SOC & MISP

David Crooks
david.crooks@glasgow.ac.uk

The issue

- Lots of discussion of new security context
- VMs, new malware, new actors
- Sites with different levels of expertise
- Expose useful tools to more sites to help
- Structure of security and incident handling

SOC

- Lots of interest in Security Operations Centres
- OpenSOC (CISCO)
  - Apache Metron (https://metron.incubator.apache.org)
- Wide use, though not necessarily in our community

SOC installation

- Typical SOC installs can be complex:
  - Data ingest
  - Stream processing
  - Network monitoring
  - Distributed storage
  - Visualisation
  - Response
  - Data sharing
- Not all sites have expertise in all these areas

A place to start

- Looking at this work, and in discussion with Liviu, a useful tool: MISP

- misp-project.org

- **M**alware **I**nformation **S**haring **P**latform

- Coordinate and structure incident response information and sharing of IOC data (Indicator of Compromise)
  - See also openioc.org

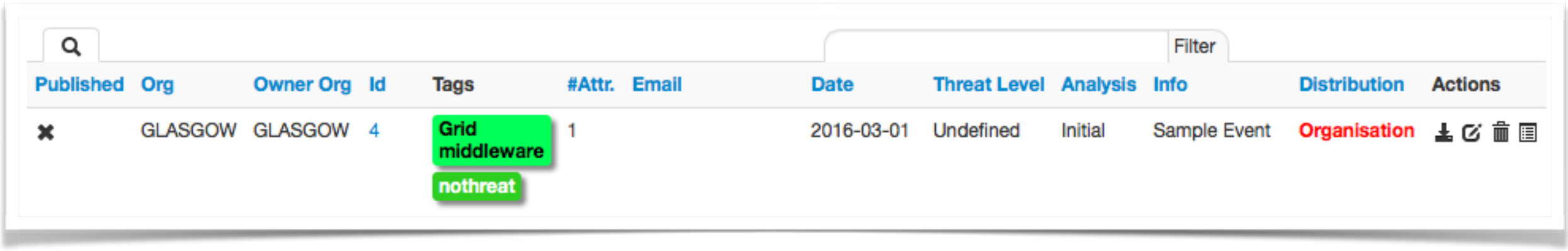
Information sharing:MISP

- Starting to work with this in the UK
- Intention to have small set of sites to share information
- Proof of concept installs in place, need to be properly secured but useful for initial work with fake data
  - Ansible playbook
  - Puppet module?

Preliminary findings

- Over the next few slides point out some useful and thoughtful features which can aid admins during incident response in what can be a very stressful time

Event list



Filter

Published	Org	Owner Org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✖	GLASGOW	GLASGOW	4	Grid middleware nothreat	1		2016-03-01	Undefined	Initial	Sample Event	Organisation	

