NETWITNESS

WHITE PAPER

Boosting Operational Effectiveness with Intelligent Orchestration

How Threat Intelligence Supercharges Security Automation and Orchestration

Executive Summary

Security operations teams are constantly looking for ways to stay ahead of cyber attacks. Many believe that the more security monitoring and prevention tools they have, the stronger their security posture will be, and the faster they can react. But the more-is-more approach poses two distinct problems:

- "Security tool sprawl" leads to an exponential increase in both data and alerts. To manage the deluge, security teams must arrange and process information in ways that support quick decision-making and execution. That's hard to do when the problem continues to scale.
- More tools also means more chances for siloed data—and more likelihood that each tool will offer only an isolated view of any problem. Security personnel spend their time chasing less important problems, making it harder to focus on the threats that matter most.

For these reasons and more, many organizations are finding that point products deliver diminishing returns, and trying to correlate data from multiple interfaces wastes time and reduces efficiency. In contrast, an orchestrated security approach informed by intelligence on both external threats and internal activities is more effective, resilient and adaptive.

To address today's threats, security professionals must draw on intertwined factors: Intelligence makes it possible to adapt in response to a changing environment, while security orchestration helps organizations plan program improvements. And they must use situational awareness and historical data to determine when and how each task is done.

NetWitness® Orchestrator gives security teams the collaborative, threat intelligence-powered capabilities they need. It provides insight into massive amounts of information from multiple sources, identifies relationships among the pieces, and learns from previous actions to generate a shared, easy-to-use, panoramic view of the threat landscape. Clear reports in plain language help decision-makers communicate risk to stakeholders. And a combined NetWitness Platform workflow supports security operations planning and action—allowing team members to focus on the incidents that matter while speeding detection, investigation and remediation of potential threats.

NetWitness® Orchestrator provides insight into massive amounts of information from multiple sources, identifies relationships among the pieces, and learns from previous actions to generate a shared, easy-to-use, panoramic view of the threat landscape.

Is There Such a Thing as Too Much Data?

At the core of virtually every security team is the never-ending quest to stay ahead of cybercriminals in an ever-changing threat landscape. Protecting against the bad actors—from commodity malware, insider threats and crimeware, to state sponsored exploits, hacktivists and terrorists—has become increasingly complex. In the past, threat analysts would cobble together data from disconnected silos of prevention, monitoring or investigation technologies to try to hunt for threats, but continue to fall short in seeing the full picture.

As threats become more pervasive and sophisticated, the need to converge security orchestration and automation, security incident response and threat intelligence platform capabilities becomes paramount.

Security operations teams are constantly looking for ways to stay ahead of cyber attacks. Many believe that the more monitoring and prevention tools they have, the stronger their security posture will be, and the faster they can react. But the more-is-more approach poses two distinct problems:

- "Security tool sprawl" leads to an exponential increase in both data and alerts. To manage the deluge, security teams must arrange and process information in ways that support quick decision-making and execution. That's hard to do when the problem continues to scale.
- More tools equals more chances for siloed data—and more likelihood that each tool will offer only an isolated view of any problem. Security personnel spend their time chasing less important problems, making it harder to focus on the threats that matter most.

For these reasons and more, many organizations are finding that point products deliver diminishing returns and trying to correlate data from multiple interfaces wastes time and reduces efficiency. To counter these issues, many have turned to solutions designed to automate and orchestrate aspects of their cybersecurity operations, in the hope that such tools will reduce workload and boost productivity. Where full automation is not possible or advisable, these solutions are expected to present relevant data, helping staff make fast, informed decisions.

While the problem of "too much data" exists at all levels of the organization, it's felt most drastically in operations. Companies are automating massive amounts of data, even though most can't yet translate it into useful intelligence. Even for the most skilled team, keeping up with the threat landscape, more and more complex IT environments, changing regulatory compliance mandates, and mounting security alerts is not easy. In response, many organizations have multiple cybersecurity teams, each focused on a different initiative.

Historically, coordinating these teams has been a challenge. But new security offerings can help orchestrate security activities, aligning workflows and automating shared objectives for faster, more effective results. A single platform also makes it possible to coordinate detection and response initiatives, supporting fast, seamless knowledge sharing across teams.

