A Guide to Optimizing Proactive Security Services

Transforming Your Security Service Provider Business to Maximize Profitability with Premium Offerings and Invested Clients

PlexTrac®

Contents

The demand for quality cybersecurity services from reputable providers is growing consistently, but the competition to deliver those services is intense. Security service providers and managed security service providers (MSSP) face the ongoing challenge of driving revenue by maintaining and growing a loyal client base. Offering higher value, differentiated services and building efficiency into internal workflows will increase service margins and ensure profitability. To get there differentiation and automation are critical.

Differentiation is key to gaining and maintaining your market share, and one area ripe for service expansion and differentiation is proactive service delivery. Offensive services like pentesting, red teaming, purple teaming, findings validation, and advising are highly effective ways for enterprises to stay ahead of threats and prevent breaches before they happen.

Service providers that can identify the highest priorities for their clients and build specific risk and threat-based offering will see greater client stickiness. New targeted offerings can move the needle more quickly than broad, sweeping testing and provide immediate value to clients and something new to sell or upsell. The more service providers can express the value of proactive services, the more targeted services they can offer to keep clients making progress and returning frequently.

> **Differentiation is key to gaining and maintaining your market share, and one area ripe for service expansion and differentiation is proactive service delivery.**

Efficiency maximizes the value of your human resources to increase service margins making it possible to develop new services and spend more time collaborating with clients without adding significant resources. Process efficiency enables testers to spend as much of their valuable time as possible doing the highest level of work. Effective collaboration is also important to achieve efficiency, both among team members and with clients. Eliminating barriers to efficiency and effective collaboration help your service provider not only deliver more services for more clients but also keep those clients satisfied by meeting deadlines and demonstrating value. Automation is the catalyst to enabling efficiency.

This eBook provides valuable insights and practical strategies to help your cybersecurity service organization optimize its business strategy. Automating pentest and assessment reporting workflows can be a powerful mechanism to support differentiation in service offerings and the efficiencies needed to make it possible. Implementing a pentest reporting automation solution can have a positive business impact far beyond the report deliverable, including the following:

- Offering new services to become a trusted advisor
- Providing actionable insights to increase client satisfaction
- Driving efficiency to boost service margins
- Increasing effectiveness to scale service delivery

Read on for insight on leveraging reporting workflow automation to realize key business outcomes at your security service provider.

Deliver New Proactive
Security Services
to Become a
Trusted Partner

The first pillar to positioning your security service provider for success is perhaps the most significant and desirable: diversifying offerings to become an indispensable partner to clients. Doing this requires offering new and innovative services and leveraging them to deepen existing client relationships and create new ones in order to build new revenue streams.

The 2023 Professional Services Maturity™ Benchmark report from Certinia found, "In 2022, technology spending and particularly PS [professional services] spending rose to new heights. A critical talent shortage added fuel to the PS fire as clients simply cannot find and keep skilled technical talent, so they increasingly bring in consultants. No matter how well-positioned and comfortable existing client relationships may be, all firms must aim to develop new client relationships. New clients bring new ideas, new challenges and the potential for new services, which can then be sold to the existing client base. New clients and new services are essential for growth."

> "New clients bring new ideas, new challenges and the potential for new services..."

Aligning Services with Client Business Objectives

The objective is twofold: bring in new clients and offer new, innovative services. These objectives work hand in hand both to grow the profits of the business and to up level the standard of services. Both of these goals can be achieved by understanding the business objectives of clients and aligning your offerings to those needs.

Tony Robbins in an article titled "14 Ways to Increase Profit Margin" states, "Today, successful businesses tend to strategically innovate by expanding on existing ideas in a way that appeals to their customers. To truly understand how to increase profit margins, focus on identifying your customers: Who are they, and what need do they have for your product?"

What are the latest attack vectors making news that your clients' leadership is hearing about? How can your services address those concerns specifically? How can you help your clients understand the value your services are providing them in light of their most pressing objectives?

To align to customer needs, you'll need both to build services around those needs and effectively communicate the value of those services. Your clients will use more services when those services are relevant and the clients' progress is measurable.

