WHITEPAPER

ThreatConnect™

Intelligence-Driven SOAR:

What You Need to Know to Solve the Biggest Operational Challenges Faced by Cybersecurity Teams

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: +1.703.229.4489
www.ThreatConnect.com

Introduction

All too often, security operations teams are the unsung heroes of the modern enterprise. When their efforts are successful, they often go unacknowledged. Though security analysts and incident responders put in long hours at the console and experience high stress levels, business leaders don't always recognize the extent — or value — of their contributions. But a single instance of failure in the Security Operations Center (SOC) can have devastating and far-reaching consequences for the entire enterprise.

As a case in point, let's consider the widely-publicized breach that Target experienced in 2013. Payment card information belonging to more than 110 million of the retail giant's customers was compromised in an attack leveraging credentials stolen from a third-party vendor supplying HVAC services to Target. [1] Reports indicate that a state-of-the-art anti-malware solution from cybersecurity vendor FireEye was in place in the environment; it generated multiple alerts during the early stages of the attack, but these warnings were dismissed or overlooked in the overseas security monitoring center, located in Bangalore, India, that Target relied on for initial event triage. [2]

The total direct and indirect costs associated with the Target breach ultimately exceeded $300 million, making it one of the most expensive cybercriminal attacks in history. Target's final payment of $18.5 million to close the investigation into the causes of the breach made it into what New York Attorney General Eric Schneiderman called "the largest multistate accord ever reached over a data breach." [3] Target's stock value plummeted because of the incident, though they did eventually recover. The reputational damage that the retailer suffered, however, persists to this day.

---

1 "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet, Feb. 2015, https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

2 Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg, March 2014, https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

3 A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach," New York State Office of the Attorney General, Press Release Archives, May 2017, https://ag.ny.gov/press-release/2017/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

In the years that have passed since then, security operations (SecOps) teams' jobs haven't gotten any easier. If anything, security professionals are being stretched even thinner than before, with the number of unfilled positions in the field currently exceeding 3 million worldwide. Fifty-six percent of security leaders now believe that their organization faces moderate to extreme risks directly resulting from staffing shortages. [4]

Meanwhile, global cybercriminal activity continues to increase in volume and sophistication, with attackers opportunistically exploiting new vulnerabilities that the events of 2020 have brought about. These include cloud misconfigurations created because organizations were rushing to enable remote work at scale to cope with the coronavirus pandemic as well as gaps in monitoring coverage for hastily re-architected networks. Criminals are also looking to take advantage of increased consumer reliance on digital technologies such as videoconferencing and mobile banking.

Last year saw an unprecedented surge in ransomware attacks, with the average ransom paid by organizations in the U.S. growing from $115,123 in 2019 to $312,493 in 2020, a year-over-year increase of 171%. [5] JBS USA, the world's largest meat processing company, recently paid an $11 million ransom to the notorious Russian cybercriminal gang REvil.

Researchers also observed a worrisome uptick in nation-state level threat activity. They estimate that 'significant' state-sponsored cyberattacks increased by 100% from 2017 to 2020, with attacks becoming more frequent, techniques more varied, and attackers more brazen over the course of that period. [6]

The result of these trends is all too familiar: ever-larger breaches continue to make headlines, increasingly destructive critical infrastructure attacks abound, and intellectual property theft is costing enterprises billions of dollars. In the face of today's threats, worldwide spending on cybersecurity products and services continues to increase, too. Research from Gartner predicts that spending in this category will grow by 12.4% to reach $150.4 billion per year by the end of 2021. [7] Yet all this spending isn't enough to turn the tide.

The reality is that the fundamental paradigm underpinning how cybersecurity works in the modern enterprise is broken.

The good news is that the systemic issues that continue to prevent SecOps programs from being as effective as they need to be have been identified. Security leaders across industries broadly agree upon the fact of their existence. There's also widespread consensus about the urgency of solving these problems.

