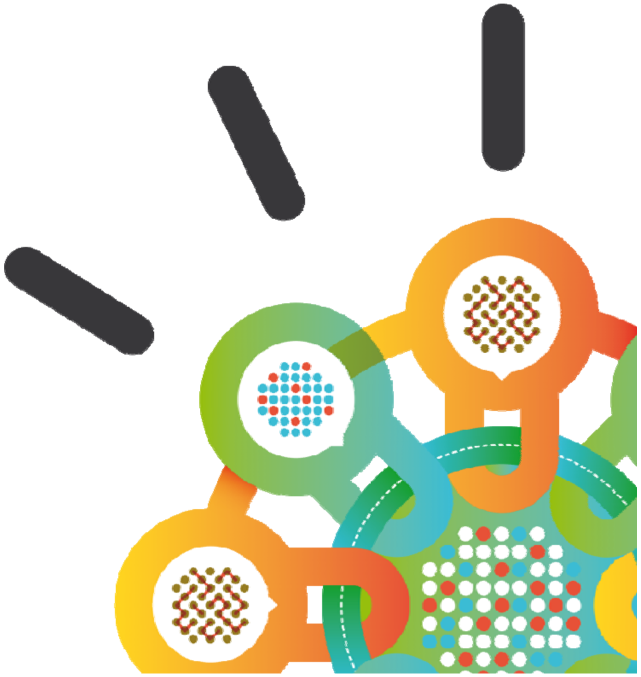
Security Intelligence.
Think Integrated.

QRadar SIEM 7.2 Event Architecture Overview

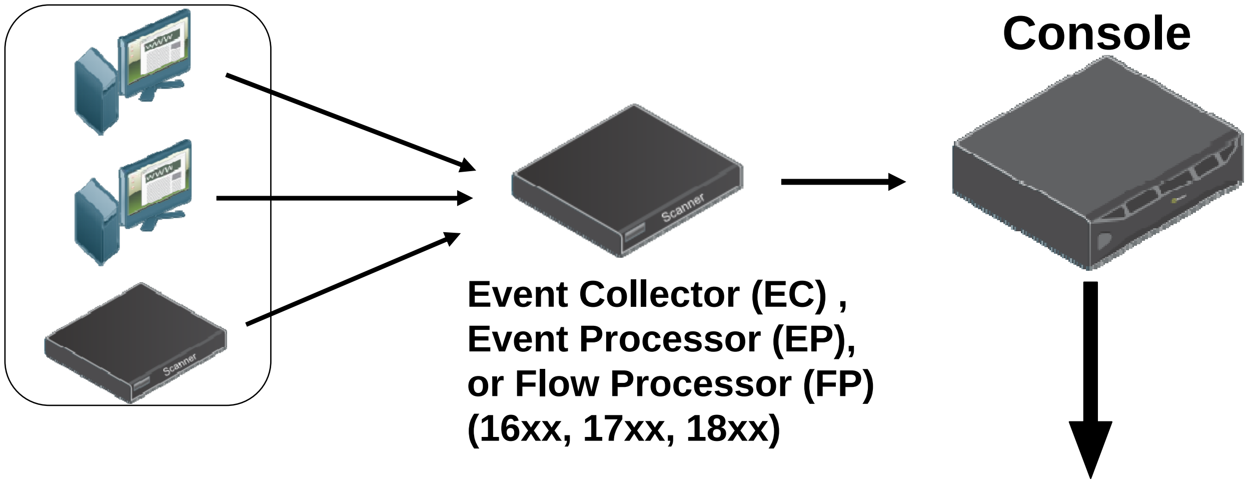
- Dwight Spencer - Principal Solutions Architect & Co-founder of Q1 Labs
- Scott Dubreuil - Support Services Group Manager
- Adam Frank - Principal Solutions Architect
- Mark Wright - QRadar L2 Support Manager
- Jonathan Pechta - Support Technical Writer
- Jeff Rusk - Team Lead, QRadar Integration Services and Maintenance
- John Cotter - QRadar User Experience Lead



