

Africa to get three top-notch cyber security facilities

NEC XON is creating three new Cyber Defence Operations Centres (CDOC), one in Nigeria, another in Senegal, and the third in Mauritius in addition to the existing facilities in South Africa.

The new cyber security facilities form the nucleus of pan-African collaboration for sharing global threat intelligence to help African law enforcement agencies rapidly respond to attacks, help identify hackers, and help apprehend the perpetrators.

“These three centres form part of NEC’s global footprint of hybrid cyber security centres, complementing the facilities in Japan, Australia, Singapore, South Africa, Brazil, Vienna, and the US,” says Vernon Fryer, head of NEC XON’s CDOC. “Together they form a global nexus of unparalleled threat intelligence and kernel of expertise that will, for the first time, offer visibility into the threat landscape within Africa.”

NEC also collaborates closely with Interpol and various other global organisations in the fight to secure the safety and wellbeing of citizens in many countries.

African threat intelligence has so far been slender. It has been possible to determine if attacks are intercontinental, originating elsewhere and targeting Africa, or vice versa, but little more.

“The countries where we are establishing the new hybrid cyber security facilities will act as hubs to also serve their neighbours,” says Fryer. “Infrastructure and expertise of the kind we are now establishing has so far been limited because many of these countries face numerous challenges not limited to national physical and cyber security. They are, subsequently, challenged to find the resources to deal with all of them separately. Being able to provide hybrid cyber security services that link the cyber world to the real world, as well as the related skills transfer and training functions that form part of the development, represent an enormous boon to the continent’s security capabilities.”

The initial primary focus of the security facilities will be serving government law enforcement agencies and the financial sector.

“African countries are increasingly coming under heavy cyber attacks,” says Fryer. “Ethiopia is subject to the most numerous government hacks of any African nation. Zimbabwe is driving a rigorous cyber strategy because they’ve been hit so hard. My system tells me that Nigeria has 1 571 attacks occurring right now. Nigeria, South Africa, and Central African Republic are currently three of the hottest cyber attack spots in Africa.”

Fryer says that these are often gateway attacks. Those attacks originate elsewhere in the world but use African locations as springboards to off-continent attacks so they appear to originate here.

“Our customers also get the full range of services and solutions from creating data centres to field infrastructure and services, even including alternative energy, and the networks that connect everything,” says Fryer. “The CDOC unites the worlds of physical and cyber security that include analytics and biometrics systems. The individual services are too numerous to mention but range from access and perimeter control and surveillance to fingerprinting, iris recognition, to big data analytics to provide facial recognition at scale, crowds in public areas behaviour monitoring and control, and then the increasingly crucial cyber security technologies and services.”