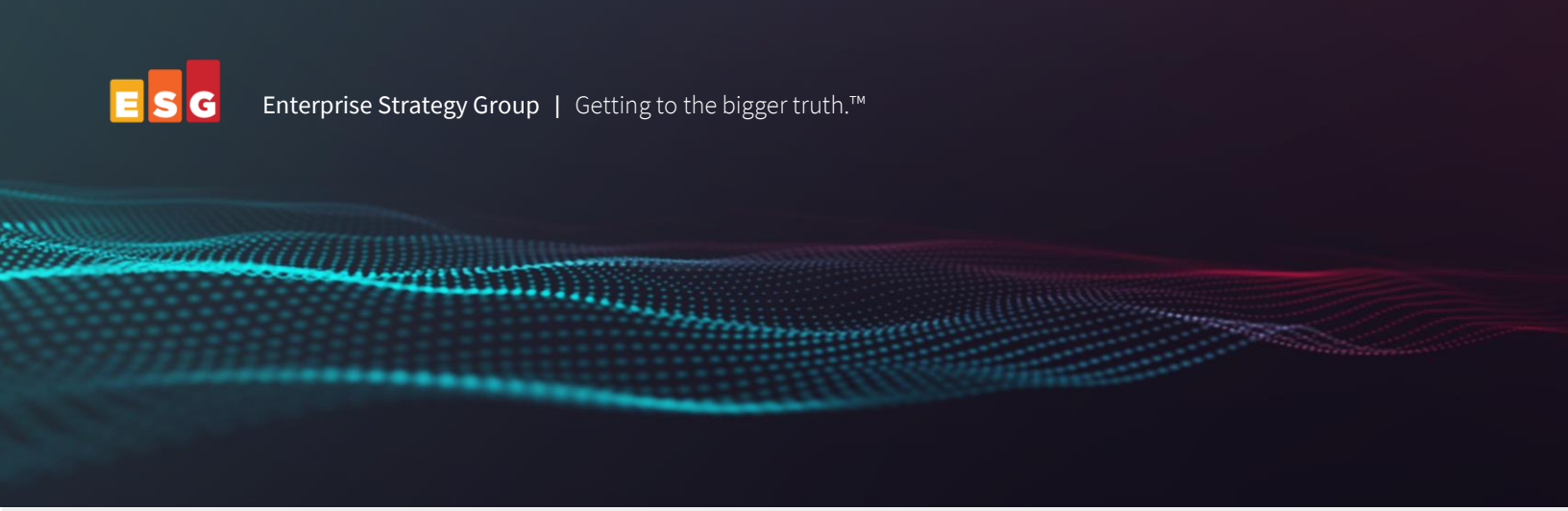


ESG WHITE PAPER

Managed Security Services Automation: The Formula for Profitable Growth

Accelerating MSSP Success with Cortex XSOAR by Palo Alto Networks

By Kevin Rhone, Practice Director; and Sallie Martin, Senior Consultant
ESG Channel Acceleration

September 2020

This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from ESG.

Contents

Introduction: Opportunity in the Evolving Managed Security Services Environment

During Q2 2020, ESG conducted partner-based primary research to uncover key business issues for managed security service providers (MSSPs) with practice leads and security operations center (SOC) managers responsible for the strategy and long-term success of their firms.[1]

This research features deep-dive qualitative interviews with 14 MSSPs in the North America, EMEA, and Asia-Pacific markets, and was designed to uncover the key business issues MSSPs face and the benefits of investing in automation tools on SOC operations, specifically the effect that Palo Alto Networks (PANW) Cortex XSOAR security, orchestration, and response platform has had on their overall business.

We asked participants to share their investments, experiences, and vision for the future, including where they think the best opportunities lie for their business to grow and prosper, and how they plan to leverage the Cortex XSOAR platform in the future to enhance their success. Results summarized in this paper provide guidance to MSSPs, including how to evaluate security, operations, and response (SOAR) options, and priorities that partners should consider in order to deliver continuous customer value.

Key Findings on Benefits of Cortex XSOAR Paint a Compelling Picture

Today's IT is defined by multi-cloud environments, and the applications and associated data they produce, manage, and store. Security is at the forefront in the world of application-driven outcomes, and MSSPs are increasingly using SOAR platforms to provide the expertise and resources to help secure transformative customer environments.