QRadar Open Mic Webcast #1 – June 18, 2014

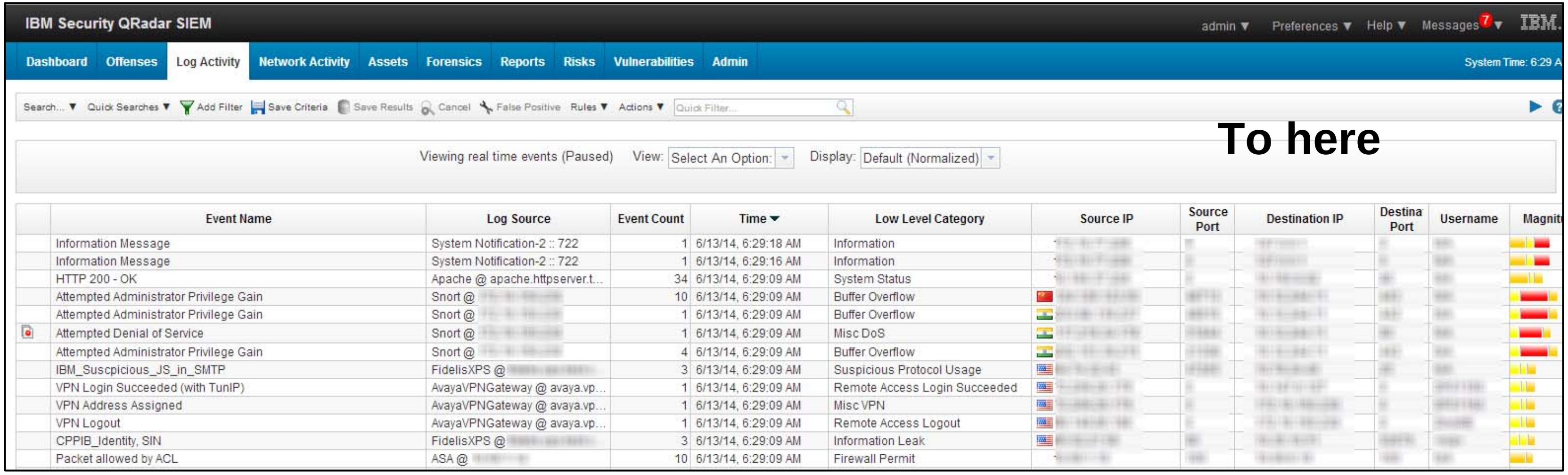
Goal: Provide insight on the QRadar components responsible for event collection.

To get your events sources from here:



Console

Event Collector (EC) ,
Event Processor (EP),
or Flow Processor (FP)
(16xx, 17xx, 18xx)