Helping Clients Articulate the Value of Their Security Investment

Making sure your clients understand the value your services provide and helping them demonstrate that value to their internal stakeholders in the boardroom is necessary to becoming a trusted advisor. While those in the cybersecurity function at your clients' organizations may understand and appreciate your reports and recommendations, they can face internal challenges putting the value in layman's terms and advocating for budget. They are under pressure not only to maintain the security status quo but also to answer for every new vulnerability making headlines. They need a partner who can provide them not only valuable services but also visibility into their progress — all in a way that can make a compelling case to leadership.

To partner with clients at the strategy level, consider how you can deliver differentiated reports that have sufficient executive level summary and technical detail. Provide visualizations and analytics on progress over time. Doing so will not only help your contacts see the value of your services and be able to articulate it meaningfully but also keep coming back for more services as their usefulness becomes apparent.

To have value to demonstrate you must offer services that are relevant to customers' most urgent concerns. This area is where new, focused service offerings can be added that address specific attack vectors or the latest zero day — those areas that your client will be expected to account for because they are on the radar of leadership. New services will, of course, add strategic value to your client's posture, but they will also give the service provider additional products to attract new customers.

Creating Opportunities for New, Innovative Service Offerings

Consider expanding to new services in the proactive risk management space. Offering services that help clients stay ahead of threats and strategically shore up defenses to mitigate risk before an event is the way of the future. Proactive security activities are also the ones most difficult for an organization to manage internally, thus making them prime for outsourcing to a provider.

Opportunities for new proactive security services to consider in addition to traditional pentesting and compliance assessments could include offerings around specific frameworks and threat intelligence.

> To partner with clients at the strategy level, consider how you can deliver differentiated reports that have sufficient executive level summary and technical detail.

Framework-based Assessments

Framework-based service offerings are testing done to assess controls according to a specific set of standards. These models include NIST, CMMC, SOC2, ISO 27001 and ISO 27002, and many others across industries. Assessment preparedness services for organizations that must comply with an assessment framework are a great addition to general pentesting services. Even if organizations are not required to meet a particular compliance framework, these service offerings can still provide a lot of value and help your clients measure and communicate about their posture more effectively.

Threat-informed Testing

Another area with potential for new services is targeted testing around real world threat intelligence. Helping clients understand their risk and vulnerability to known attack vectors, like ransomware or a specific zero-day, provides an excellent foundation on which they can grow their posture and do so more quickly.

These more targeted services can be much more actionable because they are specific, manageable, and easier to gain resources for from leadership. Pentesting services with a broad scope performed annually or biannually are valuable but can be very overwhelming and difficult for clients to make meaningful progress on. Adding services to your offerings that are more focused can create new revenue streams with new and existing clients and make it easier to create and communicate value.

Promoting Continuous Validation Strategy

Helping clients understand the value of your services is essential for moving them to the gold standard of proactive security strategy: continuous assessment and validation. Clients willing to engage with you as their trusted partner to advise and provide continuous services will be the stickiest, most valuable in your portfolio and, in turn, will be the most secure and mature in their posture.

In order to sell clients on continuous assessment and validation, you must communicate value and collaborate closely. This is an area where a reporting and workflow automation solution can lift the capabilities of your service provider. Remediation tracking, data analytics, audience-differentiated reporting, and real-time collaboration features are all ways to communicate progress and value to your clients without adding significant manual workload to your team.