Today's business and security leaders are aware that they're challenged by:

- The increasing sophistication of cyberattacks and cyber adversaries
- A critical shortage of skilled cybersecurity professionals
- A lack of threat intelligence and operational information-sharing
- The inability to assess, communicate and manage the financial impact of cyber events — and thus the business risk to the organization
- Underinvestment and a lack of buy-in from the business as a whole

---

4 (ISC)² Cybersecurity Workforce Study 2020, (ISC)², https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

5 Ransomware Threat Report: 2021, Unit 42 at Palo Alto Networks, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf?utm_source=marketo&utm_medium=email&utm_campaign=2021-05-10%2015:30:22-Global-DA-EN-21-03-05-7014u000001ZIEtAAO-P3-Cortex-unit-42-ransomware-threat-report

6 Nation States, Cyberconflict and the Web of Profit, Dr. Michael McGuire, Sr. Lecturer in Criminology at the University of Surrey and HP Wolf Security, https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf

7 "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021," Gartner Newsroom, May 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

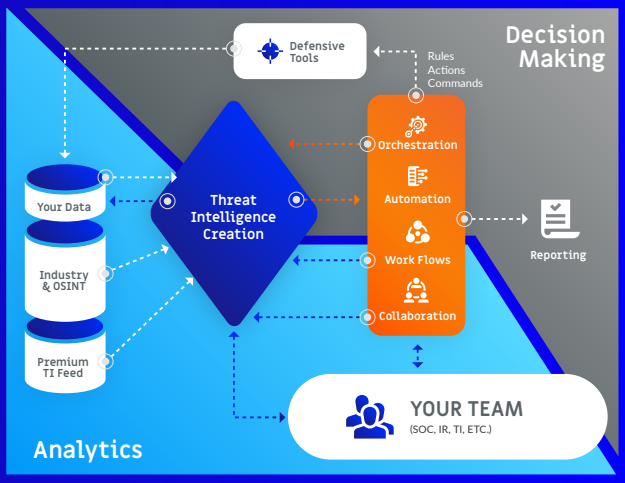
The second piece of good news is that it's now possible to find a real answer for these long standing issues. What's needed is a new approach, one that prioritizes real-world risk mitigation — so that SecOps teams can concentrate their efforts where they'll have the biggest impact. In a world where there's too much data and too few resources, it's essential to implement intelligence-driven solutions that will enable security analysts to focus on what matters most – so that they can build sustainable processes that make their daily workflows more manageable.

The right security orchestration, automation and response (SOAR) platform is an essential technology underpinning this approach. SOAR makes it possible for SecOps teams to rapidly respond to the greatest operational risks their enterprise faces, and to do so from within a single, centralized hub that houses all the processes and workflows, related insights and intelligence, and necessary reporting capabilities they need to collaborate successfully. This saves time and labor by reducing the high volumes of decontextualized alerts with which most SecOps team members are inundated, simplifying the triage process and eliminating repetitive manual tasks. For the individual analyst, the end result is that there's less frustration and burnout – and a greater sense of job satisfaction.

How ThreatConnect Built a Smarter SOAR: Fusing Intelligence, Automation and Orchestration

ThreatConnect has long been known as a leader in the Threat Intelligence Platform (TIP) market. But we were never just an intel feed. In fact, our history of gathering global threat intelligence gave us a unique perspective on exactly why it's so important to integrate threat intelligence into SecOps workflows, and how great the need currently is for unified systems that can launch automated responses to current, real-world risks.

That's why we added SOAR to our platform in 2019. The term was coined by Gartner in 2015, but the market category arose in response to a near-universal need that had existed long before that: to better integrate security technologies' capabilities with human security analysts' and incident responders' needs, and to introduce the most useful automated workflows.