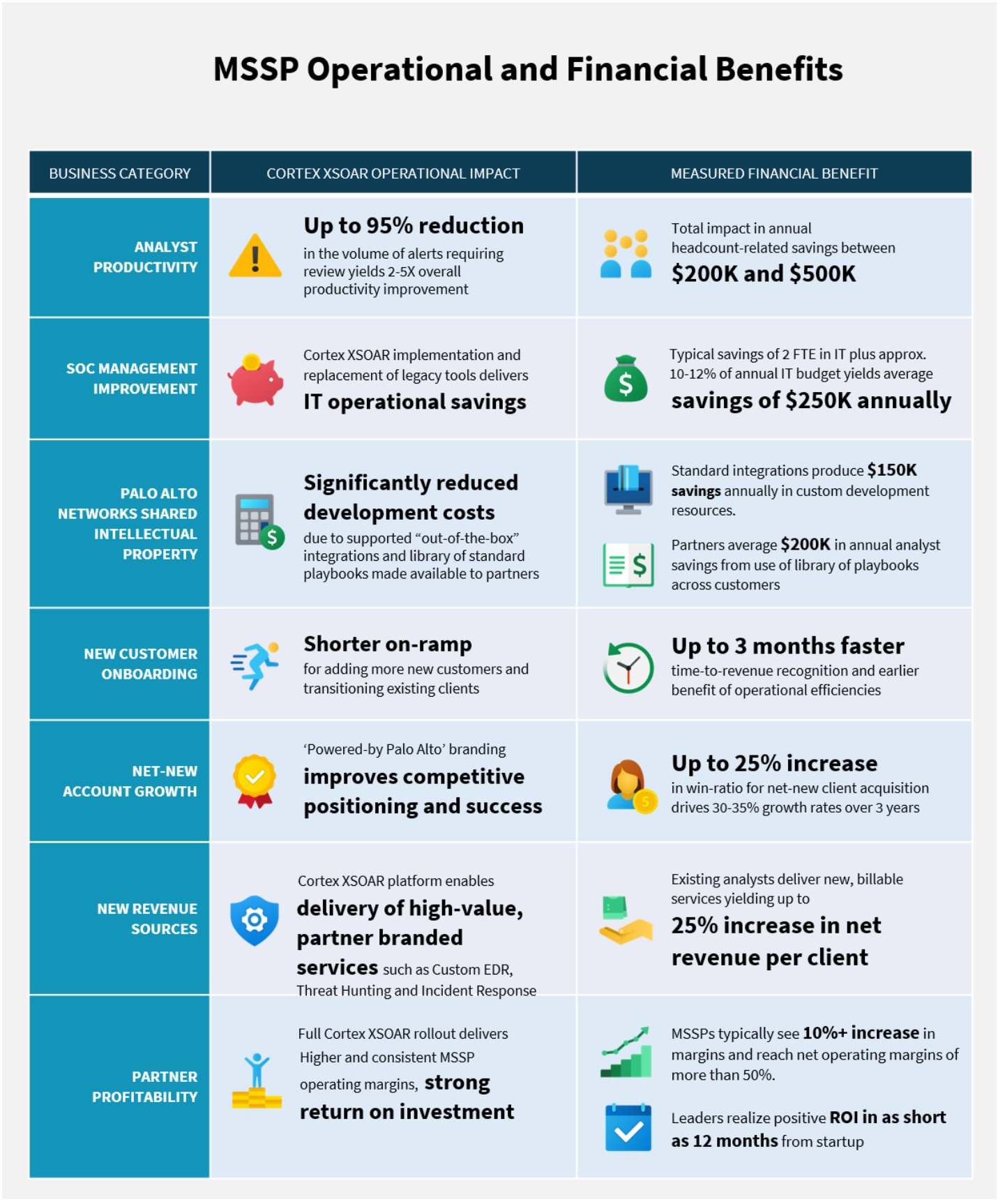
Cortex XSOAR is a single platform that orchestrates actions across the entire security product stack and enables faster and more scalable incident response. MSSPs can streamline processes, connect disparate tools and automate manual, repetitive tasks that don't require human intervention. MSSP SecOps teams have used Cortex XSOAR to automate up to 95% of all response actions, enabling their analysts to focus on the critical incidents that require their attention.