55% of respondents name detecting advanced threats as their top security operations challenge.[1]

A Framework for Automated and Orchestrated Threat Detection and Response

Security orchestration and automation requires integrating multiple technologies to stop, contain and prevent attacks. Where point solutions can be difficult to implement and hard to reconcile data from, integrated solutions offer a broad understanding of activity across the environment.

Early tools in this category had difficulty balancing speed and effectiveness. Automation can speed up repetitive processes and orchestration can automate decision-making, but until recently neither was able to go beyond mundane tasks requiring little or no intelligence. Today, effective orchestration still depends on analysts' knowledge of attackers' methodology. And because adversaries will try multiple routes to their goals, overly narrow security orchestration can be easy to circumvent.

Orchestration With—and Without—Intelligence

Today, the most effective, resilient and adaptive security choice is orchestration informed by intelligence about both threats and the environment. This intelligence-led approach informs orchestration strategy in two ways:

- It offers intelligence on adversaries' capabilities, attack patterns and intent, informing how you build and configure orchestration capabilities to defend your network.
- Orchestration playbooks can respond to internal and external threat intelligence, adapting to changing attack capabilities, patterns and infrastructure. In some cases, threat intelligence can trigger automatic process changes and drive further decision-making.

This approach also combines situational awareness and historical data to determine when and how each task is done. Intelligence makes it possible to adapt in response to a changing environment, while security orchestration helps organizations plan program improvements. And situational awareness and historical data help determine when and how each task is done.

Intelligence, Deconstructed

It's important to understand the meaning of "threat intelligence" in this context. It's often misunderstood as referring only to indicators of compromise (IOCs). These indicators are typically delivered through low-context data feeds. While IOC feeds have their place in defensive operations, they don't come close to encompassing all that threat intelligence can be. Most are best characterized as information, not intelligence.

Automation vs. Orchestration

It's not easy to speed up cybersecurity processes. And instead of focusing on identifying threats and prioritizing response efforts, too many teams are scrambling to keep up with an ever-growing lists of simple, repetitive tasks. Both automation and orchestration address this problem. The terms are often used interchangeably, but there are important differences.

Security automation is automating tasks (such as querying logs or managing user privileges) that would otherwise be done manually by cybersecurity professionals, much more quickly than a human could. Automation is a straight shot from A to B—it doesn't cover complex operations involving multiple decision points or systems.

Security orchestration is a holistic solution involving people, processes, technology and information. It coordinates multiple security tasks and decision points in one (often complex) process. It typically uses conditional logic and branched processes to connect and integrate security systems, applications and teams in streamlined workflows; correlates disparate data; and coordinates effective security responses.

