**Team:** Team 1

**Inject Number:** 10

**Inject Duration:** 60 Minutes

**Inject Start Date/Time:** Sat, 10 Nov 2018 15:58:36 +0000

**From:** IT Director

**To:** Infrastructure Team

**Subject:** Evaluate Exposure

Use a tool, like Wireshark, on the Windows10 system which is outside the PA firewall. Look at the inbound and outbound traffic and develop a memo that:

- Illustrates your evaluation of whether the network has unexpected flows, i.e. packets to services on servers that are not legitimate. Likewise, traffic flows
coming from inside the network that are unexpected and unexplained. These might be signs of compromised systems and ongoing attacks.

- Catalog, specifically, what steps you have taken with the PA firewall, and/or local software firewall policies to mitigate these.

Thank you.

*IT Director*