To here

IBM Security QRadar SIEM

System Time: 6:29 A

Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

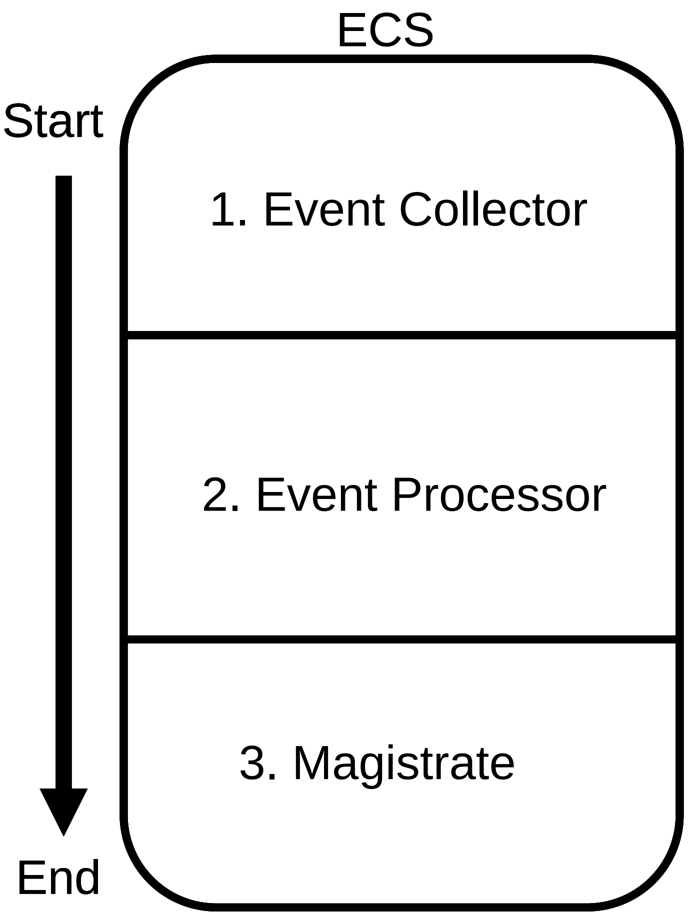
	Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnit
	Information Message	System Notification-2 :: 722	1	6/13/14, 6:29:18 AM	Information	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	Information Message	System Notification-2 :: 722	1	6/13/14, 6:29:16 AM	Information	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	HTTP 200 - OK	Apache @ apache.httpserver.t...	34	6/13/14, 6:29:09 AM	System Status	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	Attempted Administrator Privilege Gain	Snort @ [redacted]	10	6/13/14, 6:29:09 AM	Buffer Overflow	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	Attempted Administrator Privilege Gain	Snort @ [redacted]	1	6/13/14, 6:29:09 AM	Buffer Overflow	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	Attempted Denial of Service	Snort @ [redacted]	1	6/13/14, 6:29:09 AM	Misc DoS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	Attempted Administrator Privilege Gain	Snort @ [redacted]	4	6/13/14, 6:29:09 AM	Buffer Overflow	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	IBM_Suscpicious_JS_in_SMTP	FidelisXPS @ [redacted]	3	6/13/14, 6:29:09 AM	Suspicious Protocol Usage	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	VPN Login Succeeded (with TunIP)	AvayaVPNGateway @ avaya.vp...	1	6/13/14, 6:29:09 AM	Remote Access Login Succeeded	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	VPN Address Assigned	AvayaVPNGateway @ avaya.vp...	1	6/13/14, 6:29:09 AM	Misc VPN	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	VPN Logout	AvayaVPNGateway @ avaya.vp...	1	6/13/14, 6:29:09 AM	Remote Access Logout	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	CPPIB_Identity, SIN	FidelisXPS @ [redacted]	3	6/13/14, 6:29:09 AM	Information Leak	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
	Packet allowed by ACL	ASA @ [redacted]	10	6/13/14, 6:29:09 AM	Firewall Permit	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

The Event Correlation Service (ECS)

ECS is the core service responsible for event collection and event processing for QRadar.

ECS is comprised of three core components:

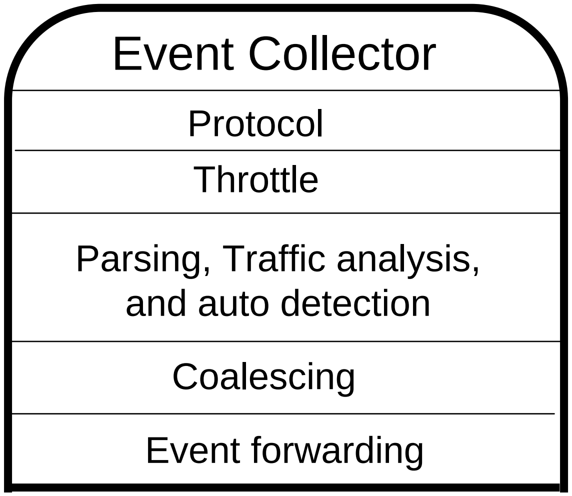
- Event Collector component
- Event Processor component
- Magistrate component (Console only)



Note: ECS also does flow collection and processing, but flows will be discussed in a future presentation.

What is an Event Collector component?

The Event Collector component completes a number of functions for ECS.



Event Collector

Protocol

Throttle

Parsing, Traffic analysis, and auto detection

Coalescing

Event forwarding

- **Protocol**: Receives data off of the wire from log source protocols (Syslog, JDBC, OPSEC, Log File, SNMP…)

- **Throttle**: Monitors the number of incoming events to the system to manage input queues and licensing.