Becoming a trusted advisor will not happen overnight but by creating new targeted proactive security services that move clients toward a continuous approach, you can demonstrate your service provider's expertise and become an essential partner to clients. Reaching this level with existing clients and attracting more that are ready for premium services requires not only offering new services but making sure existing service offerings are moving the needle.
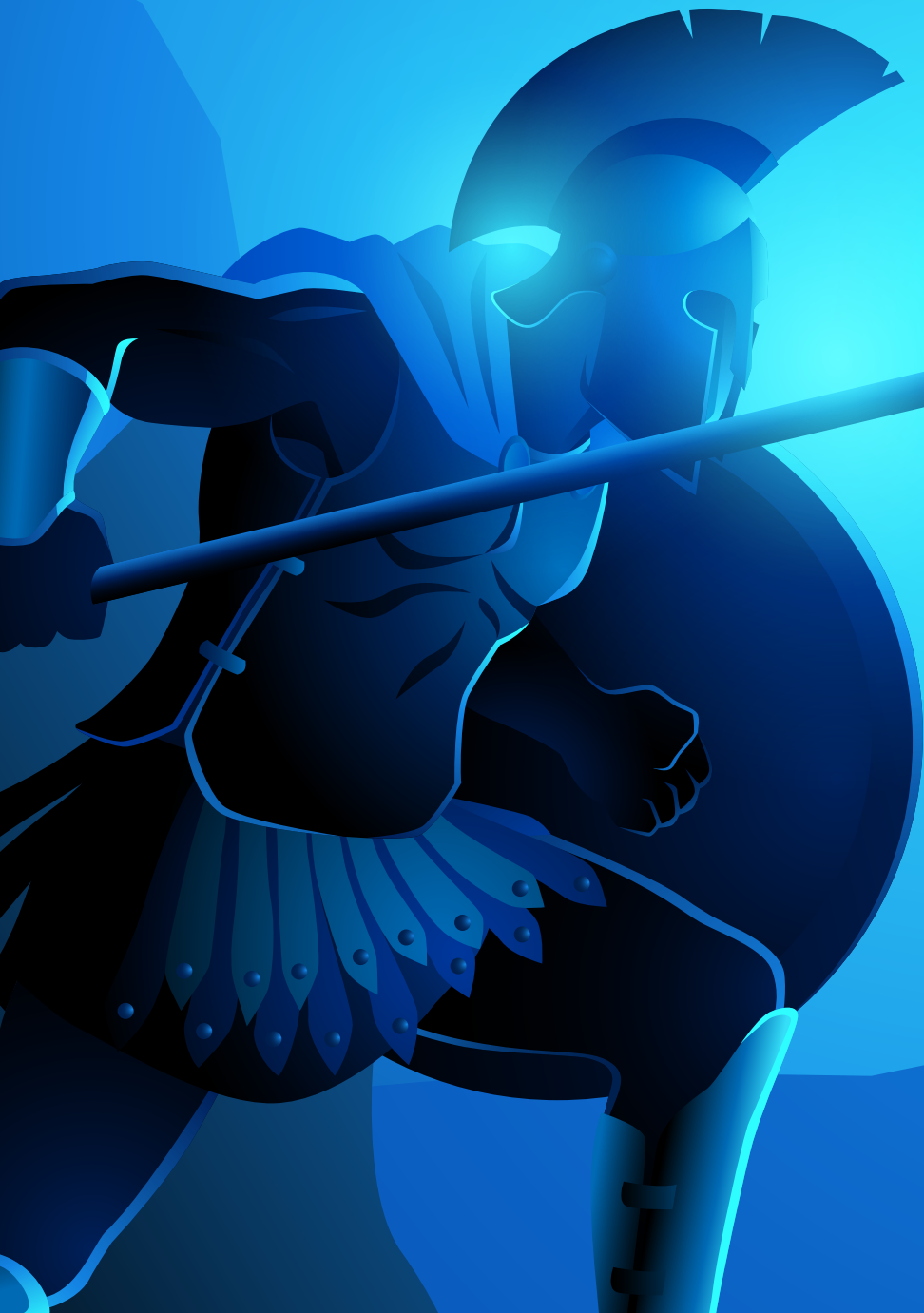
Provide Actionable Insights to Increase Client Satisfaction

To support business growth to a level of trusted advisor, providing quality client communication at every touch point is key. Adopting a client-centric approach to service delivery will reap dividends in retention and upsell opportunities. Here, too, reporting and workflow automation can ensure your organization is laying the foundation for client satisfaction by ensuring deadlines are always met and recommendations actionable and communicated clearly to all stakeholders.

A white paper from Deloitte on client-centricity reads, "Too many organisations focus on trying to deliver 'world class' service – rather than giving customers what they actually want, which in most cases is a quick and easy process to follow, that is right first time." While "world class service" may be the ultimate goal for a professional services organization, you must first meet baseline expectations every time with a consistent, easy-to-implement product. When your clients begin to see value in the form of measurable progress on their security posture, you'll have the platform on which to grow the relationship.

> Adopting a client-centric approach to service delivery will reap dividends in retention and upsell opportunities.

