Beyond IoCs – Transforming Cyber Intel with DevOps and ISR

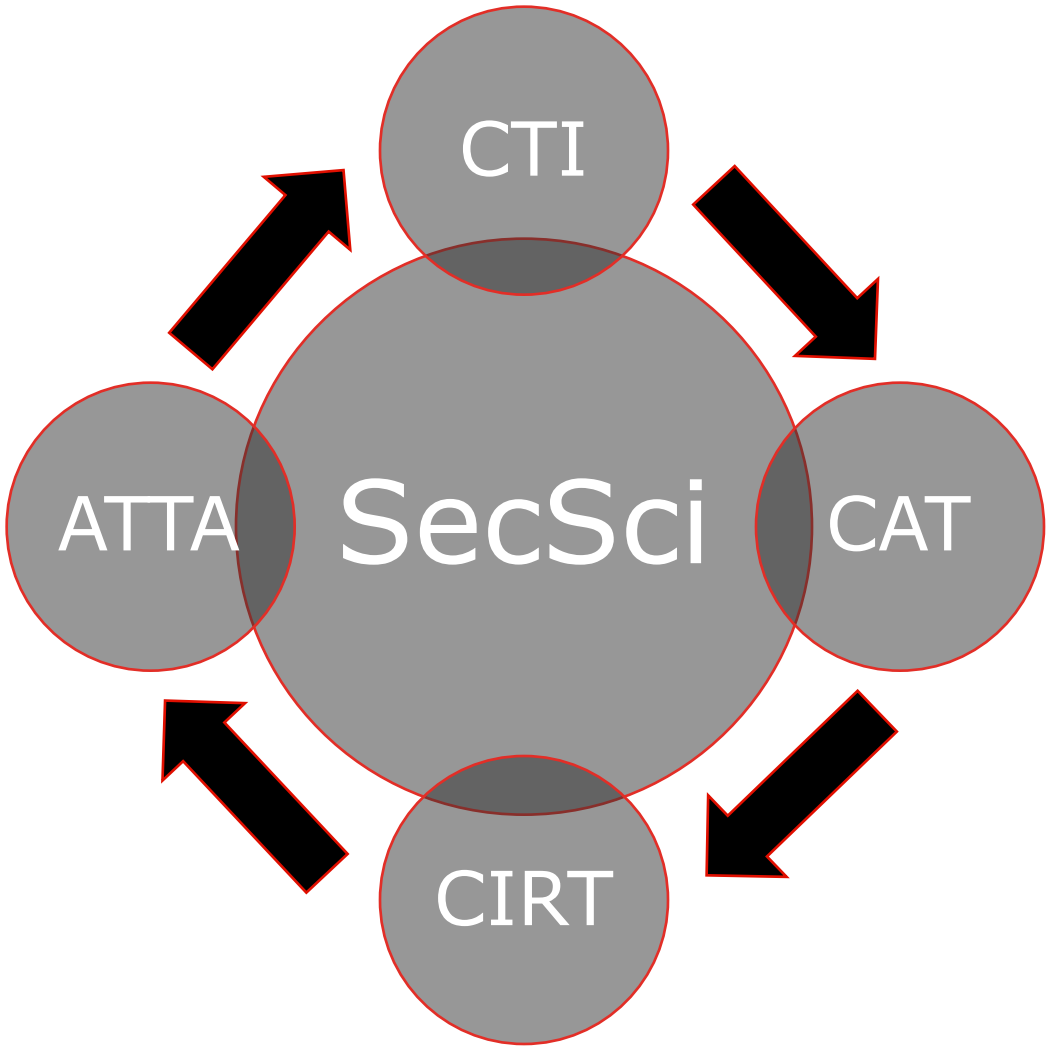
Andrew Rutkiewicz - Dell CSIRT

Greg LeBlanc – Dell CSIRT

#RSACharge

RSA Charge 2016

Circle Of Life



Evolution

Spreadsheet

- Internal INCs
- No Actors
- Kill Chain Optional
- Manual Push to SIEM and Controls

Dedicated Application

- Paid For Feeds
- Actor Optional
- Kill Chain Required
- Fixed Tier Alerting
- Hunting
- Basic Automation

Complete Program

- Formal Internal Intel Development
- ISR
  - Lifecycle Management
- Calculated Response Tier Alerting
- Hunting > Alerting
- Mostly Custom Content
- No IP Alerting
- Full Automation

IoC Hoarding

- Dedicated Application
    - CRITs, Soltra, etc.
- Adversary Information Required
- Paid Feeds
    - Basic Context Enrichment
- Closed Source Portals
    - ISACs, DSIE, ONA
- Actor Criticality
    - Fixed Response Tiering
- Kill Chain Stage
    - Inbound or Outbound
- Automation

Today and Future

- DevOps
- ISR
- BigData – SecSci
- Producer Consumer Model
- Hunting
- Automation

- Custom content on the fly
- No intel left behind
- Data driven decisions
- Streamlined operations
- Hunting > Alerting
- More time for real work

Current CTI-Framework

- CTI Framework Completed
  - 20+ Git Commits and over 4,500 lines of new code
  - Scalability & modular Python framework
  - Robust logging and internal monitoring
  - Import, enrichment, storage, context and dissemination
  - Makes integrating with new intel source or mitigation control an hour task instead of a week

