Valiant Communications Limited
(An ISO 9001:2015 and ISO 14001:2015 Certified Company)
Regd. Office : 71/1, Shivaji Marg, New Delhi 110015, India
Corporate Identity No. : L74899 DL1993 PLC056652 | GSTIN : 07 AAACV4250G 1ZJ
T : +91-11-2592 8415, 2592 8416, 2541 0053 | F : + 91-11-2543 4300, 4105 5604
E : admin@valiantcom.com | W : www.valiantcom.com

VALIANT COMMUNICATIONS

Date: 21-08-2023

The Secretary,
BSE Limited
Phiroze Jeejeebhoy Tower,
25th Floor, Dalal Street,
Mumbai – 400 023

Ref: Press Release titled "Pilot project award for Valiant Cyber Security equipment by Grid Controller of India"

Dear Sir/ Madam,

With above reference, please find enclosed herewith the press release in compliance with SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

We hope you find the same in order.

Sincerely,
For Valiant Communications Limited

MANISH
KUMAR

Digitally signed by MANISH KUMAR
DN: c=IN, st=Delhi,
2.5.4.20=f8edcf657137457d93b17a1edcd18195cef
b71ed2525fd086a42a5ecf81910f4,
postalCode=110015, street=71/1,Shivaji
Marg,Delhi,New Delhi,Delhi-110015,
pseudonym=964f0dccdc75cb9356ec86ec263f0256
,
serialNumber=78667909cac1632b9441ec4965632
2a483976e102d509a6bc7998b933e4e0f38,
ou=COMPANY, o=VALIANT COMMUNICATIONS
LIMITED, cn=MANISH KUMAR
Date: 2023.08.21 09:38:40 +05'30'

Manish Kumar
Company Secretary

Pilot project award for Valiant Cyber Security equipment by Grid Controller of India

21-08-2023

Valiant Communications Limited announces the receipt of its pilot order from the Grid Controller of India (formerly known as POSOCO) a Government of India Enterprise, for its Cyber Security equipment for deployment in power grid network in India.

Since Grid Controller of India is the apex body and the National Load Despatch Centre, it supervises over the Regional Load Despatch Centres and monitors the operations and grid security of the National Grid, the scale of the opportunity is large.

The initially selected products by the Grid Controller of India are designed based on the guidelines of the Central Electricity Authority (CEA) on “Cyber Security in Power Sector Guidelines, 2021” with a need to detect undetected intrusions that result from firewall breaches, the presence of trojans which can be planted or introduced from within, detect any unlawful and unwarranted activities that may already be taking place within the network that would open holes for back-door entry from within the existing firewalls resulting in a cyber-attack or ransomware attacks. The selected products also enable in creating isolation zones / “hard isolation of OT Systems” in case of cyber-attacks / ransomware-attacks or unauthorized network intrusions.

One of the selected products - the VCL-2143, Network MouseTrαp, is an advanced Honeypot and is an essential network security and forensics tool that enables users to detect firewall breaches and unauthorized network intrusions in their network, in near real-time. It provides alerts in real time, including audio and visual alerts on detection of a network security breach / ransomware attack etc. It also fingerprints the credentials of the hostile entity who have entered the protected network by maintaining a complete log of their credentials such as IP address, domain and the originating location details of the intruder along with providing a trace-route of the intrusion.

This solution not only provides seamless scalability, is infrastructure neutral and transparent to networks and network applications.

The use of the VCL-2143, Network MouseTrαp becomes critical to any organization. By providing “Early Warning and Response Systems” behind the firewalls detection of cyber security incidents and helping mitigation of such cyber threats, safeguarding computer systems using early cyber-attack warning and intrusion detection algorithms with suitable audio-visual alerting mechanisms, and detecting cyber-attacks on SCADA and ICS systems, the VCL Network MouseTrαp plays an important role of strengthening cyber security systems of an organization.

In addition to the above, the selected VCL-2702, Network Isolation (Kill) Switch assists in creating Isolatable Operational Zones, which would include:

- To have the capability to automatically carry out physical asset isolation (the ability to isolate a specific location or an individual telecom rack which may be source of the threat.
- To instantly disconnect the critical zones within the LAN network from the WAN network in the event of the detection of a cyber-attack.
- Implementing automatic hard isolation of all ***back-up*** OT Systems (such as NAS/SAN, Data Storage Servers) from any network facing IT infrastructure in the event that a network breach is detected to ensure that the back-up sensitive data always remains un-compromised and protected.
- Create operational zone isolation and mechanisms of islanding of all critical assets such as protection relays, bay-control units and data storage devices in the event that a network breach is detected.

The need for implementing an effective cyber security and counter-defence strategy becomes an utmost important aspect of protecting our critical infrastructure like Thermal Power Plants, Hydro-Electric Generation and Transmission assets, Grid Operations as well as largely distributed renewable and power distribution infrastructure to ensure reliability and security in the National Power Grid. Firewalls alone cannot form the centrepiece of the cyber-security strategy as firewall can be breached not only from outside but (more often) from the inside by trojans, viruses or malware which may have been planted or introduced these from within the most vulnerable points of the network.

The artificial air gap created between IT and OT Systems by deploying only firewalls between any IT and OT System can be easily circumvented by any insider or any outsider. In short, having only firewalls as a tool to address a cyber-security defence strategy is a myth.

Commenting on award of the project, Mr. Inder Mohan Sood, CEO said “We are very happy with the opportunity to deploy our Cyber Security Suite in the Power Grid network in India. While various initiatives taken by the Government of India, under the leadership of our Hon'ble Prime Minister, such as “*Aatamnirbhar Bharat”,* “Make in India”, “Digital India” and “PMA Policy”, the initiatives taken by the Government of India are helping domestic manufacturers of telecom, communications, transmission, synchronization and cyber security equipment in India. This support is further helping us to take these unique and advanced cyber security solutions to the world”.

About Valiant Communications: Valiant Communications is a manufacturer of a comprehensive range of IT and OT products and solutions which are used to provide end-to-end communication, transmission, protection, synchronization and cyber-security in Government, Defence, Transport, Utilities and the Power sector. VCL is an approved manufacturer to various reference customers across the globe, with track record of successful installations of its communications, transmission, protection, synchronization and cyber-security solutions in more over 110 countries.