University Relies on Hillstone Networks to Address Scale and CyberSecurity

The Customer

Instituto Tecnológico Bolivariano is an accredited Institution of Higher Education in Ecuador. It is inclusive and recognized for its leadership, commitment to academic quality and excellence. It has mission to deliver critical and innovative education and training of technical professionals and technologists with a focus on the development of the environment, economic progress and social welfare of Ecuador. Currently, the ITB is one of the largest educational institutes in the country, with 10,000 students enrolled,and its continued growth is remarkable,

The Challenge

For the last three years, ITB has relied on entry level Hillstone T-series intelligent Next-Generation Firewall (iNGFW) solutions for networking, security, and content inspection. However, to address fast-growing throughput requirements, the university needed to upgrade its technology.

In addition, today's cyber attacks don't simply try to compromise and break into a victim host machine and network. Instead, the attackers carefully design and utilize post breach activities at different stages, such as DGA and botnet attacks. In such cases, it requires defense technologies at both the network perimeters, as well as inside the victim network for post breach threat detection and protection.

University Relies on Hillstone Networks to Address Scale and CyberSecurity

The Solution

With more than 10,000 students, 1,200 faculties, 20,000 active devices per day, the campus needed a more robust security platform. It turned, once again, to Hillstone Networks. After careful examination of the university's needs, Hillstone Networks recommended deploying two higher end T Series iNGFWs to provide optimal security, scalability and performance.

ITB deployed two T-series Intelligent Next Generation Firewalls (iNGFWs) in high availability mode, both hosted in their datacenter. In addition, the Institute deployed E-Series Next Generation Firewalls (NGFWs) in one of their branches located in another city, Guayaquil. These devices are connected via VPN to the Hillstone iNGFWs that are located in the datacenter. Through these VPNs, the Institute can use and also protect critical assets and applications including biometrics, VOIP server, laboratories, mail server, and NTP server, among others. To manage all these devices, they also deployed a virtual Hillstone Security Management (vHSM) platform in their datacenter.

"We wanted to future-proof the environment for at least the next three years, and we were already very happy with Hillstone Networks, who understand our requirements and can offer best-in-class performance and security while improving total-cost-of-ownership, combined with an intuitive user interface," adds Nelson Villacres, ITB CTO.

In addition to providing ITB with exceptional value, the Hillstone Networks platform has also delivered on the Institute's most important security requirements with a preventive, next-generation approach to network security that keeps even the most elusive cyberthreats at bay.

The Cyber Kill Chain (CKC) model on the iNGFW from Hillstone Networks provides real time visibility and deep insights into the post-breach threat attack path inside the victim network. Threat intelligence information is provided from multiple detection engines and mapped against the CKC stages with forensic evidence data and other actionable options. The detection engines include signature based Intrusion Prevention System and Antivirus, they also include iNGFW's Advanced Threat Detection (ATD) and Abnormal
Behavior Detection (ABD) Engines. ATD engine leverages machine learning to recognize abnormal and potentially damaging network behavior, such as malware CnC callbacks; the ABD engine monitors the network over time to build normal network behavior profiles, then subsequently monitors for any behavior abnormalities. Together, with other post breach threat detection mechanisms, it is a powerful and effective weapon to defend against today's most sophisticated cyberattacks.

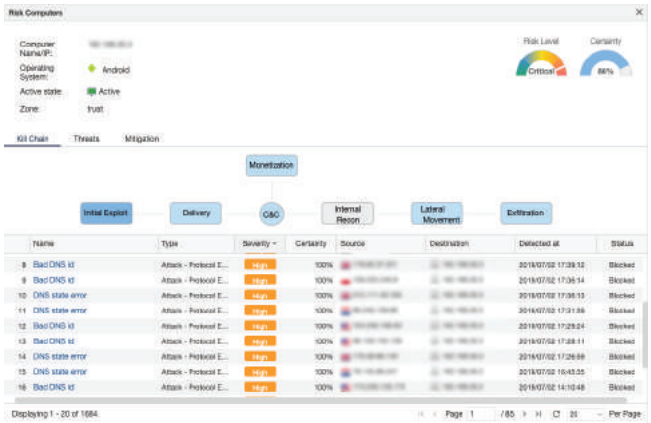

Figure 1. Detected Risk-Computers

The conclusion

"We have partnered together for more than four years and are very happy with the technology, service and support provided by Hillstone Networks," concludes Nelson. "We know it has solid position in this industry and are confident we will continue to work together for many years to come."

In summary, Hillstone is the solution that has resolved and addressed the needs of the Institute, by protecting of business continuity, while at the same time, delivering forensics and analysis, along with the necessary visibility to take prompt action in response to security events. Cybersecurity becomes that much easier to deliver.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more
or contact Hillstone at **inquiry@hillstonenet.com**