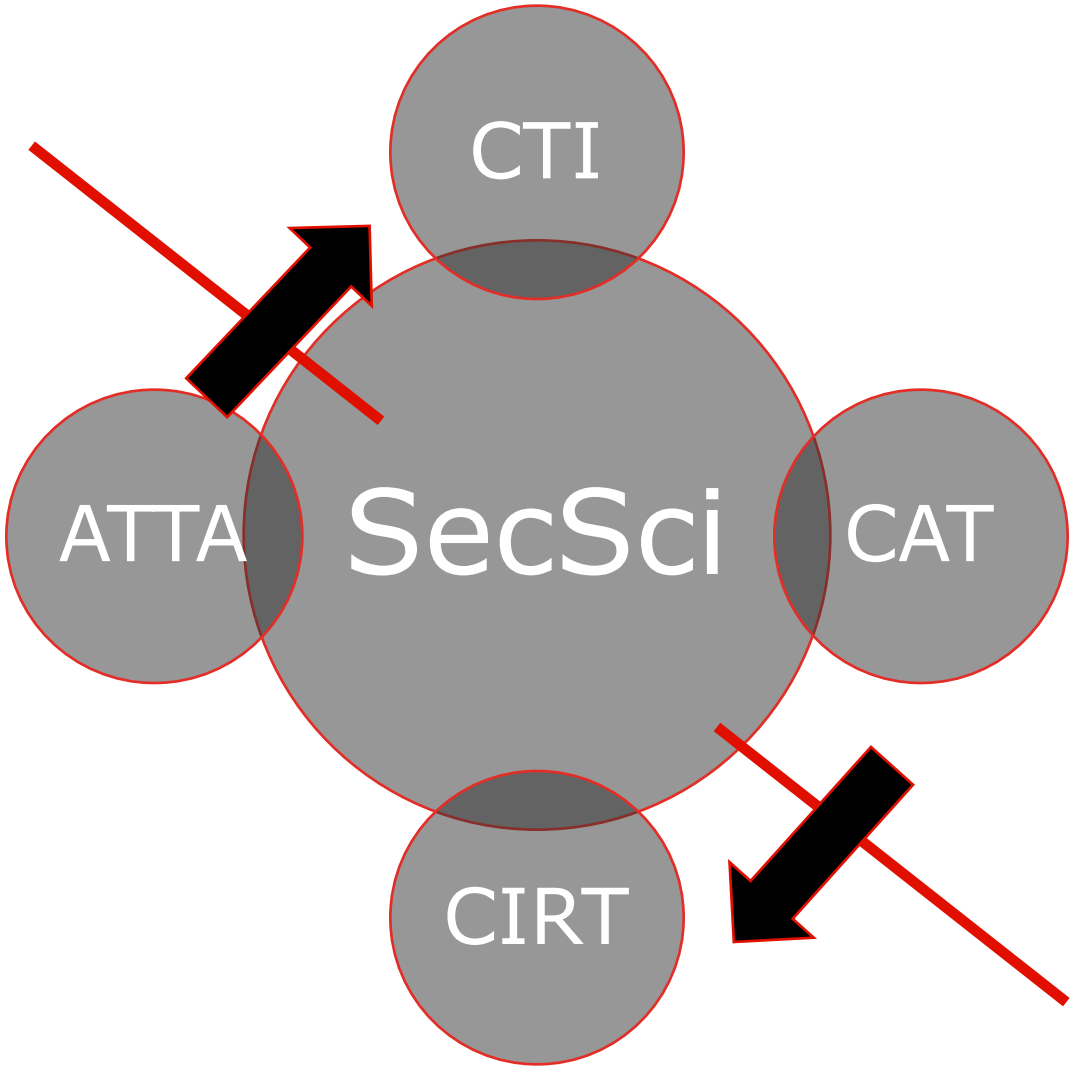
CTI: Import

- Currently importing 34 different sources of intelligence
- 25% of them automated (Most are OSINT related)
  - 100% of our commercial sources
  - 50% of our private sources
- STIX/TAXII is no where to be found
  - Sticking with JSON based REST API

Future: CTI-Framework

- Move production CTI logs to NetWitness
- Alerting on CTI hosts (for program execution and system resources)
- Tier 3 Hunting reports integration, enrichment and automatic PDF creation

Producer Consumer



ISR

- An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

ISR and TCPED

- Intelligence
  - The product resulting from processing information
- Surveillance
  - Systematic collection of information through sensors
- Reconnaissance
  - Collection of information missing from surveillance

- Task
- Collect
- Process
- Exploit
- Disseminate

- Feedback loop & gap analysis

DevOps

- No single tool for all processes
- APIs for everything
    - Internal API endpoints
    - Web Services
- Integration Code
- Custom Alerting
- Continuous Integration – aka Jenkins
- Code Repos – aka GitLab

Putting it All Together

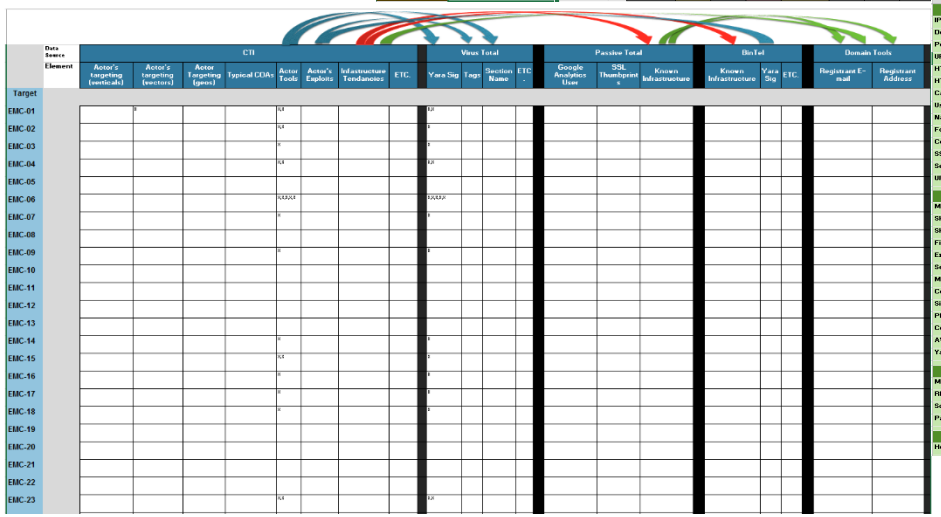
- Collection Requirements
- Target Acquisition
- Gap Analysis
- Risk and Vulnerability Data
- Automation
- Getting data where it needs to be
  - Extracts
  - Imports
  - Transforms
  - APIs

- Where are my data sources?
- What data do I need to detect/mitigate?
- Who is targeting us with what?
- Where are we blind?
- Where are we weak?
- How do I do more with less, quicker than before?