Embracing Dynamic Delivery

To build that platform, you'll need to embrace dynamic findings and recommendations delivery so clients can begin to take more immediate action. The old paradigm of providing a massive report and then washing your hands of it until the next annual or semi annual engagement with that client isn't enough anymore. The onus is on the service provider to not only provide expert insights but also to present them in a way that the client organization can prioritize and act on them.

A reporting automation platform that provides secure client access is an efficient way to begin delivering a more consumable report. By allowing clients to see recommendations not only in a formal report but also to view and track them dynamically, they can take action much more quickly and be rewarded by seeing progress before more testing or validation occurs.

Delivering Comprehensive Services

In addition to taking on more work from more clients, extra time gained in efficiencies in process and communication can be poured back into existing engagements, where necessary, to give them additional depth and breadth. More robust, comprehensive services, over time as their value becomes apparent, can demand more premium pricing.

As customers begin to make measurable progress due to your actionable recommendations, you will have the opportunity to offer them more frequent testing and move them toward more mature strategies. Doing so can increase service margins and build a stable recurring client base. Consistent, happy clients will recommend your services and will enable you to level-up your advising services leading to more growth.

Drive Efficiency
to Boost Service
Margins

Although leveling up service offerings to support premium pricing is one method to service margins. It is not the low hanging fruit. Reducing costs and increasing efficiency are the two other options to make the most of your existing services while improving and creating new ones. Increasing pricing is challenging in a crowded industry and reducing costs is difficult when you rely highly skilled labor and professionals with those skills are scarce and come a premium. This leaves increasing efficiency as one of the easiest ways immediately support revenue growth.

> **Introducing efficiencies in these processes will increase capacity without increasing investment in resources.**

Implementing Automation

Unfortunately, proactive security workflows common in a cybersecurity service practices are typically full of inefficiencies in low level, repetitive tasks performed by highly skilled professionals — from working with data from disparate tools to tracking information in static spreadsheets to tedious manual formatting of reports. Introducing efficiencies in these processes will increase capacity without increasing investment in resources.

Reporting automation can introduce efficiency throughout the pentest or assessment life cycle. During the planning phase an automation solution can help with communication by capturing scoping information into a centralized location where data from pentesting tools can also be saved and aggregated as the test progresses. Artifacts can be captured and stored and then eventually added to the report with ease. Collaboration on content can be managed in real time and a report built in a few clicks.

A recent Forbes article on scaling professional service businesses concurs, stating, "Streamlining and automation are key. With a service-based business, the primary investment is human capital since it will be your team who will be providing the servicing."

Efficiency in the pentesting or assessment workflow through automation can reduce time spent in documentation by fifty percent or more with the right solution. This time savings can be reallocated to conducting more engagements with the same or new clients thus increasing capacity with existing resources.

Maintaining Quality

The balancing act comes in ensuring that efficiency does not trump the quality of the process or product. However, reporting automation in most cases improves the quality of the deliverable by creating consistency in every report across all testers. Quality assurance processes become simpler when performed in a dynamic environment. And errors are mitigated when you can avoid copy and pasting findings writeups and narrative content from older reports or disparate storage repositories.

Creating process efficiency is the simplest and most immediate step you can take to begin transforming your service provider business. Your testers will thank you for helping remove tedious pain points and your margins will expand without a price increase on your services.

Increase Effectiveness to Scale Service Delivery

Efficiency alone isn't enough to truly transform your security service provider. Gains in workflow efficiency must translate to improved effectiveness. In other words, gaining capacity won't grow the business unless that additional capacity is used to deliver more and better services. Once the path is cleared for your team by implementing automation in processes, it's time to improve utilization, the time spent on the right work.

The 2023 Professional Services Maturity™ Benchmark notes, "To improve utilization, PSOs [professional services organizations] must improve resource management effectiveness." Resource management at your security service provider can take a couple of forms: maximizing human resources and leveraging technology.

> **Gaining capacity won't grow the business unless that additional capacity is used to deliver more and better services.**

Maximizing Human Resources

An effectively managed team can define and meet service-level agreements (SLA) and other deadlines consistently because they have streamlined, repeatable processes that promote predictability. Predictability enables increased productivity.

