Low-Regret Response Actions

Kimberly Watson Technical Director, IACD
Geoff Hancock Principal, Advanced Cybersecurity Group

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

Fighting Perception

- No one is automating response actions
- Organizations don’t trust automation
- We can’t risk impacting business operations

FACT: You allow automated response actions everyday

The Opportunity

- Why do you let vendors take actions?
- Risk vs. Reward
- When do actions have little likelihood of impacting operations?

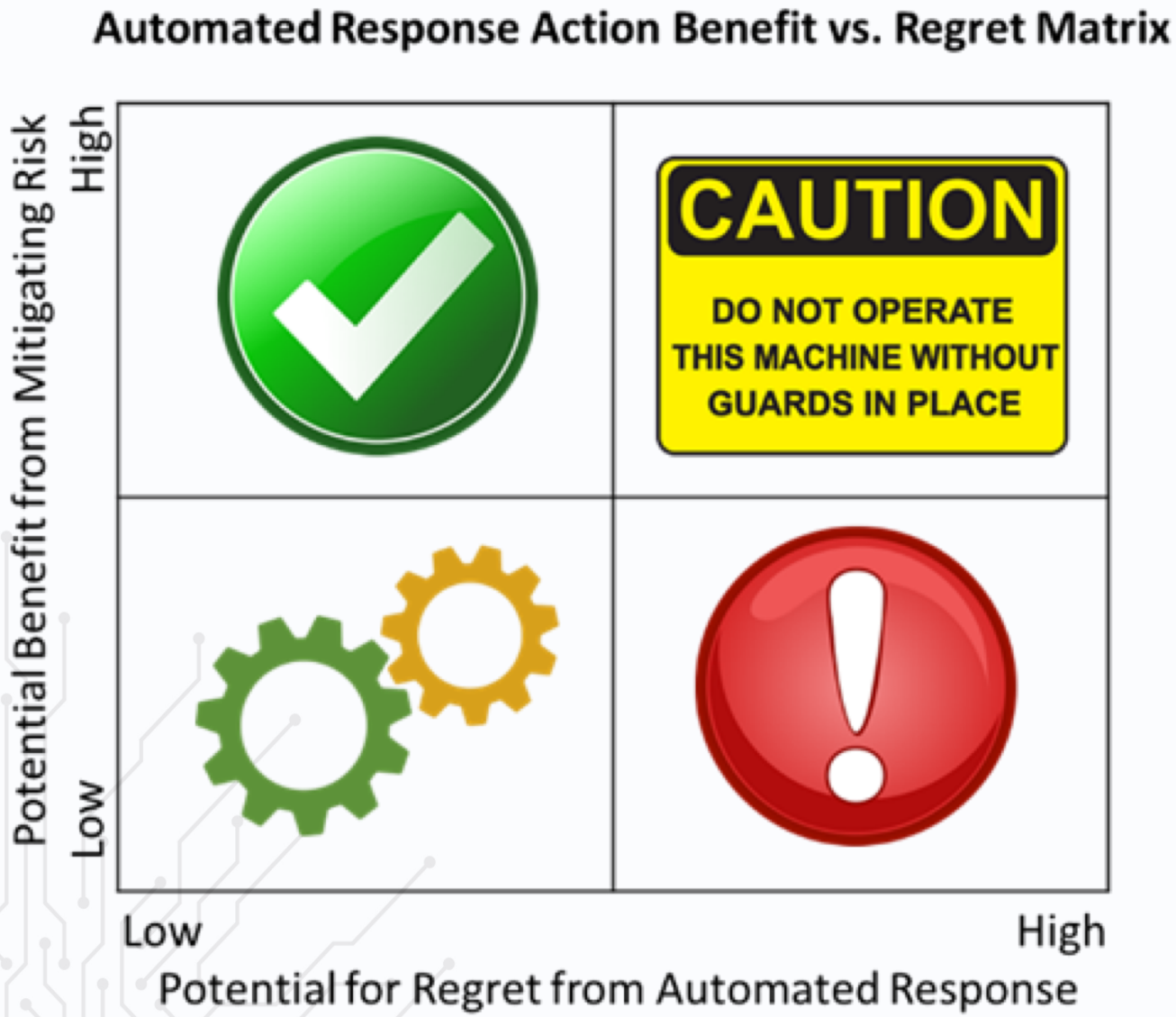
Its not WHAT action to automate, but WHEN…When is an action Low-Regret?