Our research found that the Cortex XSOAR (XSOAR) platform delivered quantifiable value to MSSPs, highlighting:

- Up to 90% of tickets are typically automated by the end of the first year
    - Translates to 000s of items at scale
    - 30% reduction of resources for Level 1 support that is now automated
    - Up to 5x efficiency reported for routine tasks
    - Up to 2x overall productivity reported
- Analysts can now deliver high-value services at increased margins of up to 25% increase in net revenue per client through a range of services:
    - Custom managed detection and response (MDR)
    - Threat hunting
    - Phishing-as-a-service (analysis)
    - Custom incident response work

[1] Please note that due to the qualitative nature of this study and its small sample size, the research herein should be considered anecdotal and used in a directional manner.

Figure 1. Economic Impact at a Glance: What SOC Leaders Need to Know



Source: Enterprise Strategy Group

With this type of positive impact to their business, SOC leaders easily justify rolling out the platform in order to optimize their MSSP operations, and innovative MSSPs gravitate to best-in-class vendors like Palo Alto Networks that provide resources and tools to get the job done. With Palo Alto Networks, this starts with rock-solid technology and then goes beyond just the tech with programs architected to help partners adjust and maximize their business models, build high-margin service-led offerings, and generate net-new and recurring revenue sales to drive sustainable bottom lines.

The Changing Work Environment and Opportunity It Creates

Shifting work patterns are radically altering businesses worldwide, and most observers believe this will force short-term adjustments and may produce long-term change and opportunity. As businesses look to the future, they must adapt to these changes, especially the introduction of the demands of securing the remote workforce. As a result, businesses and the IT pros that support them are looking to new operating models that are designed to protect against risk by relying on MSSPs to improve business resiliency and operational flexibility.

MSSP executives navigating this new world need a roadmap that helps them equip their SOCs to operate remotely, and to focus on the opportunities ahead. This paper is designed to provide a view into the future for partner executive leaders who are adapting themselves and their organizations to prepare for the future.

Top Components of MSSP Economic Value

Key findings from our study point to a range of benefits for MSSPs that have adopted the Cortex XSOAR platform.

#1 – Operational Savings and Efficiency

Improved efficiency was the top factor that interviewed MSSPs used for their investment decisions, which were almost always justified based on projected productivity and efficiency improvements. These savings can be summarized in terms of impacts on "back-of-house" IT savings and "front-of-house" impacts like faster customer onboarding and consistency of service delivery.

Examples:

- Reduced costs by 10%+ versus maintaining legacy software and systems
- Significantly reduced development costs due to supported "out-of-the-box" integrations
- Reduced need for staff to provide Level 1 support/ticket handling
- Shortened time to revenue due to rapid customer onboarding to the new platform
- "Soft benefits" that accrue as a byproduct of efficiency and reliability:
  - More predictable pricing yields competitive edge
  - Repeatability and consistency of high-quality delivery

> **"It will cost less than continuing to maintain our legacy internal tools…My estimated margin (including cost of tools) moved up at least 10% and this flows right to the bottom line."**
>
> - MSSP Director – EMEA

#2 – Improved Analyst Productivity, Skills, and Customer Value

ESG found positive impact on how analysts at the organizations we interviewed spent their days, the activities they performed, and the ways in which automation of massive amounts of data enabled them to add value to their customers. With up to 95% reduction in the volume of alerts requiring review, analysts' day-to-day activities were transformed, and the benefits accrued to both the individual analysts and the MSSP operations leaders.

Examples:

- Freedom from routine tasks/ticket handling such as sifting through volumes of data in search of true threats
- Scalability to serve more customers and endpoints with the same number of analysts
- Using standard, available playbooks, analysts can develop their own partner use case libraries across customers and workloads, saving time and money
- Improved analyst job satisfaction, which positively impacts recruiting, retention, and motivation

#3 – Expanded, Incremental Revenue Opportunities

"Cortex XSOAR builds better analyst teams."

