Cynet
AUTONOMOUS BREACH PROTECTION

The Security Outsourcing Guide

Created: May 2020

Executive Summary

As cyberattacks continue to proliferate in volume and increase in sophistication, many organizations acknowledge that some part of their breach protection must be outsourced, introducing a million-dollar question of what type of service to choose form. The **Security Outsourcing Guide** attempts to provide IT Security executives with clear and actionable guidance on the pros and cons of each outsourcing alternative.

There are numerous variations of security services in the market. To simplify understanding we have divider them into the following groups:

- **IR Oriented:** this group includes outsourcing only IR related activities and features a wide range of variance from mere monitoring and notification through remote assistance and guidance to full forensic investigation and remediation activities. In terms of business models it could be retainer-based or on demand. Typical service providers of this families are **MSSP , MDR** and pure play **IR providers**
- **Ongoing Management Oriented:** this group applies to organizations who would rather that even the continuous operation of their prevention and detection technologies will be carried out by more skilled team, and is mostly found among organizations with little security expertise and without a dedicated security team. Here, as well, there are various flavors that can range from management of just the more advanced detection and monitoring tools to full management of the entire security stack. Typical service providers of this families are **MSSP** and **MSP**.
- **Design and Set-Up Oriented**: that's the widest group in terms of outsourced functionalities and includes an end-to-end outsourcing of the decision what product to choose and install, how to integrate them together and which threats should be prioritized in terms in what products to invest. Typical service providers of this families are **MSSP**, **MSP** and **System Integrators.**
- **Virtual CISO (VCISO):** an individual that has typically gained a rich security background holding positions at organizations with mature security posture and has thus acquired significant knowledge on cyber technologies and services. As a result, he\she is in an optimal position to advise less mature organizations – often without a CISO themselves – on how to tailor a best fit security for their needs.

Each group, while introducing many variations within, represents a different division between in-house and outsourced security functionalities. We advise the reader to go over the detailed description of each group and see whether there is a one that best matches the posture of its organization.

In addition to the three service groups that outsource various functionalities

How we have Built this Document

Cynet serves a global install based of hundreds of end customer across all industries, geolocations and sizes as well as a wide range of service providers providing a unique perspective and insight into both security needs and outsourcing alternatives.

Cynet is the provider of Cynet 360, the world's first Autonomous Breach Protection Platform that consolidates and automates endpoint, network and user protection across the full security lifecycle: proactive monitoring and control, attack prevention and detection, and response orchestration. Cynet 360 technology is complemented and enhanced by CyOps Managed Detection and Response (MDR) service, which is included in Cynet 360 offering without additional payment.

By natively integrating all these capabilities into a single platform, Cynet 360 eliminates the need to manually deploy and integrate multiple point products. Cynet 360 enables security teams to conduct all their operations from a single console, introducing simplicity, speed and efficiency, that translate into an unprecedented level of breach protection.

Visit the Cynet 360 website to learn more on how to introduce unmatched simplicity, speed and robustness to your environment's security

Security Outsource Options

IR Oriented

In terms of business model, what sets the **IR Oriented** path apart is that it's an **event-based** rather than **continuous** engagement.

This path best fits organizations that possess a considerable level of cybersecurity knowledge, enabling them to pinpoint what is and what isn't in the scope of their internal capacity.

Indeed, in many ways, Incident Response represents the high-end side of the cybersecurity skillset which is less likely to be found within the standard organization's workforce.

IR oriented range of services

Engagement trigger

- Suspicion of malicious presence within the customer environment, stemming from a detected IT anomaly (user activity, network connection, endpoint exception resource consumption, etc.)
- Concrete alert of a security product that indicates a possible of hidden malicious activity of yet unknown scope

Services Included

- **Investigation - Initial containment**
  This service is the cyber equivalent to first aid and is meant to rapidly identify and eliminate live attack instances such as infected hosts, malicious processes, active C2C communication and compromised user accounts
- **Investigation - root cause analysis\incident impact**
  This part comes after the initial containment and is meant to unveil hidden attack components and mainly to reveal what was the initial compromise vector, what entities have been impacted and whether there is a malicious infrastructure that can enable attackers to repeat their operation
- **Remediation – direct\proactive**
  The discovery of the attack's scope is followed by actual IT actions: isolating machines, disabling user accounts, terminating processes, blocking network communications, etc. in addition to the elimination of the specific attack, this stage includes also leveraging the lessons learned to proactively prevent its repeated occurrence by implementing the discovered IoC in the security products in place

Delivery options

All IR services are available in both remote and on-site offerings:

- **Remote**
  In this model the service provider operated from its own SOC and relies on the inputs from the customer's security products. On some occasions it will connect remotely to the customer's environment. The remediation part in this model is mostly in a consultancy manner and the customer's IT\security team are the ones who perform it. This mode suits low to mid severity incidents and is carried out by **MDR** and **MSSP**.