Because of our unmatched TIP capabilities, we were able to incorporate current, accurate and highly relevant information about the threats that matter most into an intelligence-driven platform that can unify the activities of the entire security team. When provided with this sort of intelligence, SOAR enables SecOps professionals to prioritize effectively, so that they can train their attention on the most significant risks.

The Need for Better, Smarter, More Effective SecOps

Global cybersecurity spending continues to grow at a record pace, eclipsing investments in many other areas of technology, risk management and operational infrastructure. And this is taking place even though few SecOps programs are achieving the meaningful and demonstrable results that Chief Information Security Officers (CISOs) are hoping to see. Why does this problematic trend persist?

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

"...the cybersecurity industry has created an untenable situation for the skilled professionals who staff today's security operations centers."

A big part of the answer lies in the fact that security leaders often can't communicate risks effectively to the business, especially in the quantitative and financial terms that are most important to accurately convey their scale. This inability gives rise to misplaced spending, as well as underinvestment in the areas that matter most. Ultimately, it leads to a widening disconnect between security and the business.

In today's world, building and maintaining a SOC is incredibly expensive, and creating a top-performing one costs even more. According to research conducted by the Ponemon Institute, the average annual cost for staffing and maintaining an enterprise-grade SOC in 2020 was $2.86 million, but a SOC that was rated "highly effective" cost an average of $3.5 million per year to operate. One whose effectiveness was rated "low" cost only $1.9 million per year. The largest line-item expenditure involved in maintaining a SOC is security analyst salaries. On average, a Tier 1 analyst was paid $102,315 in 2020, and salaries are expected to increase 29% in the coming year. [8]

Tool sprawl is also driving costs upwards without consistently contributing to SecOps teams' effectiveness. The average enterprise is now running 45 different security tools and technologies, but those that have more than 50 solutions in place are actually rated 8% less able to detect a cyberattack — and 7% lower in their ability to respond — than organizations using fewer than 50 tools. [9] Past a certain point, adding more tools to the security technology stack increases complexity, adding more dashboards that must be monitored, and more disparate data that must be correlated, without giving security analysts centralized visibility or a better understanding of what to prioritize.

Adding more technologies also leads to overwhelming increases in data volumes and alert numbers, decreasing SecOps teams' capacity to triage and respond to these alerts, especially when they're dependent upon manual processes for doing so. According to one recent survey, 54% of organizations collect, process and analyze more than six terabytes of security data on a monthly basis. [10] There's simply no way that humans can be counted on to distinguish a signal indicating true malicious activity from the noise of endless event streams.

The result is that the cybersecurity industry has created an untenable situation for the skilled professionals who staff today's security operations centers. High stress levels and excessive job turnover are endemic among security analysts, who continue to be in high demand and short supply. In a survey of security analysts conducted by the Cyentia Institute, more than 25% of respondents expressed dissatisfaction with their current position and one-third were currently looking for another job. Tellingly, 28% had never stopped an actual intrusion or couldn't remember having done so.

---

8 The Economics of Security Operations Centers: What is the True Cost for Effective Results?, Ponemon Institute,https://d53g0hkpcf8eh.cloudfront.net/wp-content/uploads/Ponemon-Report-The-Economics-of-Security-Operations-Centers.pdf

9 Cyber Resilient Organization Report 2020, IBM Security, https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/pdf

10 ESG Research Report: Cybersecurity Analytics and Operations in Transition, Enterprise Strategy Group, https://www.esg-global.com/research/esg-research-report-cybersecurity-analytics-and-operations-in-transition

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

The most valuable resource in SecOps: Security professionals' attention

The lesson is clear: there's an overwhelming need to better allocate the one resource – human attention – which is of the highest value and in shortest supply in today's security operations programs. Enabling security analysts to become more effective and to see evidence that their labors have borne fruit is key for increasing job satisfaction and retention rates among security analysts and incident responders.

