NETWITNESS

5 Ways Threat Intelligence Improves Orchestration and Automation

Benefits of Applying Intelligence to Better Respond to Incidents

There is a lot of conversation around the need for security orchestration, automation, and response (SOAR). Security organizations agree that having a system to automate tasks and keep the entire security team working from the same game plan has become more critical as the number of alerts and incidents that must be addressed increases. The bigger question these organizations must answer is, “How do we know that the threats and incidents we are investigating are the ones that we should be focused on?” This is where threat intelligence working in unison with your orchestration and automation system can help. Here are five reasons why:

Lower-level tasks no longer consume valuable resources

As orchestration and automation systems work to automate detection and prevention tasks, validated threat intelligence derived from a broad range of sources ensures that the system is quickly alerting and blocking the incidents that could cause your organization the most harm. This process eliminates the repetitive tasks that require a large amount of analysts’ time while properly identifying the incidents that matter and reduces false positives.

Increased accuracy and precision

The key to getting in front of threats? Awareness and understanding the context of the situation early on. To do this, threat intelligence can automatically identify and extract key evidence to be applied to a case under investigation. This allows your organization to work quicker and prevent attacks or stop them in their tracks, minimizing impact. Be more proactive by automating more tasks up front.

Fine-tune your threat intelligence

Your own team and data are the best sources of intelligence you will ever have. The analysts know your environment and they can determine how insights, artifacts, and sightings automatically captured using threat intelligence apply to your specific organization. This process refines the vast amounts of threat intelligence gathered to understand how new indicators of compromise (IOCs) and adversary tactics and techniques will have an impact on your specific environment.

Orchestrate with more confidence

Analytical processes applied to external threat intelligence and backed by internal intelligence allows for more accurate alerting, blocking, and quarantine actions with fewer false positives. It goes beyond simply ingesting multiple threat intelligence feeds or acting from a shared indicator of compromise (IOC). It is about making sense of them at scale using techniques like adaptable scoring and contextualization to know what actions to take, if any.

Constant improvement

The automated extrapolation of context and tasks based on threat intelligence thresholds, such as indicator scores, followed by the memorialization of data enables security organizations to undergo strategic reviews and hone processes. As a result, the team’s improvement grows, allowing it to rise to the challenge of growing threats.

Many orchestration and automation solutions only incorporate intelligence to trigger certain workflows. NetWitness® Orchestrator is different – it gets the highest value from external and internal intelligence enabling security organizations to automate tasks, work systematically across teams, and address potential business-impacting threats with greater efficiency.

Learn more at **netwitness.com**

NETWITNESS
An RSA Business