From the Desk of Michael Yelland

Before the coronavirus pandemic, we all thought we were invincible and prepared because our emergency plans were in place with the worst-case scenario being …"we go old school and work with pen and paper!"

Then the pandemic hit, and we all had to execute our plans. Unfortunately, some of us discovered that our plans consisted of dated technology with obsolete or untested references. Which puts us in the position of making ad hoc decisions based on the sustainability and continuity of the business.

In moments like these, I always think of Scotty on Star Trek operating the *Enterprise* transporter system. He always, just in the nick of time, manages to do the impossible to save Captain Kirk and the *Enterprise*. Yeah, I know. It's typical Scotty; always cleaning up the mess. The part we don't see behind the scenes is Scotty and his engineering team saving the stars while taking the time to upgrade the systems in order to revert everything back to a functional state.

It's been a week and many of you have started to stabilize your technology stacks. Now it's time to double check that nothing critical was overlooked or leaked out. We are seeing the bad guy networks come online and adjust for the new attack service… your mobile workforce who now are using their personal devices to connect to your network.

RAVENii has been working with our premier partners to help in this endeavor at no cost to you and in a seamless matter to Identify new risks on your perimeter and edge-based technology.

MixMode, a leading network intelligence and AI integration tool for hunting and preemptive monitoring, is offering 90 days of on-premise baselines and hunting capabilities to identify unauthorized movement on the network. With today's larger dependency on RDP or its equivalent, there is a higher risk of cross contamination and incidents tapping into data exfiltration.

Tenable Security Center, a leader in vulnerability risk management, has graciously offered Tenable.io scanning to all our clients and partners through April 30, 2020. This will help identify all new and old ports, vulnerabilities and any items outside of our previewed risk.

Cylance, the leader in AI antivirus prevention, is offering 30 days of protection for all your mobile users. The greatest value add with Cylance is its prevention model is based on sequencing and signatures. This provides mobile users with a micro AV footprint while seamlessly exceeding the bloated footprint.

As tragedy hits and in this time of uncertainty, RAVENii recognizes the need for immediate action. Our SOC, Incident Response team, and architecture and engineering teams are at the helm and ready to help. Please don't hesitate to reach out if you want to harden the security posture of your remote workforce by taking advantage of these offers.

Stay safe and be well,

Michael Yelland

Michael Yelland
RAVENii Chief Security Officer