To do so, we must:

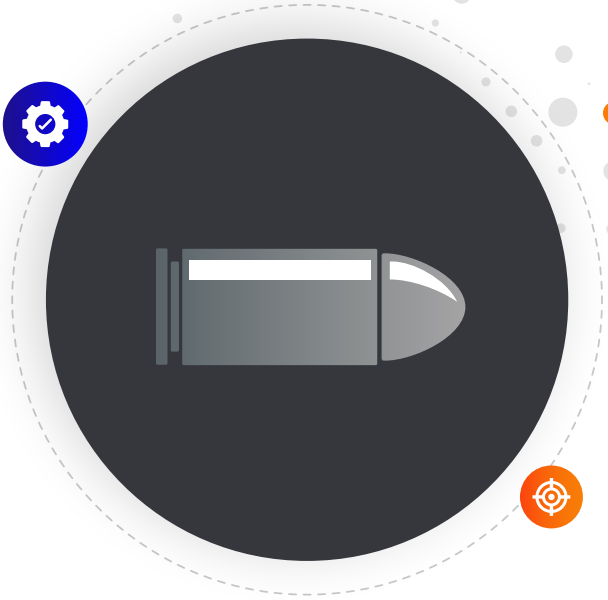
- Use automation to replace the most common and repetitive manual workflows
- Increase contextual awareness to improve speed and accuracy of event triage and incident response
- Improve processes and document effectiveness so that analysts can better understand where they're making an impact

XDR isn't the silver bullet we'd been hoping for

Extended detection and response (XDR) is an emerging category of security solution that's recently attracted a great deal of attention in the marketplace. Gartner defines XDR as a set of Software-as-a-Service (SaaS)-based tools that automatically collect and correlate data from multiple security products into a single, cohesive security operations system. [11] The goal is to improve threat detection and bolster incident response capabilities.

XDR expands upon the concept of endpoint detection and response (EDR) by augmenting an EDR solution's capabilities to provide visibility across the whole of the network and cloud infrastructure. Tacitly, the "X" in XDR acknowledges that merely considering endpoints is inadequate to secure a large and complex computing ecosystem.

The core premise behind XDR — expanding logging, coverage and monitoring attention beyond the endpoint — is absolutely essential for effective SecOps in today's world.



XDR enables:

- End-to-end analytics across hosts and networks at an unprecedented level of granularity
- Speedier detection and investigation across complex distributed, hybrid environments
- Security teams to collect enough data and evidence to detect even the most covert operations conducted by highly sophisticated adversaries

Currently, XDR is primarily marketed by security vendors that have their own portfolio of security and infrastructure protection products and is managed by its own offerings. But ideally, many organizations use multiple security products, like firewalls, IDPs, and EDR, from different vendors. These products are typically installed over time and operated by different individuals and teams. So XDR lacks the option to integrate with existing infrastructure to improve the efficiency of existing SOC teams.

The strength of individual SOAR products, on the other hand, lies in integrating with existing infrastructure and enhancing the SOC automation capabilities for better quality intelligence and faster remediation of alerts.

[11] "Innovation Insight for Extended Detection and Response,"Gartner Research, https://www.gartner.com/en/documents/3982247/innovation-insight-for-extended-detection-and-response

Solving Real-World SOC Challenges with Intelligence-Driven SOAR

In a world of ever-growing data volumes and increasingly sophisticated threats, how do we help security analysts and incident responders focus on what matters most? How can we unite teams so that they can build robust and effective processes to eliminate wasted effort and accelerate response times? What will enable SecOps teams to prioritize accurately and consistently?

The answer is intelligence-driven SOAR.

By definition, SOAR solutions combine **automation** and **orchestration.** Automation involves creating standardized, repeatable, automatically-executed processes to handle tasks (such as querying logs, creating a ticket, or running a vulnerability scan) that would otherwise be performed manually. Orchestration involves bringing together multiple, disparate security tasks into a single, coordinated response workflow, which usually incorporates conditional logic so that it can manage decision points.