- **Parsing**: Takes the raw events from the source device and parses the fields as QRadar friendly events.

- **Log source traffic analysis & auto discovery**: Applies the parsed event data (normalized) to the possible DSMs that support automatic discovery.

- **Coalescing**: Events are parsed and then coalesced based on common patterns across events. Once 4 events are seen with the same source IP, destination IP, destination port and username, subsequent messages for up to 10 seconds of the same pattern are coalesced together. This is done to reduce duplicate data being stored.

- **Event forwarding**: Applies routing rules for the system. Such as sending data to offsite targets, external Syslog systems, JSON systems, other SIEMs, etc.

What is an Event Processor component?

The Event Processor component completes a number of functions for ECS.

Event Processor
Custom Rules Engine
Streaming
Storage

Custom Rules Engine (CRE): The Custom Rules Engine (CRE) is responsible for processing events received by QRadar and comparing them against defined rules, keeping track of systems involved in incidents over time, generating notifications to users and generating offenses.

- **Streaming**: Responsible for sending real-time event data to the Console when a user is viewing events from the Log Activity tab with Real time (streaming). Streamed events are not provided from the database.

- **Event storage (Ariel)**: A time series database for events and flows where data is stored on a minute by minute basis. Data is stored where the event is processed. Remember, that both Consoles and 16xx, 17xx, and 18xx can all process events.

Note: Not shown is the host profiler which is responsible for resolving asset information from passive flow data.

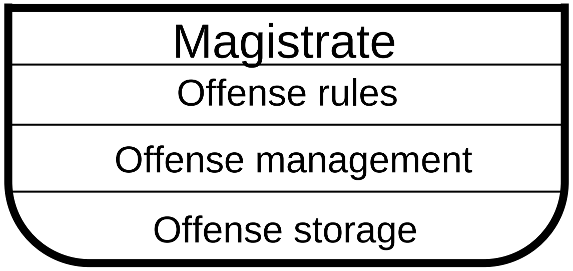
What is the Magistrate (MPC) component?

The Magistrate Processing Core (MPC) is responsible for correlating offenses with event notifications from multiple Event Processor (EP) components. Only the Console will have a Magistrate component.

Layers

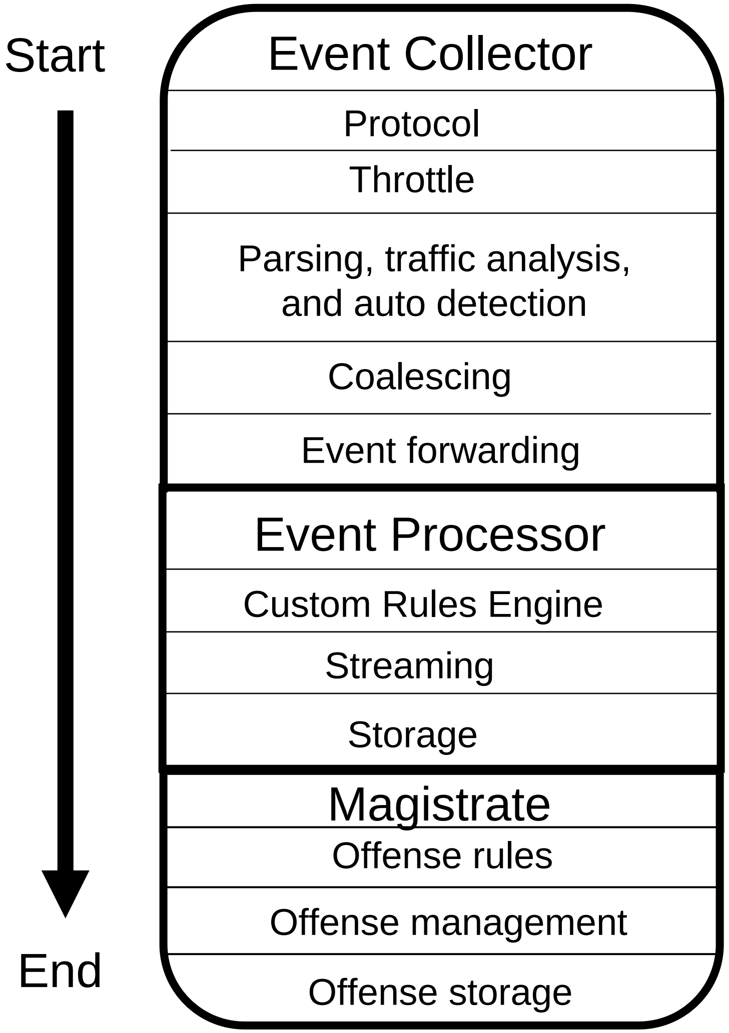
- **Offense rules**: Monitors and takes actions on offenses, such as generating email notifications.