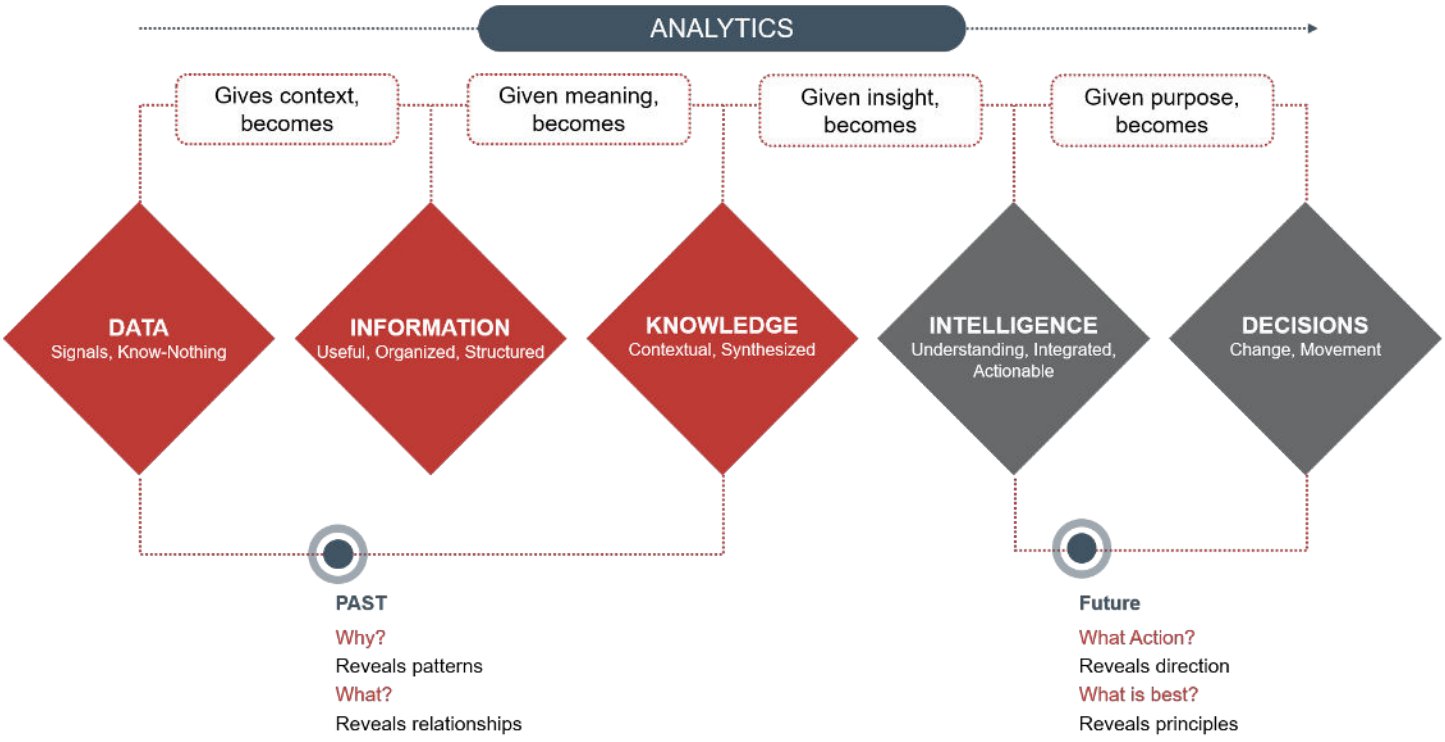
But intelligence is not raw data, and it's not just information. It's threat knowledge that can inform decisions and even support predictions. And threat intelligence does not exist for its own sake. Rather, it exists to inform operational, tactical and strategic security decisions.

The Intel-Ops Feedback Loop

While only some organizations have a threat intelligence analyst on staff, all use what they know about the threat space to inform operations, and the relationship between intelligence and operations is present in all security teams.

Intelligence and operations should be both cyclical and symbiotic. Intelligence informs operations decisions, which drive actions. Actions (e.g., cleanups, further investigations or other mitigations) beget data artifacts (lists of targeted or affected assets, identified malware, network-based IOCs, newly observed attack patterns, etc.). And these can in turn be refined into intelligence that informs decisions for future operations, creating a feedback loop.

Intelligence and operations should be both cyclical and symbiotic. Intelligence informs operations decisions, which drive actions.



Intelligence-Driven Orchestration: What to Look For

With all the value to be gained from intelligence-driven defense, why is it not available in every orchestration and automation solution? The answer lies in the organizational challenges that arise when disparate security functions, with varying levels of maturity, try to work together.

Such fragmentation happens whenever groups get too big or processes too complex—a common effect of growth. To deliver intelligence-driven defense in a fragmented environment, a security solution must address that fragmentation, using orchestration and automation to evolve threat intelligence across information, people, technology and process.

- **Information:** To translate information into usable intelligence, it must be correlated, enriched and contextualized. And to do that, you need to remove any silos segmenting relevant data, creating a common source of record. An intelligence-driven orchestration solution aggregates internal information, incident response (IR) investigation details, notable SOC events, and even curated intelligence from an in-house team.
- **People:** Functional teams within and around the security organization—including IR, SOC, intel, risk, and business and executive teams—need unsiloed access to information from other teams and from outside the organization. They should also be able to collaborate in a dynamic workflow. Your chosen security solution should support exchanges of tips and tasks across teams, create and funnel intelligence to relevant functional organizations, and report threats to relevant decision-makers. It may also facilitate or automate information sharing with supply-chain or community partners.
- **Technology:** Most organizations today have heterogeneous and disconnected point defenses; coordinating their actions means coordinating tickets between IT and multiple facets of the security team. A strong security solution should be able to coordinate intelligence-driven action and automation across an evolving library of applications and integrations.
- **Process:** Once you've removed the silos separating information, people and technology, the right platform should help you streamline processes, with playbooks that draw on both internal and external intelligence to inform human and technology actions. It should also be able to learn from past experiences and apply that learning in a range of scenarios.