Operational Perspective

- **Machine tasks are tedious and mundane**
  - Monitoring and Detection
  - Data Management
  - Incident Response
  - User Permissions
- **Human Involvement**
  - Organize data sets-deeper analysis
  - Reverse engineering
  - Handling sensitive and critical systems
  - Understanding the business value and impact of systems attacked and the ability to be proactive

Machine Tasks = Defensive Actions
Human Tasks = Proactive Actions

The Benefit vs. Regret Matrix



High-Benefit/Low-Regret

High-Benefit/Low-Regret response actions are common practice

Where Automation is Focused Today

Risks that are well understood and where associated response actions are well documented fall in the upper left quadrant.

These are the actions that vendor products and services are designed to address or regulatory best practices require.

High-Benefit/Low-Regret

Build trust and show value

Implement Existing Policy

Look at CONOPs and SOPs that result in an explicit set of response actions

Determine what it means to meet the conditions that define acceptable/approved response actions

Since already authorized, automating these actions builds trust in automation and team

Low-Benefit/Low-Regret

Low-Regret is low-regret, even if your wrong

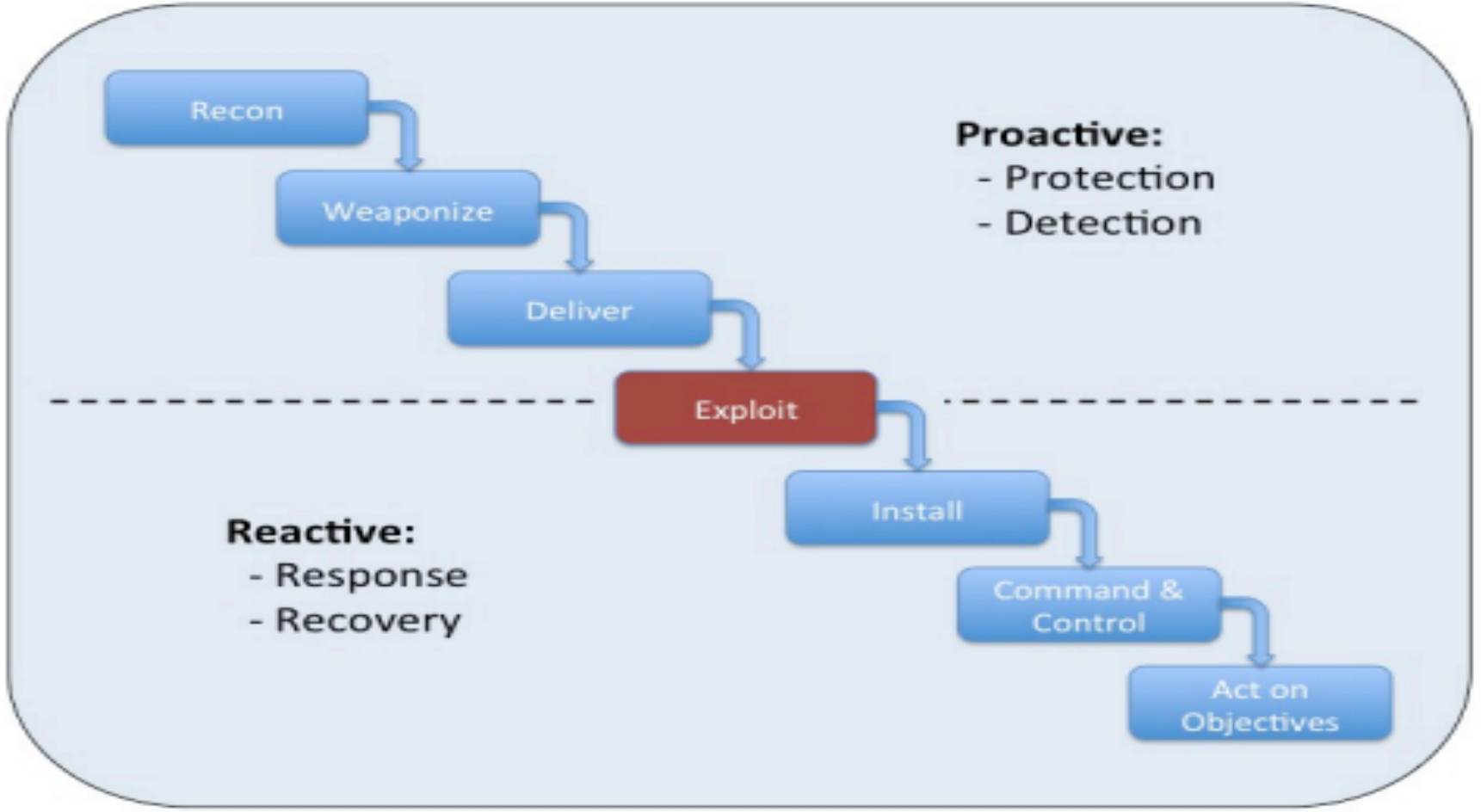
Best Place to Add Automated Response Actions

Risks that are not confirmed or verified but where the associated response action meets low-regret conditions are the lower left quadrant.

