MISCONFIGURED SECURITY TOOLS CAN LEAVE YOU EXPOSED

It's time to validate the effectiveness of your cybersecurity solutions and here's why. A recent study showed that only a small percentage of attacks generate alerts and most intrusions go undetected due to misconfigured security tools.

"Due to the times we live in and this digital spell we're under, we all need security tools to protect us. But those tools need to be configured correctly in order to effectively block attacks." says Ray Panfil*, RAVENii's vCISO & Security Analyst.

Have you thought about that? Are your security tools configured to provide you with the most coverage and protection available?

In many cases security tools are not optimized, which can result in malicious activity in your network. Causes of this could be unchanged default configurations, changes to the infrastructure, or failure to care and feed the tools after their deployment.

One real example of this would be an insurance company that had misconfigured their security tools which allowed over one-third of the malicious file transfer attempts to land on their infrastructure. The attempts that were blocked did not trigger any alerts in the SIEM. In another instance, a Fortune 500 company that discovered the data about actual detected security events was not making it to the SIEM. The reason was because of a misconfigured load balancer.

RAVENii strongly encourages that everyone has a set of defined and actionable security standards to follow; like the 20 CIS Controls. Their purpose is to give you clarity on what to prioritize and focus on to defend your business from cyber-attacks.

"The controls will define what the best practices are for configuring your security tools," says Panfil. "The controls will expose your vulnerabilities and gaps in your security stack."

RAVENii can help you audit your security assets and assess your security posture. We're here for you if you don't know where to start, don't have the human capital, don't have the time or you just want another set of eyes as we believe we are all in this together!

*Panfil serves as the vCISO for multiple organizations. He guides them through the Controls and advises them on best practices, security policies and procedures, and security tools to consider.