A security solution must address fragmentation, using orchestration and automation to evolve threat intelligence across information, people, technology and process.

Buyer Beware

Many security orchestration products offer some level of security automation and orchestration. Often, they use intelligence to trigger specific workflows or enrich a particular context. Most don't enable adaption for future playbook runs or create new intelligence as an integral part of the workflow—setting themselves up to struggle in the four focus areas above.

Some threat intelligence platforms (TIPs) will let you aggregate external data feeds, create internal intelligence and even connect to defensive products using operational threat intelligence. While this is a great place to start, a solution should also be able to get the most value possible out of that intelligence it collects, through cross-team coordination and workflow orchestration.

Having It All

Only a single platform that brings together threat intelligence, orchestration, automation and response can support truly holistic insight, enabling you to:

- **Alert, block and quarantine based on relevant threat intel.** Even for lower-level tasks such as alerting and blocking, relevant threat intelligence is important. You can automate detection and prevention, but you need multisourced, validated threat intel to make sure you're getting alerts for, and blocking, the right things.
- **Increase accuracy, confidence and precision.** Situational awareness and historical context are key to decision-making. Working directly from threat intelligence allows you to work faster and prevent more attacks before they happen. The more you can automate up front, the more proactive you can be. By eliminating false positives and using validated intelligence, you take more accurate actions—which in turn improves speed and precision.
- **Understand context and improve over time.** Automate tasks based on threat intelligence thresholds (such as indicator reputation scores), then memorialize all that information—and you can strategically look at your processes and see how to improve.
- **Orchestrate with confidence.** Native sense-making analytics on external threat intelligence allows for more accurate alerts with fewer false positives, blocks and quarantines. Unfortunately, you can't just ingest lots of threat intel feeds or act from a shared IOC. You need to make sense of them at scale, using adaptable scoring and contextualization to drive action, and know whether action is needed.
- **Build organic intelligence from security operations and response.** Your team and your data are the ultimate intelligence sources. You want to be able to capture insights, artifacts and sightings from operations and response engagements, then immediately refine them into intelligence, in the form of new IOCs, adversary tactics and techniques, and knowledge of security gaps.
- **Adjust processes automatically as information and context change.** You should be able to adapt your orchestration capabilities to changing threat intelligence, automatically adjusting internal processes in response to indicator classification and threat assessment scores. Dynamically update these processes and workflows to make your team's efforts more relevant and effective.

A solution should be able to get the most value possible out of the intelligence it collects, through cross-team coordination and workflow orchestration.

Intelligence-Based Orchestration and Automation with NetWitness

NetWitness Orchestrator gives your security team the collaborative, threat intelligence-powered capabilities you need in a rapidly evolving security landscape, delivering intelligence in all aspects of security operations including orchestration and workflow. As part of the NetWitness Platform, it provides insight into massive amounts of information from multiple sources, identifies relationships among them, and learns from previous actions to generate a shared, easy-to-use, panoramic view of the threat landscape.

Clear reports in plain language help decision-makers communicate risk to stakeholders. And a combined NetWitness Platform workflow supports security operations planning and action—allowing team members to focus on the incidents that matter while speeding detection, investigation and remediation of potential threats.

Drawing on multiple software development kits (SDKs) and a community development app framework, NetWitness Orchestrator features more than 500 apps and integrations that enable countless security actions. Security analysts can use it to accelerate enterprise-wide threat detection and response with comprehensive data across logs, network, endpoint, security and nonsecurity solutions.

NetWitness doesn't just feed data to our customers' networks. Instead, we refine data from relevant sources, generating an intelligence service for security teams. Each of our services helps businesses integrate data, analyze it to add context and determine relevance, provide insights and recommendations, and—most powerfully—take immediate and appropriate action. And our SDKs and app framework make it possible for NetWitness Platform to align with any organization's operational or business requirements, and for our customers to grow with, and far beyond, our hundreds of supported applications.

NetWitness Orchestrator gives your security team the collaborative, threat intelligence-powered capabilities you need in a rapidly evolving security landscape, delivering intelligence in all aspects of security operations including orchestration and workflow.