Example Documents

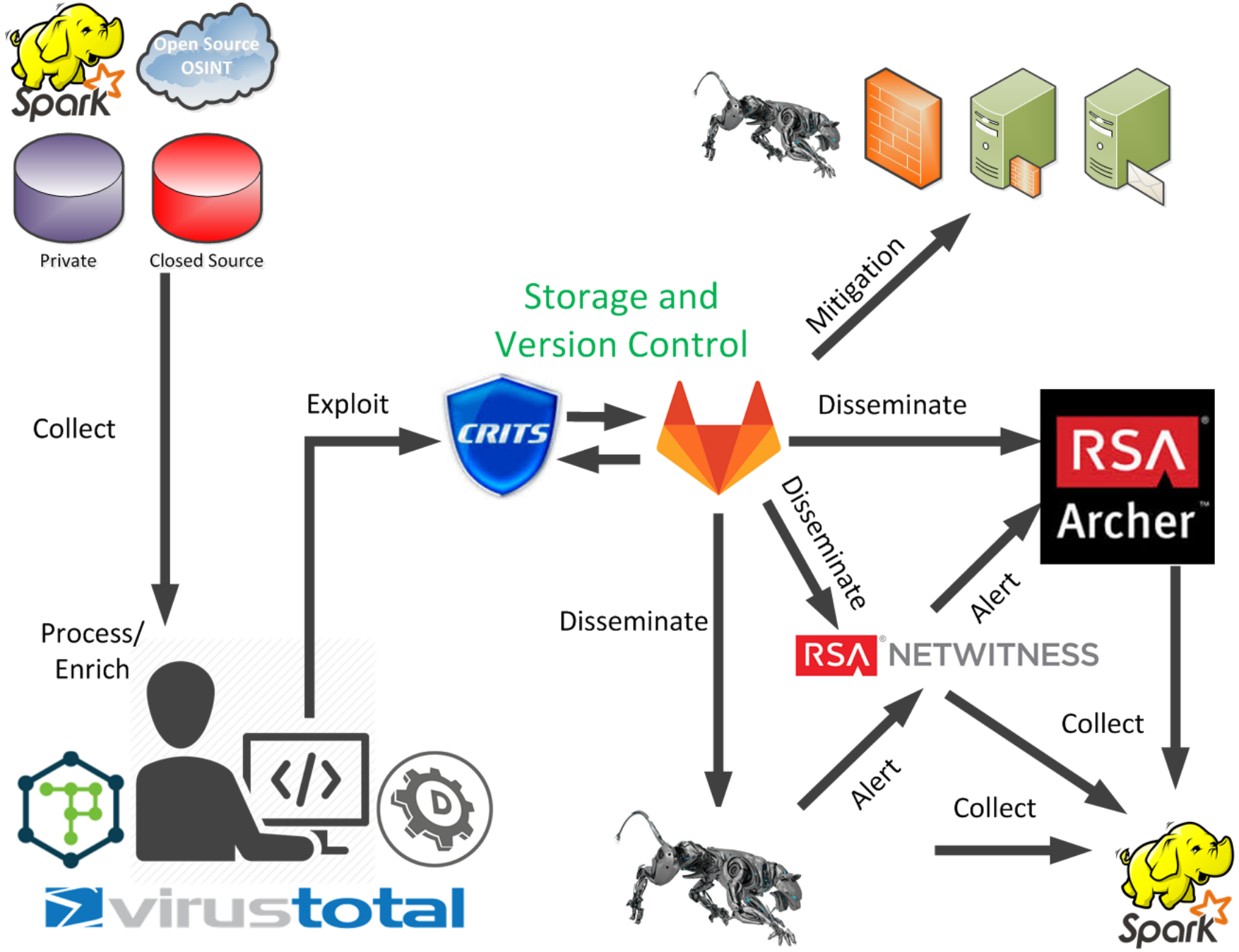
- Visibility Matrix
  - 3 Domains
    - Physical
    - Logical
    - Persona
  - Tool Efficiency by Domain
- Collection Requirements
  - Data to be collected at all sensors
  - Detect, Mitigate, Hunt
  - Defining Current Capabilities
- Reconnaissance Matrix
  - List of all actors
  - List of tools
  - Fill the gaps