Intelligence on adversarial capabilities, attack patterns and strategies can be built into the logic that enables orchestration to defend your environment. When intelligence is incorporated into a SOAR solution, each decision is made on the basis of current information about how today's real-world adversaries are most likely to act. Incorporating internal and external threat intelligence can allow the orchestrated process to automatically adjust itself. This creates an ongoing feedback loop that supports better and better decision-making.

Using intelligence and orchestration together makes it possible for the platform to make decisions based on current situational awareness and historical patterns. This way, decision-making is both informed and adaptive, enabling security operations and incident response teams to solve real-world problems dynamically. Once threat intelligence has been used to drive orchestrated actions, the result of those actions can be used to create or enhance further threat intelligence.

This intelligence-driven feedback loop empowers SecOps teams to work smarter not harder, so that they can make better operational decisions and find the most effective strategies. When resources are scarce, it's imperative that security teams find and use technologies that will help them streamline processes to reduce the complexity of their jobs.

Here are five ways that an intelligence-driven SOAR platform can help your SecOps team manage today's challenges:

1

As threats grow in frequency, complexity, and diversity – and as your attack surface increases – you'll be better able to prioritize, so that your team can focus on the most pressing issues first.

The current reality is daunting: attacks continue to increase in volume and sophistication. And as threats diversify, it's essential to add more tools and monitoring capabilities to protect your infrastructure, increasing the complexity of your security stack and the amount of data it generates. To manage this situation, your security strategies, tools and processes must all be designed to operate at an accelerating tempo and to handle more and more incoming data.

If all this data is to provide value, however, it must be usable for monitoring, analytics and decision-making purposes. It must be possible to separate the signal from the noise, so that only the most relevant information is highlighted. And the number of distractions — false positives and uncorrelated events — must be reduced. To accomplish this aim, it's essential to create a centralized collection and analysis hub where information is gathered automatically, and where relevant threat intelligence is used to determine what's most important.

An intelligent SOAR platform can serve as this central hub, supporting operational decision-making by assembling data from pre-existing security technologies in one place where it can be synthesized, correlated and tracked. Instead of becoming a bottleneck that leads to growing numbers of false positives — and overwhelmed security analysts — additional data then becomes a means of increasing detection accuracy. This makes event triage and incident response much more manageable. It also makes it possible for the security tools you've already implemented to finally deliver the value that they initially promised.

For example, one of the world's largest financial institutions was able to reduce several hundred million SIEM events per month to a dozen by leveraging ThreatConnect's intelligence-driven SOAR. Implementing SOAR enabled their team to cultivate predictable response patterns, saving time and prioritizing their efforts.

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

In order to work in this way, a SOAR solution must be able to integrate seamlessly with the existing tools in your environment in order to transform them into high-value information sources (rather than extra consoles to monitor).

> Having a complete understanding of your operating environment is what allows you to move with the depth and breadth of a larger force and the agility and speed of a small team. It's a force multiplier."
>
> – Jack Boss, ex-Navy SEAL and CEO of Momentive

2

Because SOAR serves as a force multiplier for smaller teams, you'll be able to accomplish more with fewer resources, a must-have given the extent of the current cybersecurity skills gap.

Because SOAR makes it possible to create repeatable playbooks, automated processes and structured workflows, it enables SecOps teams to reduce the number of manual steps they must perform during their day-to-day responsibilities. Actions can be completely automated — requiring no human input whatsoever — or configured to run when an analyst or incident responder deems them necessary. In either case, the end result is that small teams can accomplish much more in less time.

Removing mundane tasks from SecOps jobs will give skilled professionals more time to spend on higher-value activities. This increases cognitive engagement, feelings of productivity and job satisfaction. When security analysts believe they're actually "stopping the bad guys," they're less likely to experience burnout, and more likely to remain with the same employer for longer periods of time.

