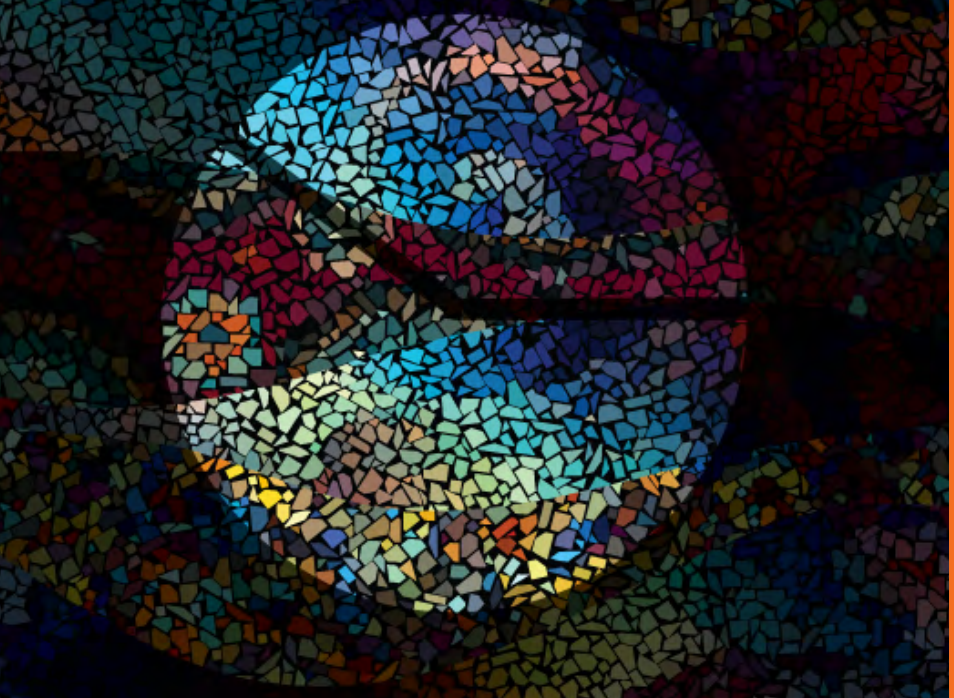
SEC AUTONOMOUS INVESTIGATION™

How to Grab a (Bigger) Piece of the Managed Security Services Market



Market analysts predict that the Managed Security Services market will continue to grow at double-digit rates over the next few years. This prediction doesn't come as a surprise considering the increased complexity and frequency of data breaches, along with the rising cost of a serious cybersecurity investment. As a result, new players are constantly joining this already fragmented market comprised of pure plays, IT providers, telcos, security consultants and vendor companies.

Each MSSP niche offers strong assets, such as global IT integrators' strong customer base and cyber vendors' best-of-breed solutions. Yet, they all lack a solution to solve their common challenge; a solution which would give them the business tools to rise above the crowd in this increasingly crowded market.

MSSPs' Success Depends On:

New revenue streams with expanded services

- ✔ Advanced continuous, full scope detection
- ✔ Automated response
- ✔ "Hunting-as-a-service"
- ✔ Audit functionality

Greater personnel productivity from automation

- ✔ Better ROI on operating expenses
- ✔ Fewer highly skilled analysts required

Fast, simple deployment and API integration

- ✔ Unlimited scalability
- ✔ Multi-tenancy

Core capabilities to increase bottom-lines

- ✔ Detection extending beyond traditional signature-based detection
- ✔ Automated, centralized, orchestrated response
- ✔ Unsupervised and supervised machine learning in a network traffic analysis platform to continuously monitor and process massive data volume for advanced threat detection

Enabling MSSP Differentiation: Personnel Productivity, Flexibility and Scalability

The most significant ingredient needed for an MSSP to grab a big piece of the market lies in the area of personnel productivity, with the flexibility of maintaining contracted service levels per customer. Key differentiators are derived from machine-learning tools that can automate with precision and free up hours of time currently spent on chasing random alerts and false positives.