Because most of these decisions involve enforcement of local policy or are based on local conditions, vendors rarely perform these response actions by default.

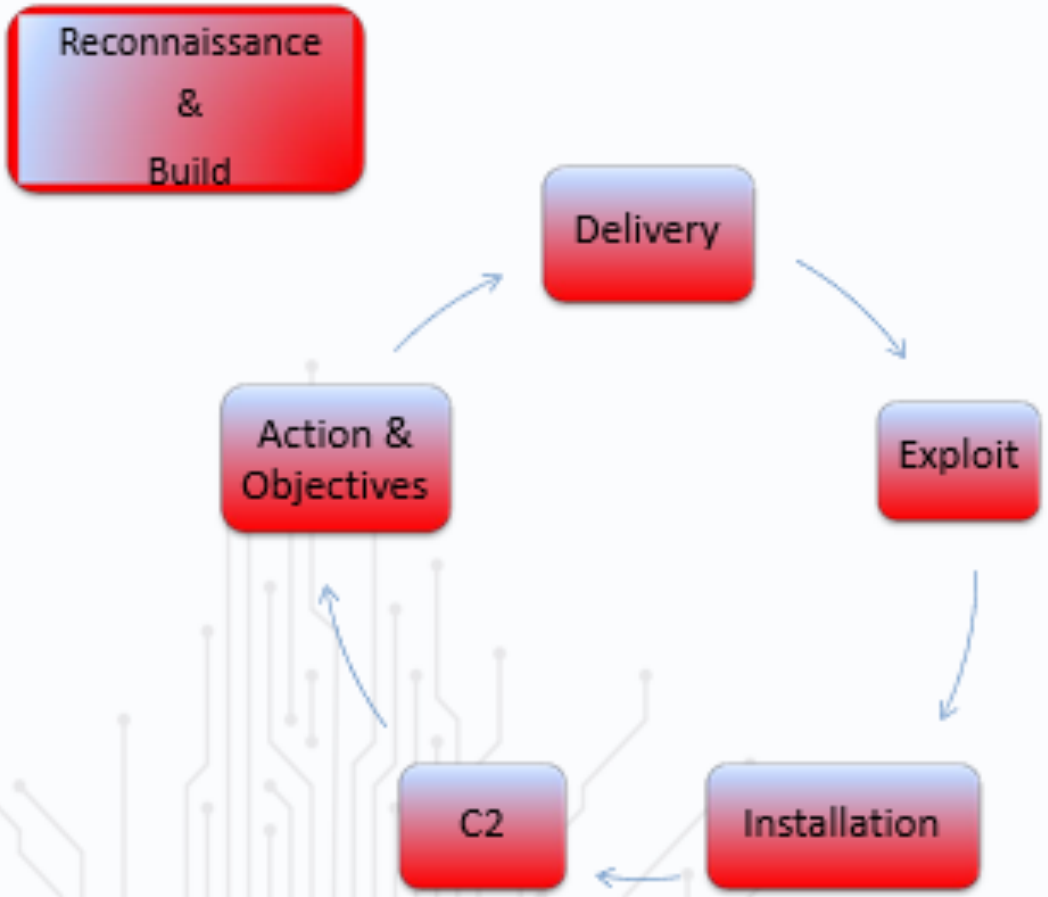
Low-Benefit/Low-Regret

Operations

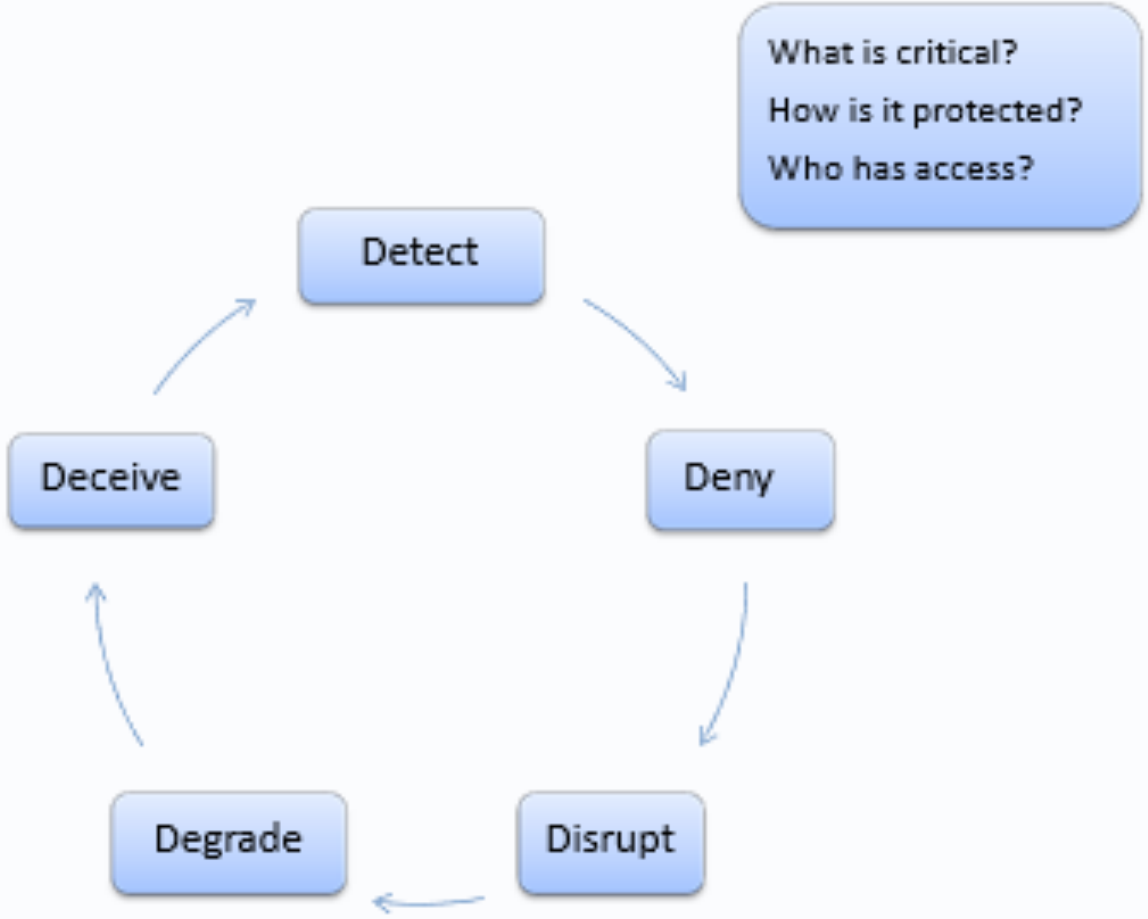


Low-Benefit/Low-Regret

Kill Chain



Response to the Kill Chain



Low-Benefit/Low-Regret

Improve morale and focus on more complex decisions

Capture Analyst Insights

Identify the decisions your most experienced or advanced analysts deem routine

Derive when an action is low regret

Shows respect to operations personnel, improves operations, and shows team you are not replacing them

High-Benefit/High-Regret

Prevention, prevention, prevention…and automated decision support

Risk Posture Defines Automation Opportunities

Risks that are only valid for a window of time or where the mitigation has significant potential to negatively impact the system are in the upper right quadrant.

These type of events require a process that includes oversight and the organization needs to be protected during the window of vulnerability or threat.

High-Benefit/High-Regret

Build trust in proactive processes as response actions

Understand Existing Asset Management Processes

Identify when modifications to assets are allowed

Determine when a situation is equivalent to the initiating condition of an existing approved process

Establish a routine to “respond” at a pre-defined interval even when an event is not detected – use this to identify when an action is low-regret.

Low-Benefit/High-Regret

Investigation and cyber hygiene minimize this quadrant

Move it to Another Quadrant

Risks that are not confirmed or of unknown severity where the associated response action has significant potential to negatively impact the system are in the lower right quadrant.

Most organizations do not implement automated response actions because they do not believe that they have the necessary information to reliably determine impact potential.

