The Role of Security Orchestration in Managed Detection

Introduction

Managed detection and response (MDR) is a fast-growing managed security offering focused on detecting and responding to threats that have bypassed traditional security controls. Gartner predicts by 2020, 15% of organizations will be using MDR – up from fewer than 1% today.

MDR was born to fill a gap in traditional managed security services (MSSP) offerings, which typically focus on forwarding alerts to the end customer for handling. Too often, end customers are understaffed or ill-equipped to effectively investigate, triage, and remediate the alerts from their MSSP.

Why MDR

The high-growth, high-value nature of MDR is spurring several companies to introduce MDR offerings. From MDR pure-plays to traditional MSSPs and technology vendors such as EDR and SIEM, it seems everyone is looking to get on the MDR bandwagon.

Making the transition to MDR requires careful planning. Here are some of the major issues anyone looking to get into MDR must be prepared to tackle.

Security Staffing

At the crux of it, managed services require people. Unless you've been hiding under a rock for the last decade or so, you probably know there is big cybersecurity talent shortage. Unfortunately, this problem is a bigger hurdle for MDR services, as they require the highest-skilled analysts which are – you guessed it – in even shorter supply. If you're lucky enough to recruit them, you must ensure that they are doing meaningful work and are well compensated, otherwise you risk them accepting one of the job offers they get every day. And when those skilled analysts leave, they take the precious knowledge that they have acquired while working for you with them.

Things To Consider

- Befriend your local engineering schools. With the right training plan in place, hiring fresh engineering grads can be a great source of analyst talent that doesn't break the bank. Your experts can teach classes, sponsor events and attend job fairs. Sure, some grads may use you as a stepping stone and leave for the next best thing, but others will grow their skill set over the years to become your seasoned security experts.
- Document and maintain your playbooks through a **security orchestration and automation platform**, not static files, to retain analyst knowledge and expedite onboarding.
- Automate repetitive and mundane tasks to keep morale high by letting analysts focus on higher value work.

Incident Response

The biggest change for MSSPs transitioning to MDR is the shift from merely sounding the alarm to actually owning incident response and basic remediation activities such as isolating hosts, blocking processes or disabling users. Simply speaking, if you're not responding you're not actually doing MDR.

Some obvious challenges involve potential liability from executing remediation actions, but the main challenge stems from the fact that remediation involves a much higher degree of customer intimacy. The service provider and customer have to agree and what constitutes acceptable activity that the service provider can execute. Moreover, technically executing that activity will vary based on the technologies deployed by each customer.

Security Orchestration Platforms

Make sure you define what the process for remediation looks like with each and every customer. Some customers may require approval before executing certain actions while others are comfortable with the service provider jumping in to remediate. It helps tremendously if you have a solution that can capture these processes in defined playbooks that can be applied to each customer in a multi-tenant environment.

Look at ways to abstract the end-customers' underlying technologies so analysts can execute remediation activities without becoming experts on every platform. Here too, security orchestration platforms can be extremely helpful.

Interaction Methodology

Evaluate your customer interaction methodology. Once response is introduced into the mix, customers often expect “white glove” service. Customer portals and IVRs with lengthy wait times may be good enough when all you did was manage firewall rules, but if a ransomware attack is in play and the CEO’s machine has just been kicked off the network, customers probably require more than “Your call is very important to us”.

Demonstrating Security Value

MSSPs typically rely on customer portals and emailing reports for communicating with customers, with varying levels of success. Demonstrating ongoing value to customers is increasingly important when providing MDR services, as they are outcome-driven as opposed to activity-driven.

If you provide vulnerability management services, it is easy to demonstrate value by showing how many scans were run and how many patches were applied. However, if your job is to detect and stop threats on your client's network – how do they know you've done a good job? Or done anything, for that matter?

MDR and MTTR

Define and measure KPIs that are MDR-specific such as mean time to respond (MTTR), dwell time and others.

Many MSSPs spend considerable resources generating reports. Look at how you can automate reporting to both external customers and internal stakeholders.

Conclusion

Most MSSP services, such as firewall management, vulnerability management and DDoS mitigation are becoming increasingly commoditized. MDR is not only high-growth, high-value, it's also a great way to demonstrate expertise and differentiation to current and prospective customers. With the right commitment to change, and some help from the right technologies, service providers can successfully navigate this transformation.

Want to see it in action? See how one MSSP is leveraging **security orchestration** to automate repetitive tasks, better leverage limited analyst talent and support heterogeneous customer environments.