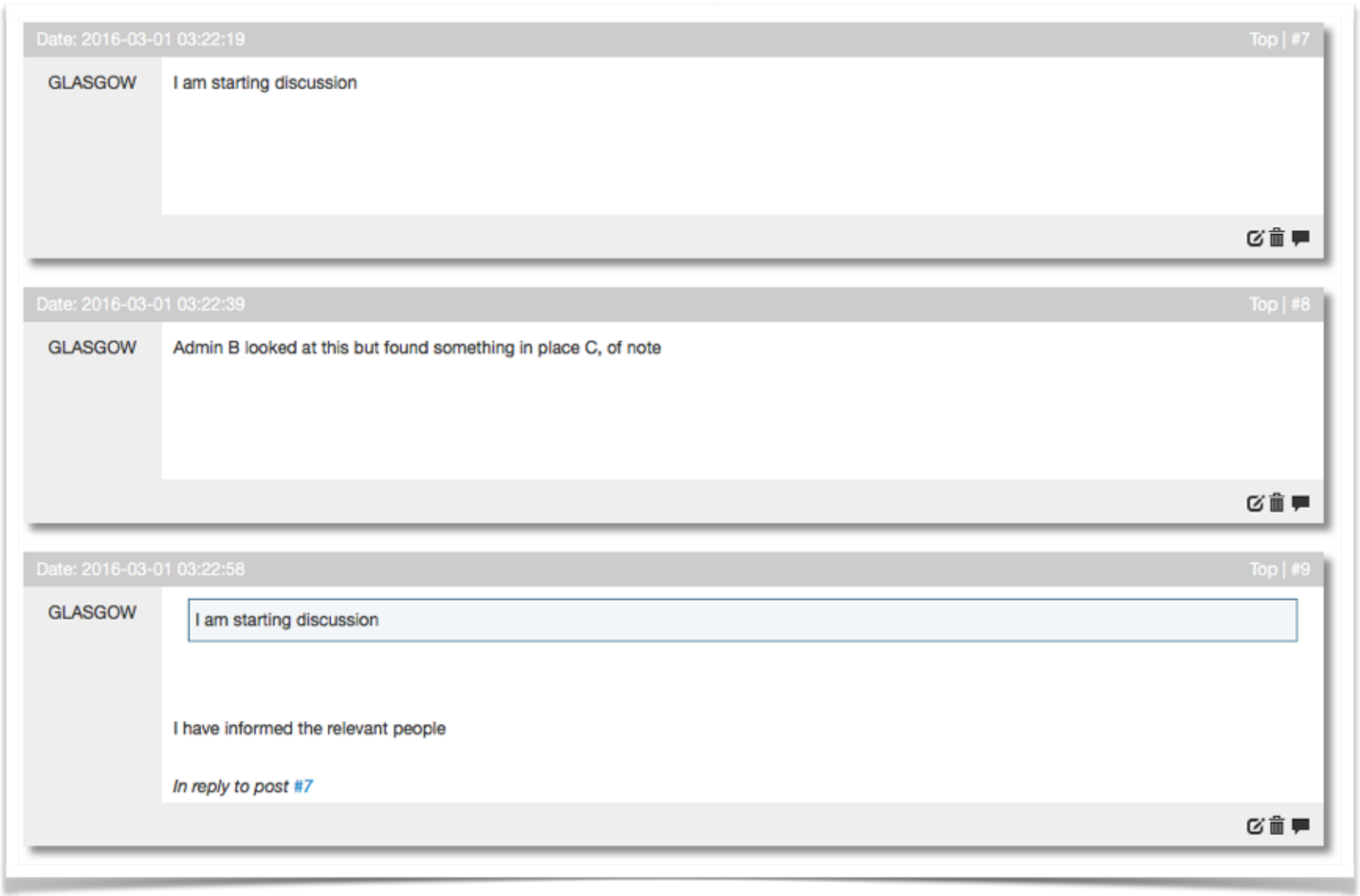
Event information

Sample event

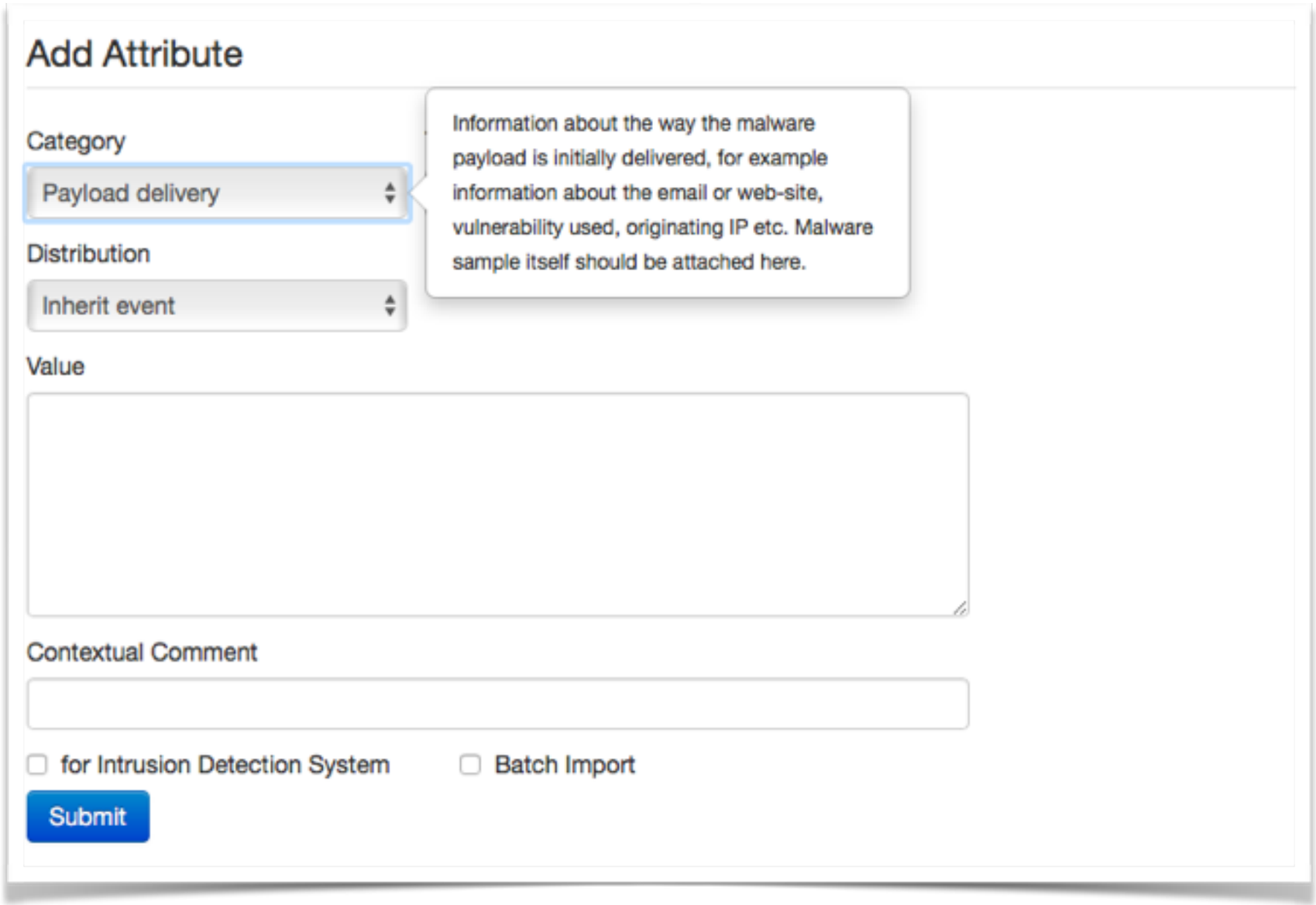
Event ID	3
Uuid	56d4fa46-8900-414b-aaae-03b50a00020f
Org	GLASGOW
Owner org	GLASGOW
Contributors	
Email	
Tags	+
Date	2016-03-01
Threat Level	High
Analysis	Initial
Distribution	This community only
Description	Sample event
Published	No