	Layer	Physical							Logical											Persona				
	Element	Network	Endpoint	Storage	Server	Peripherals	Phone	Tablet	Office	VDI	VMs	ESX	DMZ	CORE	TPA	Demo	RMA	Cloud Conne	Lab	Open	Corp	SSO	FIM	LocalNonDoma	External
Sensor	Instrumentation																								
SA Packets	DPI	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	DNS	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	HTTP User	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	HTTP System	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	FTP	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	ICMP	P	P	P	P	NA	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	IPPort	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	Service	P	P	P	P	P	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Application	P	P	P	P	NA	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Authentication	N	P	N	P	NA	N	N	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	P	P
	DHCP	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	N	P
	Volume	P	P	N	P	NA	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	N	N	P	P
SA Logs	Authentication	P	P	N	P	P	P	P	NA	P	P	N	N	P	P	N	F	P	N	P	F	N	N	P	P
	DHCP	NA	F	NA	NA	P	P	P	P	P	P	NA	NA	P	P	N	F	P	N	F	P	NA	NA	P	NA
	AV	NA	P	NA	P	NA	NA	NA	NA	F	F	NA	P	P	P	NA	P	P	NA	NA	F	NA	NA	P	N
	ICMP	N	P	NA	P	P	P	P	NA	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Application	P	P	N	P	NA	P	P	P	N	N	N	N	P	N	N	P	N	N	P	P	N	N	N	P
	DNS	P	P	P	P	P	P	P	P?	P	P	P	N	P	P	N	P	P	N	P	P	N	N	N	N
	LDAP	P	P	P	P	NA	P	P	NA	P	P	N	P	P	P	N	P	P	N	P	F	N	N	N	P
	SMTP	N	N	N	N	N	N	N	NA	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	VPN	F	F	NA	NA	NA	F	F	P?	F	F	NA	NA	F	F	N	F	F	N	NA	F	NA	NA	F	N
	HTTP user	F	F	NA	F	NA	P	P	NA	F	F	NA	P	F	F	N	P	?	N	F	F	NA	NA	F	N
	HTTP System	P	N	N	P	NA	NA	NA	NA	P	P	P	P	P	NA	N	NA	?	N	NA	P	N	N	P	N
	Source Code	NA	NA	P	P	NA	P	P	NA	NA	NA	NA	NA	P	NA	N	NA	NA	N	NA	P	N	N	N	N
	iDRAC	P	NA	NA	P	NA	NA	NA	NA	P	P	N	P	P	NA	N	NA	NA	N	NA	P	P	P	P	N
	FTP	P	P	P	P	NA	P	P	NA	N	N	P	N	N	P	N	P	?	N	N	P	P	P	P	N
ECAT	DNS	NA	P	NA	P	NA	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	HTTP	NA	P	NA	P	NA	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	LDAP	NA	P	NA	P	NA	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	File System	NA	P	NA	P	P	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	File	NA	P	NA	P	P	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	Application	NA	P	NA	P	P	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	Processes	NA	P	NA	P	P	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
	Services	NA	P	NA	P	P	NA	NA	NA	P	P	NA	P	P	N	N	N	N	N	NA	P	NA	NA	N	NA
VCM	Processes	NA	NA	NA	NA	NA	NA	NA	NA	N	F	NA	?	F	N	?	N	?	N	N	P	P	P	P	N
	Services	NA	NA	NA	NA	NA	NA	NA	NA	N	F	NA	?	F	N	?	N	?	N	N	P	P	P	P	N
	File System	NA	NA	NA	NA	NA	NA	NA	NA	N	F	NA	?	F	N	?	N	?	N	N	P	P	P	P	N
	Authentication	NA	NA	NA	NA	NA	NA	NA	NA	N	F	NA	?	F	N	?	N	?	N	N	P	P	P	P	N
Splunk	FTP	P	P	P	P	P	P	P	P	P	P	P	P	P	P	N	P	?	N	N	P	P	P	N	N
	DNS	P	P	P	P	P	P	P	P	P	P	P	P	P	P	?	P	?	P	P	F	NA	NA	N	N
	SMTP	P	P	P	P	P	P	P	P	P	P	P	P	P	P	N	P	?	P	N	P	NA	NA	P	P
	Application	P	P	P	P	P	P	P	P	N	N	N	P	P	N	N	N	?	N	N	F	F	F	N	N
	Authentication	F	F	N	P	P	P	P	N	P	P	N	P	P	P	N	P	?	N	N	F	F	F	P	N
	Source Code	NA	NA	NA	P	NA	NA	NA	NA	NA	P	NA	P	P	NA	NA	NA	?	P	NA	P	NA	NA	N	N
	HTTP System	NA	NA	N	P	NA	NA	NA	NA	N	N	N	N	N	NA	N	N	?	N	NA	N	P	P	N	N
LogInsight	Processes	N	N	P	P	NA	N	N	N	F	F	F	P	P	N	P	N	?	N	NA	P	P	P	N	N
	File System	P	N	P	P	NA	N	N	N	F	F	F	P	P	N	P	N	?	N	NA	P	P	P	N	N
	Authentication	P	N	P	P	NA	N	N	N	F	F	F	P	P	N	P	N	?	N	NA	P	P	P	N	N
	IPPort	P	N	P	P	NA	N	N	N	F	F	F	P	P	N	P	N	?	N	NA	P	P	P	N	N
Veronis	Filesystem	P	P	P	P	N	P	P	NA	P	P	N	P	P	P	N	P	N	N	NA	P	NA	NA	N	N
	Authentication	P	P	P	P	N	P	P	NA	P	P	N	P	P	P	N	P	N	N	NA	P	NA	NA	N	N
Unity	Authentication	P	N	P	P	P	P	P	NA	F	F	F	P	P	P	?	P	P	N	P	F	F	F	P	P
	Application	P	N	P	P	P	P	P	NA	F	F	F	P	P	P	?	P	P	N	P	F	F	F	P	P
	IPPort	P	N	P	P	P	P	P	NA	F	F	F	P	P	P	?	P	P	N	P	F	F	F	P	P
	Domain	P	N	P	P	P	P	P	NA	F	F	F	P	P	P	?	P	P	N	P	F	F	F	P	P
SCCM	MAC	NA	P	NA	N	P	NA	NA	NA	F	P	NA	N	P	P	N	NA	N	N	P	P	NA	NA	N	N
	User	NA	P	NA	N	P	NA	NA	NA	F	P	NA	N	P	P	N	NA	N	N	P	P	NA	NA	N	N
	System Info	NA	P	NA	N	P	NA	NA	NA																
	Applications	NA	P	NA	N	P	NA	NA	NA																