- MSSP Director – North America

Cortex XSOAR impacts overall team performance:

- Analysts are not just following/tracking events
- They are guided to take on more complex tasks
- They enjoy greater quality of job and role satisfaction
- They are identified and rewarded as top performers

While most MSSPs we interviewed justified their investment in Cortex XSOAR based on the savings and efficiencies called out in the previous two sections, many are now beginning to see a significant upside for their business units in terms of the impact the platform has on their top lines. This impact has the potential to be greater than the efficiency savings in terms of new revenue from existing contracts, incremental revenue from new products and offerings, and the positive effect on the sales process in terms of competing effectively and adding net-new customers.

Examples:

- Increased upsell revenue from existing customers.
- Increased contract extensions and strong renewal rates.
- Improved win ratios in competitive deals.

"Cortex XSOAR brings us the ability to upsell more services to existing customers and then expanded packages to future customers."

- **MSSP Director – North America**

- Support for the addition of incremental, partner-branded services.

The Bigger Truth

Solving MSSP Operational Challenges and Seizing Opportunity

Core digital transformation and cybersecurity trends that were already in motion have been accelerated with the advent of the remote workforce, and MSSP leaders have been presented a unique chance to create sustainable value for their

customers. Today's customers are looking for leadership from MSSPs to provide a sustainable, reliable set of services that allows them to satisfy their growing security demands while serving the changing needs of their users.

Fortunately, each of the service areas supported by Cortex XSOAR, comprising a broadly applicable set of security use cases that customers need and are preparing to fund, also represent a solid, profitable market opportunity for forward-looking MSSPs and are ready for prime time.

While operational efficiencies were the primary goal and initial justification for investing in Cortex XSOAR, the leading MSSPs we interviewed are realizing several other benefits:

- Automation of massive amounts of data drives operational efficiencies and margins across analyst teams.
- Analyst productivity is enhanced, as they support more clients and "raise their game" to deliver customer value.
- Standard integrations with a broad array of systems and alliance partners saves development costs.
- Playbook libraries and templates save time and money and deliver consistent, repeatable tools.
- The platform establishes the foundation for new services, such as managed detection and response (MDR) or threat hunting.

Cortex XSOAR enables a new range of services:

- Phishing-as-a-service
- Threat intelligence/hunting
- Email security with automated firewall
- High-value strategy and compliance consulting

As a result, MSSPs reported to ESG that they can deliver faster investigation and response times, and consistently meet or beat aggressive SLAs. This has translated into better risk reduction for their customers, higher satisfaction, and less customer churn. The statements in Table 1 from successful MSSP leaders interviewed by ESG illustrate the value that the Cortex XSOAR platform has brought to their business.

"Sharing playbooks to create default libraries is a real benefit; we don't have to reinvent so it provides both best practice and efficiency."

- MSSP COO – EMEA

Table 1. MSSP Partner Leaders Speak About the Impact of Cortex XSOAR on Their Business

C-level Functional Leader	Cortex XSOAR Impact
Executive	"Cortex XSOAR forms the basis for our threat hunting service. It creates significant and sizable add-on incident response work (consulting) engagements!"
Technical	"Hands down the best product I've ever worked with in my career. The possibilities and efficiency yields are amazing."
Marketing	"We're 100% co-branded and actively promote 'powered by Palo Alto Networks' as part of our brand."
Sales	"We wanted to go with a true business MSSP. Joint funnels and joint prospects. With Demisto, and then the Palo Alto Networks acquisition, this was a good bet."

Source: Enterprise Strategy Group

In order to take advantage of the opportunity presented to MSSPs through automating SOC operations using Cortex XSOAR, and supported by our findings in this research, ESG believes partners should consider the following steps:

1. Commit to the Cortex XSOAR platform – Those partners who take full advantage of the functionality and benefits outlined in this paper see Cortex XSOAR as a "force-multiplier" in terms of the overall impact on their business.
2. Build a multi-level go-forward plan – Partners who create a strategy and success plan that anticipates efficiency improvements, but then goes beyond those to proactively design the organization to deliver new revenue sources and services offerings will be the most successful in the long term.
3. Organize for success – By creating an organizational investment plan that takes advantage of the new ways in which analyst and support experts can deliver enhanced services, MSSP leaders can fully leverage the platform and create differentiated, high-value relationships with their customers.

"Each person can now handle much more, and at the same time will also be able to go faster to deliver in-depth analysis of alerts."

- MSSP SOC Head – North America

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188