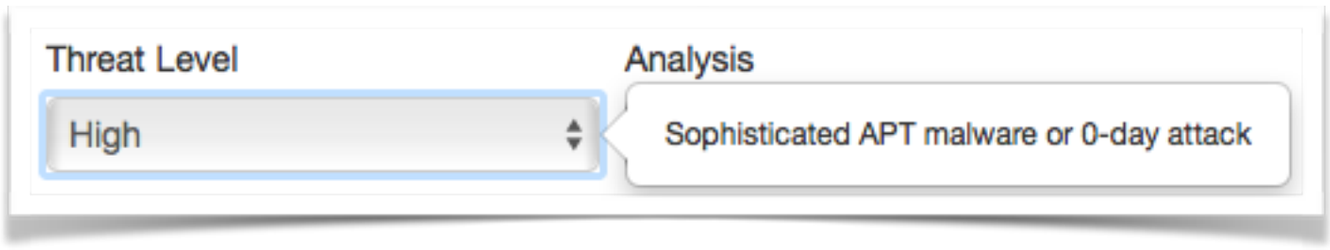
+ Pivots + Attributes + Discussion

Discussions

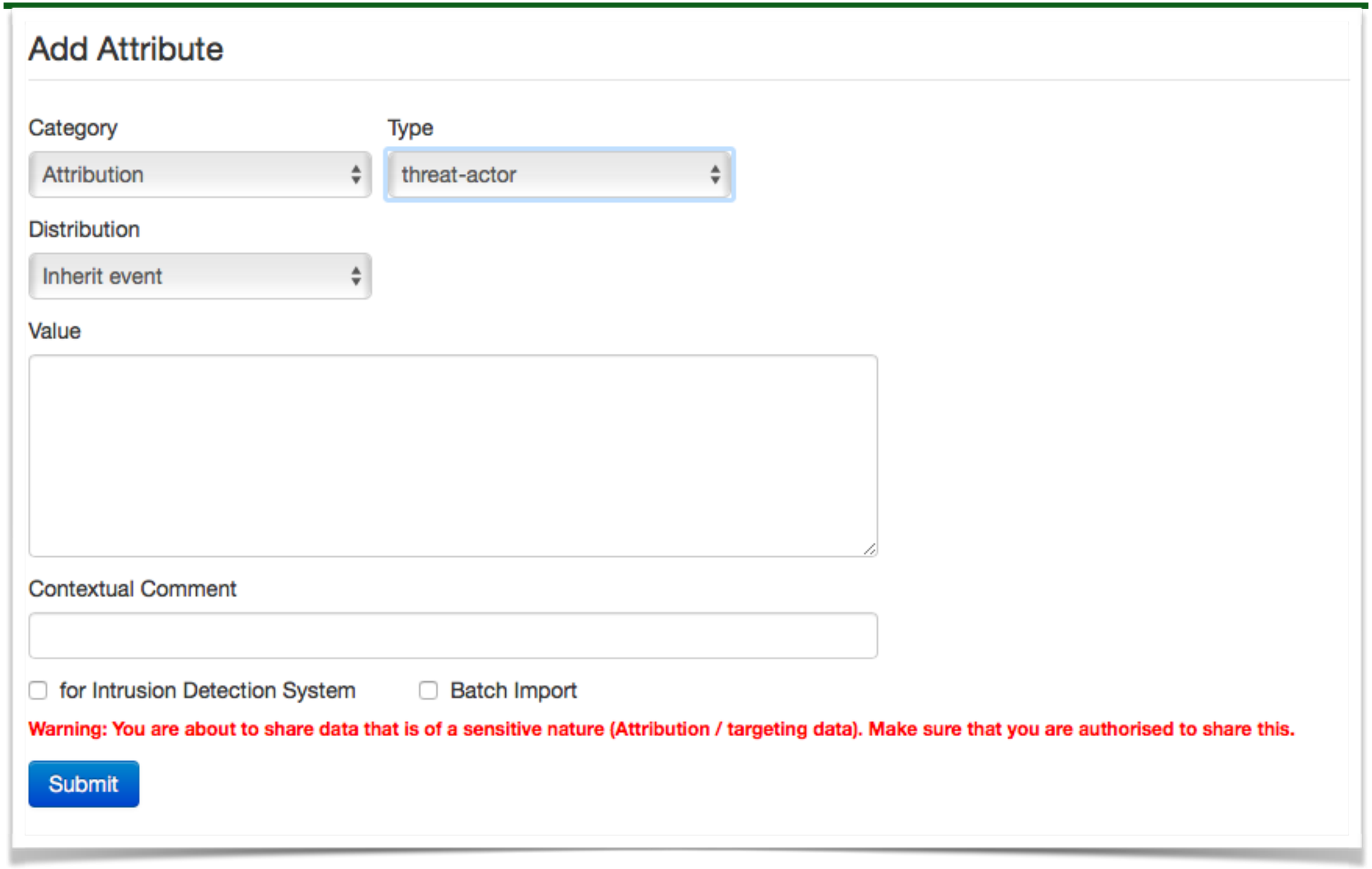


Attributes (tooltips)

