eTrust

Background

The eTrust analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze security trends, suspicious behaviors, users insights and much more. This logs analysis App helps measure, troubleshoot, and optimize your network integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

- The eTrust application is based on the logging from the eTrust audit log.
  For enabling the application on the XpoLog software, please do the follows:
- Create a TCP\UDP listener in your XpoLog environment.
- Enter to your eTrust console and direct it to sent the logs as syslog to the relevant listener which was configured in the previous section.
  When adding/editing the eTrust log to XpoLog, it is mandatory to apply the correct log types:
- **syslog, etrust, audit**
- Once the required information is set, edit the log pattern, this step is crucial to the accuracy and deployment of the eTrust App. Use the following patterns for each of the logs:
  {text} {text:Server Name,ftype=servername} {text:CEF} {text:Version}|
  {text:CA,ftype=ca}|{text:PIM,ftype=pim}|{text:SP,ftype=sp}|{text:Header,ftype=header}|{text:Event Description,ftype=eventdescription}|{text:EventCode,ftype=eventcode}|
  {properties:Properties,keysSep==;propSep=space;,event_header#_#ftype=eventheader#_#name=Event Header;shost#_#ftype=sourcehost#_#name=Source Host;dhost#_#ftype=targethost#_#name=Destination Host;event_type#_#ftype=eventtype#_#name=Event Type;status#_#ftype=status#_#name=Status;susr#_#ftype=username#_#name=Source User;dst#_#ftype=dst#_#name=DST;program#_#ftype=program#_#name=Program;start;time#_#date::dateFormat=HH:mm:ss#_#dateUIFormat=dd/MM/yyyy HH:mm:ss;message#_#ftype=message#_#name=Message;User_Logon_Session_ID#_#ftype=sessionid#_#name=User Logon Session ID;Audit_flags#_#ftype=auditflags#_#name=Audit Flags;nStatus#_#ftype=nstatus#_#name=Nstatus;rt#_#ftype=rt#_#name=RT;nReason#_#ftype=nreason#_#name=Nreason;nStage#_#ftype=nstage#_#name=Nstage;act#_#ftype=action#_#name=Action;administrator#_#ftype=administrator#_#name=Administrator;class#_#ftype=class#_#name=Class;object#_#ftype=object#_#name=Object;command#_#ftype=command#_#name=Command;on_behalf#_#ftype=onbehalf#_#name=On Behalf;resource#_#ftype=resource#_#name=Resource;access#_#ftype=access#_#name-Access;on_behalf_of#_#ftype=onbehalfof#_#name=On Behalf Of;daemon#_#ftype=daemon#_#name=Daemon;service#_#ftype=service#_#name=Service;file#_#ftype=file#_#name=File;deployment_task#_#ftype=deploymenttask#_#name=Deployment Task;engine_service#_#ftype=engineservice#_#name=Engine Service;event_name#_#ftype=eventname#_#name=Event Name;server_name#_#name=Server;event_date#_#name=Event Date;host#_#ftype=host#_#name=Host;account_type#_#ftype=accounttype#_#name=Account Type;is_disconnected#_#ftype=isdisconnected#_#name=Is Disconnected;suid#_#ftype=suid#_#name=SUID;suser#_#name=Suser;user_last_name#_#ftype=lastname#_#name=User Lastname;nimbus#_#ftype=nimbus#_#name=Nimbus;opt_nimbus#_#name=Opt Nimbus;attributes#_#ftype=attributes#_#name=Attributes;mac_address#_#ftype=macaddress#_#name=Mac Address}