Breaking-Down Managed Detection and Response

Cybersecurity is a very important issue for any organization, and events can lead to a variety of negative outcomes; incidents often result in data theft, financial loss, and even damaged reputation. The cost of an attack is very high, which is why it's important to be prepared for the worst-case scenario. Managed Detection and Response is an outsourced array of services delivered by a Security Operations Center (SOC). These services include the detection of threats and a structured plan for mitigation and/or containment correlated over multiple cybersecurity products.

What is Threat Hunting?

Threat hunting is the proactive approach cybersecurity organizations use to identify threats before they happen. The process includes proactively searching for adversarial activity within an organization's computer network. A threat hunting and incident response team is responsible for finding and analyzing cybersecurity breaches and are also responsible for mitigating the risk of future breaches. Threat hunting teams work to identify potential threats before they become actual incidents which can be done through deep packet inspection, network forensics, and other techniques. They can find out what type of malware is being used or where a vulnerability exists on customers networks by proactively monitoring those networks with tools like PaloAlto Cortex, Carbon Black, Azure Sentinel to name just a few. As soon as they have identified an issue, they can take appropriate measures to resolve it before it becomes a full-fledged cybersecurity incident. Lumifi Cyber utilizes its home-grown automated threat hunting platform, ShieldVision which allows our SOC to be tool agnostic and provide proactive threat hunting to stay ahead of today cybersecurity threats.

What Is Incident Response?

Incident response (IR) is a process of responding to and containing an incident. It includes preparation, detection, containment, eradication, recovery and documentation of lessons learned. The purpose of incident response is to minimize the impact on the organization's business operations while reducing the risk of future incidents. Incident response teams should be prepared for all types of cyber threats which could include malware infections or ransomware attacks. These incidents disrupt systems and or steal sensitive data such as credit card numbers or personal information throughout the network. The goal of IR is to ensure that the data has not been compromised or exfiltrated and to mitigate the damage of future incidents.

Why choose Lumifi?

Companies looking into MDR need to take a holistic view of their providers and their teams. Often, the least considered factor in the security provider selection process in the human element. While technology is an important factor in first-class MDR, Lumifi's biggest differentiator is the expertise. Lumifi provides the experience needed to stand out from the

saturated MDR market with leadership and management having decades of experience, stretching back to before MDR was even a term. Our approach to security is focused on a balance of custom solutions, client-centric partnerships, and proactive approaches. Lumifi has its own team of threat Content Developers, Web Developers, experienced Engineers and seasoned Analysts to provide unparalleled proficiency. We not only utilize the industry's leading threat intelligence platforms, but also deliver personalized security recommendations through scheduled calls with a dedicated Engagement Manager. Lumifi leverages a proprietary platform called SHIELDVision to provide leading AI Orchestration capabilities. This tool allows us to discover malicious activity within a client's environment and then utilize that information to detect and respond across our client base who may be experiencing the same malicious activity. Our suite of services allows you peace of mind knowing your organization is being monitored around the clock by an industry leading SOC which takes pride in its customers security.

Comment [CP1]: Is this how we are typing this these days, may want to validate with David on this one.