Leveraging Machine Learning to Orchestrate & Automate Your SOC

RSA NetWitness® Orchestrator top machine learning use cases

In an era of ever-expanding attack surfaces, protecting against threat actors—from commodity malware, insider threats and crimeware to state-sponsored exploits, hacktivists and terrorists—has become an increasingly complex activity. Not all threats are created equal, yet disconnected silos of prevention, monitoring and investigation technologies continue to fall short in empowering security operations center (SOC) teams to rapidly weed out false positives and eliminate manual repetitive actions. This is where machine learning comes to assist SOC personnel on their journey to an intelligent SOC.

The RSA NetWitness® Platform leverages machine learning to improve threat detection and streamline SOC operations. While improving threat detection focuses on abnormal user, entity, network and endpoint behaviors to highlight sophisticated threats such as insiders or a compromised account trying to exfiltrate IP and focusing on Mean Time To Detect (MTTD), a streamlined SOC is laser-focused on learning from past experiences, looking at the security analysts' actions and trying to identify how security teams can work in a more efficient, standardized manner to reduce Mean Time To Repair (MTTR).

> Such machine learning technology marks the first time in the security industry when a solution learns from experts rather than relying only on historical security data.

Critical machine learning capabilities for a security orchestration automation and response solution include:

- Quick to zero in on the right course of action
- Efficient incident assignment
- Expert-based suggestions
  — "Would you like to run this command for this attack?"
  — "Would you like to create an automated playbook for this set of actions?"
- Threat and business context visualization
- Work an incident. Once.

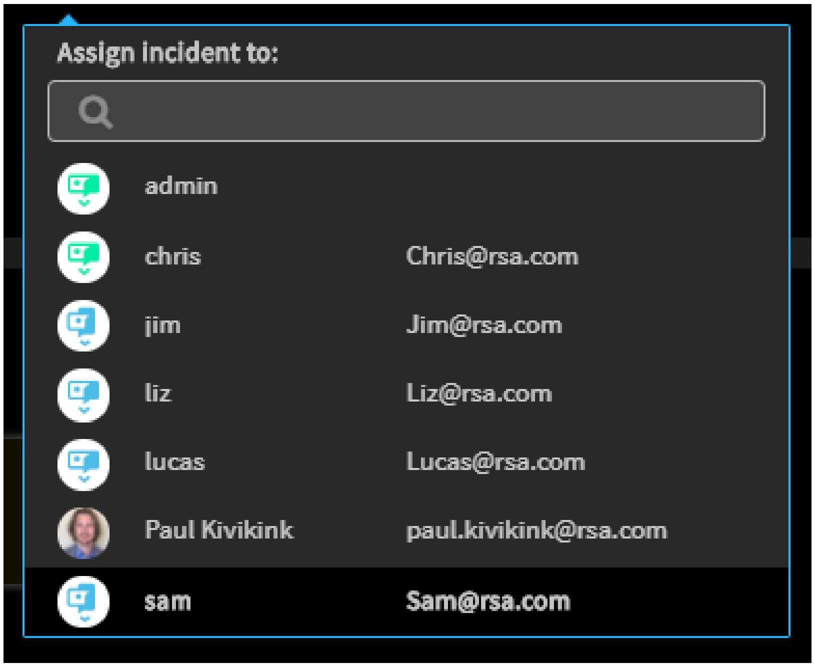
Here, we present a set of use cases that describe the challenges security operations teams face on a daily basis, how the machine learning capabilities included in RSA

NetWitness Orchestrator help solve those problems, and benefits SOC teams can derive from these capabilities.

Use case 1 : Incident owner recommendations

Challenge

As SOC teams grow, they tend to take a “who’s next in line?” approach to assigning incident owners. This approach creates two problems: It frequently leads to more work for security analysts who are already overburdened with assignments, and it fails to take into consideration each analyst’s expertise, leading to improperly assigned incidents. (And we all know that improperly assigned incidents often lead to improperly handled incidents.)



Assign incident to:

admin	
chris	Chris@rsa.com
jim	Jim@rsa.com
liz	Liz@rsa.com
lucas	Lucas@rsa.com
Paul Kivikink	paul.kivikink@rsa.com
sam	Sam@rsa.com

Machine learning solution

Whenever incident owners need to be assigned, RSA NetWitness Orchestrator uses machine learning to study details of all relevant incidents in the system. This data is then cross-referenced with analysts’ workloads and skills to suggest the top three analysts for a given incident.

