Explanation of Wireshark and NORSE

**Wireshark**

Wireshark is a packet sniffing program that reads the network traffic from a network adapter on the computer. It can watch several types of traffic that runs on the TCP, UDP, ARP and ICMP protocols. It specifies to the user what kind of traffic being transmits through ports such as ARP, MDNS, DNS, ICMP, HTTP, TLSv6, LLMNR, SMB, and other protocols. The intended purposes of using Wireshark for network administrators use it to troubleshoot network problems, network security engineers use it to examine security problems, developers use it to debug protocol implementations, and people use it to learn network protocol internals. The features that Wireshark provides is it available for UNIX and Windows. Capture live packet data from a network interface. Open files containing packet data captured with tcpdump/WinDump, Wireshark and number of other packet capture programs. Import packets from text files having hex dumps of packet data. Display packets with very detailed protocol information. Save packet data captured in real time. Export some or all packets in many capture file formats. Filter packets on many criteria. Colorize packet display based on filters. Create various statistics and a lot more. Wireshark is not an intrusion detection system. It will not warn you when someone does strange things on your network that he/she is not allowed to do. However, if strange things happen, Wireshark might help figure out what is really going on. Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

**NORSE**

NORSE is a cybersecurity map that shows attacks occurring in real-time. It lists which countries that highest amount of attacks originated. The United States is the highest country with the most attack targets and origins. It lists the type of attacks by port and service type. The common attack types occur on ports 25, 23, and 8080 and service type STMP, telnet and http-alt. NORSE maintains the world’s largest dedicated threat intelligence network. With over eight million sensors that emulate over six thousand applications – from Apple laptops to ATM machines, to critical infrastructure systems, to closed-circuit cameras – the Norse intelligence Network gathers data on who the attackers are and what they’re after. Norse delivers that data through the Norse Appliance, which pre-emptively block attacks and improves your overall security ROI, and the Norse Intelligence Service, which provides professional continuous threat monitoring for large networks. Norse receives instant attack telelmetry from more than 8 million sensors deployed everywhere in the world. Norse operates the world’s largest commercial attack intelligence database, with more than 7 petabytes of detailed attack histories. Norse sensors and honeypots can emulate more than 6,000 commonly-attacked devices and applications. Norse runs in 47 countries around the globe. Norse weighs more than 1,500 actuarial variables in risk score calculations for every IP address, and resources more than 1 million discusses every day. Norse tracks more than 200,000 tor exit nodes: that five times more than any other intelligence source. Norse receives instant attack telemetry from more than 8 million sensors deployed everywhere in the world. Norse is marketed to government agencies. The company is based on the philosophy that Norse is dedicated to delivering live, accurate and unique attack intelligence that helps our customers block attacks, uncover hidden breaches and track threats emerging around the globe.