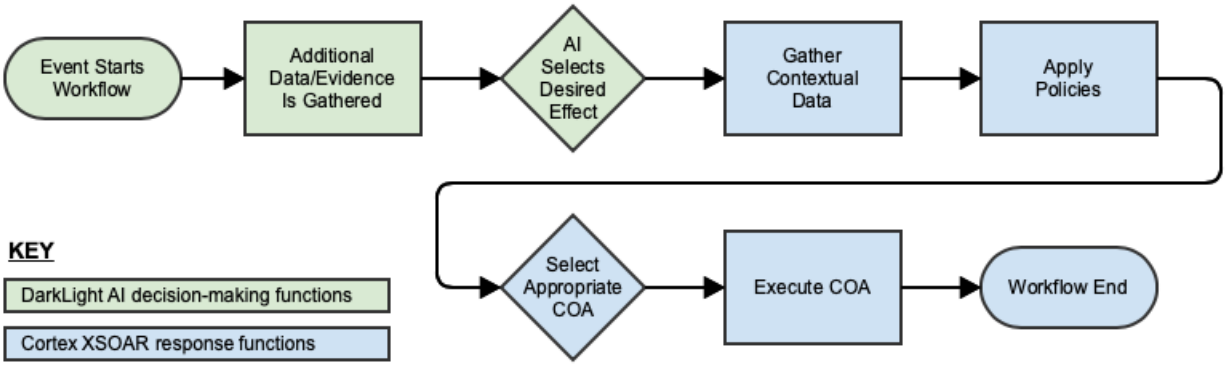
Effects-Based Courses of Action

Cybersecurity attacks are increasing in volume, scale, and complexity. To address the growing threats, cybersecurity solutions are also becoming more complex. To help manage this complexity, Security Orchestration, Automation, and Response (SOAR) technology is used to coordinate the actions of multiple security tools. The widespread adoption of SOAR technology creates a need to ensure that the proper information is exchanged between products to provide the necessary context to achieve a coordinated response.

SOAR platforms currently enable all the functions of cyber defense required to Observe, Orient, Decide, & Act, more commonly known as the OODA loop, for decision-making and operations. However, SOAR products often focus on performing the Observe and Act functions. Now, many security vendors are adding artificial intelligence (AI) and/or machine learning (ML) capabilities to their products, which could be used to address and improve decision-making functions for cyber security. This division of labor between AI/ML solutions and SOAR platforms could help manage the complexity, speed, and scale required of cybersecurity solutions: AI/ML solutions can be applied to find patterns and ***decide*** faster and at scale, while SOAR can be applied to ***act*** faster and at scale. Integrated Adaptive Cyber Defense (IACD) demonstrated how to bridge these technologies while maintaining human control using effects-based courses of action (COAs).

An effects-based COA is a set of response actions to a cyber attack, selected based on the desired high-level cyber effect – the goals of the response – rather than having to specify the exact steps to be executed via a course of action. In a traditional COA workflow, a SOAR platform starts the workflow, gathers additional data/evidence, selects an appropriate COA, and performs its execution – covering all the functions of the OODA loop within that single platform. With an effects-based COA workflow, an AI capability can be used to gather additional data/evidence and select an appropriate COA based on that data and the desired cyber effect, and then the SOAR platform can be used to automate and orchestrate the actions required of various security products to achieve that desired response and outcome.

IACD conducted an experiment to demonstrate the benefits of combining AI and SOAR technologies using effect-based COAs. In the experiment, IACD used the DarkLight AI expert system to provide sense-making and decision-making capabilities, corresponding to the Orient and Decide functions of the OODA loop. IACD used the Cortex XSOAR platform to control response actions, corresponding to the Act function. The figure below depicts the workflow for an effects-based COA, where DarkLight performed the first few decision-making functions and Cortex XSOAR performed the remaining response actions.



In the experiment, IACD successfully demonstrated the combination of DarkLight AI and the Cortex XSOAR platforms to select and execute effects-based COAs in the face of different attack scenarios, all with a human monitoring "on the loop" instead of a human having to decide and act "in the loop." DarkLight made sense of two different attack scenarios – malware conducting data exfiltration versus ransomware – and selected an appropriate effects-based COA response for the particular attack. DarkLight then triggered Cortex XSOAR to execute the appropriate COA for the attack, and Cortex XSOAR orchestrated the response actions of the enterprise security products. Throughout the process, a human monitored the performance of both the AI and SOAR components via metrics and summaries of the actions taken. The human had specific criteria defined for situations where he/she would take over control, and the human was available for decision escalation in cases where the AI could not decide with a certain threshold level of confidence.

The effects-based COA experiment successfully demonstrated the ability to coordinate the activities of an AI/ML product and a SOAR platform, allowing each to perform functions of the OODA loop to which each is best suited, while enabling human monitoring and control.

For more information on effects-based COAs, SOAR technology, and other experiments, please see the resources in the References section and visit https://www.iacdautomate.org.

References

[1] IACD. (December 2019). IACD Spiral 17: Effects Based COAs Experiment Summary Version 1.0

[2] Darklight. (2020). https://www.darklight.ai/

[3] Palo Alto Networks. (2020). https://www.paloaltonetworks.com/cortex/xsoar