Benefit

With more intelligent and more informed incident assignment recommendations, SOC managers can ensure incidents are handled properly and expeditiously, and that workloads are distributed intelligently across SOC staff.

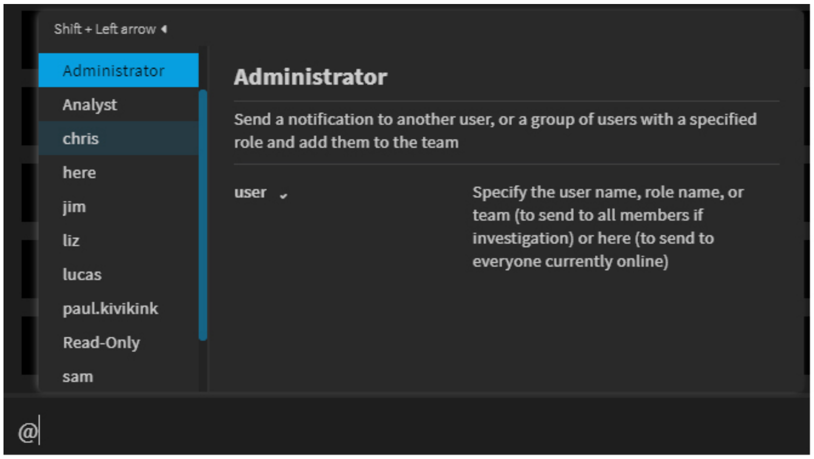
Highlight

RSA Netwitness® Orchestrator studies incident fields and analyst workloads before making incident ownership recommendations.

Use case 2 : Collaborative investigation via suggested experts

Challenge

End-to-end handling of incident response investigations is rarely an isolated process, yet SOC analysts often operate in silos when performing investigations—unaware of which colleagues' skills might come in handy for complex incidents. Junior analysts are especially prone to this, as they are often left to contend with incidents alone while senior analysts are occupied with other responsibilities.



Administrator

Send a notification to another user, or a group of users with a specified role and add them to the team

Specify the user name, role name, or team (to send to all members if investigation) or here (to send to everyone currently online)

Machine learning solution

The RSA NetWitness Orchestrator "War Room" facilitates collaborative investigations: Analysts can invite their teammates to conduct joint investigations. Here, RSA NetWitness Orchestrator uses machine learning to study the history of all closed incidents, specifically looking at manual actions analysts performed in the past. After closely examining this data, RSA NetWitness Orchestrator suggests the top three analysts who can provide relevant assistance for a particular incident.

Benefit

By enabling joint investigations and facilitating intelligent team composition, the "War Room" can help your SOC resolve incidents faster, with fewer errors, and can help address skills gaps by pairing junior and senior analysts. This feature also acts as a guiding hand and a "starter kit" for junior analysts by highlighting which experts can help them through specific incidents, thus reducing error rate and analyst anxiety.

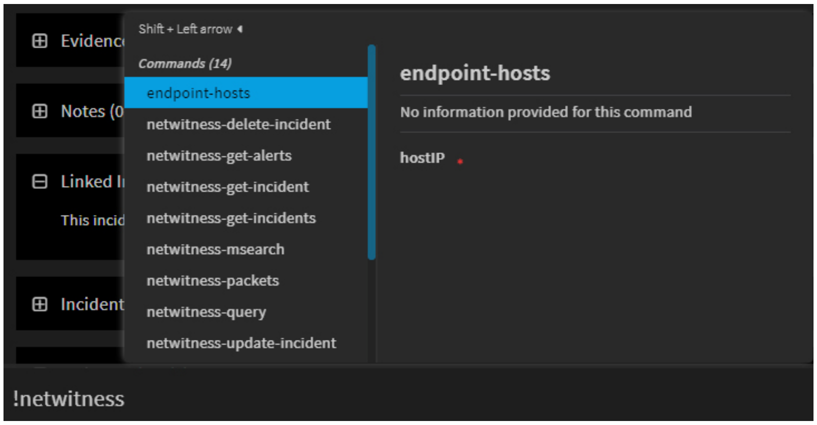
Highlight

RSA NetWitness® Orchestrator recommends analysts based on actions they've taken in the War Room in the past and the history of closed incidents.