- **On customer site**
  In this model the service provider provides the full investigation and remediation process on the customer's site owning the process end-to-end. This mode better suits severe ad more complex incidents that require heavy weight forensic investigation. It is mostly delivered by **MSSP.**

Service Provider Type:

- MSSP
- MDR
- IR

Ongoing Management Oriented

As the name implies, this option represents a continuous engagement in which the service provider owns the ongoing management of the security stack. In terms of responsibly share, the main difference from the IR oriented model is that here the service provider is responsible for the **initial detection** as well as the investigation that follows.

Ongoing Management Oriented Range of Services

Engagement trigger

The customer acknowledges that it lacks either the staff, the skill or the budget resources to efficiently operate and manage the threat detection layer of its security products. There are various flavors to the balance of what products to manage in house and what to outsource but it mainly falls into two groups: Threat Detection and General Security

Managed Products

- **Threat Detection**
  In this model the organization outsource the management of the more advanced security products such as EDR, SIEM and Network Traffic Analysis. Efficient operation of these products is beyond the skillset of the standard IT team and the ability to translate a product alert to a concrete risk is important enough to justify its outsourcing to a service provider that has this skillset at hand. Often, purchase of an advanced detection product is coupled by engaging with Threat Detection services from the same vendor. In other cases, the service provider would deploy its detection technology of choice on the customer's environment.
- **General Security**
  This model includes any variation of outsourced management that includes additional security products: AV, Firewall, Email Protection, and others. The rational here would be that the service provider would be able to perform continuous monitoring of the protected environment and not be limited to alerts from the detection-based products.

Services included

- **Alert monitoring**
  Advanced security products generate wide array of alerts and discerning between false positives and actual threats require skill and experience. The service provider owns initial alert classification and monitoring per severity and risk potential. Critical alerts are escalated to investigation, similar to the one described in the IR Oriented section.
- **Threat hunting**
  This service complements the Alert Monitoring by proactively searching for dormant and active threats within the customer's environment prior to alert generation with the rational that it pays off to invest in early detection of attack instances prior to its maturing into actual damage. Threat hunting mostly relies on IoC from threat intelligence feeds but also on analysis of endpoint, user and networking activities to discover any anomalies that can indicate malicious presence.

Service Provider Type

- MSSP
- MDR

Initial Design and Set-Up Oriented

This offering represents the most heavy-lift security outsource. While former offerings maintain the IT side skills - choice, deployment and maintenance operations – internal and outsource the missing security skill, organizations that choose this path seek the peace of mind of managing zero to none of both their security products and operation. In some cases it involves setting up the security stack from scratch, making a cloud delivered products a favorable.

Initial Design and Set-Up Range of Services

As a rule of thumb, the more product management responsibility from the service provider side carries more involvement in what product to install – which basically is what the design aspect is about. In most cases, the service provider will analyze the customer's security needs and provider several SLAs to choose from, varying in their threat coverage and

Engagement trigger

The customer either doesn't possess in-house security knowledge or finds it more cost effective to outsource it altogether. This might be coupled with outsourcing IT operations altogether, making it appealing for small organizations with IT\security needs that are better addressed by a service provider. However, it can also be found in large organization with relatively low security posture that have come to acknowledge cyberattacks as a critical risk and need to rapidly heighten their security level to comply with either external or internal requirements.

Managed Products

It is rather hard to identify a clear classification in this category since the various combinations are endless: managed firewall, managed SIEM and managed EPP are just few prominent examples.

Service Provider Type

- MSSP
- MSP
- System Integrator

Virtual CISO (VCISO)

Along the three groups described above, there is an increasing outsourcing trend in the recent years to outsource, either partially or completely the security decision making role itself to a what is known as virtual CISO or VCISO – an individual with vast security background that can provide a wide range of services from consultancy to actual design and vendor choice.

Service options

Disclaimer: since VCISO is an emerging service category there are not yet fixed definition regarding its various tiers and SLAs. Hence, what represented in this section is an optional breakdown of outsourced responsibilities.

- **Tier 1**: including customer and partner questionnaire support, information security program creation and management, annual information security training, annual business continuity table-top exercise, and an annual qualitative information security risk assessment.
- **Tier 2:** all the above plus annual external audit support (HIPAA, SOC2, etc.), compliance with regulations and standards, periodic IT security assessment; and security vendors reviews.
- **Tier 3:** for organizations with over 500 employees. Includes all the above plus a periodic information security risk assessment.
- **Tier 4:** full CISO responsibilities covering design, implantation, set-up of internal compliance requirements, auditing vs. requires external regulation

Conclusion

As we have outlined in this document, the range of security outsourcing variation is extremely wide, and reflects a respective wide range of organizational considerations. Outsourcing can stem from multiple reasons – overall company strategy, specific need that cannot be addressed in house, budgetary considerations, and others. At the end of the day, regardless of the initial motivation the bottom line is that business goals would be better achieved by engaging a service provider rather than allocating internal resources.

From our experience, the key factor in outsourcing decisions is precise mapping of the existing cybersecurity capabilities within the organization and hence our main purpose in this document was not just describing the various outsourcing options but to unveil what are the capabilities profile that suits them best. Thus, we hope that the service landscape this document delivers is both wide and granular enough to provide decision makers with actionable insights regarding which type of service to engage with.