And in the cases when employees do leave, you'll be able to get new hires up to speed much more quickly. The fact that processes and workflows are structured and repeatable means it's easier to teach them to incoming analysts. It also means that the entire team can work to a higher standard.

Improving Automation and Orchestration with Playbooks 2.0

Our recent release of ThreatConnect 6.2 introduces a new Browser Extension and Playbooks 2.0 for improved ease of use and collaboration.

When we think of "collaboration" we usually think about groups of people working together, maybe from different teams, to achieve a common goal. In cybersecurity, that may mean the threat intelligence team provides much-needed context to the SOC, or the SOC team feeds telemetry back to generate new intel. ThreatConnect 6.2 covers that use case, but there's also so much more to collaboration. Software can work together, too, like when a detection rule is sent to the SIEM, which triggers an alert, which queries some data, which initiates a block action.

ThreatConnect 6.2 gives our customers access to our new Browser Extension, allowing anyone on the security team to benefit from rich, contextualized threat intelligence from any web page or SaaS tool. If your SOC needs intel at the moment of an investigation, this is it: next-level collaboration between intel and ops. 6.2 also includes a total revamp of our Playbooks capability, giving you more power and flexibility to get your tools talking to each other: it's collaboration via automation. Interactive Playbooks allows anyone on the team to get up and running collaborating with another Playbook builder.

Using a platform like ThreatConnect and changing how security works starts by creating a foundation of collaboration between teams and tools, and ThreatConnect 6.2 makes it easier than ever.

The automation and orchestration of security processes greatly benefit organizations of all types and sizes and clunky usability and difficult management are oftentimes blockers to implementation. Utilizing Playbooks to handle the creation of these automated workflows across different teams and technologies sometimes falls to a specific individual or two with the subject matter expertise required of Playbook Building.

Playbooks 2.0 is the next generation of playbook capabilities, and is the result of understanding the intricacies and nuances of the Playbook Building process, removing complexities, and replacing them with enablers to make repeatable and scalable automation a reality.

This release introduces nearly 50 improvement and updates to the Playbook Building and Management process, all with the following goals:

- Revamped look and feel increases usability and decreases frustrations
- Improved management capabilities for better collaboration, visibility, and control
- Increased confidence in the Playbook Build with more granular resting and improved troubleshooting
- Easy-to-use mechanism for documentation and collaboration with interactive note-taking capabilities

With Playbooks 2.0, we are changing what's been deemed acceptable and giving users the ability to feel more comfortable and confident during Playbook development – eventually increasing usage of automation and orchestration and empowering more individuals across the team to utilize Playbooks. Across those nearly 50 new capabilities, the following highlights some of the improvements users will experience include:

- Ability to collaborate easier across teams through notes with Interactive Playbook and improved Playbook sharing capabilities
- Understand how your playbook build is going with the ability to run tests at the App level and not at the time of completion – saving users from the time and frustration that comes with thinking you're done something and having to start over or go back and fix things
- Proactive notification of playbook failure, giving you confidence that things are running smoothly and you don't have to do status checks to know that constantly

3

> To reduce the load on our security and IT staff, we introduced over 60 workflow automations with ThreatConnect Playbooks. This ultimately saved us over $1.3 million per year in labor costs."
>
> – CISO in a large healthcare organization

Strong workflow and process management capabilities enable SecOps teams to save time while enhancing effectiveness.

Intelligence-driven SOAR makes it possible to improve processes and workflows across the entirety of the incident lifecycle. Automated and templatized workflows can enable resource-constrained teams to make threat hunting a reality, while threat intelligence and process orchestration can reduce the amount of time that analysts spend on each alert — as well as shrinking the amount of time they waste on false positives.

Because it leverages current threat intelligence, a solution like ThreatConnect's SOAR will automatically improve detection accuracy. The events that have the highest statistical probability of being malicious will be prioritized by default. And automating analysis of and response to the most common attack techniques will reduce dwell times and speed mean time to recovery (MTTR).

