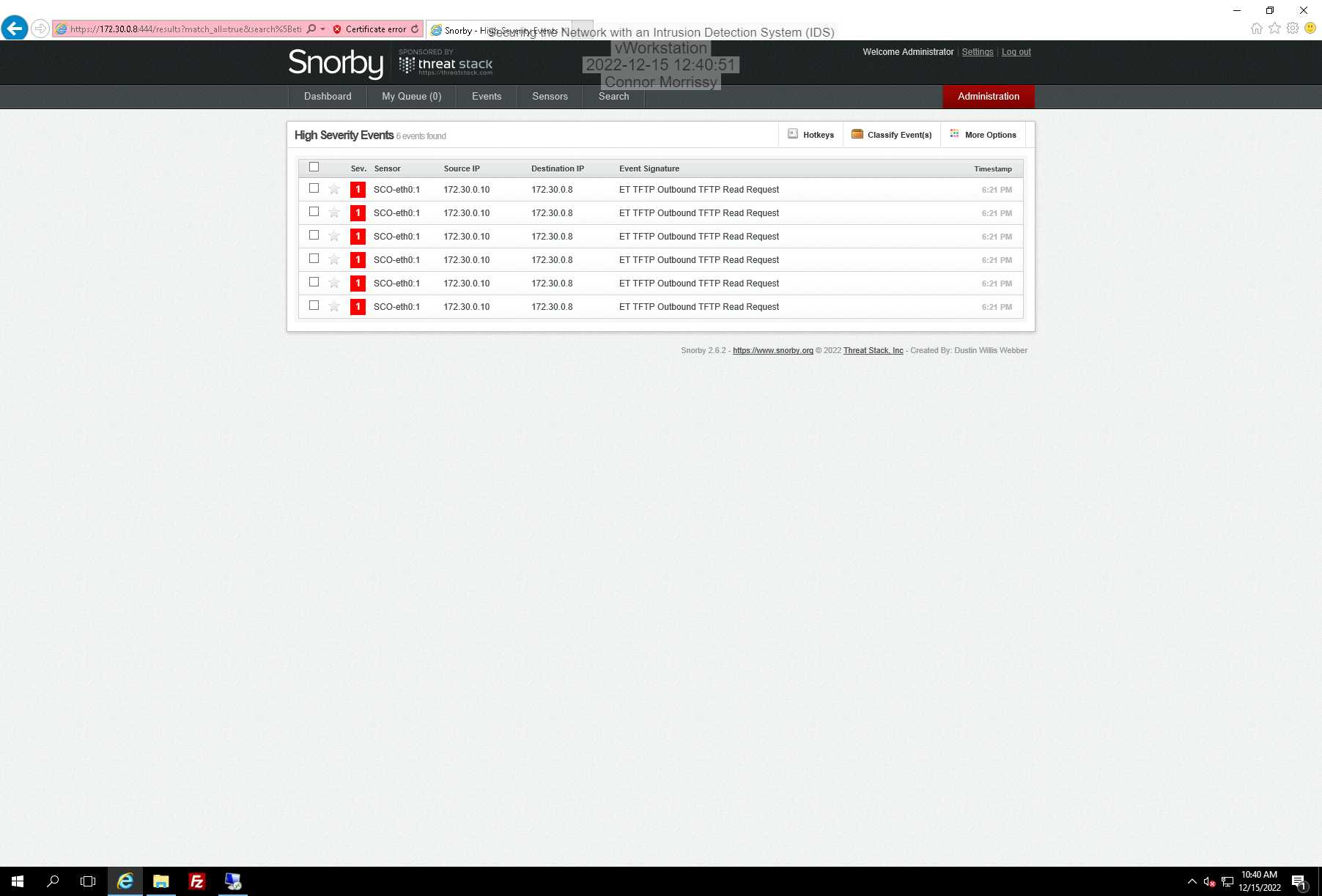