The other aspect requiring improvement in effectiveness, facilitated by efficiency, is in team collaboration and customer communication. Streamlining and systematizing quality assurance processes, for example, can dramatically improve the quality of the final deliverable. Additionally, addressing siloed knowledge application, in drafting findings writeups for example, can also improve both the consistency and quality of the product without adding resources.

Client communication is another vital component of a professional's workload that can often be managed more effectively to support scaling service delivery. Standardizing and automating pre-engagement questionnaires, for example, can reduce time spent meeting or allow the tester to focus time with the client on their unique requirements that may differ from the standard engagement. Giving clients more direct access to recommendations from an engagement also changes the nature and quality of the communication a tester can have with them.

But remember that gains in efficiency can only scale service delivery if your team was working within reasonable constraints in the first place. If testers were drafting reports on evenings and weekends just to keep up, process efficiency gains in the reporting workflow will likely improve morale but not necessarily increase capacity dramatically. This is where automation technology can bridge the gap.

Leveraging Technology

Automation technology applied in the cybersecurity services space can not only boost efficiency by eliminating manual processes but also improve quality and consistency. These gains together can improve the productivity of your team, and, depending on their existing capacity, can translate into increased service delivery, higher quality deliverables, or both.
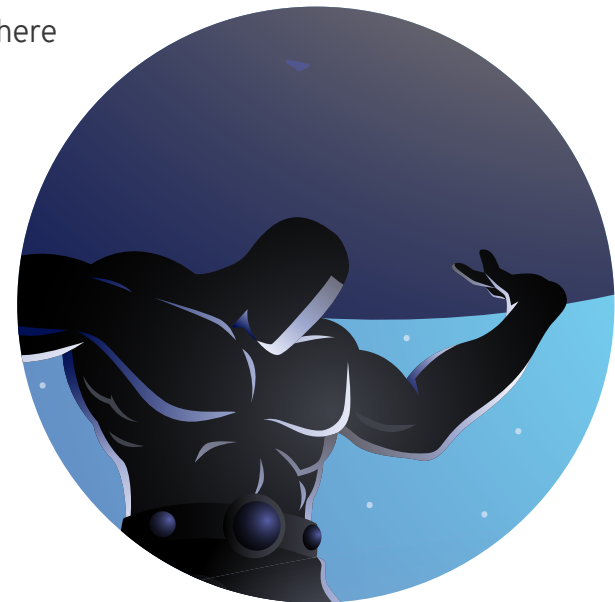
To continue scaling will eventually require additional resources. Investment in a comprehensive reporting and collaboration automation solution can help an organization scale service delivery exponentially when additional resources, like more testers, are applied. In part, this is because increased efficiency and automated processes have a compound effect as the team grows. It is also true because automation can lessen the investment needed to bring on junior testers.

The article "How to Scale a Service-Based Business" from Forbes suggests, "Invest in training so that you can hire entry-level team members, and try anchoring your price to value rather than time, so that you can get more efficient and thereby more profitable over time." The right automation solution can scaffold junior testers with training and access to collective team knowledge that can help them be effective more quickly and at entry-level salaries.

Maintaining or even improving the quality and timeliness of the deliverable is key to communicating value to clients so that efficiency gains can truly scale service delivery.

> **Investment in a comprehensive reporting and collaboration automation solution can help an organization scale service delivery exponentially when additional resources, like more testers, are applied.**

Transform Your Security
Service Provider Business

It is essential to position your security service provider for sustainable success in a highly competitive cybersecurity services marketplace. Differentiating your business and delivering unparalleled value to clients as a trusted partner is the ultimate goal, but to get there your business must maximize efficiency, effectiveness, and communication — which will make it possible to create the services and relationships to become that integral part of clients' strategy.

Conquering these areas enables necessary business growth outcomes of increasing service margins, scaling service delivery, improving customer satisfaction. For professional services organizations in the cybersecurity industry, reporting and workflow automation can be the catalyst to achieving these goals.

PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking. PlexTrac allows service providers to increase margins, scale service delivery, and enhance client outcomes.

Request a personalized platform demo to see PlexTrac in action at PLEXTRAC.COM/DEMO

PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking, allowing service providers to enhance margins and client outcomes and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

www.plextrac.com