Cloud Security: The Necessity of Threat Hunting

What is threat hunting?

Threat hunting is the proactive search for real and potential threats that may be hidden in a network's environment. These threats are tricky and malicious and are designed to pass through endpoint defenses undetected. If unfound, these attacks can compromise critical data, even gaining access across your entire environment. While traditional security programs are important, threat hunting goes above and beyond by identifying and ultimately helping to remediate vicious attacks.

Why It Needs to Matter to YOU

This is where YOU come in. The best front-line, security defense starts with the individual. As a security professional, you must know the best practices of the industry and be aware of existence and tendencies of these (and other) types of attacks. At Cloud Security Alliance (CSA), we aim to raise awareness of best practices to help ensure a secure cloud computing environment.

Each year there are an increasing amount of cloud security roles within organizations. No matter what your security focus is, having an understanding of how a threat actor thinks, how they operate, vulnerabilities they exploit along with an overview of the tools they use for attacks will allow you to be a more effective security professional. Having a better understanding from a threat actor point of view, whether deep or high-level, will assist you and your career in the following ways:

- Enable you to better explain security decisions to your peers, work colleagues and leaders.
- Promote better and more informed decision-making practices.
- Open the door to new opportunities and career paths.
- Share experiences by mentoring our next generation of security professionals.

What YOU Can Do

First, it is crucial that you know what "normal" looks like on your network. This is where you need to create a baseline, so comparison is easier. Anything not considered normal should immediately raise a red flag. Additionally, try to remain unbiased and do not let any preconceived notions affect your judgement of what normal looks like. Anything unordinary should be flagged for investigation or potential remediation.

Knowing what normal looks like on your network is a great baseline to begin threat hunting, however, it is just the beginning. Knowledge is power, as they say, and a security professional can never be overly informed. That is why CSA has partnered with RSA. With this partnership, RSA will begin to offer ongoing virtual threat hunting workshops. These workshops will cut through all the nonsense and give you real-world, practical, hands-on knowledge of why threat hunting is a critical part of any security program and give you the tools you need to stop the most malicious attacks.

To sign-up for the Hands On Threat Hunting Workshop please register using the following link - https://webinars.on24.com/rsa/VirtualHUHOCSAMinneapolis.

Any questions about the hands on workshop please send them to info@csamn.org.