Automation is a central aspect in today's SOC to keep up with the speed and sophistication of cyberattacks, yet automation typically doesn't come with advanced detection or response functionalities. SecBI is alone in the market to combine the technology for continuous detection of "unknown" threats with flexible automated response, enabling security teams to focus on other tasks that still require manual intervention. And its software-only design allows MSSPs to match their business models per the requirements of each end customer.

Solving Productivity Challenges While Expanding Services

Unfortunately, most MSSPs still offer only traditional security services, such as firewalls or intrusion detection/prevention systems (IDS/IPS) that provide little to no visibility into stealthy attacks. While MSSPs may pick up suspicious indicators, they need better visibility into the network to confirm these indicators as attacks. This technology gap leaves customers completely unaware of stealthy attacks or, at best, facing a long investigation processes with little confidence of finding true results.

SecBI's solution mimics and automates the way cybersecurity analysts and incident response teams operate. The technology, based on both unsupervised and supervised machine learning, instantly unveils an attack's full scope, including all the affected entities and full kill chain. This accelerated detection and investigation is followed by automated response. In this manner, MSSPs offer automated advanced technical capabilities, with nonstop network traffic monitoring, threat detection, triage, and incident response in a much more productive and efficient manner for greater returns.

MSSPs providing "SOC-as-a-Service" can easily take advantage of this end-to-end automation not only in breach response, triage and filtering, but also to perform audits on end customers' networks. This gap analysis includes identifying customers' network blind spots and may be followed by consultation on remediation and implementation.

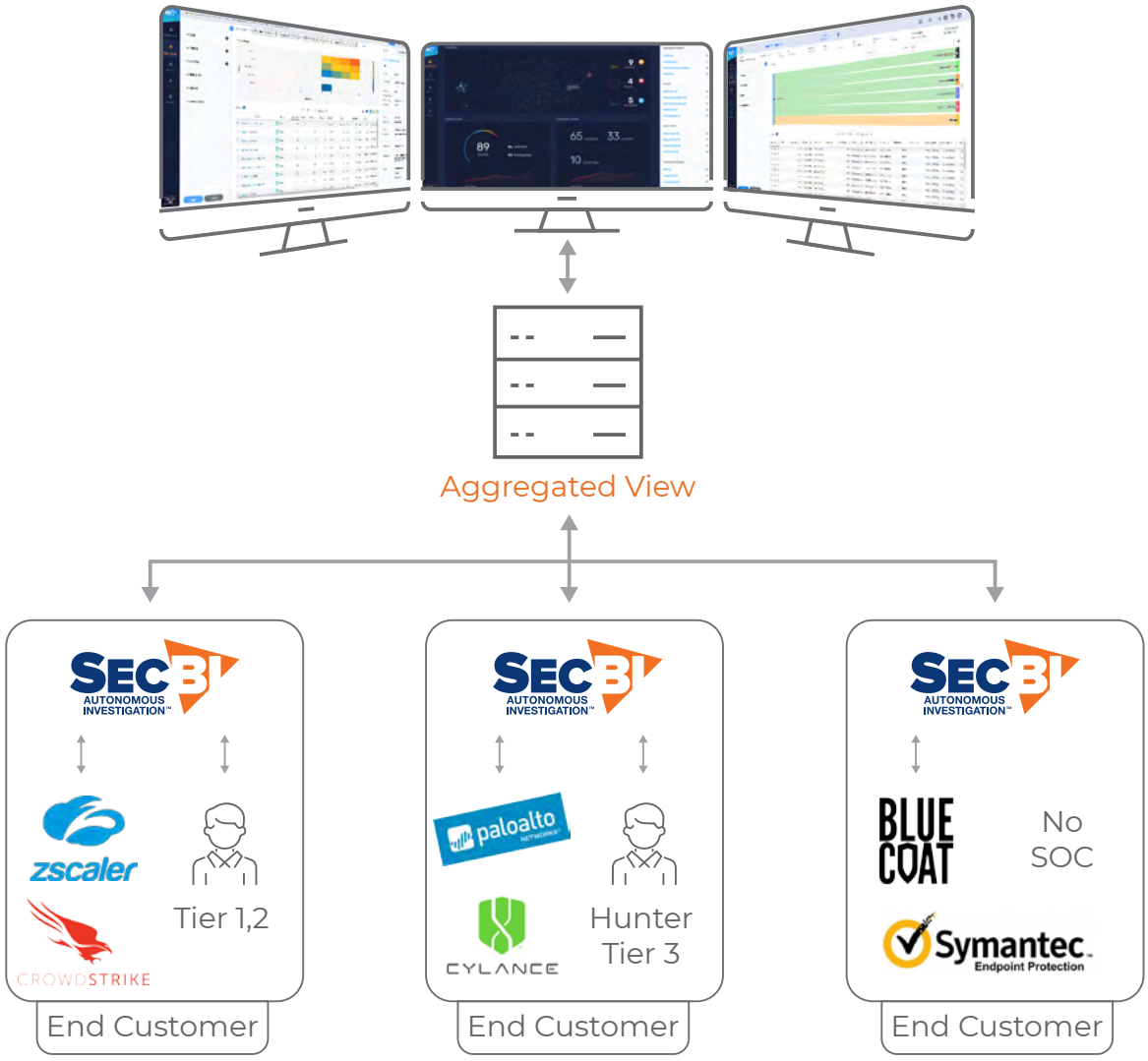
In addition, MSSPs can offer SecBI's "hunting-as-a-service", a cost-efficient approach to augmented threat hunting based on full network traffic analysis. The behavioral profiles of all users and hosts built by SecBI's machine-learning technology provide comprehensive context for hunters to fully investigate their theories and to perform efficient threat hunting over specific time durations.