	Storage				Alerting				Blocking					Hunting/Gathering			
	CRIts	Mongo	ECAT	MAPR	SA	Sourcefire	ECAT	RPZ	SA	ECAT	Ironport	McAfee/HIPS	Proofpoint	Checkpoint	PT	VT	iDefense	OT
NETWORK																		
IP Address	X		X	X	X	X	X	X	X		X	X	X	X	X	X	X	
Domain Name	X		X	X	X	X	X	X	X		X	X	X		X	X	X	X
Ports			X	X	X							X		X				
URL	X			X	X	X										X	X	
HTTP Header (Server)				X	X	X			X						X			
HTTP Header (Client)				X	X	X			X						X			
Campaign Codes																		
User Agent			X	X	X				X				X			X		
Named Pipes				X	X													
FormData																		
Cookie				X	X													
SSL Cert Info				X	X				X									
Service Type				X	X							X						
URI Components (Directory, File, Query)				X	X				X							X		
FILE																		
MD5	X		X	X			X			X					X	X	X	
SHA1	X		X	X			X			X						X	X	
SHA256	X		X	X			X			X						X	X	
Filename	X		X	X	X	X	X			X		X	X			X	X	
Export Names																X		
Section Names			X													X		
Meta (Company name, version, etc)			X													X		
Compile Time			X													X		
Signing Info			X													X		
PDB Path																X		
Comm Channel (HTTP, Binary, FTP, etc. if applicable)									X								X	
AV Detect name (if any)									X							X		
Yara			X	X			X									X		
SYSTEM																		
MUTEX	X			X			?									X		
REGISTRY KEY	X			X			X									X		
Source Port																		
PATH	X			X			X					X				X		
EMAIL																		
Header Information	X			X									X					

RSA Charge 2016



RSA Charge 2016

RSA NetWitness Integrations

- All Custom Feeds pulled from Gitlab raw document (CSV)
    - Domain
    - IP
    - URLs
    - User-Agents
    - Hashes
    - Rules and Response
    - Tags
    - Whitelisting
- Custom Parser Code, Application Rules
- CI to push to devices as changes are made
    - REST API on decoders
- Warehouse Connector to Hadoop

RSA NetWitness Endpoint Integrations

- Blacklist Feed from Gitlab
    - Hashes
    - Domains
- IIoCs
    - Alert output to NetWitness Logs
    - Apache Spark SQL Access
    - Full Backend DB Access
        - Tracking Data
        - Network Connections
        - Too much data to list

NetWitness SecOps Integrations

- Alerting with UCF
  - Event Aggregation (Many alerts → 1 INC)
  - R&Rs in Alert payload
- Threat Management
  - Scrubbed IoC notes
  - Time based Information
    - Created, modified, demoted
- Archer Data Services
  - Simple DB access to Incident data
    - Exposes data to Visualization Tools
    - Direct Apache Spark SQL access

Gitlab

- Yara
  - ECAT
  - Mail Meta
- AvroCoversion
  - Warehouse Connector Utilities
- Feed Library
  - Blacklist
  - Whitelist
- Parsers
  - Custom log Parser
  - Custom Packet Parsers
    - Service/Application ID
    - Malware Detection
    - Meta Creation

@CAT

Joint CIRC Content Analytics Team projects are here.

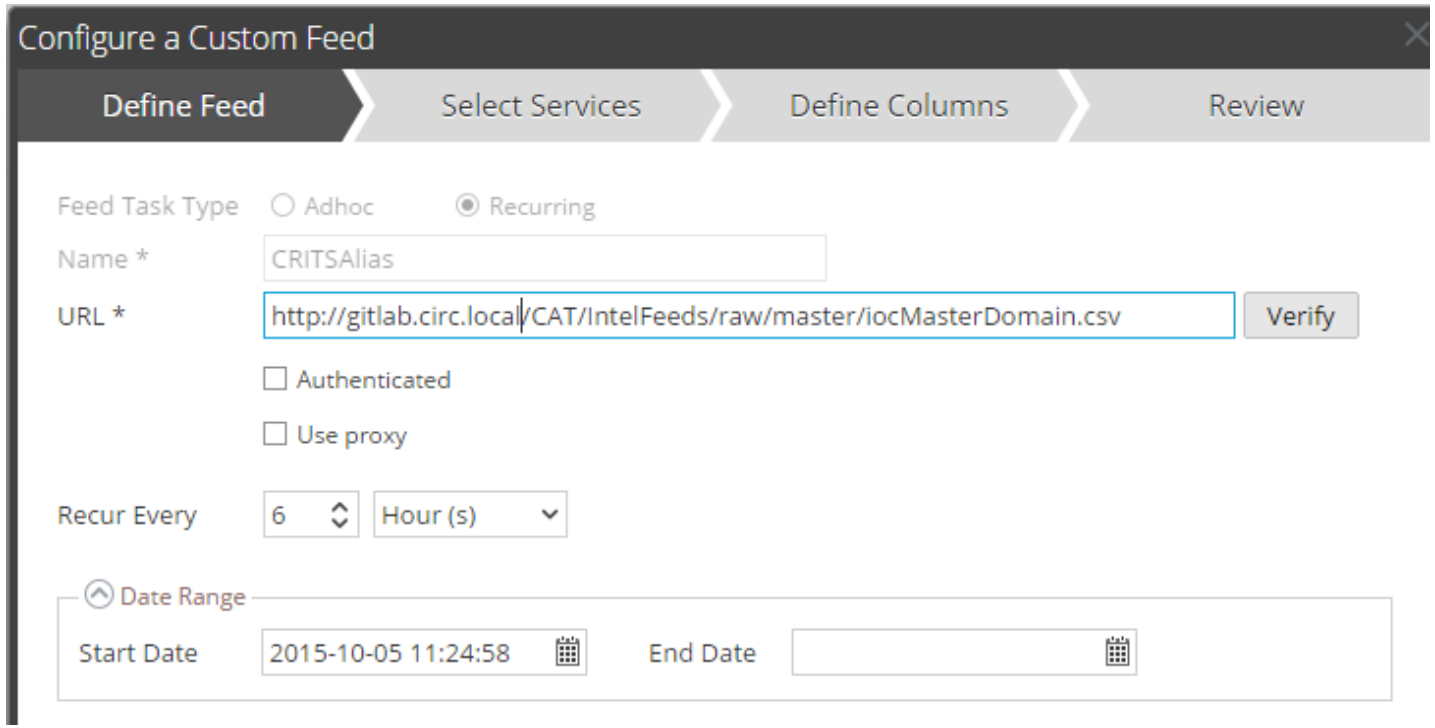
All Projects | Filter by name | Last updated | New Project

