UWO CSIRT Processes (High-Level)

Preparation
- Ongoing by UWO ITS (CISO, Security Working Group, Network Security Office, and others)

Detection
- HelpDesk Reports (to ITS)
- IDP Events (NSO)
- FW Events (NSO/ITS)
- SysAdmin Reports (ITS/others)
- HW/SW Alerts (many)

Triage & Response
- Categorize, Prioritize & Assign (CISO/ITS)
- Technical Response (ITS/others)
- Management/Legal Responses (CISO/others)
- Incident Closure (CISO/ITS/others)
- Lessons Learned (CISO/ITS/others)

Protection
- Ongoing by UWO ITS (CISO, Security Working Group, Network Security Office, and others)