ProtectedIT

Government Case Study

ONE OF THE LARGEST DEFENCE ESTABLISHMENTS IN THE WORLD.

Escalating conflict at the borders necessitated hardening of cybersecurity measures

PROVIDING SPECIALISED & MSSP SERVICES

ProtectedIT
www.protectedit.net sales@protectedit.net

ProtectedIT
Elevating & Unifying Security Technologies

GOVERNMENT CASE STUDY 2020

"As the world grapples with deepening cybersecurity threats, we too have faced multiple cyberattacks and the number of attempts was substantially higher than witnessed last year. ***ProtectedIT was able to deploy advanced SIEM capabilities within a couple of weeks which was crucial to our security and success."***

Senior Defence Officer

THE SITUATION

The situation presented is one of constantly moving parts. While cyber security is important on many levels relating to business and people's livelihoods, the bar is set at a whole different level when it comes to government and defence entities infrastructure protection. This case study focuses on the cyber and network security of one of the largest government defence entities in the world.

The amount of information and people that need to come together on a daily basis in order to coordinate operations of all different scales in a country is phenomenal. For success, they all require seamless communication - from large scale operations relating to coordinated military action or critical infrastructure, vital lawmaking processes, public relations, down to small scale everyday municipal work in carrying out essential government services. Modern communication is all through networks. Essentially, cyber warfare on government is infiltrating another country's network(s) to find vulnerabilities, extract data through them, and interfere with functionality to confuse and weaken a nation. And with the spread of COVID-19 across the world, every single line of a supply chain could theoretically be points of weakness. They could be targeted for an attack because more mayhem equals more payout for these types of bad actors.

ProtectedIT

Access the most powerful security program from prevention through detection and remediation.

OUR APPROACH: DEPLOYING ADVANCED SIEM – RSA NETWITNESS

As a Managed Security Service Provider (MSSP), ProtectedIT's approach was to work with award winning Cybersecurity and Operational Security product partners RSA® to provide this defense client with predictive and proactive threat detection capabilities through the utilization of an evolved SIEM, RSA Netwitness. This state-of-the-art approach assures the client gets:

Pervasive visibility: Visibility across Endpoints (OS-level), Logs, Networks (Packets), VMs and the Cloud - combined with threat intelligence and business context

Detection of advanced types of attacks: Multiple sets of analytic techniques: Data science modeling and machine learning; user & entity behavior analytics (UEBA) to find unknown threat Library of known threat indicators alongwith 3rd party and Community derived Threat Intelligence

Ability to investigate and respond to attacks immediately and precisely: Validation of incidents with Endpoint and Cloud visibility and analysis

Connecting with the business to enable security teams to act and mitigate the full attack before it could impact the business and provide the teams with Automated response to drive efficiency

RSA NETWITNESS® PLATFORM

PERVASIVE VISIBILITY

Detection of Advanced Attacks

Investigation & Response

THE RESULTS

For the client, the support provided by ProtectedIT ensured that the client now has the full enterprise visibility across networks and can understand the breakdown between various threat vectors and the points in their process where these weaknesses exist.

With confidence, this defense entity is now able to anticipate their areas of highest risk based upon our risk assessment across the spectrum of the operation. From the initial probe/phishing marking the origin of an intrusion attempt, the client can now directly point to key answers of what was targeted, how the exploitation occurred, how attackers moved around once inside their network, and if others were then infected. The advanced RSA Netwitness Platform utilized by ProtectedIT provides the next level of insight and clarity so that essential factors like compliance reporting, orchestration and automation.

Learn more:

www.protectedit.net | sales@protectedit.net