- **Offense management**: Updates active offenses, transitioning inactive offenses to active and provides access to offense information to the user through the Offenses tab.



- **Offense storage**: Writes offense data to a Postgres database.

ECS, the big picture



Start

Event Collector

Protocol

Throttle

Parsing, traffic analysis, and auto detection

Coalescing

Event forwarding

Event Processor

Custom Rules Engine

Streaming

Storage

Magistrate

Offense rules

Offense management

Offense storage

End

Remember:

- ECS runs on any appliance that processes events, such as 16xx, 17xx, and 18xx appliances.

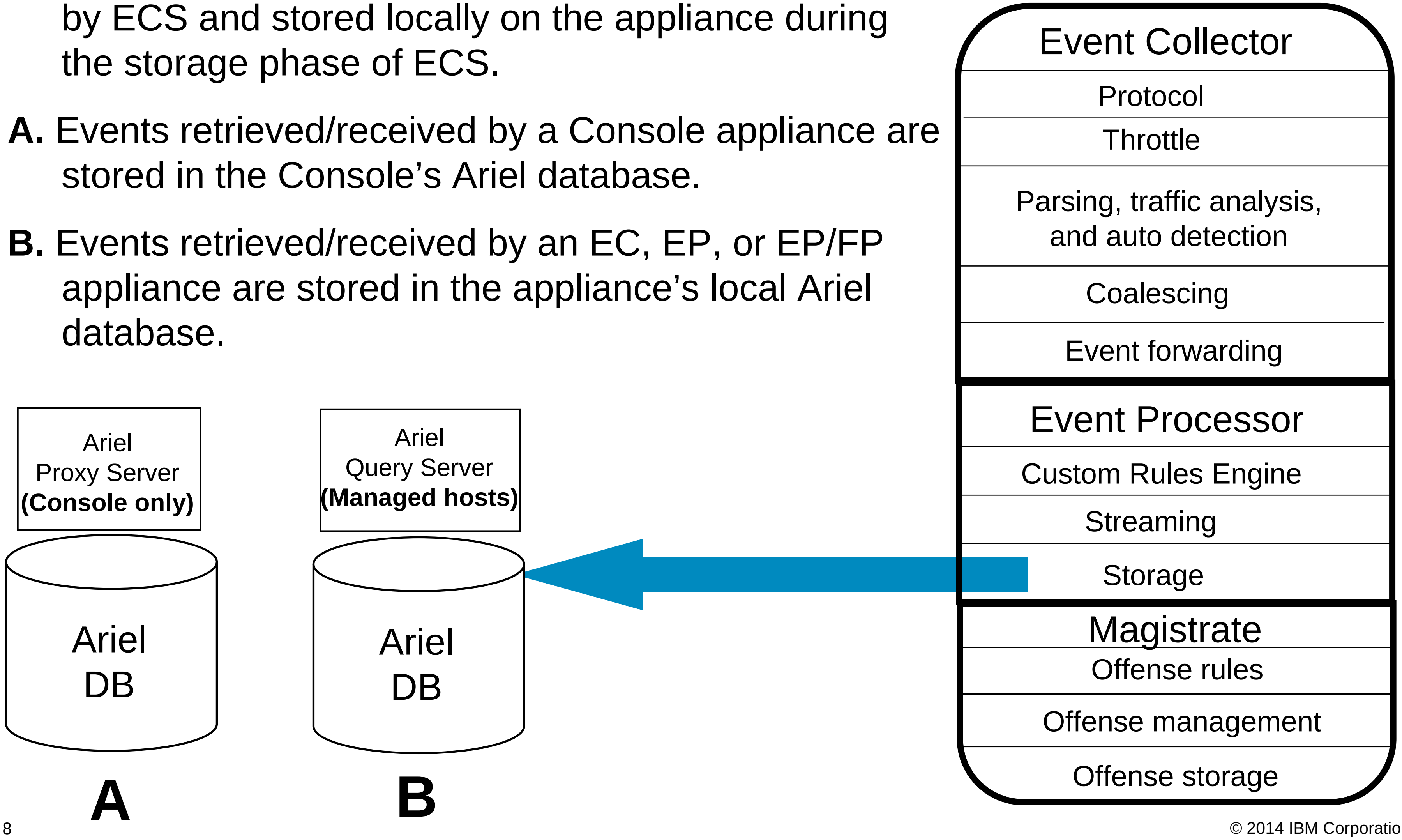
- This means that ECS is running simultaneously on a number of appliances in a multi-system deployment. Each ECS is taking in events, processing them, evaluating rules, etc.