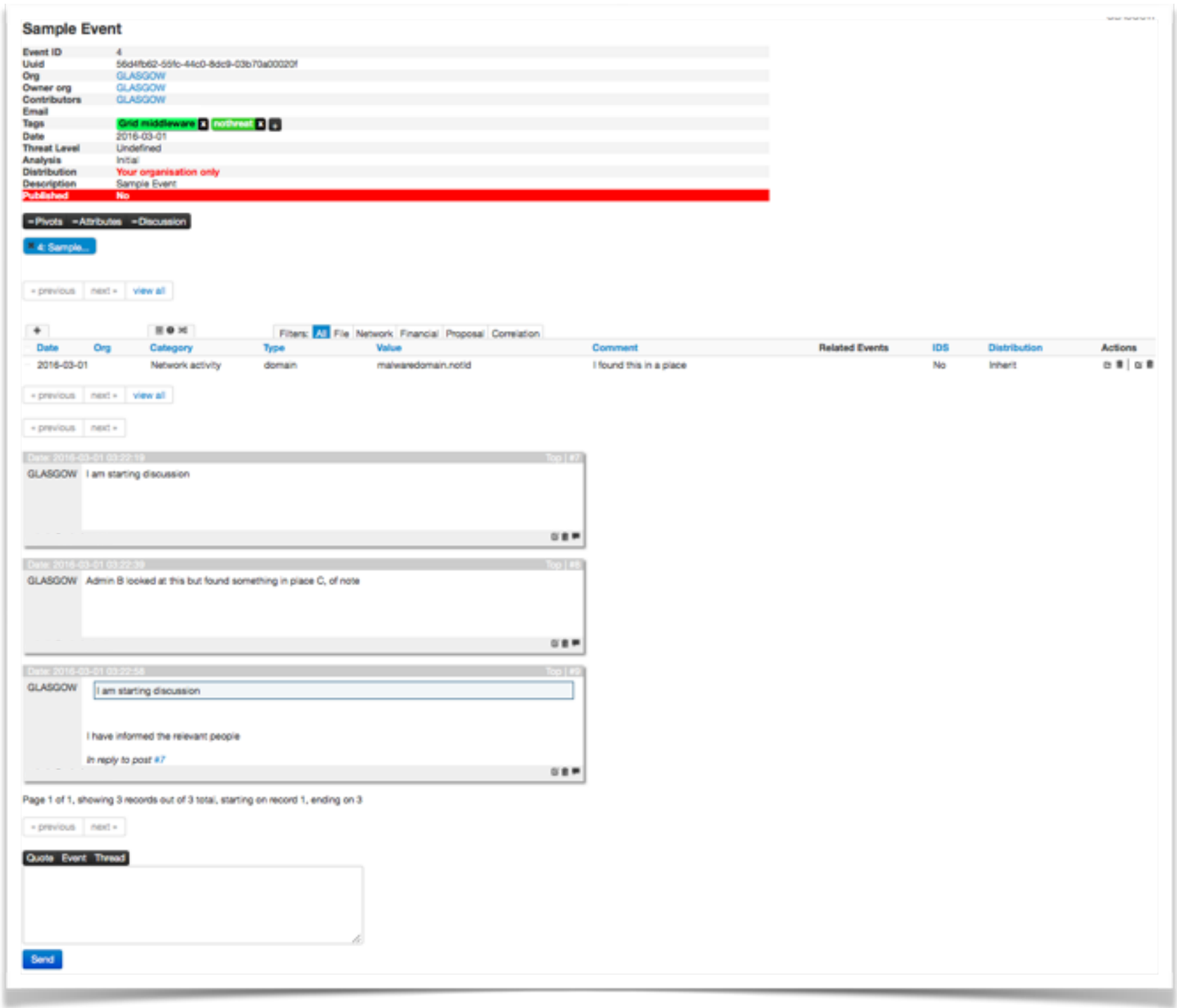




Contextual warnings



Event information



Features

- Early days for us, but useful aspects:
  - Events with attributes - common, structured information about incidents in progress where local admins can add data in well understood fashion
  - Data can be shared in granular fashion - local organisation, different communities
  - Tags, data attributes can be added to each event
  - Built-in discussion forums; all information in one place
  - Potentially useful for NGI security teams to assist sites in handling incidents following EGI CSIRT?

Future work

- Build small network of sites to test granular data sharing with fake (not live!) data, before proceeding to further steps

- Cluster management modules