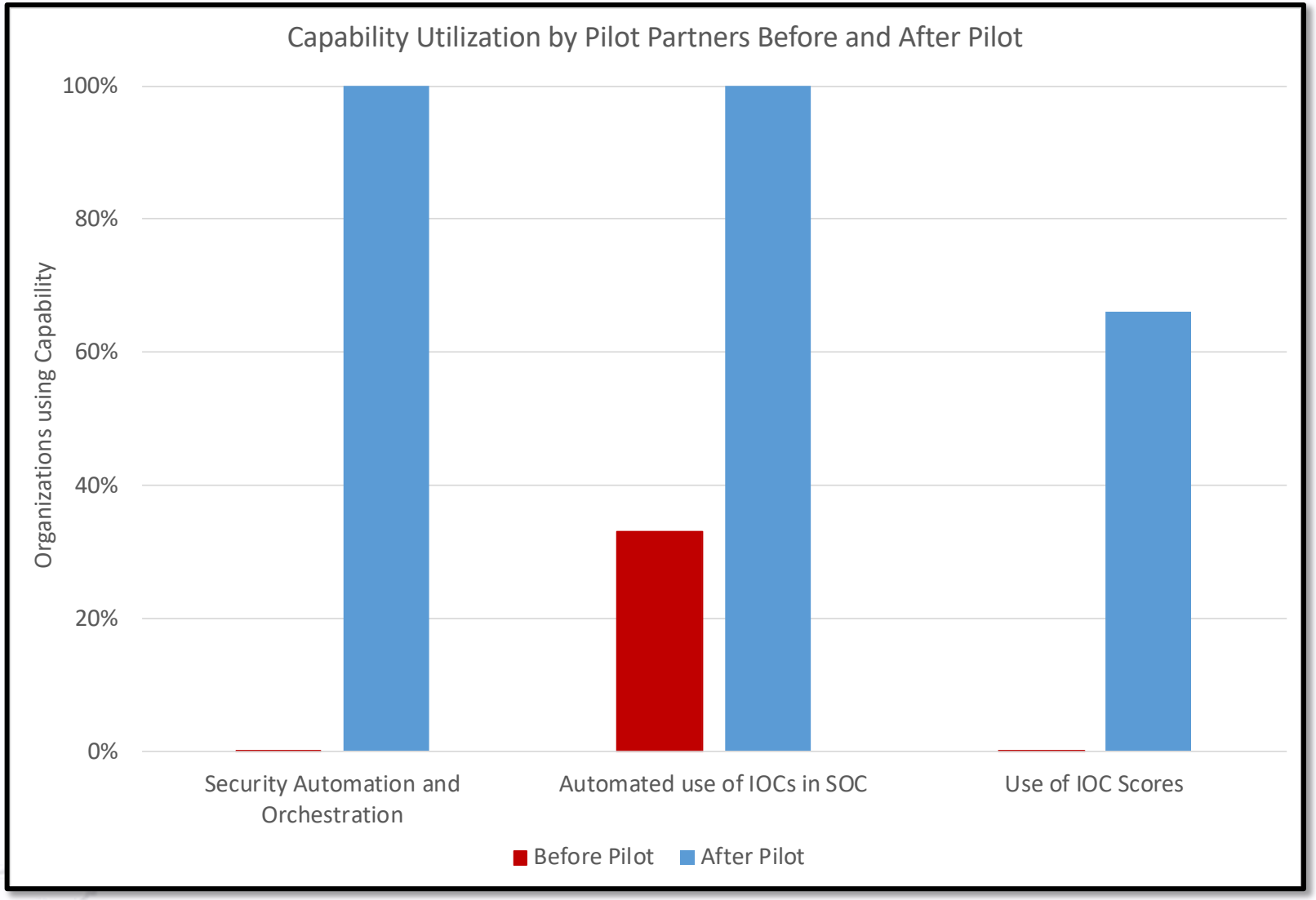
Addressing information sharing and SAO as a combined ecosystem allows for these types of improvements



TLP - WHITE

Pilot participant survey results

- **Pilot participation had positive impact on pilot organizations**
- **Prior to pilot, no partner was using Security Automation and limited use of IOCs in SOC workflows**
- **Post Pilot, all partners plan to deploy Security Automation and integrate IOCs into the SOC**



Conclusion

Conclusion

- Previous demonstrations have shown Security Automation and Orchestration can reduce time spent on repetitive tasks

- This pilot demonstrated the use of Security Automation and Orchestration combined with Information Sharing to make data more actionable and enable consistent execution
  - Processing IOCs using manual tasks leads to a lack of consistency in execution and ad-hoc integration
  - Using automation for the generation of IOCs and to augment response allows

- The cooperation between IACD, FS ISAC, and the Financial Institutions was critical to capturing these findings in actual Critical Infrastructure environments

Discussion

Integrated Adaptive Cyber Defense is sponsored by the Department of Homeland Security and the National Security Agency in collaboration with The Johns Hopkins University Applied Physics Laboratory.

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.

https://iacdautomate.org

@IACD_automate

https://www.linkedin.com/groups/8608114

icd@jhuapl.edu