Where does the data go?

As events come in to your appliance, they are processed by ECS and stored locally on the appliance during the storage phase of ECS.

A. Events retrieved/received by a Console appliance are stored in the Console’s Ariel database.

B. Events retrieved/received by an EC, EP, or EP/FP appliance are stored in the appliance’s local Ariel database.



Ariel
Proxy Server
(Console only)

Ariel
DB

A

Ariel
Query Server
(Managed hosts)

Ariel
DB

B

Event Collector
- Protocol
- Throttle
- Parsing, traffic analysis, and auto detection
- Coalescing
- Event forwarding

Event Processor
- Custom Rules Engine
- Streaming
- Storage

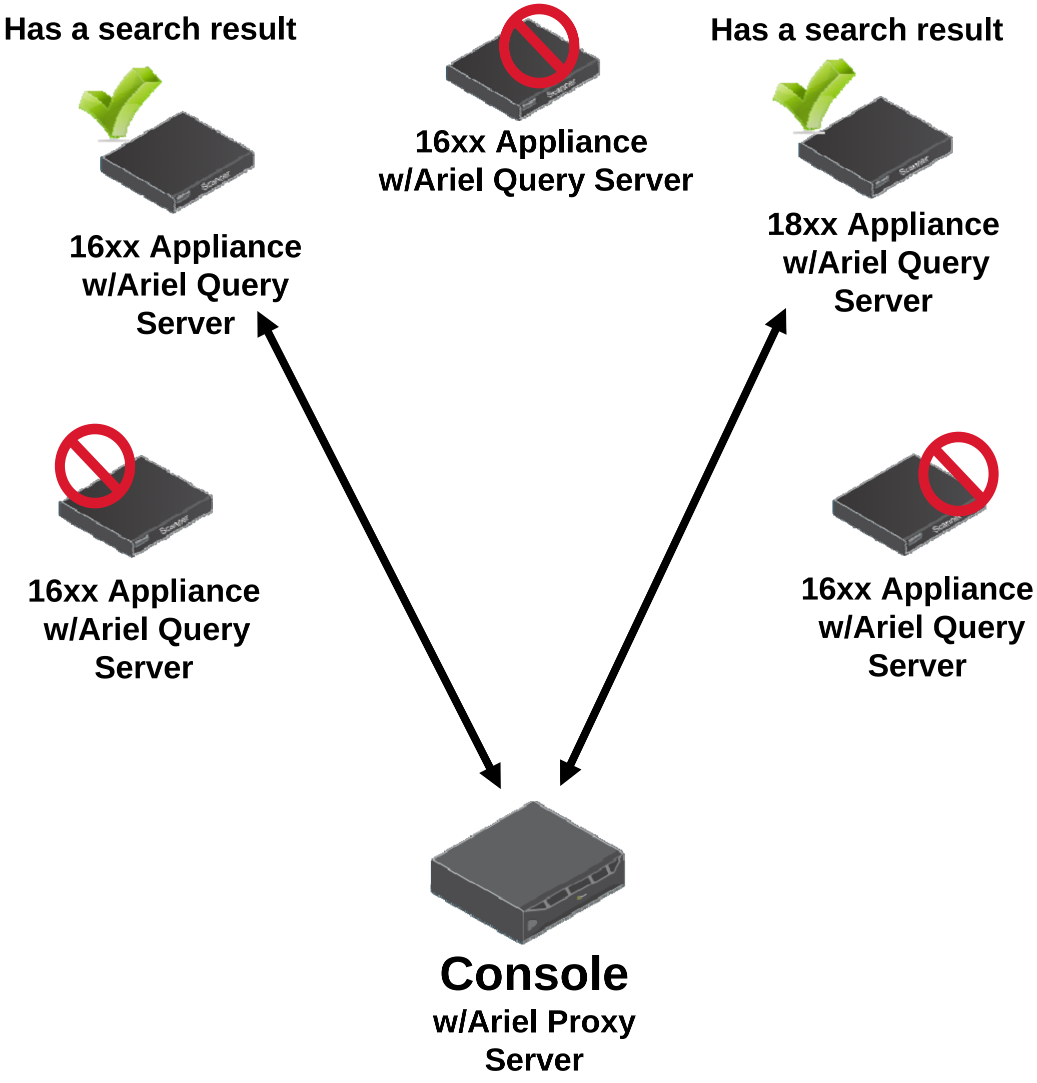
Magistrate
- Offense rules
- Offense management
- Offense storage