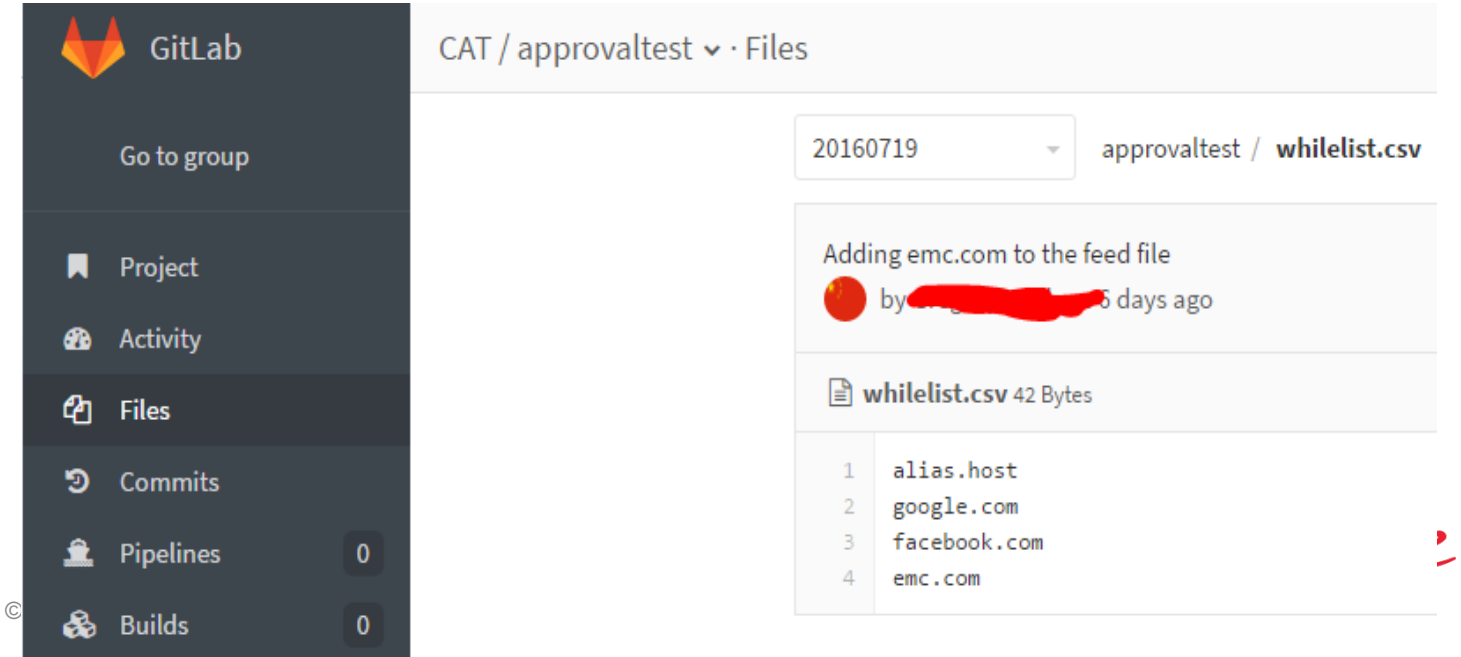
I	IntelFeeds	
P	PacketParsers	Lua
A	ApplicationRules Rules for Internal and External packet Decoders	
Y	yara This is where the CIRC yara rules will be kept and developed.	Python
A	approvaltest TEST PROJECT PLEASE IGNORE	
A	AvroConversion Convert Avro over to parquet files in batch form using Spark and Scala	XSLT
S	SAfeeds Feeds not generated by CRITs that need to be pushed to decoders. All recurring feeds should point to here so that a single file can be updated and SA Live can be p...	
M	mailMeta	Python
S	SAIndexing Indexes for all SA gear	
S	SAAlerting	
M	MalwareScripts	

db.rpz	35 minutes ago	RPZ COMMIT FOR 2016-07-25 20:07:13
db_external.rpz	35 minutes ago	RPZ COMMIT FOR 2016-07-25 20:07:13
ecatBlackList.csv	about 13 hours ago	ECAT EXPORT FOR 2016-07-25 07:07:04
exportIoCForArcher.csv	39 minutes ago	CTI EXPORT FOR 2016-07-25 20:07:20
iocMasterDomain.csv	39 minutes ago	CTI EXPORT FOR 2016-07-25 20:07:20
iocMasterIP.csv	39 minutes ago	CTI EXPORT FOR 2016-07-25 20:07:20
iocMasterUA.csv	3 months ago	TEST COMMIT
iocMasterURL.csv	39 minutes ago	CTI EXPORT FOR 2016-07-25 20:07:20