In addition, SOAR supports comprehensive and unified incident response. It helps teams coordinate activities that are handled by different people within the SOC, improving information-sharing and overall efficiency. And because a SOAR platform like ThreatConnect's includes hundreds of pre-built blueprints for Playbooks based on the most common real-world use cases, it enables you to leverage the expertise of hundreds if not thousands of security analysts and incident responders the world over.

A SOAR is only as strong as the teams, data and processes that fuel it. The more processes that a SOAR houses, the more of a force multiplier it will become, and the more predictable, adaptable and effective the entire security program will become.

4

With intelligence-driven automation and orchestration, your entire SecOps team will be able to make better decisions about how to allocate their time and attention, increasing efficiency.

Security leaders are broadly aware of the value of high-quality threat intelligence. They know that it drives better outcomes, and fosters improved decision-making. Not all are aware, however, of what it takes to transform raw threat intelligence into better real-world outcomes. This is where intelligence-driven SOAR comes in. It's the missing link in many SecOps programs.

SOAR enables the seamless merger of machine automation and human ingenuity to bring out the best aspects of both. It reduces the time it takes to figure out how threat intelligence relates to event data patterns, and speeds time-to-insight for security analysts and incident responders. After all, intelligence is only valuable if it drives the right action, and action is only meaningful if it's timely and effective. Intelligence-driven SOAR enables SecOps teams to prioritize effectively, so that they can invest their time in examining the problems and evidence that are most likely to be meaningful.

Real-World Results: ThreatConnect's SOAR Increases Efficiency for our Customers

In actual deployments, we've found that intelligence-driven SOAR is able to:

- reduce MTTR by 90%
- save thousands of hours that would normally have been spent on repetitive manual tasks
- reduce the burden on analysts by more than half
- lower operational and labor costs

How Threat Connect Helps

Below are actual results acheived by ThreatConnect customers during their first year of adoption

Resolves alerts faster
Average single alert resolution decreased from 30 minutes to 3 minutes significantly reducing MTTR.

Automate Repetitive Tasks
Repetitive analyst actions automated across 40 Playbooks to save 100's of hours previously spent on tasks like manual lookups and notifications.

Prevent Employee Burn Out
A reduced burden on analysts by 50% in the first year – decreasing burnout and attrition.

Save Time and Money
Over $1.3 million per year saved in labor costs with 60 automated workflows.

5

Intelligence-driven SOAR makes it possible to provide documentation and metrics that business leaders can readily understand.

When a SecOps team is highly successful, the result is zero downtime — something that no one in the business notices. When you're able to create metrics around how well you've achieved specific outcomes, however, you can transform security operations professionals from unsung heroes to meaningful contributors to risk mitigation and business value.

A SOAR platform that delivers targeted metrics — showing, for instance, the number of attacks blocked, mean time to detection (MTTD), mean time to recovery, or how far attacks have progressed at the time of their containment — can provide invaluable evidence that security leaders can draw upon when discussing risks and results with business stakeholders. This facilitates more meaningful conversations and contributes to the creation of a common language that can elevate security from a cost center to an essential safeguard of brand reputation and operational continuity for the business.

SOAR's Role in the Risk, Threat, Response Paradigm

Bringing together capabilities across the entirety of the incident lifecycle and SecOps workflow makes it possible to achieve results that would otherwise be unattainable for security teams. In particular, by combining risk quantification (RQ), TIP and SOAR capabilities within a streamlined and powerfully integrated product portfolio, ThreatConnect is enabling SecOps teams to:

- Reduce operational complexity
- Make decision-making easy
- Unite processes and technology
- Continually drive down risk
- Multiply their defenses (and effectiveness)

The Risk, Threat, Response paradigm makes it possible for SecOps professionals to concentrate their time and efforts in the areas where they'll have the biggest impact. First, they identify and scope the scenarios that pose the greatest financial risks to the business. This process is supported with an accurate, current understanding of the real-world threat landscape. Then, SOAR allows the team to unify and streamline processes and orchestrate responses across the entire technology stack. This approach resolves what were once competing priorities into a set of clear directions, giving the business a north star focus and showing it where to head next.

