Transform Your MSP to an MSSP

Perspective by Edward Amoroso, TAG Cyber

Every managed service provider (MSP) agrees on two things:

- Their customers are shifting from premise-hosted applications and systems to cloud-based, subscription services for their present and future IT needs. This does not remove the need for continued MSP support, but it obviously changes the day-to-day mission, along with the skill sets required to handle the as-a-service computing preferences of customers.

- There is increasing pressure to support the day-to-day cyber security needs of their customers. If this new challenge is just absorbed into existing service agreements, then it can produce serious hits to both productivity and profitability. But if improved security can be used as the basis for new business opportunities, then true win-win outcomes can be achieved for both the MSP and its business customers.

In short, the goal should be for the MSP to be transformed into an MSSP, and this must be done without any degradation to existing support. But it also must be done without the need to recruit new staff with cyber security skills. Rather, the goal must be to find methods that can improve day-to-day security support for existing customers, while also enabling new for-pay security services that can be added as new offers

DECISION AUTOMATION

The solution to this problem can be summarized in one word: Automation. If an MSP can find platforms to improve data security analysis – essentially augmenting staff with intelligent tools, then customers will see much improved security support. But perhaps more importantly, with such automation comes the potential to defined new service offers. This makes the MSP an MSSP – which implies an increase in revenue.

All MSSPs use a commercial or customized platform to support data analysis and event management by on-site analysts. We can refer to this ubiquitous support capability as an analysis support platform (ASP). Each MSSP team can fill in the details of how their local ASP ingests event and environment context data, and how it supports security case management, incident response, and correlation analysis for customers.

The challenge, as security experts will attest, involves figuring out how to translate data from the ASP into actionable management intelligence. Where this MSSP task has been traditionally supported by just adding more human beings in a SOC, modern ASP platforms try to use intelligent algorithms for both basic and advanced analytics – but fresh solutions are needed to augment their baseline capability with support functions that can optimize automation.

- Respond Software offers the world-class Respond Analyst platform for MSSPs that be viewed as an automated analyst for the SOC. That is, Respond Analyst plugs directly into the existing ASP, just as a human SOC team might. It has a self-driving capability to augment the existing MSSP team by performing various support tasks – each of which requires the dependable operation of an automated and intelligent expert system. Below are some of these supported tasks:

- Knowledge Base Management. The basis for traditional expert systems, as well as modern machine learning systems, is the collection and storage of information into a knowledge base that can be managed through defined interfaces. “Respond Analyst is designed to help gather facts and infer context,” explained Chris Calvert, co-founder of the company. “This is a function that automation can perform more efficiently than human analysts.”

  The good news is that if you are running an MSSP and you plug the Respond Software solution into your ASP, the result will be a high-quality knowledge base, constructed and maintained automatically, and providing autonomous

support for your analysis and response activities. This is a welcome capability, since most SOC hunters and analysts use home-grown or special tools to store and manage available knowledge.

Decision Engine Processing. The decision engine in Respond Analyst combines basic expert system decision structures with modern machine learning methods. The result is an advanced decision-making function for the MSSP that makes both rudimentary and advanced choices about observed security information. Such decision-making is based on underlying probabilistic mathematical models developed within the company.

CAPABILITY

SOC analysts thus have access to a powerful decision function, readily available to support the development of management recommendations. By some estimates, the SOC workload augmentation from the Respond Analyst platform approaches the equivalent of twenty-six full-time human analysts. That type of capability leap is exactly what is required for modern enterprise SOC teams to deal with a rapidly advancing cyber threat.

- Case Building and Support. The core unit of predictive analysis and reactive incident response is the notion of a case, which is basic to the practical operation of a working SOC. To that end, the Respond Analyst platform supports case building and incident management, with reporting to the security team responsible for response decisions. "Our solution is designed to emulate the judgment of a human security analyst," explained Calvert.

The decision to generate cases is influenced by Respond's Probabilistic Graphical Optimization (PGO) technology, which performs analysis based on a multitude of different factors. The goal of the PGO processing is to determine severity, likelihood, and consequence of a potential incident. This capability is one of the most powerful aspects of the self-driving SOC, because the decision to respond is based only on relevant information.

FINAL WORD

These automated tasks are complemented by ingest of external threat intelligence feeds from Respond Software – and can include any threat intelligence feed you might be using at your company via the STIX/TAXI standard. The result of the automation and feeds is a system that really does look like a self-driving SOC. Granted, the approach does not remove the need for human beings, but it does introduce an element of welcome autonomy in tasks that a machine is likely to perform more effectively than any person.

If you are an MSP and you are interested in learning more about Respond Analyst, Probabilistic Graph Optimization, or any other aspect of the Respond Software commercial offering, please reach out to Chris Triolo, VP of Customer Success ctriolo@respond-software.com.