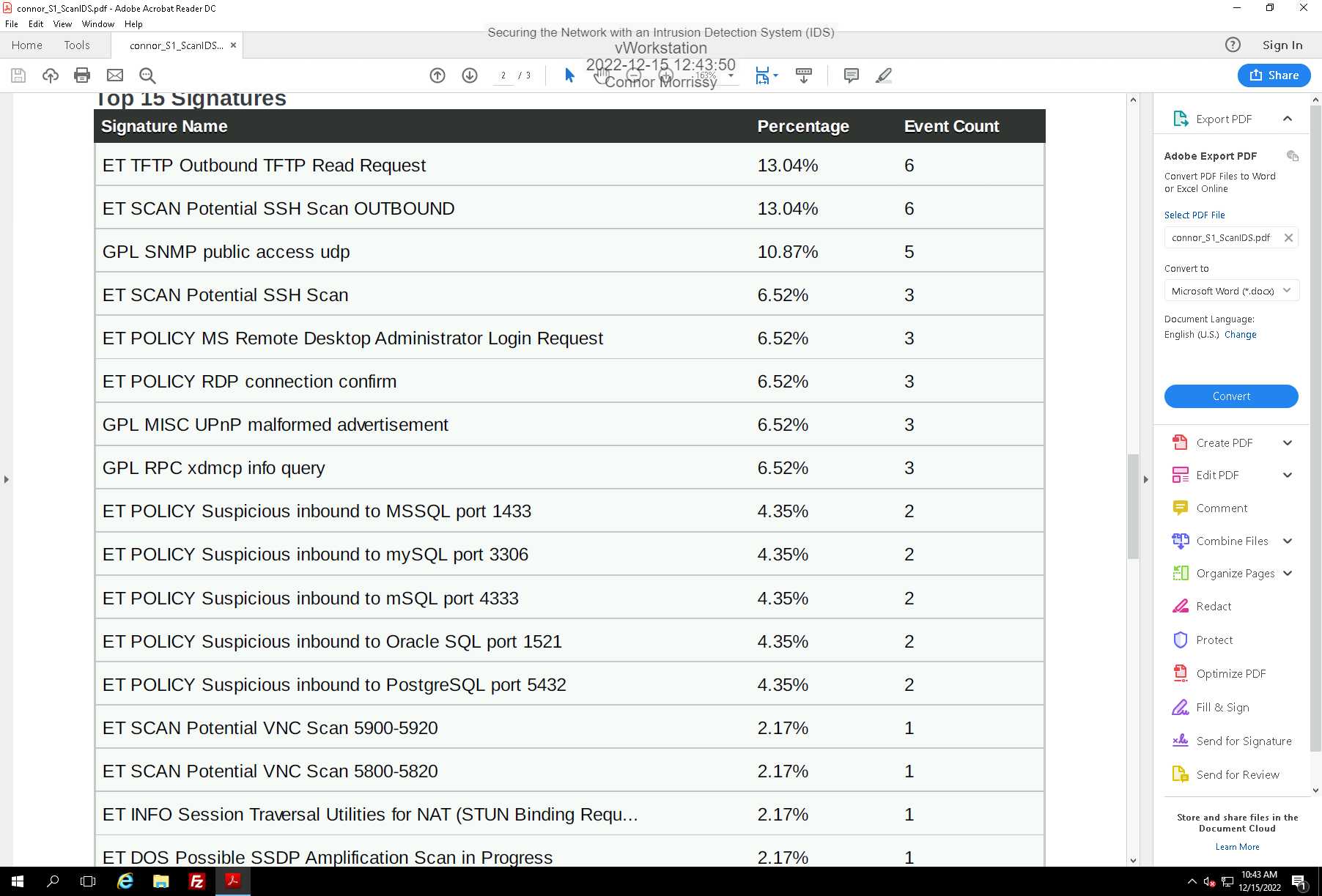
**Section 1:**