Tools in Action

- IoC Domain List
  - Full Dump From CRITs to NetWitness
  - Notes field
  - EMC Actor
  - IoC Type
- Whitelist w/ Approvals
  - Merge only after L3 Approval
  - Per Content type Feed
  - Right Click in NetWitness UI





Netwitness Alerting

- CRITs Information
  - Directly in the UI
  - Notes
  - CAT and Tier

- Rule and Response
  - Why did the rule fire
  - What was the rule looking for
  - External References (Right Click)
  - Known False Positives

IR Alert (7 values)

circ_t2_saip_ioc_domain (32) - circ_t1_saip_ioc_domain (12) - possible_b64_shell (12) - possible_poison_ivy_handshake (10) - circ_t1_saip_
Loaded in 4.425 secs. Total running time 4.427 secs. (10.219.70.10:56005 loaded in 1 secs., 10.219.86.10:56005 loaded in 1 secs., 10.254.49.17:56005 loaded i
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 4 secs.)

CRITS IoC Attribution (15 values)

emc-unk-non (514,962) - emc-unk-apt (16,415) - emc-bot-06 (5,961) - emc-09 (2,905) - emc-01 (654) - emc-35 (196) - emc-15 (72) - emc-l
Loaded in 2.217 secs. Total running time 2.219 secs. (10.219.70.10:56005 loaded in 0 secs., 10.219.86.10:56005 loaded in 0 secs., 10.254.49.17:56005 loaded i
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 1 secs.)

CRITS IoC Intelligence (20 of 20+ values)

this is related to the teamview compromise. emergency block ... (161,586) - 2012-04-16 12:24:02 demoted as spyware (147,998) - 2013-0
website to prevent ... (18,441) - malware spam: emailing: mx62edo 10.02.2016 / documents@... (15,797) - 20160302-140100 | openvas r
by gso websec (13,254) - gso request - dns block for [redacted] from simon ... (9,030) - cryptowall (8,366) - notes - crapware (
inc-33724494 | scamware | uses vanilla msie 11 us... (4,450) - 2012-06-13 11:10:43 related to [redacted] com d... (2,874) - p
dns block list | no specific intelligence o... (2,154) **... show more**
Loaded in 1.328 secs. Total running time 1.331 secs. (10.219.70.10:56005 loaded in 1 secs., 10.219.86.10:56005 loaded in 1 secs., 10.254.49.17:56005 loaded i
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 1 secs.)

CRITS IoC Type (2 values)

domain (492,504) - ipv4 (48,796)
Loaded in 1.084 secs. Total running time 1.089 secs. (10.219.70.10:56005 loaded in 0 secs., 10.219.86.10:56005 loaded in 0 secs., 10.254.49.17:56005 loaded i
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 0 secs.)

CRITS Category (4 values)

cat 3 (508,721) - cat 2 (31,692) - cat 1 (878) - cat 4 (18)
Loaded in 1.219 secs. Total running time 1.22 secs. (10.219.70.10:56005 loaded in 0 secs., 10.219.86.10:56005 loaded in 0 secs., 10.254.49.17:56005 loaded in

CIRC App Rule Syntax (4 values)

looking for a t2 ioc domain (32) - looking for a t1 ioc domain (12) - looking for a user agent of google not going to google (2) - looking for a xored windows exe
Loaded in 0.95 secs. Total running time 0.951 secs. (10.219.70.10:56005 loaded in 1 secs., 10.219.86.10:56005 loaded in 1 secs., 10.254.49.17:56005 loaded in 0 secs., 10.254.49.18:5600
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 1 secs.)

CIRC Content Objective (4 values)

standard ioc alert from crits (44) - rat uses an abnormal user agent that is easy to detect (2) - xoring an exe or any file is a way to evade ids via obfuscat... (1) -
Loaded in 0.947 secs. Total running time 0.949 secs. (10.219.70.10:56005 loaded in 0 secs., 10.219.86.10:56005 loaded in 0 secs., 10.254.49.17:56005 loaded in 0 secs., 10.254.49.18:560
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 0 secs.)

CIRC Known False Positives (2 values)

depends on the intel (44) - none (3)
Loaded in 0.876 secs. Total running time 0.876 secs. (10.219.70.10:56005 loaded in 0 secs., 10.219.86.10:56005 loaded in 0 secs., 10.254.49.17:56005 loaded in 0 secs., 10.254.49.18:560
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 1 secs.)

CIRTian References (3 values)

do not google domain (44) - deep panda malware (2) - 'xor' and malware (1)
Loaded in 1.052 secs. Total running time 1.053 secs. (10.219.70.10:56005 loaded in 0 secs., 10.219.86.10:56005 loaded in 0 secs., 10.254.49.17:56005 loaded in 0 secs., 10.254.49.18:560
10.254.49.42:56005 loaded in 0 secs., 10.254.49.47:56005 loaded in 0 secs., 10.254.49.12:56003 loaded in 1 secs.)