Driving Performance with Analytics

NetWitness Orchestrator turns automation into a force multiplier. Push a button, or just accept behind-the-scenes enrichments, to make security operations or incident response investigations faster and more effective. Use artifacts and insights from those investigations to develop new intelligence, then rinse and repeat. Capture, record and measure the entire lifecycle to help you prioritize risk and drive team and process improvements.

Our range of integrations and automation capabilities help you optimize use cases including phishing email triage, infected host containment, SIEM detection and alert enrichment, intelligence report creation and sharing, and more.

NetWitness also makes it easy to figure out which processes or tasks are taking up the most time, and where efficiencies can be gained—then reduce time between compromise and detection, and between detection and remediation. The first step is to use NetWitness Orchestrator's reporting capabilities to record the time between key milestones—then analyze those metrics using any number of custom dashboards. Security operations and incident response teams often start with four basic metrics:

- **Dwell time by affected system.** This can be calculated as a mean time to detect (MTTD) for all incidents. There will likely be differences in the time it takes to detect intrusion attempts based on an adversary's targets, techniques, tradecraft and capabilities. Identifying these "time gaps" can help you prioritize closing certain holes in your detection.
- **Time from alert to triage.** Instead of measuring mean time from detection or alert, this metric identifies how long it takes, once alerts are triggered, to validate and initiate response.
- **Time to mitigation/containment.** How long does it take to bring those bad things under control? This is also known as mean time to respond (MTTR).
- **Time to close.** How much time, on average, between a case being opened and it being closed?

NetWitness Orchestrator also makes it easy to figure out which processes or tasks are taking up the most time, and where efficiencies can be gained—then reduce time between compromise and detection, and between detection and remediation.

A Focus on Values

Beyond just tracking the time between milestones, performance analytics should focus on specific values that matter to your organization—and support effective response. To optimize performance, consider tracking these five values:

- **Time to collect artifacts/evidence broken down by source or origin.** Understand where your information is coming from and how long it takes to get to you, and you can optimize your processes. Is gathering event logs from endpoints, for example, a bottleneck?
- **New intelligence created from operational or incident investigations.** A key part of the intelligence cycle is generating new intel from boots on the ground. Insights gained here can help identify processes or policies that need changing.
- **False-positive ratio on alerts.** Are wild goose chases more common on certain teams than others? With certain incident types? These time wasters can drain morale and reduce effort devoted to true threats.
- **Most active playbooks.** This is just good situational awareness. Where are my automations kicking off and providing value? Is there any anomalous activity—for example, broken or overactive playbooks?
- **Team workload and efficiency.** Understanding who's working on what (and how effectively) can help you identify team bottlenecks. Are you hitting due dates and SLAs? Is anyone overworked? Are we understaffed?

The above, of course, is just a sample of what you can do with NetWitness Orchestrator. Take the time to understand where your own teams, tools and processes falter, then start measuring and improving, and you'll continue to discover new things as the security landscape, and your organization, evolve.

Conclusion

As the threat landscape evolves and expands, security operations teams must stretch to keep pace. The more data that must be rationalized and correlated, the longer it takes to detect, investigate and remediate security incidents—and multiple point tools may be delivering diminishing returns. Orchestration and automation solutions can speed incident management, but without inherent threat intelligence they can flag far too many false positives and inconsequential events, wasting security analysts' time and energy.

Threat intelligence consists of far more than threat feeds. An effective security orchestration and automation solution must derive intelligence from information, people, technology and process. It must go beyond initiating playbooks and workflows, adapting in response to new learning from past events.

NetWitness Orchestrator uses collaborative, threat intelligence-powered capabilities to provide insight into massive amounts of information from multiple sources. It identifies relationships among the pieces, and learns from previous actions to generate a shared, easy-to-use, panoramic view of the threat landscape. The result is a shared, easy-to-use, panoramic view of the threat landscape. Clear reports in plain language help decision-makers communicate risk to stakeholders. From there, security operations can easily plan and act through a combined workflow within the NetWitness Platform. And a combined NetWitness Platform workflow supports security operations planning and action—allowing team members to focus on the incidents that matter while speeding detection, investigation and remediation of potential threats.

A combined RSA NetWitness Platform workflow supports security operations planning and action—allowing team members to focus on the incidents that matter while speeding detection, investigation and remediation of potential threats.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to **netwitness.com**.

1. **Threat Hunting 2018 Spotlight Report**, Crowd Research Partners, 2018.

NETWITNESS
An RSA Business