

# SOC & MISP

---

David Crooks

[david.crooks@glasgow.ac.uk](mailto: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](https://misp-project.org)
- **Malware Information Sharing Platform**
- Coordinate and structure incident response information and sharing of IOC data (Indicator of Compromise)
  - See also [openioc.org](https://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

---

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	<a href="#">GLASGOW</a>
Owner org	<a href="#">GLASGOW</a>
Contributors	
Email	
Tags	<a href="#">+</a>
Date	2016-03-01
Threat Level	High
Analysis	Initial
Distribution	This community only
Description	Sample event
<b>Published</b>	<b>No</b>

[+ Pivots](#) [+ Attributes](#) [+ Discussion](#)

# Discussions

---

Date: 2016-03-01 03:22:19

Top | #7

GLASGOW I am starting discussion



Date: 2016-03-01 03:22:39

Top | #8

GLASGOW Admin B looked at this but found something in place C, of note



Date: 2016-03-01 03:22:58

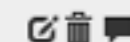
Top | #9

GLASGOW 

I am starting discussion

I have informed the relevant people

*In reply to post #7*



# Attributes (tooltips)

---

### Add Attribute

Category  
Payload delivery

Distribution  
Inherit event

Value

Contextual Comment

for Intrusion Detection System     Batch Import

**Submit**

Information about the way the malware payload is initially delivered, for example information about the email or web-site, vulnerability used, originating IP etc. Malware sample itself should be attached here.

Threat Level  
High

Analysis  
Sophisticated APT malware or 0-day attack

# Contextual warnings

## Add Attribute

Category

Attribution

Type

threat-actor

Distribution

Inherit event

Value

Contextual Comment

for Intrusion Detection System

Batch Import

**Warning: You are about to share data that is of a sensitive nature (Attribution / targeting data). Make sure that you are authorised to share this.**

Submit

# Event information

### Sample Event

Event ID: 4  
Uuid: 56d4fb62-55fc-44c0-8dc9-03b70a00020f  
Org: GLASGOW  
Owner org: GLASGOW  
Contributors: GLASGOW  
Email:  
Tags: **Grid middleware** **nothreat**  
Date: 2016-03-01  
Threat Level: Undefined  
Analysis: Initial  
Distribution: **Your organisation only**  
Description: Sample Event  
**Published: No**

[Pivots](#) [Attributes](#) [Discussion](#)

4: Sample...

[previous](#) [next](#) [view all](#)

Filters: All File Network Financial Proposal Correlation

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2016-03-01		Network activity	domain	malwaredomain.netid	I found this in a place		No	Inherit	<a href="#">edit</a> <a href="#">delete</a>

[previous](#) [next](#) [view all](#)

[previous](#) [next](#)

Date: 2016-03-01 03:22:19 [Top](#) | #7

GLASGOW I am starting discussion

Date: 2016-03-01 03:22:39 [Top](#) | #8

GLASGOW Admin B looked at this but found something in place C, of note

Date: 2016-03-01 03:22:58 [Top](#) | #9

GLASGOW

I have informed the relevant people

In reply to post #7

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

[previous](#) [next](#)

[Quote](#) [Event](#) [Thread](#)

[Send](#)

# 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