IR Tags

Closed - Click to Open

2016

CRITs to SecOps Datafeed

Threat Indicators: [redacted]

New | Copy | Save | Apply | Edit | Delete | Record [redacted] of [redacted] | Related | Recalculate | Export | Print

General Information

Tracking ID:	[redacted]	Block Date:	11/7/2013
Id:	[redacted]	Comments:	2013-11-07 10:41:28 Operation Hangover Domains
Initial Date:	11/7/2013 12:00:00 AM	Last Updated:	7/21/2016 12:48 PM
Indicator:	[redacted]	Data Type:	Domain
Category:	tier_1	Intrusion Set:	EMC-49
Indicator Type:	C2		
Tip Category:	Cat 1		
Feed Name:	ioc_master		
Immortal:			
First Published:	7/21/2016 12:48 PM		

Security Incidents (Threat Indicators (Security Incidents))

Incident ID	Date Created	Incident Status	Incident Owner	Title	Domain
No Records Found					

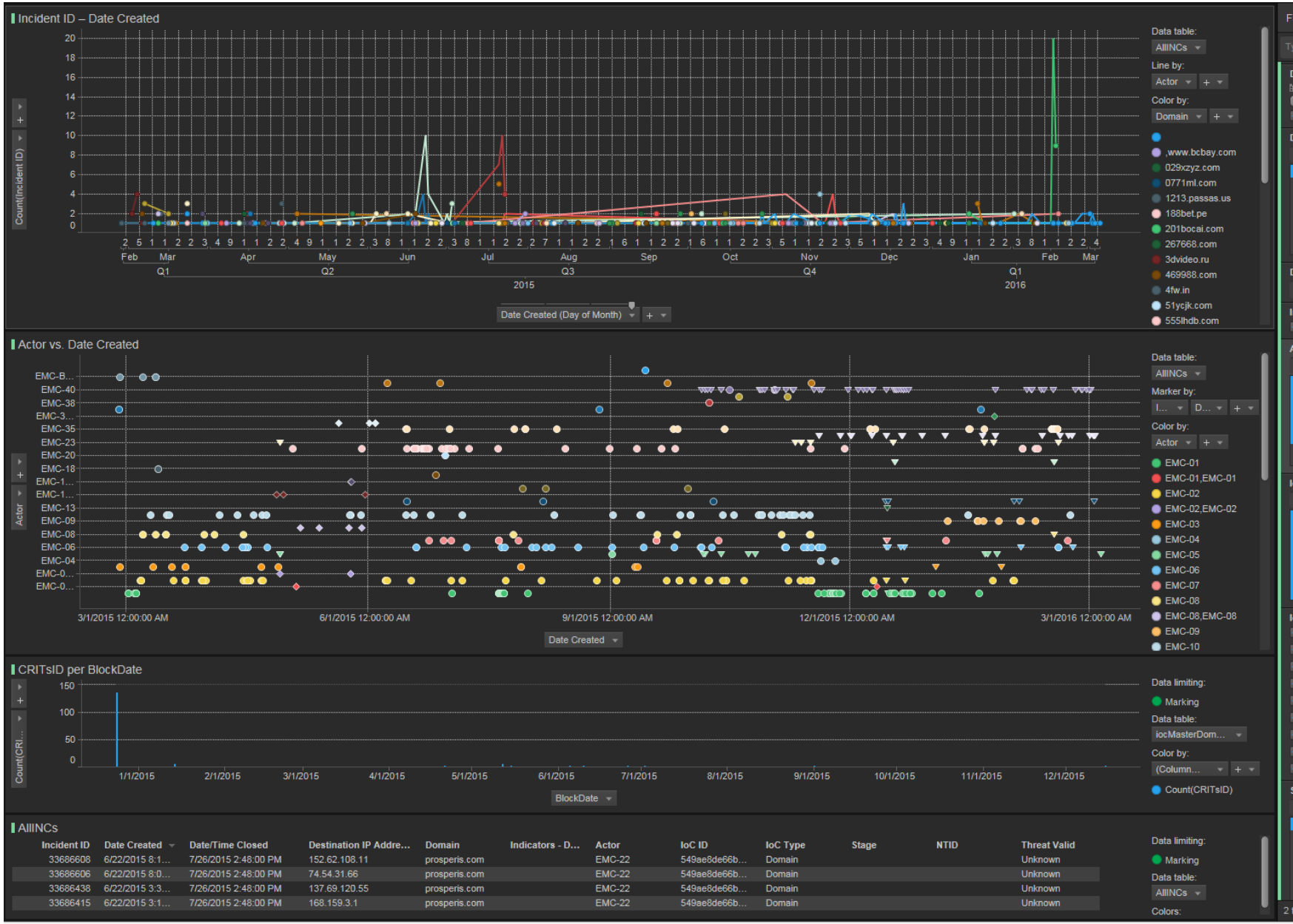
Threat Indicator_History Log | Compare Record Versions |

Date	User	Field	Action
7/21/2016 12:48:45 PM	Data Feed Service, circarcher	Block Date	Initial Entry: "11/7/2013"
		Category	Initial Entry: "tier_1"
		Comments	Initial Entry: "2013-11-07 10:41:28 Operation Hangover Domains"
		Data Type	Initial Entry: "Domain"
		Feed Name	Initial Entry: "ioc_master"
		Id	Initial Entry: [redacted]
		Indicator	Initial Entry: [redacted]
		Indicator Type	Initial Entry: "C2"
		Initial Date	Initial Entry: "11/7/2013 12:00:00 AM"
		IntrusionSet	Initial Entry: "EMC-49"
		Tip Category	Initial Entry: "Cat 1"

RSA Charge 2016

Pulling Data from All Sources

- RSA NetWitness Endpont
- RSA NetWitness Logs
- RSA NetWitness Packets
- RSA NetWitness SecOps Manager
- CRITs



Questions?

Please Complete Session Evaluation

#RSACharge

RSA Charge 2016