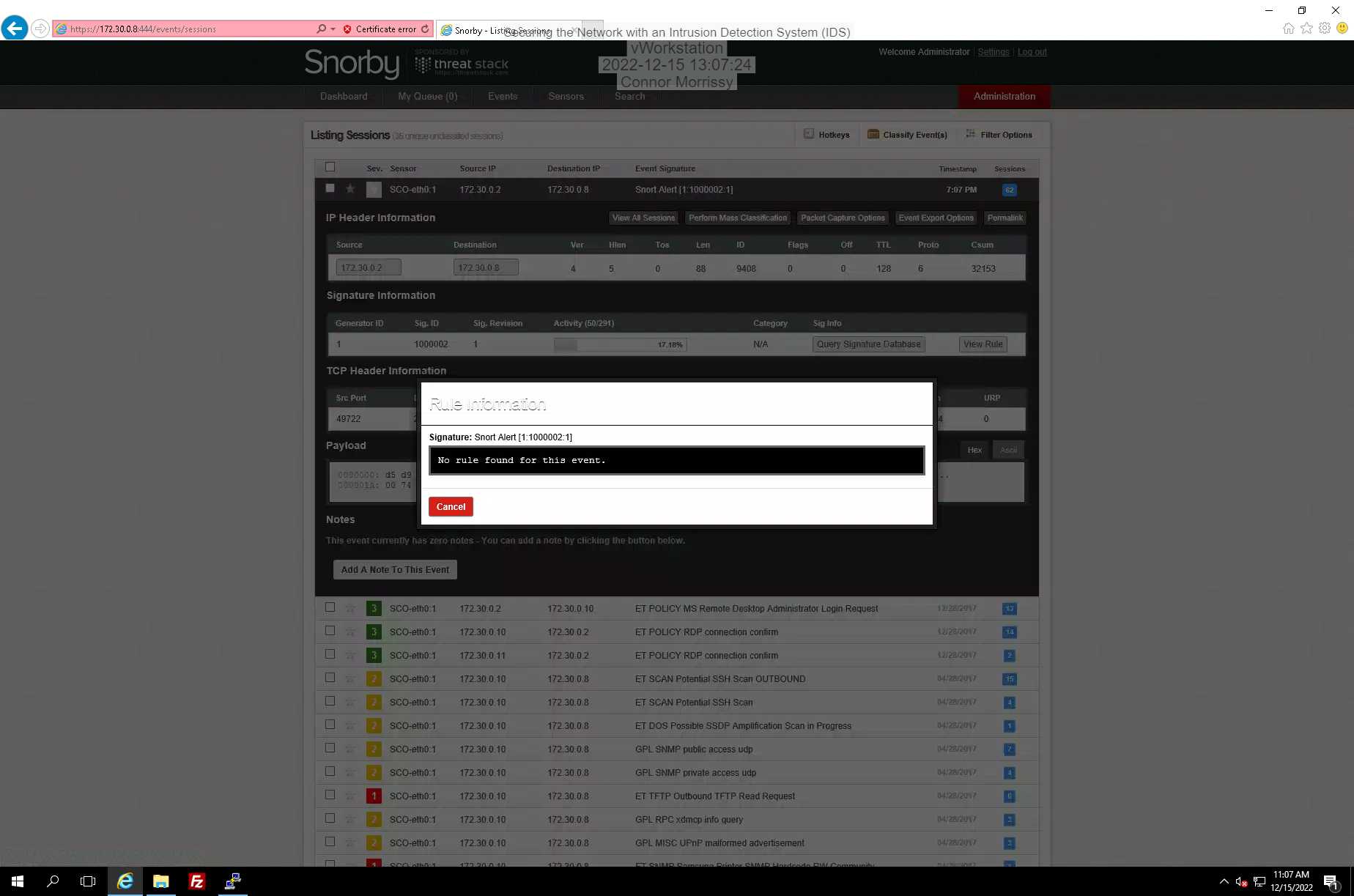


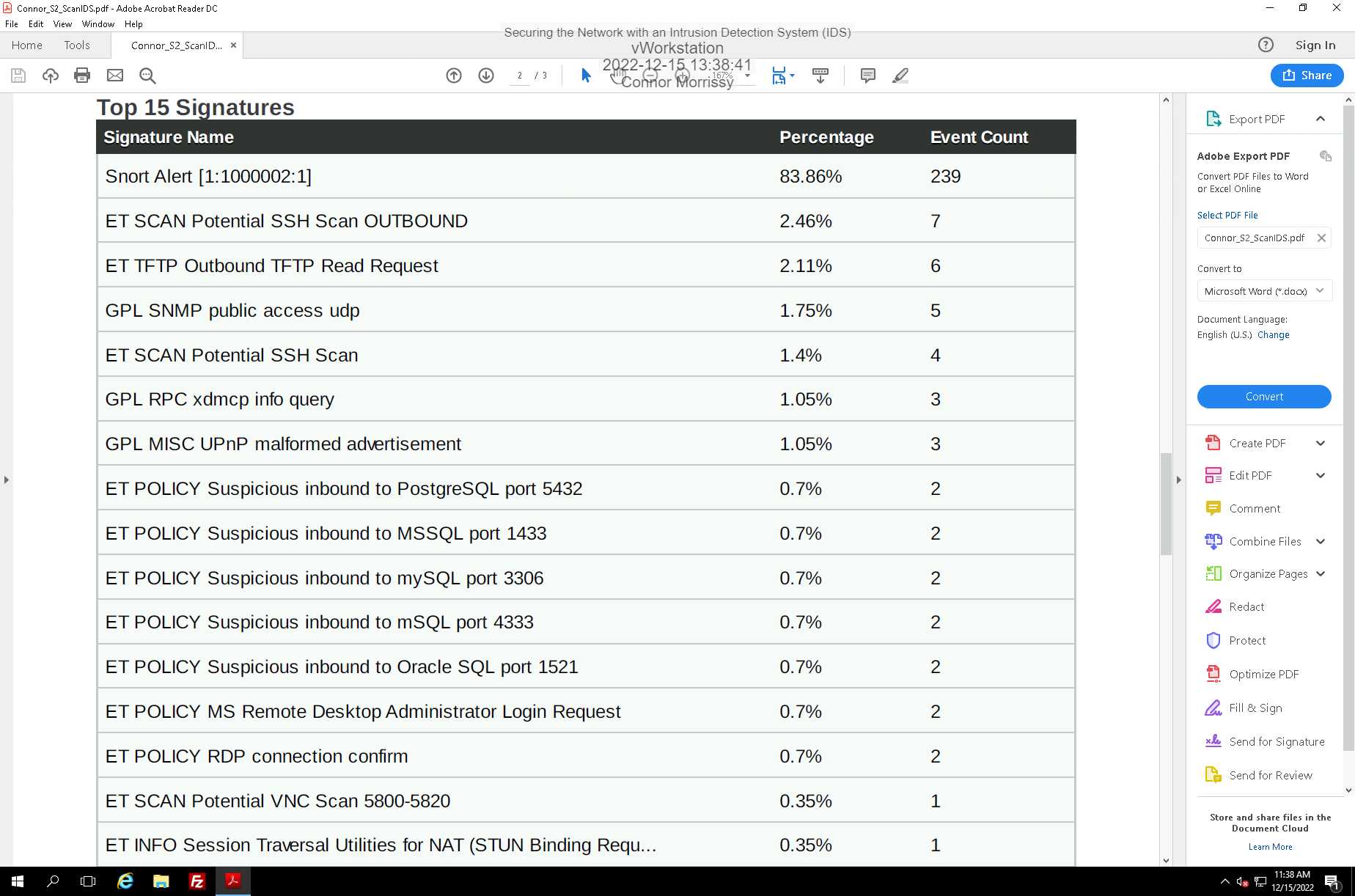




**Section 2:**







ET SCAN Potential SSH Scan OUTBOUND:

alert tcp $HOME\_NET any -> $EXTERNAL\_NET 22 (msg:"ET SCAN Potential SSH Scan OUTBOUND"; flow:to\_server; flags:S,12; threshold: type threshold, track by\_src, count 5, seconds 120; reference:url, en.wikipedia.org/wiki/Brute\_force\_attack; reference:url,doc.emergingthreats.net/2003068; classtype:attempted-recon; sid:2003068; rev:7; metadata:created\_at 2010\_07\_30, updated\_at 2010\_07\_30;)

ET TFTP Outbound TFTP Read Request:

alert udp $HOME\_NET any -> [$EXTERNAL\_NET,!255.255.255.255] 69 (msg:"ET TFTP Outbound TFTP Read Request"; content:"|00 01|"; depth:2; reference:url,doc.emergingthreats.net/2008120; classtype:policy-violation; sid:2008120; rev:4; metadata:created\_at 2010\_07\_30, updated\_at 2017\_01\_12;)

ET POLICY Suspicious inbound to mySQL port 3306:

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3306 (msg:"ET SCAN Suspicious inbound to mySQL port 3306"; flow:to\_server; flags:S; threshold: type limit, count 5, seconds 60, track by\_src; reference:url,doc.emergingthreats.net/2010937; classtype:bad-unknown; sid:2010937; rev:3; metadata:created\_at 2010\_07\_30, former\_category HUNTING, updated\_at 2018\_03\_27;)

**Section 3:**

Part 1: