Shared Intelligence Platform for Protecting our National Cyberinfrastructure

NSF Campus Cyberinfrastructure PI and
Cybersecurity Innovation for Cyberinfrastructure PI Workshop

Alex Withers, alexw1@illinois.edu
National Center for Supercomputing Applications
October 18, 2016

NCSA

Science DMZ Actionable Intelligence Appliance

- "CICI: Secure Data Architecture: Shared Intelligence Platform for Protecting our National Cyberinfrastructure" NSF Award #1547249
- What is the "Science DMZ Actionable Intelligence Appliance" (i.e. SDAIA?)
  - A virtual security appliance that will significantly enhance the security posture of open science networks (i.e. Science DMZ deployments).
  - Collects and shares data, analyzes data in aggregate and creates new intelligence feeds.
  - Provides the potential for active protective measures against attacks.
- Collaboration between NCSA/UIUC and Pittsburgh Supercomputing Center
  - **PI: Alex Withers, NCSA, Co-PIs: Ravishankar Iyer UIUC, Adam Slagell NCSA, James Marsteller PSC**

Virtual Security Appliance

- Virtual security appliance installed on open science networks (i.e. Science DMZ deployments).
- Appliance will be very easy to deployed and will not require expensive networking hardware (network taps, aggregators):
  - Uses “honeypots” to attract attacks.
  - Instrumented with sensors to collect data.
  - Modular design using containers.
  - Take active measures if desired.

Where is the Appliance Placed?

- In general: **maximal visibility**
  - If attackers scan the network/campus/etc, then they scan the appliance
    - i.e., unused but allocated, routed IP space
  - For example, ScienceDMZ switch/router a good candidate
    - honeypots may possibly mimic available resources like ssh, http, gridftp

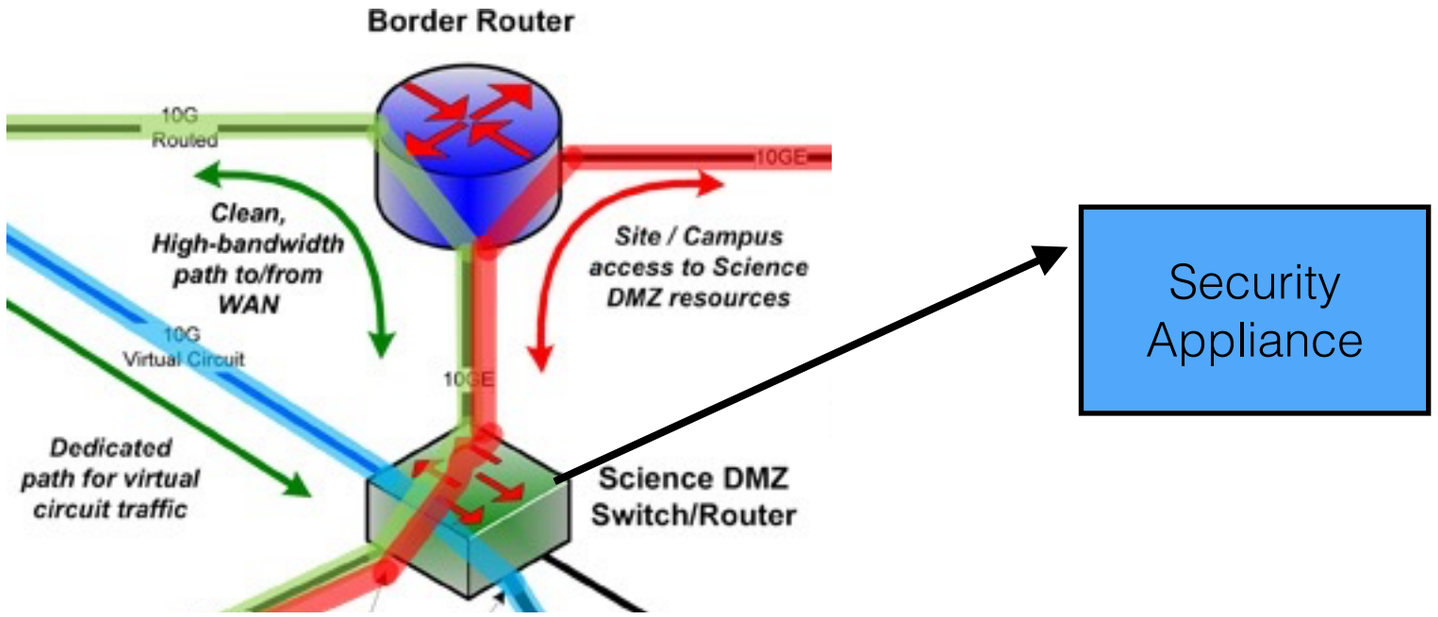
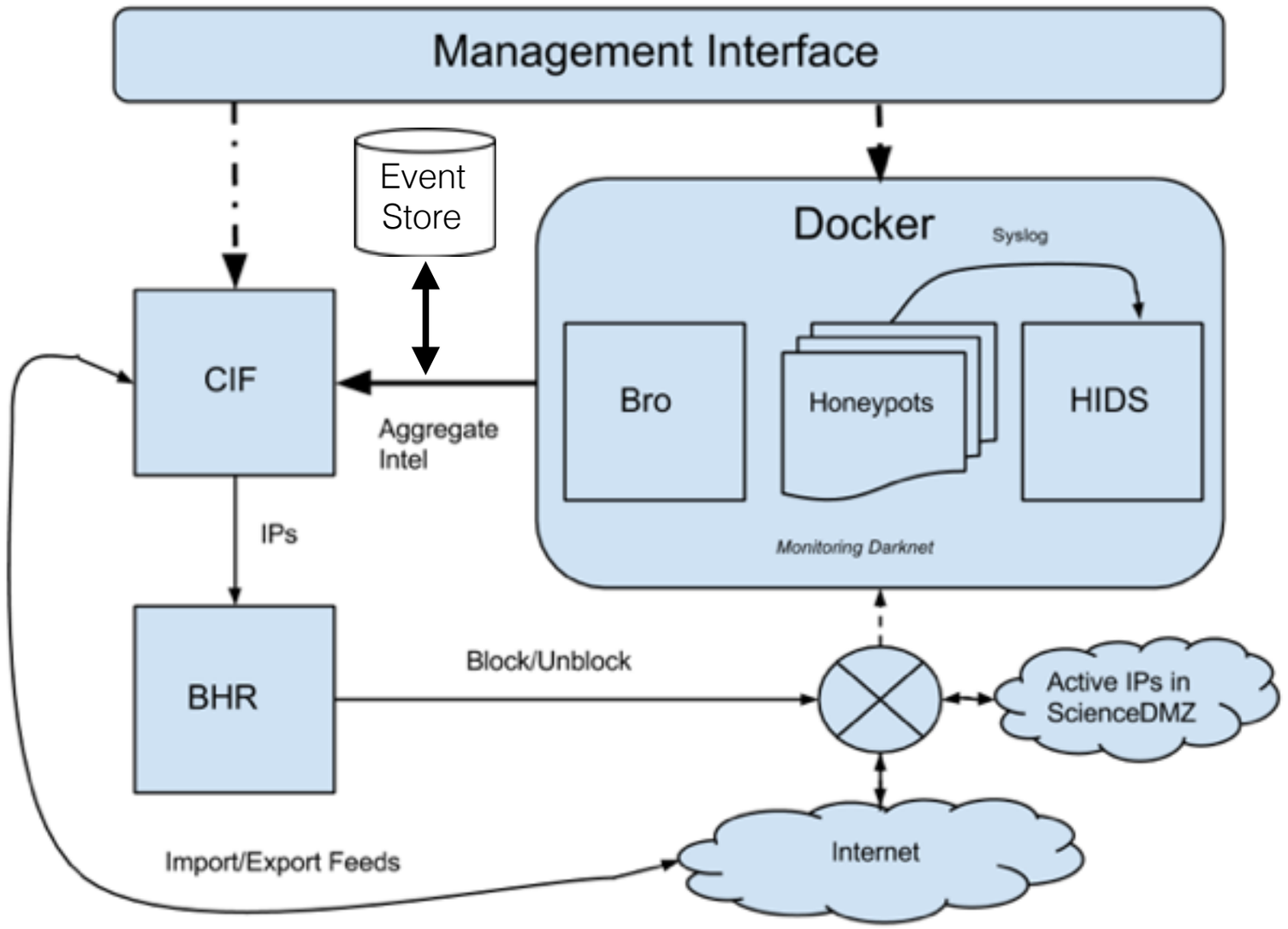


Diagram courtesy of: http://fasterdata.es.net/science-dmz/science-dmz-architecture/

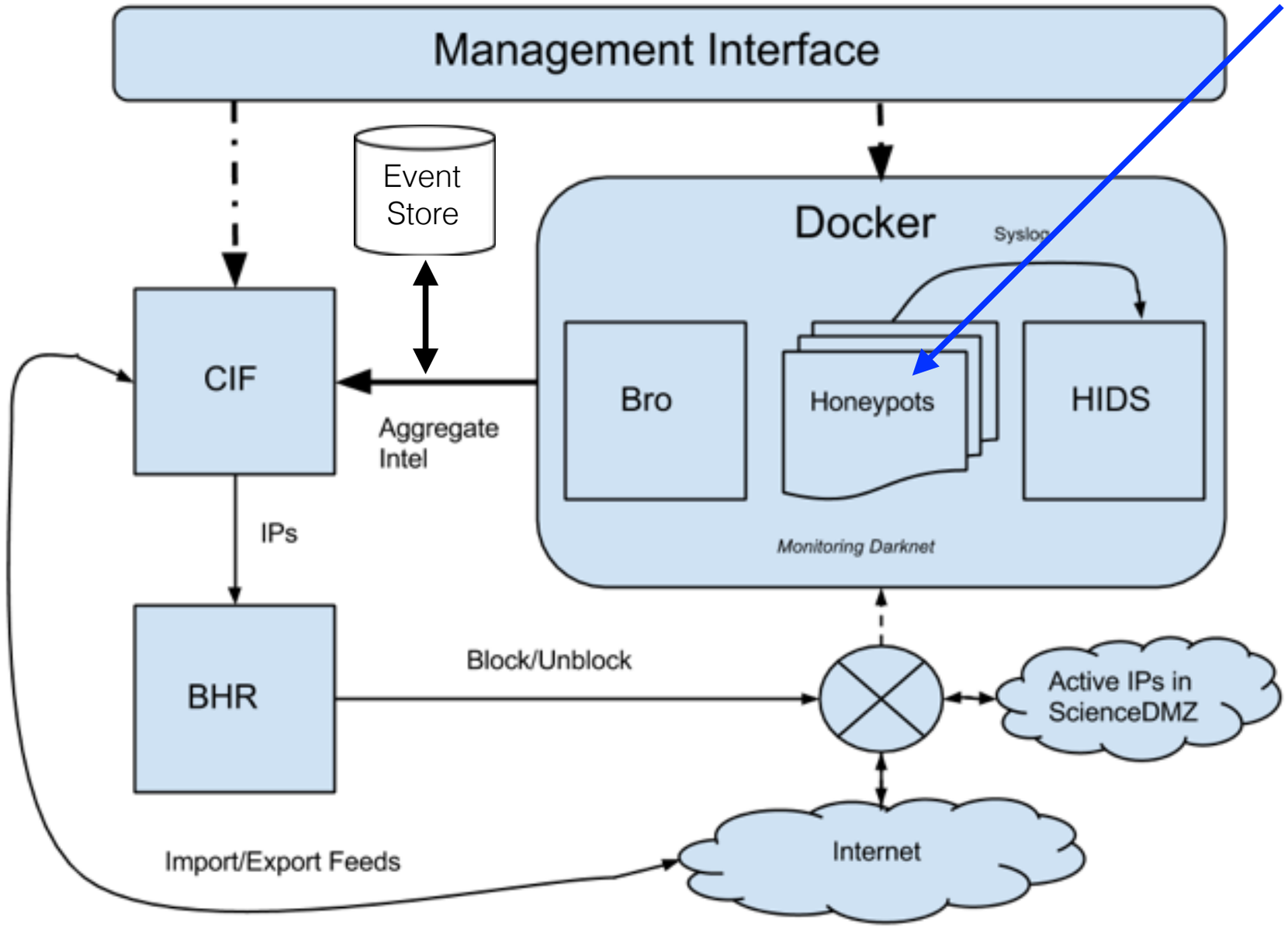
Appliance Architecture



- Using Docker containers for maintainability and ease of management
- Docker networking allows tight control and isolation of honeypots
- All containers run on kvm virtual machine

Appliance Architecture

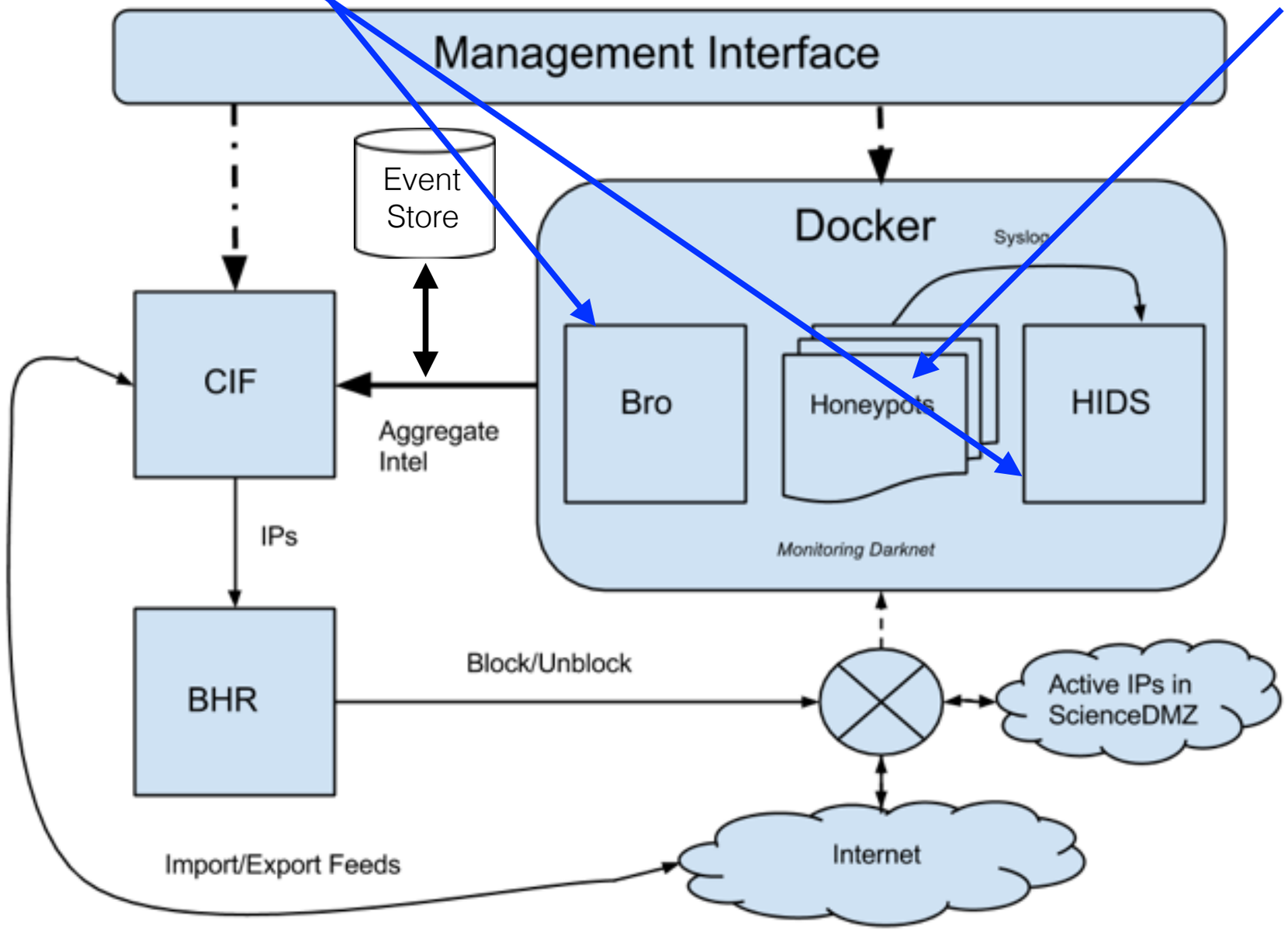
honeypot(s) exposed to outside network,
no egress traffic allowed



Appliance Architecture

sensors such as Bro and OSSEC HIDs covertly monitor activity on honeypot(s)

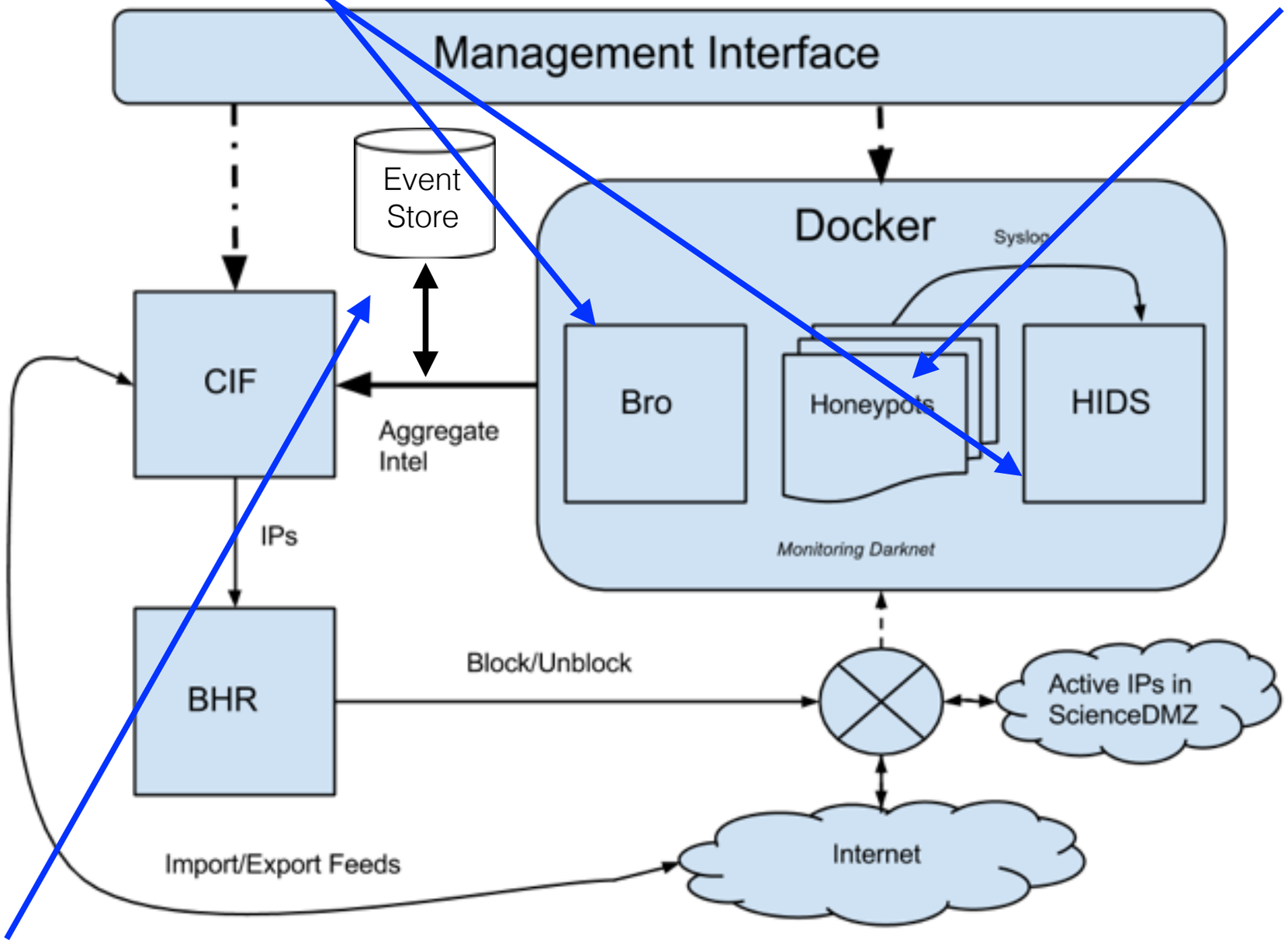
honeypot(s) exposed to outside network, no egress traffic allowed



Appliance Architecture

sensors such as Bro and OSSEC HIDs covertly monitor activity on honeypot(s)

honeypot(s) exposed to outside network, no egress traffic allowed

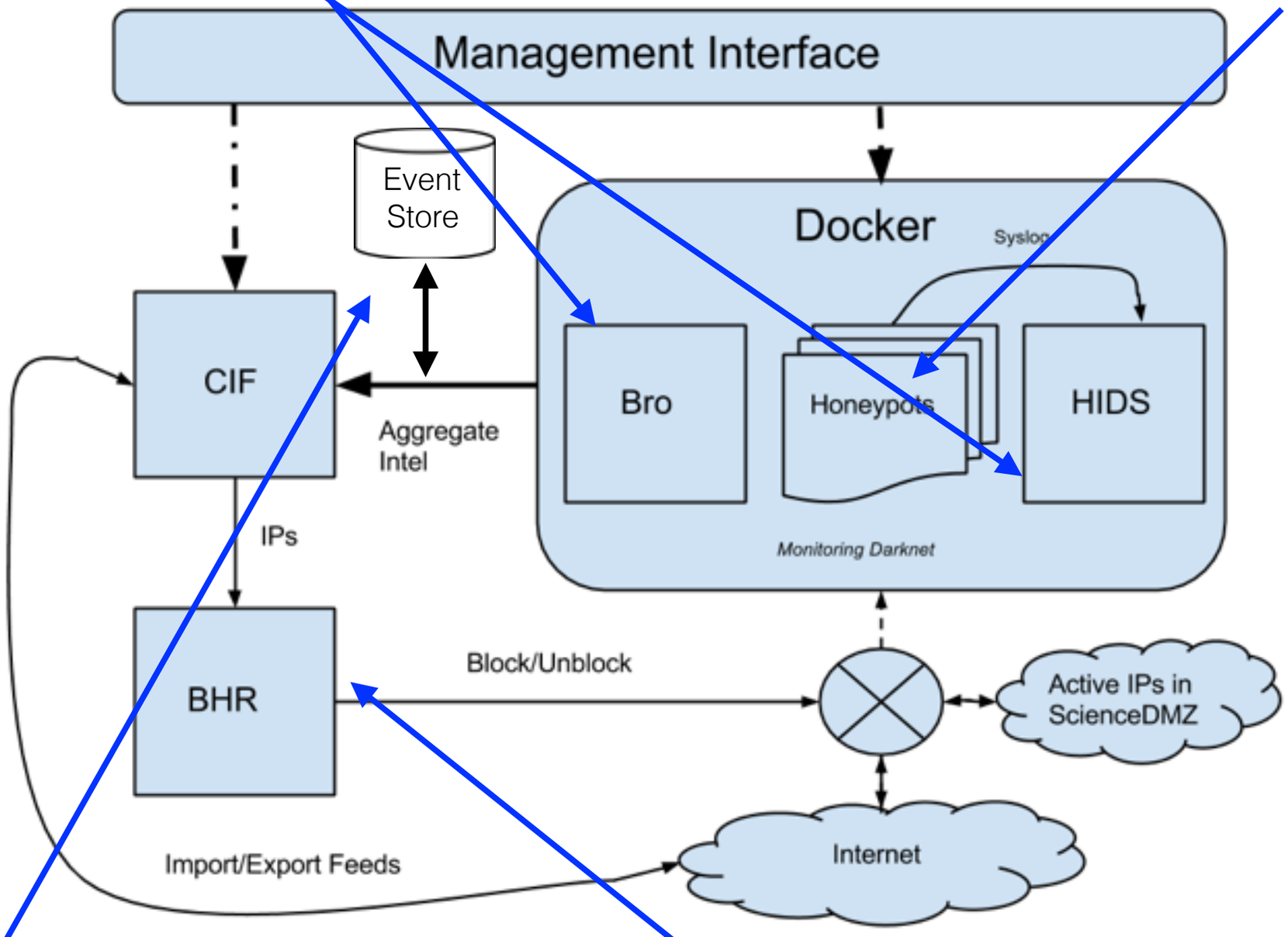


events forwarded to event store

Appliance Architecture

sensors such as Bro and OSSEC HIDs covertly monitor activity on honeypot(s)

honeypot(s) exposed to outside network, no egress traffic allowed



events forwarded to event store

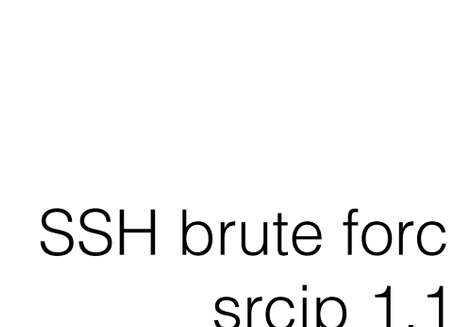
optional ability to act on events

Simple Example

SSH brute force attempt:
srcip 1.1.1.1
<login name list>

Site A

Site B

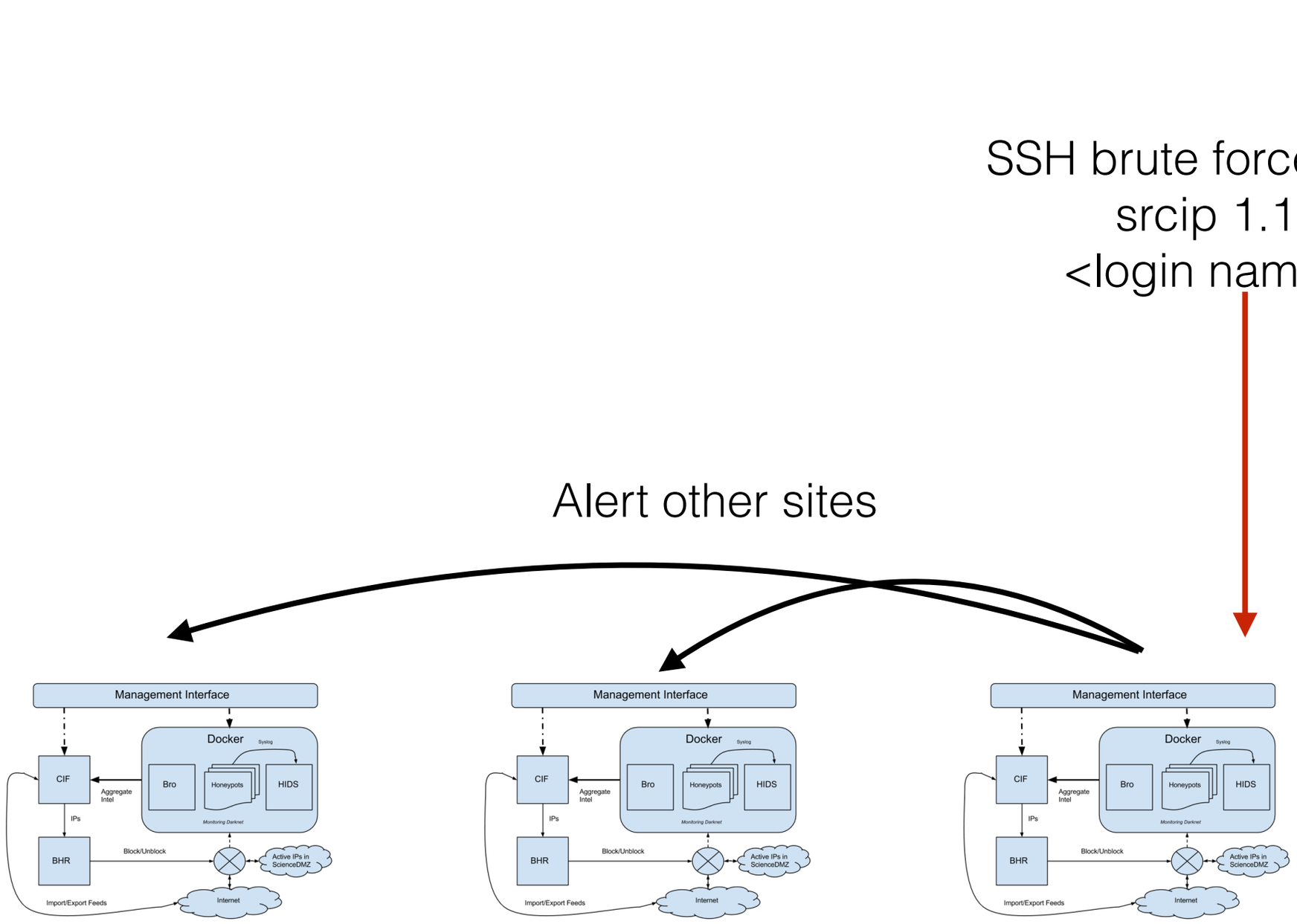


Site C

Simple Example

SSH brute force attempt:
srcip 1.1.1.1
<login name list>

Alert other sites

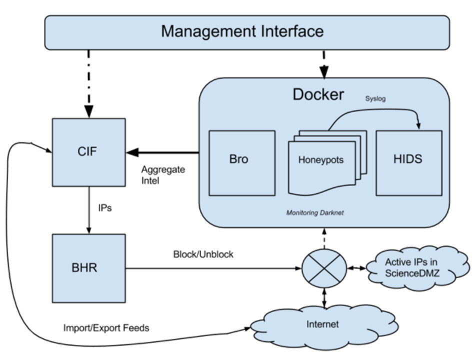


Site A Site B Site C

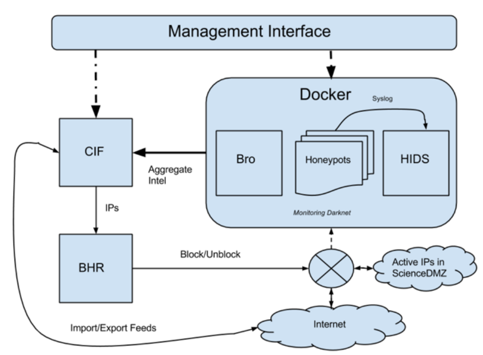
Simple Example

SSH brute force attempt:
srcip 2.2.2.2
<login name list>

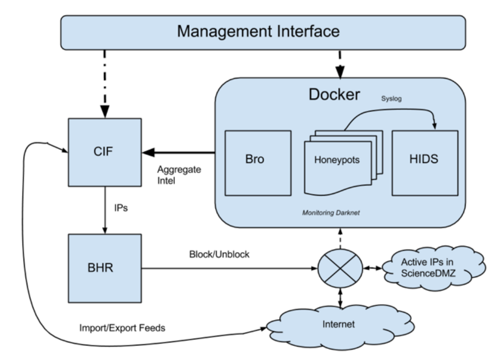
SSH brute force attempt:
srcip 1.1.1.1
<login name list>



Site A



Site B



Site C

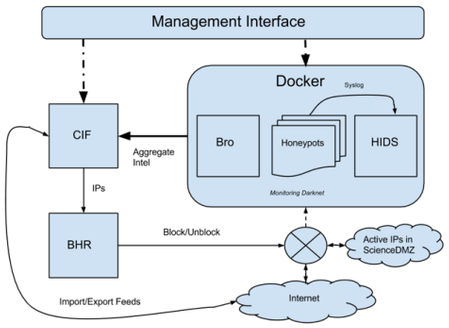
NCSA

Simple Example

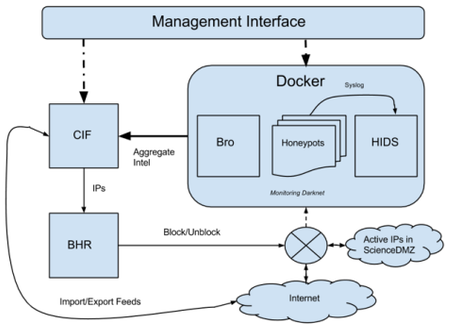
SSH brute force attempt:
srcip 2.2.2.2
<login name list>

SSH brute force attempt:
srcip 1.1.1.1
<login name list>

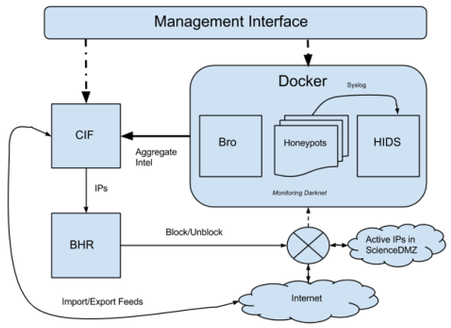
login name list identical



Site A



Site B



Site C

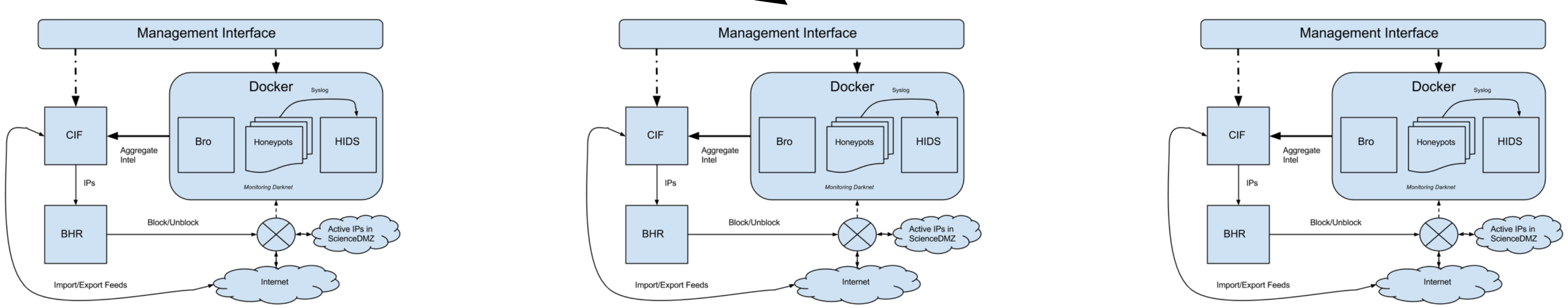
Simple Example

SSH brute force attempt:
srcip 2.2.2.2
<login name list>

SSH brute force attempt:
srcip 1.1.1.1
<login name list>

login name list identical

New event with increased confidence



Site A

Site B

Site C

Appliance Architecture, cont.

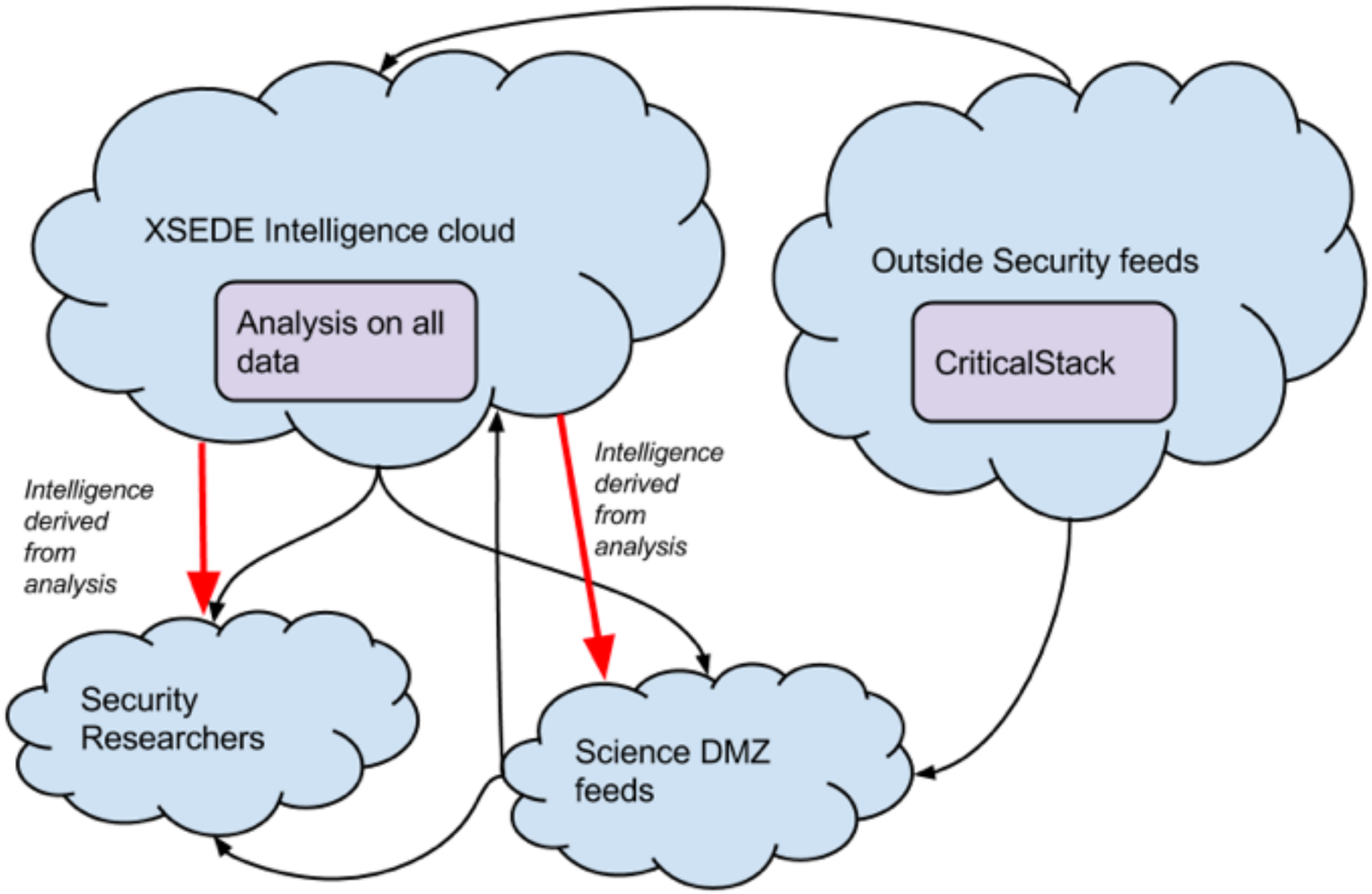
- CIF component uses event store to analyze, normalize and publish feeds
  - also subscribes and consumes outside feeds
  - optionally may act on events published or subscribed using Black Hole Routing

