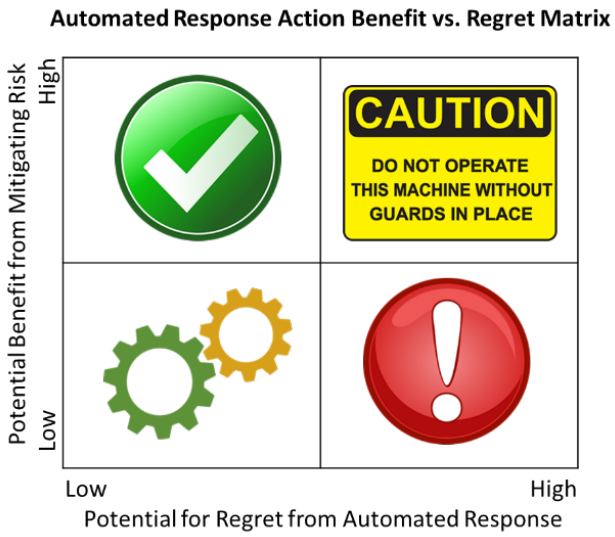
High-Benefit/Low-Regret Automated Actions as Common Practice

Whether you manage a large enterprise or just a personal laptop, you benefit daily from high-benefit/low-regret automated actions executing constantly on your behalf to mitigate risk. Some response actions are unlikely to impact your system in a manner that disrupts business operations. Other response actions are mitigating a confirmed threat in a manner recommended by experts (think your anti-virus). These types of actions are deemed high-reward (the device or network is defended) and low-regret (nothing is broken). Users and organizations have been allowing these actions to occur in an automated manner for nearly two decades.

As the deployment of Security Automation and Orchestration (SAO) solutions continues to increase, organizations are determining what response actions to automate. Many organizations are uncomfortable with blindly taking automated actions that can impact the network. They traditionally have operations personnel review or approve response actions before execution. Many of these same organizations trust their vendors (such as anti-virus) to take the same actions on their behalf without any insight into the information or decision process used or the action implemented. There are many reasons for this inconsistency, in part, it is because the local risk vs. reward analysis favors letting the vendor take the action.

We would recommend using a benefit vs. regret matrix to make decisions about implementing automated actions. ***The idea is that organizations should focus on when to take an action in an automated manner instead of whether the action should be automated.*** A benefit vs. regret matrix can highlight where automated actions are appropriate and where they may not be the best approach to mitigating threats and vulnerabilities.



High-Benefit/Low-Regret: Where Automation is Focused Today

Risks that are well understood and where associated response actions are well documented fall in the upper left quadrant. Examples include blocking or removing malware or locking accounts after repeated login failures. These are the actions that vendor products and services are designed to address or regulatory best practices require. ***Automation of an appropriate response action when an event of this type is detected or identified is accepted practice.***

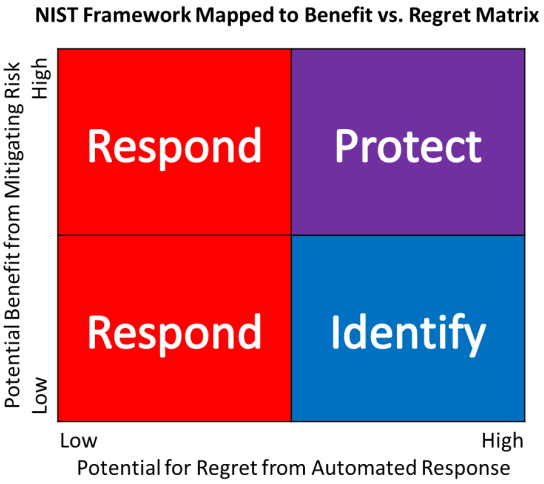
Low-Benefit/Low-Regret: Best Place to Add Automated Response Actions

Risks that are not confirmed or verified but where the associated response action meets low-regret conditions are the lower left quadrant. ***This is where security and IT operations personnel should focus implementation of automated response actions.*** Examples include blocking a suspect IP address that no

one in the enterprise has ever attempted to connect to, blocking access to unauthorized sites, and removing adware. Because most of these decisions involve enforcement of local policy or are based on local conditions, vendors rarely perform these response actions by default.

High-Benefit/High-Regret: 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. Examples include mission essential websites that have been compromised or deploying patches to address software vulnerabilities. ***These type of events require a process that includes oversight to make sure that business objectives or network functionality is not adversely impacted by a response action.*** The amount of oversight required, and hence automation accepted, is mostly defined by an organization's risk posture. In general, this quadrant is best addressed by the Protect function of the NIST Framework for Improving Critical Infrastructure Cybersecurity and not the Respond function. Mitigating risks in this quadrant requires the organization to protect itself during the window of vulnerability or threat, and that is more appropriately handled by capabilities designed to prevent exploitation or compromise and not those that detect and respond to successful exploitation. These capabilities have the added benefit of mitigating the risk from unknown threats and vulnerabilities.



Low-Benefit/High-Regret: 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. ***This is the quadrant where more investigation is necessary, and where automating response action is not advised.*** This is also the set of conditions that prevent most organizations from implementing any automated response actions. They do not believe that they have the necessary information to reliably determine the impact potential of the risk or the response action. Most of the information needed to determine when you are in this quadrant is generated by the Identify function of the NIST Framework. Identifying and mitigating risks in this quadrant requires an organization to know what is authorized for their network and have an understanding of baseline states and behaviors of users, devices, and network connections.

Summary

Organizations already implement automated response actions on their networks. Most of the time, these actions are performed by vendor products or services in response to confirmed risks in a manner that is accepted by regulators, experts, and peers. These are considered low-regret actions when taken to mitigate high-priority threats. As organizations look to implement automated actions in response to alerts, events, or new information; the use of this Benefit-Regret matrix can help determine the areas where automated responses are most helpful. ***Focusing on identification of low-regret actions, even with uncertainty about the risk, can improve the efficiency of operations personnel and tremendously scale up appropriate automation of response actions.***