TAG CYBER SECURITY

ANNUAL INTERVIEWS WITH CYBER LUMINARIES

HUMAN-LED. TECHNOLOGY-ACCELERATED.

ADVANCED TOOLS TO SUPPORT THE HUNT

AN INTERVIEW WITH
ERIC HIPKINS
CEO R9B

AS CYBERSPACE has emerged as the fifth domain of warfare, now with its own combatant command, addressing challenges has shifted. This is complicated by the crossover that exists between what might constitute an act of war and what is better classified as criminal activity. We are still on the frontier of sorting it all out. What we do know is that organizations across the public and private sectors need a new approach to defending networks.

Recently, threat hunting has become the buzzword across security circles. As the company that first introduced this concept to commercial markets in 2013, R9B has made it a priority to develop the best threat hunting products and services. R9B focuses on building powerful analysis and support tools to assist the modern hunter with the often-complex task of dealing with cyber threats. These tools range from credential-based risk analysis to active adversary tracking and hunting across either an enterprise or a larger infrastructure. We recently sat down with Eric Hipkins, CEO of R9B to better understand how R9B supports this critical task.

EA: What are the typical tasks of the modern cyber hunter?
EH: Most of the actions by threat hunters are dependent on mission requirements, so it is difficult to identify a typical set of tasks. Some organizations still view hunting as analysis against passive collection techniques, such as reviewing logs or network traffic. At R9B, we view hunting as a human-led approach to pitting a thinking defender against a thinking adversary. In this regard, some common skills needed for any hunting mission include experience with operating systems and networking, as well as an understanding of how threat intelligence integrates with mission parameters to guide the hunt and adapt to the adversary. On top of technical knowledge, a hunter's greatest ability is in creative thinking; generating hypotheses that can identify adversaries that bypass traditional defenses and hide in the network.

EA: What are the offerings from R9B that assist hunters in their work?
EH: Since 2011, we have provided training on a broad range of topics that can significantly improve the efficiency and effectiveness of a hunter. That includes courses in cyber threat intelligence analysis, adversary tactics and techniques, PowerShell foundations, and OS-specific

hunt certification. Our proprietary ORION platform was purpose-built for threat hunting. It is an agentless means of detecting, pursuing, and eliminating threats from networks. We recently gave it a new user interface and incorporated an API so that advanced hunt teams can customize it to their needs. Originally launched in 2013, ORION is currently used and has proven effective in both corporate and military environments. We also offer a credential risk assessment tool called ORKOS, which aids hunters by helping them quickly survey networks to identify connections that could make it easier for attackers to escalate privileges, moving from low-level to critical systems.

EA: Can you tell us more about how your solutions focus on credential risk?
EH: Early on, we recognized the importance of credential theft in the execution of malicious activities. In response, we developed software called ORKOS; a credential risk assessment tool designed for rapid deployment and credential risk vulnerability analysis. Administrators can quickly plug ORKOS into their network to get instant visibility into weak credentials (we use proprietary rainbow tables and hash matching to identify weaknesses while protecting privacy). Where ORKOS differs from less robust solutions is in its graphical representation of privilege associations, how they can create risks, and remediation recommendations. We believe strengthening passwords is a good first step, but we also want to make sure administrators know how an attacker might use a low-level frontline user to escalate privileges and move laterally through the rest of victim networks. ORKOS builds scenarios to provide custom remediation recommendations to mitigate identified credential risks within a virtualized environment.

EA: Do users have to be highly experienced in their craft to benefit from your tools?
EH: We have invested significant time and energy in making all our solutions easy to use. Our experiences have taught us that even the most experienced operators still appreciate quick deployment, good design, and intuitive controls. Threat hunting against advanced adversaries can still require a highly-specialized skill set and tools are only part of the equation. At R9B, our mantra is “human-led. technology accelerated.” So, to be an effective threat hunter, it does take a lot of knowledge and experience, but for those who know what they are looking for, our tools make life a lot easier.

EA: What are some hunt-related trends you’re seeing in your customer base?
EH: As the security industry continues to adopt threat hunting, it has been encouraging to see an uptick in the pace of technological development. There is better collaboration across the board. Overall data management is still a major challenge, but artificial intelligence and expert systems are powering faster and more accurate analysis. We recently made a significant strategic investment in a company called Champion Technology Company, Inc., whose DarkLight® AI expert system is helping our hunters find threats faster, so they can focus more on cleaning up the network. I look forward to continued collaboration, more development for API integrations, and better ways of making sense of the data