- **Appliance provides complete transparency**
  - **All data, configuration, etc. available to sites that deploy**
  - **No data is shared without opt-ing in**
  - **And control is provided as to what data maybe shared**

Sharing Intelligence

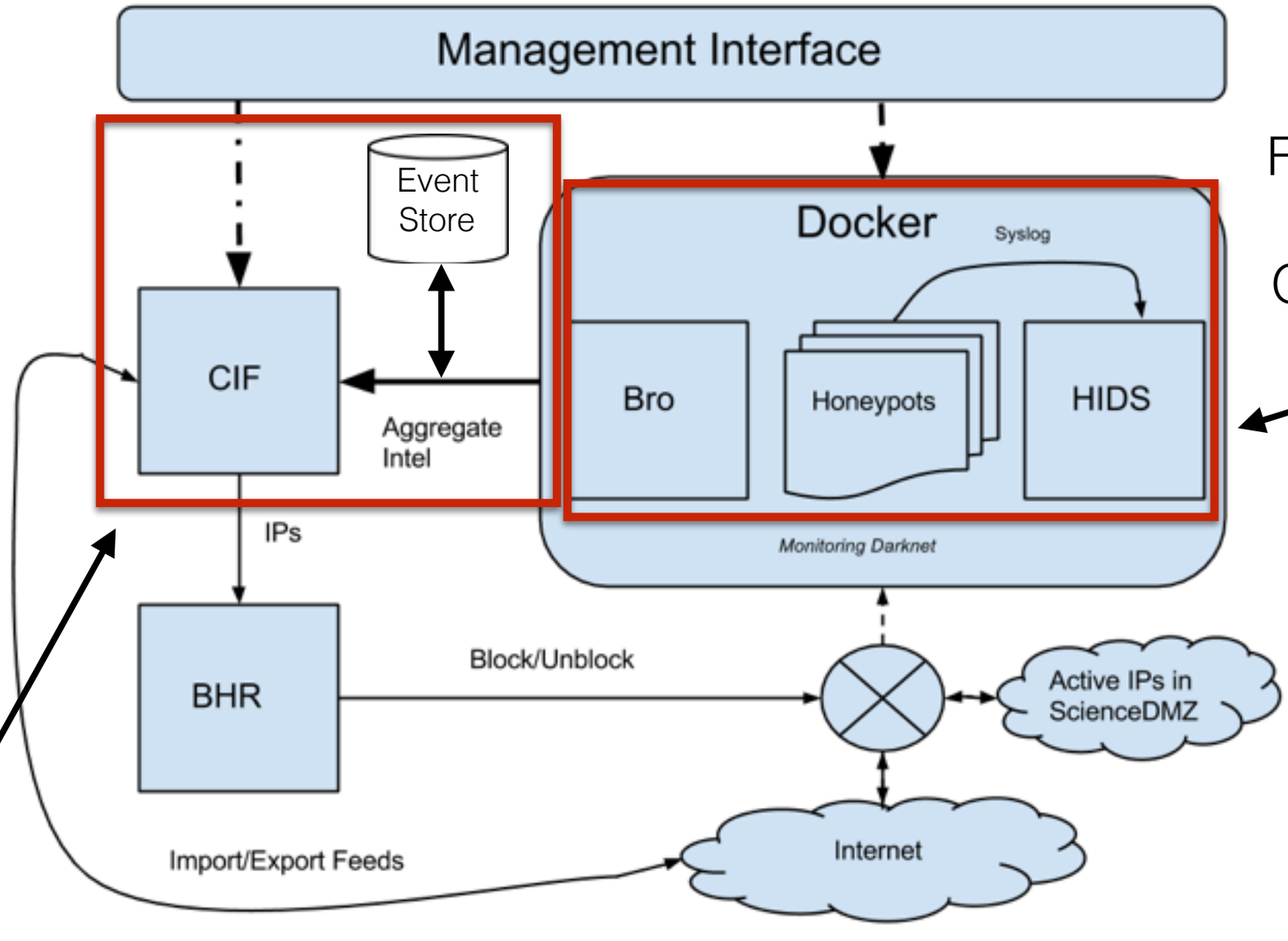
- Focus on actively promoting sharing of intelligence among Science DMZ participants as well as with national academic computational resources and organizations that wish to participate.
- Lay the foundation for an intelligence sharing infrastructure that will provide a significant benefit to the cybersecurity research community.

Intelligence Sharing Ecosystem



Sites who deploy appliance may choose to share their data with other sites and consume other intelligence feeds.

What's Been Done So Far…



Functioning Honeypot with Bro and OSSEC/HIDS sensors

Intelligence Sharing with CIFv2

Working prototypes deployed at NCSA and PSC

Future goals

- Building tools to correlate attacks across sites and assign appropriate confidence levels
- Allow deployments fine grain controls over any actions taken from the feeds
  - Including ability to integrate with site's BHR
- Management interface: focus on CLI and API, then web based app
- Extending capabilities with intelligence feeds
  - Collaboration with XSEDE
- Release by September 2017

NCSA

Thank you

Questions?

alexw1@illinois.edu
slagell@illinois.edu
jam@psc.edu

http://security.ncsa.illinois.edu
http://www.psc.edu

We thank the National Science Foundation (grant 1547249) for supporting our work. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.