Use case 3 : Standardized security commands

Challenge

When conducting real-time investigations after incident triage, analysts literally have hundreds of possible security actions to choose from. If there's no standardization regarding which actions analysts should take at various points in an investigation for a given incident, the lack of consistency can lead to varying resolution times and quality for similar incidents, negatively impacting your SOC's SLAs and KPI tracking.



No information provided for this command

```
!netwitness
```

Machine learning solution

When analysts begin to type a security command in the RSA NetWitness Orchestrator War Room, the system studies manual commands other analysts used for similar incidents in the past. The system then recommends which security command to run first. Even if analysts have already run some commands, the machine learning algorithm can set them on the right path by suggesting commands they may have missed.

Benefit

Security command suggestions move analysts towards standardized incident response actions and prevent rogue investigation processes. With more consistent incident response activities/procedures in place, you're in a better position to improve and maintain more consistent SOC metrics. This also aids in organic knowledge management and retaining expertise within the SOC.

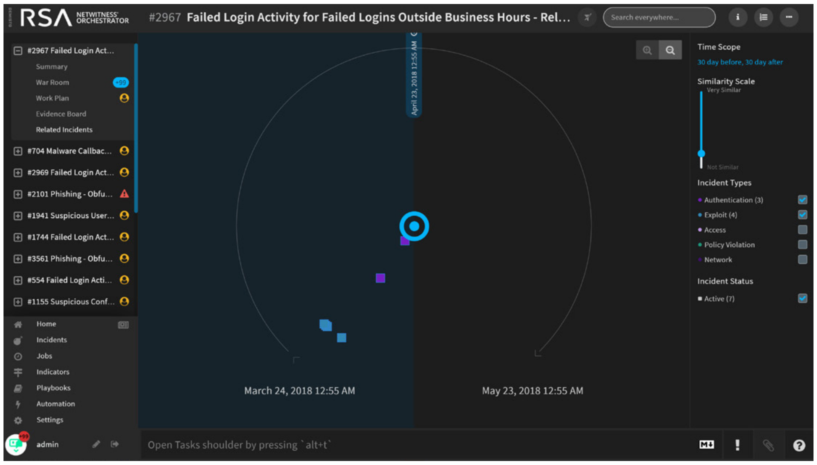
Highlight

RSA NetWitness® Orchestrator looks at manual commands analysts perform for particular types of incidents to recommend commonly used commands.

Use case 4 : Visualizing related incidents

Challenge

The speed at which incidents crop up can give any analyst myopia, impeding their ability to see patterns in data and connections to similar incidents already logged by the system. This results in redundant and potentially time-wasting work when an analyst should be responding with a process that is already stored in the platform, but they do not leverage that stored knowledge in the platform.



Machine learning solution

For each RSA NetWitness Orchestrator incident, the "Related Incidents" section presents a visual, time-based map of similar incidents that have occurred on the system. RSA NetWitness Orchestrator studies the incidents' data and indicator details, identifies patterns and similarities among them, and visualizes that data in a manner that analysts can easily act upon.

Benefit

In addition to reducing MTTR and alert fatigue, a standard benefit of security orchestration, automation and response (SOAR) tools, the Related Incidents feature goes a step further to increase analysts' investigative capabilities: It provides them with visual tools to help them understand how incidents may be related across a host of factors, including in the context of a broader attack campaign.