Unlimited Scalability and Flexibility in Deployment

To significantly improve ROI, MSSPs must seek solutions offering unlimited scalability and flexibility of deployment modes. They require cloud-based, multi-tenant solutions, rather than use solutions which require the deployment of special appliances. Given that it works on virtual appliances, SecBI lends itself to multi-tenant, cloud-based or on-premise deployment, perfect for MSSP multi-use per customer yet have an aggregated view. This ease of scalability enables MSSPs to offer various service levels and tiered pricing options. While providing network traffic analysis (NTA) level of visibility without needing any additional sensors, MSSPs can deploy multiple instances of SecBI to be activated within a few hours.

Seamless and Full API Vendor Integration

MSSPs: For Tier 1, 2, 3 Hunting, and Incident Response Services



Flexible Pricing

SecBI offers two pricing models for maximum flexibility and for MSSPs to deliver competitive and top-quality security services:

1. “All you can eat” for one year based on your current customers and estimated onboarding.
2. Pay-as-you-grow from your first customer.

Summary

SecBI’s Autonomous Investigation™ technology provides an invaluable augmentation of services currently available to MSSPs, aligning their capabilities with the ever-changing threat landscape, regardless of the type of MSSP. By embracing technologies using unsupervised and supervised machine learning, threat detection and response are empowered at new levels of automation.

With SecBI’s simple software-only deployment, MSSPs can offer the same SLA for SOC-as-a-Service, as they can via on-premise SOC implementation. MSSPs can quickly and radically upgrade their detection and response capabilities for each end customer within a few hours. They can offer their customers an expanded service portfolio that provides visibility and analytics of the IT network, continuous monitoring, and detection of the complete scope of suspicious incidents in real-time with flexible automated response. In addition, SecBI offers supplementary services such as network audits and augmented threat hunting for further revenue growth.

SECBI AUTONOMOUS INVESTIGATION™

sales@secbi.com

www.secbi.com