Low-Benefit/High-Regret

Prioritize Identify requirements based on active risks

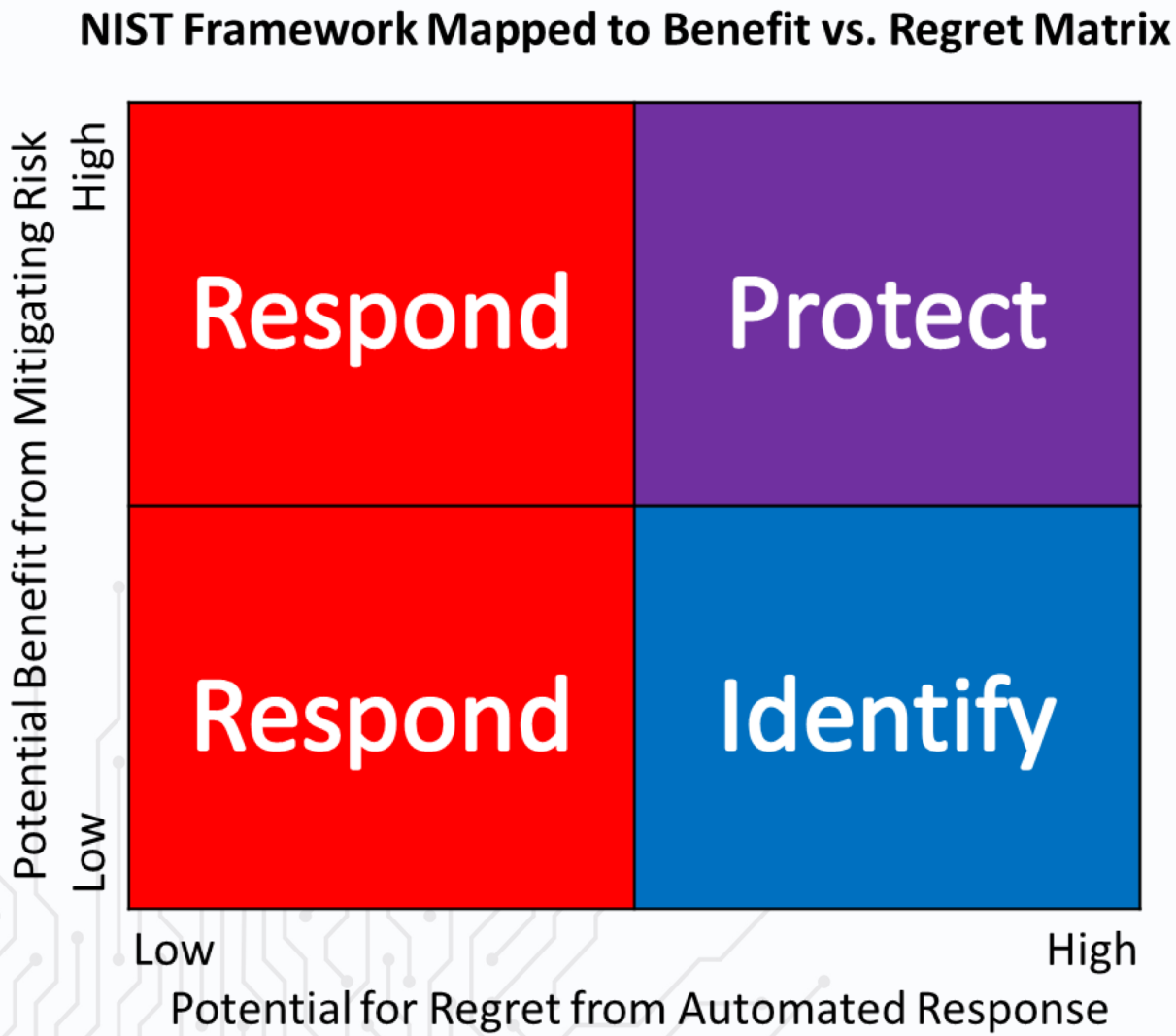
Identify What You Need Know

Review periodically with analysts – what piece of information did you need to know if this was a low-regret situation?

Determine if that information is available somewhere in the enterprise

Incrementally improve capabilities based on real-world conditions affecting speed and scale of operations

It’s Not All About Response



Respond

Detect and respond is best for low-regret actions because they can be implemented at speed and scale

Protect

When you cannot respond at speed, use protection mechanisms to defend at speed and scale

Identify

You need to know your network and your business priorities to know what is low-regret and what is high-value

If You Only Remember One Thing

Focus on identification and execution of low-regret response actions

If You Can Remember A Second Thing

- **Automate functions based on standards and requirements where possible.**
- **Use the Kill Chain and Defense Chain to your advantage**

- Do you have the right tools in place to automate?
- Is there a set of well defined tasks?
- Are they repeatable?
- Do they require human intervention?

- Do the tasks take up too much time?
- Do you have a budget for more security hires to solve this?
- Is your team experiencing fatigue?
- Is the teams ability to manage operations and respond to breaches taking to long?

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://www.iacdautomate.org


@IACD_automate


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


icd@jhuapl.edu