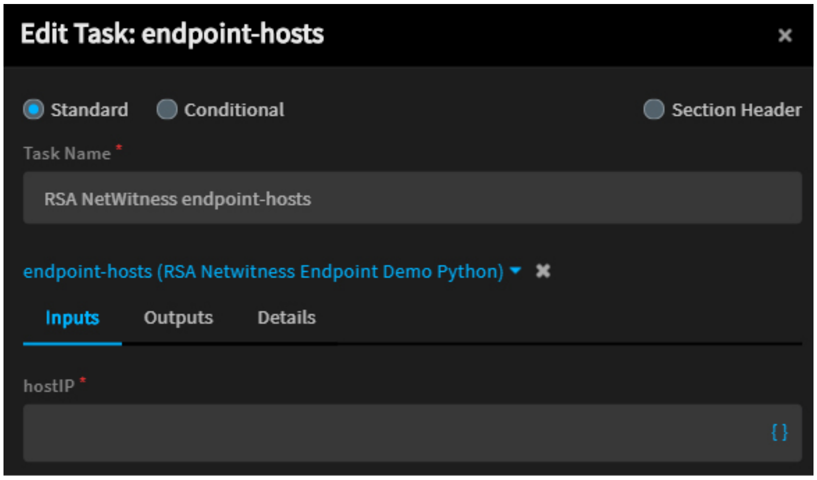
Highlight

RSA NetWitness Orchestrator correlates indicators and incident data to present a real-time, radial map of related incidents for each case

Use case 5 : Simplifying playbook task creation

Challenge

After playbooks make the initial journey from paper (or an analyst's mind) to a SOAR platform, those playbooks may facilitate automated response but they may not undergo any further measurement or review. Unless analysts capture better knowledge from elsewhere and feed it into the platform, the benefits of these playbooks plateau after a period of time.



Edit Task: endpoint-hosts ×

● Standard ○ Conditional ○ Section Header

Task Name *

RSA NetWitness endpoint-hosts

endpoint-hosts (RSA Netwitness Endpoint Demo Python) ▾ ✖

Inputs Outputs Details

hostIP *

{ }

Machine learning solution

RSA NetWitness Orchestrator not only facilitates the creation of custom playbook tasks but also uses machine learning to accelerate the conception of verifiably relevant tasks during an incident investigation. While creating playbook tasks and selecting inputs, analysts can see suggestions for arguments and parameters that fit best with those inputs. RSA NetWitness Orchestrator goes through all existing playbook tasks (both out-of-the-box and within customer environments) and studies frequency of task parameters to identify commonly used arguments.

Benefit

Rather than stopping at alert fatigue reduction and quicker incident triage, RSA NetWitness Orchestrator playbooks use machine learning to dynamically identify relevant actions for better incident response efficiency. This helps tackle the eventual stagnation in efficacy of static playbooks and certifies that even playbooks go to digital gyms to get leaner.

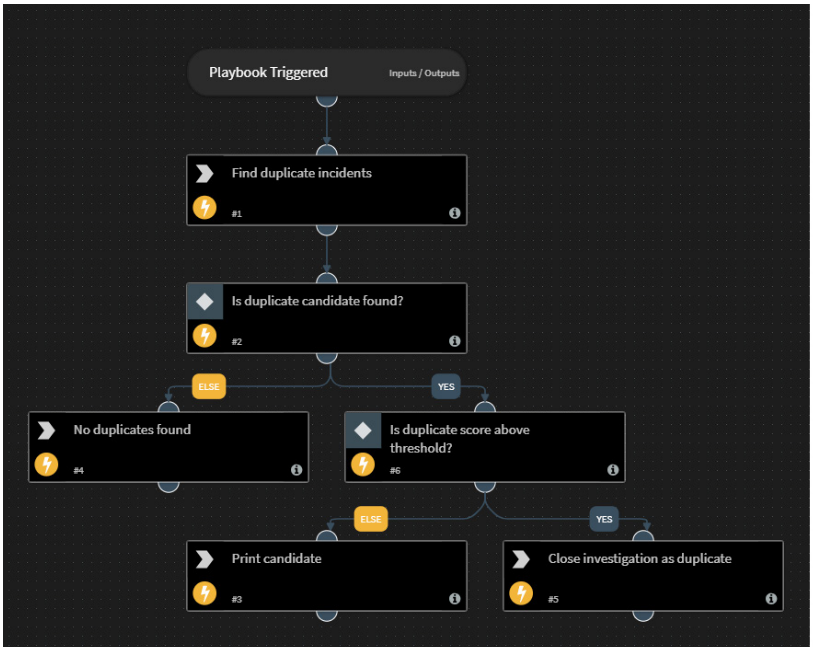
Highlight

RSA NetWitness Orchestrator digs across playbook tasks to study commonly used automation arguments and recommends these inputs during the creation of new playbook tasks.