How do searches work?

1. When users run a search in QRadar, the Console’s Ariel Proxy Server reviews the search parameters to determine which hosts have the results.

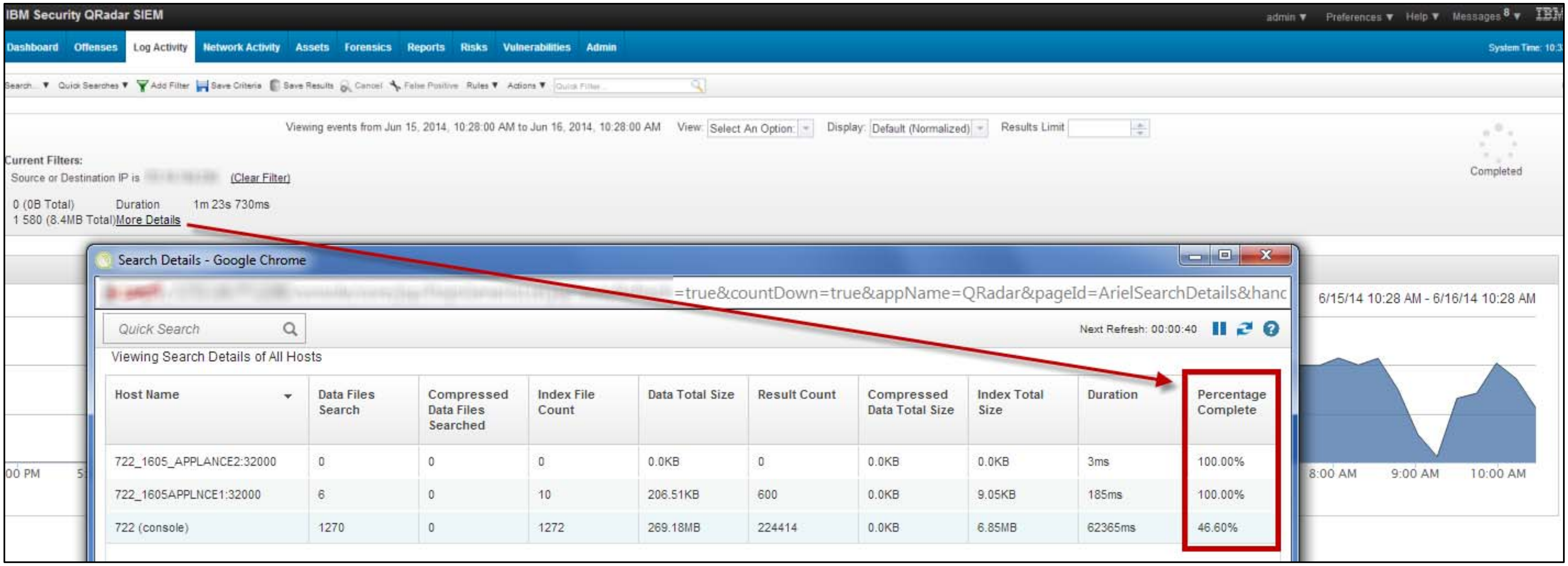
2. If an event result is on another appliance, the Console sends a request to the remote appliance’s Ariel Query Server (AQS).