IV.

ThreatConnect SOAR At-a-Glance

ThreatConnect SOAR enables every member of the SecOps team to optimize processes and workflows, increase efficiency and accelerate response by augmenting their capabilities with intelligence-driven automation and orchestration.

ThreatConnect's SOAR platform is like the brain — or central nervous system — of your security operations program. Not only does it provide comprehensive decision-making and operational support capabilities, but it serves as a central place to integrate your security tools and your core processes. It facilitates extensive process documentation, and enables you to multiply efficiencies by leveraging automation and orchestration. Because ThreatConnect SOAR incorporates high-confidence threat intelligence, it helps your team make better decisions about both tactics and strategy. It also enables you to automatically incorporate the results of your decision-making into an ongoing feedback loop that was purposefully created to support continuous improvement.

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

What You Get with ThreatConnect SOAR

High-Confidence Intelligence

You receive access to various pre-populated intelligence sources, packaged in a digestible and easy-to-use format. Because this intelligence is baked into the solution, there's no need for complicated data manipulation or time-intensive lookups. All the intelligence is converted into a predictable and easily understood format but still preserves the source's attribution information and reputation details.

Decrease Ambiguity to Make More Confident Decisions

You can make better decisions that are based on the high-fidelity intelligence that's most relevant to your individual organization. And decisions can be adjusted on the fly, based on changes in the intelligence that's driving the process. This process can be automated, to ensure that the very latest intelligence consistently informs all decision-making.

Seamless Integrations with Existing Tools for More Efficient Processes

Integrations with the tools and technologies that are already in use within your security ecosystem will make your job easier. Whether you'd rather use pre-built templates or fully customized workflows, ThreatConnect supports the integrations required for your use case.

Minimize the Time Analysts Spend Looking for Relevant Information

Relevant information can automatically be saved as Artifacts for future analysis and use. You can also leverage data from ThreatConnect's Collective Analytics Layer (CAL) to gain additional insights from thousands of ThreatConnect users around the globe. This gives you more intelligence on the latest threat actor tactics, techniques, and procedures to help you identify malicious activity faster. You can also contribute Artifacts to ThreatConnect's intelligence repository to help other security teams during future investigations.

Correlate Critical Intelligence with Events to Reduce the Risk of Overlooking Important Associations

ThreatConnect automatically alerts you to known or potential associations between threat intelligence and previous or open investigations. This gives you insight into relationships between events, data, and associated threats — before you even ask for it.

Flexible Deployment Options

ThreatConnect SOAR can be deployed in the cloud or on-premises to get you up and running quickly, the way you want. Multi-Environment Orchestration allows for orchestration across cloud, multi-cloud, hybrid or on-premises environments. No matter where your security tools and controls reside, ThreatConnect will integrate them seamlessly.

Conclusion: Changing the Game in Security Operations

Gone are the days when SecOps teams had no choice but to act on the basis of uncertainties, deliver uncertain results, or struggle to show the business the value of their actions. Instead, today's defenders should be ready to assume their rightful place at the helm of enterprise risk mitigation — and to act with the self-assurance and confidence that accurate threat intelligence makes possible.

Intelligence-driven SOAR is an essential technology that's providing the foundation for more efficient, more effective and smarter security operations.

It's doing so by enhancing visibility into the threats that matter most, enabling security analysts to hone in on the alerts and events that are most deserving of their attention, and making it possible for incident responders to move with speed and purpose. At the same time that it serves as a force multiplier for SecOps teams, intelligence-driven SOAR is also empowering them to demonstrate their true value to the business. When it comes to ROI, there's no way to lose.