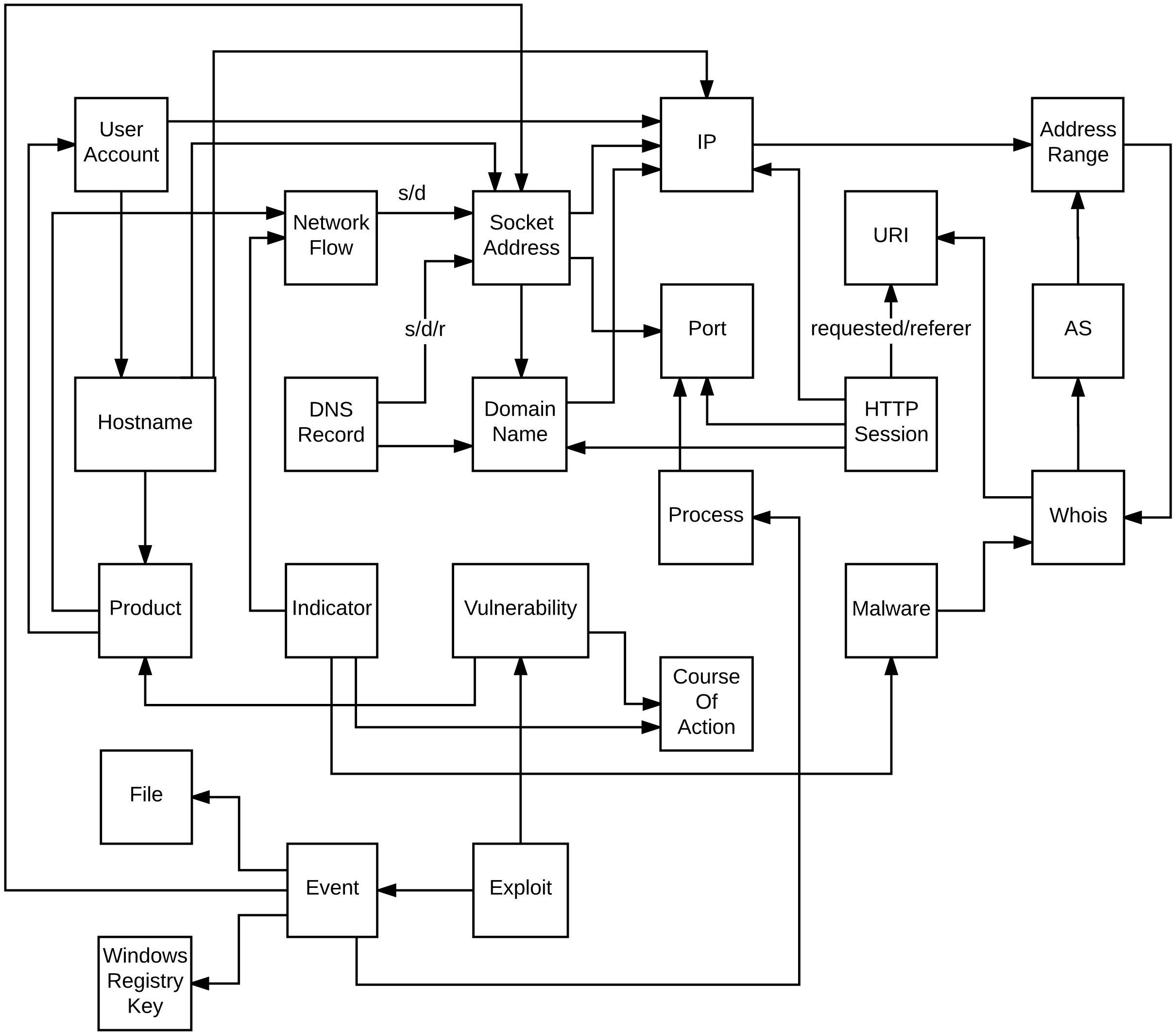
User Account
IP
Address Range
Network Flow
s/d
Socket Address
URI
s/d/r
Port
requested/referer
AS
Hostname
DNS Record
Domain Name
HTTP Session
Process
Whois
Product
Indicator
Vulnerability
Malware
Course Of Action
File
Event
Exploit
Windows Registry Key