Use case 6 : Extracting duplicate incidents

Challenge

High alert numbers usually lead to a high occurrence of duplicate incidents. However, due to varying attack vectors, different target endpoints or subtle morphing, these incidents register independently on the SOC's legacy SIEM or existing SOAR platform. This leads to tiresome, repetitive work for analysts as they investigate the same types of incidents over and over, playing a soul-sapping game of looking for the needles in malicious haystacks.



Machine learning solution

RSA NetWitness Orchestrator users can avail out-of-the-box automation to generate a list of duplicate incidents, either as playbook tasks or interactively in the War Room. RSA NetWitness Orchestrator's machine learning studies both predefined data and customer environments and looks for similar labels, email labels (relevant for phishing incidents), incident occurrence times, and common indicators to generate this list.

Benefit

Easy identification and documentation of duplicate incidents eliminates huge chunks of menial work for analysts, freeing them to concentrate on more critical problem-solving and high-quality tasks.

Highlight

RSA NetWitness Orchestrator studies both predefined data and custom environments to look for similar labels, email labels, incident occurrence time and common indicators to generate a duplicate incidents list.

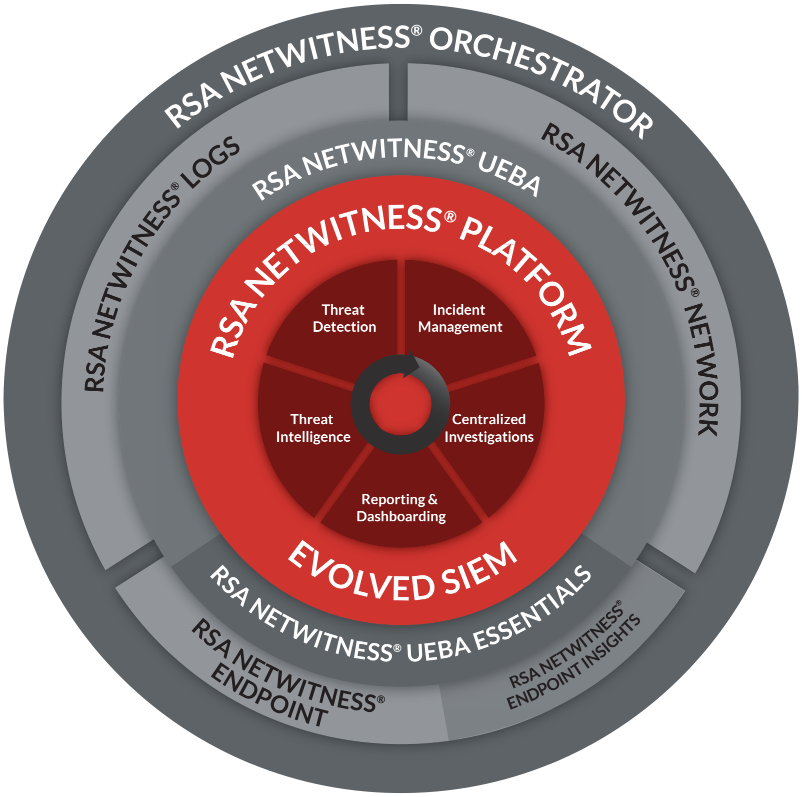
RSA NetWitness Orchestrator goes beyond simple automation to help organizations truly enable their security operations center teams. By harmonizing actions across siloed security products, managing incidents within the platform, collaborating in real time and learning from all the data at your disposal, you can truly extract the greatest value for your SOC.

Staying true to the "learning" half of machine learning, RSA NetWitness Orchestrator is always searching for new avenues to leverage its machine learning base and advance a system that gets smarter with each incident, in turn making the SOC intelligent as well.

RSA NetWitness Orchestrator acts as the "connective tissue" binding together the other solutions in the RSA NetWitness Platform and across your entire security infrastructure.

The RSA NetWitness Platform consists of RSA NetWitness® Logs, RSA NetWitness® Network, RSA NetWitness® Endpoint, RSA NetWitness® UEBA and RSA NetWitness Orchestrator. This complete and powerful platform combines risk intelligence and business context with advanced cybersecurity capabilities so your organization can better detect known and unknown threats, minimize attacker dwell time and mean time to respond, and lessen the impact of security incidents.

Your security operations center has the potential to be the cornerstone of your organization's broader effort to manage digital risk.
For more info: www.rsa.com/DoMore.



About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.
For more information, go to **rsa.com**.