3. The remote hosts package the search data for the Console and return the results to the Console.


Has a search result
16xx Appliance w/Ariel Query Server
16xx Appliance w/Ariel Query Server
Has a search result
18xx Appliance w/Ariel Query Server
16xx Appliance w/Ariel Query Server
16xx Appliance w/Ariel Query Server
Console
w/Ariel Proxy Server

How do I see searches and their status?

Users can view the progress of a search across their deployment by clicking “More Details”.



Viewing events from Jun 15, 2014, 10:28:00 AM to Jun 16, 2014, 10:28:00 AM View: Select An Option: Display: Default (Normalized) Results Limit

Current Filters:
Source or Destination IP is [redacted] (Clear Filter)

0 (0B Total) Duration 1m 23s 730ms
1 580 (8.4MB Total) More Details

[redacted]=true&countDown=true&appName=QRadar&pageId=ArielSearchDetails&hanc

Viewing Search Details of All Hosts

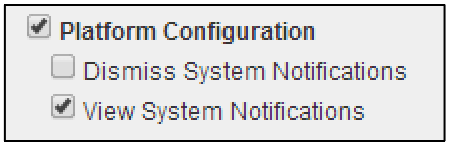
Host Name	Data Files Search	Compressed Data Files Searched	Index File Count	Data Total Size	Result Count	Compressed Data Total Size	Index Total Size	Duration	Percentage Complete
722_1605_APPLANCE2:32000	0	0	0	0.0KB	0	0.0KB	0.0KB	3ms	100.00%
722_1605APPLNCE1:32000	6	0	10	206.51KB	600	0.0KB	9.05KB	185ms	100.00%
722 (console)	1270	0	1272	269.18MB	224414	0.0KB	6.85MB	62365ms	46.60%

How do I troubleshoot ECS?

User Interface troubleshooting

1. **Review System Notifications for disk space or other warning messages. For example:**
   - **Disk usage exceeded threshold.**
   - **Connections were dropped by the event pipeline.**
   - **Process exceeds allowed run time.**

   Note: Users with QRadar 7.2.2 can see System Notifications if they have the Platform Configuration user role enabled with view system notifications.



☑ Platform Configuration
- □ Dismiss System Notifications
- ☑ View System Notifications

2. **Run a 1 minute search against a log source managed by the 16xx, 17xx, or 18xx appliance. If an error is displayed, then you should investigate ECS issues on the remote appliance.**
3. **Apply a filter against a log source managed by EP/EC appliance and view streaming events from that log source.**

Where do I get more information?

Questions on this or other topics can be directed to the QRadar forums: IBM Security Intelligence QRadar Forum.

More articles you can review:

- **Article 1622228: Event Process Pipeline Component Overview**
- **Article 1622851: My Log Activity tab reports unknown events**
- **Article 1622450: How QRadar determines hostnames and IP addresses for events**
- **Article 1622865: What to expect when you are beyond your EPS license limit**
- **Article 1674902: Using the command-line to troubleshoot an event source**
- **Useful links 1616144: Getting Support for IBM Security QRadar products**

Follow us: You Tube t BLOG

IBM Support Portal | Open a Service Request | Update your PMR | Escalate your PMR ibm.com/security