Mapping of Sources to Extracted Content

Argus:

- Network Flow
- Socket Address (s/d)
- IP (s/d)
- Port (s/d)

Banner:

- Socket Address (contains banner)
- IP
- Port

DNS Record

- IP (s/d/requested ip) (requester/server/requested ip)
- Domain Name (requested uri)
- DNS Record

HTTPR

- IP (s/server)
- Port (server)
- Domain Name (of server)
- URI (requested uri/referrer uri)
- HTTP Session

Situ

- Network Flow
- Socket Address (s/d)
- IP (s/d)
- Port (s/d)

Sno

- Indicator
- Network Flow
- Socket Address (s/d)
- IP (s/d)
- Port (s/d)

Bugtraq

- Vulnerability (ExploitTarget)
- Course_Of_Action
- Product (affected software)

Caida

- Whois (organization)
- AS (organizations' as)
- AddressRange

CIF1d4

- Malware
- IP

CIF Emerging Threat

- Malware
- IP

CIF Zeus Tracker

- Malware
- IP

CleanMX Virus

- Malware
- Socket Address
- IP
- Port
- Whois (nameservers)
- URI (server ns poiter by whois; should be referenced; stix preprocessing takes care of that)
- AddressRange

CPE

- Product

CVE

- Vulnerability

FSecure

- Malware
- Course_Of_Action
- Indicator

GeoIP

- AddressRange

Hone

- Hostname
- Product
- Socket Address
- IP
- Port
- Network Flow
- User Account

Login Event

- Hostname
- User Account
- IP
- Hostname

Metasploit

- Exploit
- Vulnerability

NVD

- Vulnerability
- Product

Package List

- Hostname
- Product

Service List

- Port
- Process

Sophos

- Malware (is pointing to event observables)
- Port
- IP
- Socket Address
- Domain Name
- File
- Process
- Windows Registry Key
- Event

Extracted Content in Relational Database

“User Account”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “User Account”

“Hostname”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Hostname”

“Product”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Product”

“File”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “File”

“Windows Registry Key”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Windows Registry Key”

“Network Flow”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Network Flow”

“DNS Record”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “DNS Record”

“Indicator”:

- vertexType: “Indicator”
- table: “Indicator”

“Event”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Event”

“Socket Address”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Socket Address”

“Domain Name”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Domain Name”

“Vulnerability”:

- vertexType: “Vulnerability”
- table: “Vulnerability”

“Exploit”:

- vertexType: “Exploit”
- table: “Exploit”

“IP”:

- vertexType: “IP”
- table: “IP”
- observableType: “Address”

“Port”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Port”

“Process”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Process”

“Course_Of_Action”:

- vertexType: “Course_Of_Action”
- table: “Course_Of_Action”

“URI”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “URI”

“HTTP Session”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “HTTP Session”

“Malware”:

- vertexType: “Malware”
- table: “Malware”

“AddressRange”:

- vertexType: “AddressRange”
- table: “AddressRange”
- observableType: “Address”

“AS”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “AS”

“Whois”:

- vertexType: “Observable”
- table: “Observable”
- observableType: “Whois”

Tables and Columns

VertexTypes/Tables	Properties/Columns														
	name	vertexType	description	shortDescription	source	sourceDocument	observableType	alias	details	ipInt	startIP	endIP	startIPInt	endIPInt	location
AddressRange	✔	✔	✔		✔	✔	✔				✔	✔	✔	✔	✔
Exploit	✔	✔	✔	✔	✔	✔									
IP	✔	✔	✔		✔	✔				✔					
Malware	✔	✔	✔	✔	✔	✔		✔	✔						
Vulnerability	✔	✔	✔		✔	✔									
Weakness	✔	✔	✔		✔	✔									
Campaign	✔	✔	✔	✔	✔	✔		✔							
Course_Of_Action	✔	✔	✔	✔	✔	✔		✔							
Exploit_Target	✔	✔	✔	✔	✔	✔									
Incident	✔	✔	✔		✔	✔		✔							
Indicator	✔	✔	✔		✔	✔		✔							
Threat_Actor	✔	✔	✔	✔	✔	✔		✔							
TTP	✔	✔	✔		✔	✔									
Observable	✔	✔	✔		✔	✔	✔	✔							