Cybersecurity Intelligence Gathering, Sharing and Reacting

SAC-PA2

Shane Filus
Security Engineer
SDAIA
ScienceDMZ Actionable Intelligence Appliance
SDAIA: NSF Award

- CICI: Secure Data Architecture: Shared Intelligence Platform for Protecting our National Cyberinfrastructure
- ACI:1547249; Principal Investigator: Alex Withers
- December 1 2015 – November 2018(estimated)
- Joint project between **NCSA**: Alex Withers(PI), Adam Slagell(Co-PI), Justin Azoff, Linh Cao, and **PSC**: Jim Marsteller(Co-PI), Shane Filus
- Development assistance from Wes Young, REN-ISAC
Project Goals - overview

• What is the SDAIA?
  • ScienceDMZ Actionable Intelligence Appliance
    • A virtual security appliance that will significantly enhance the security posture of open science networks.
    • Scalable, near real-time dissemination of threat intelligence.
    • Decentralized peer-to-peer model.
    • Collects and shares data, analyzes data in aggregate and creates new intelligence feeds.
    • Threats seen in multiple locations can provide sites an edge in threat detection.
    • Easy to deploy - large ROI for sites with limited security resources.
Project Goals – requirements/specifications

- Appliance will be easy to deploy
  - Will not require specialized networking equipment (i.e. inline taps)
  - Distributed as ansible scripts that create and setup the appliance on any routable network(VM/bare metal).
- Uses “honeypots” to attract attacks and mimic available resources like ssh, http(s), gridftp, etc
- Instrumented with sensors to collect data (i.e. bro).
- Data is securely shared with other sites - can create multiple mesh networks.
- Take active measures if desired
  - Interface with a Black Hole Router, firewall, email alerts, etc
- Share data with other sites!
  - The more data that’s collected, the better the analysis and confidence on shared indicators.
  - Confidence levels on indicators can mean more meaningful action.
Appliance Architecture

Workflow

- ssh-auth-logger and Bro IDS collect indicators from SSH authentication attempts and network scans.
- Event logs are parsed and indicators are loaded into local CIF instance.
- Indicators are shared with other sites over a secure p2p network: can also be used for local policy enforcement (BHR, firewall rules, email alerts, etc).
- Indicators are also ingested from other sites: optional placement of indicators into local Bro Intel Framework or BHR.
Appliance Architecture

Bro IDS

Honeypot Monitoring

Bro Intel Framework

Act on Events

BHR

Indicators Shared and Consumed

WAN

Single/multiple IPs in Routed address space (can be unallocated)
Appliance in action

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

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

Alert other sites

Site A  Site B  Site C
Appliance in action

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
Appliance in action

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
Appliance in action

SSH brute force attempt:
srcip 2.2.2.2

<login name list>

login name list identical

New event with increased confidence

SSH brute force attempt:
srcip 1.1.1.1

<login name list>

Site A  Site B  Site C
Appliance Components

- ssh-auth-logger
  - Low interaction SSH honeypot written in Go.
  - Collects: src ip, username, password/pubkey, ssh version.
- Zyre (zeromq+p2p)
  - Very fast p2p 1:N message passing.
- Disco
  - Simple service discovery for key exchange and gossip
- ClFv3
  - Stores indicators/events.
- Apache Kafka
  - Message/event passing queue for extensibility.
- Bro IDS
  - Monitors network traffic going into honeypot.
  - Monitors and alerts on indicators seen at other sites.
Currently working

- Easy install
  - CentOS 7 fixes not in main distro (sdaia-xsede fork)
- SSH honeypot (ssh-auth-logger)
- p2p mesh/service discovery
  - Message passing between clients
  - Roll-your-own mesh
- Bro
  - Detects scans, uses indicators from mesh in Intel Framework
- CIFv3
  - Stores indicators seen locally and via mesh
- Simple scripts to pull indicators out of zyre/mesh
  - Create bro intel files
In Development

- **Kafka**
  - Brings data together from other appliance components
  - Allows sites to read out data collected into custom ingest systems (i.e. Splunk/ELK).
  - Allows sites to write out data from other sensors and systems for sharing (i.e. BHR events).

- **Bro sensor**
  - Create intel events from detected port/address scans, etc

- **Other honeypots for commonly used/SDMZ services**
  - Web auth, smtp, ftp, gridftp

- **Usability/Integration**
  - Make it easy to deploy, configure, and tie into site’s existing infrastructure.
  - Building tools to adapt attack correlations across sites and assign appropriate confidence levels
Where is this being tested?

- Duke U
- NCSA
- PSC
- Lehigh U (testing)
- U of Illinois Urbana-Champaign (campus network)
- XSEDE (testing/development)
Additional Information/Links

- **SDAIA Main Page**
  - https://wiki.ncsa.illinois.edu/display/cybersec/SDAIA

- **SDAIA github page**
  - https://git.ncsa.illinois.edu/awithers/sdaia

- **SDAIAkeys – pubkeys/scripts**
  - https://github.com/ncsa/sdaiakeys

- **XSEDE SDAIA fork**
  - https://github.com/filusATpsc/sdaia-xseed
Additional Tools
Additional Tools/Resources

  - “CIF helps you to parse, normalize, store, post process, query, share and produce data sets of threat intelligence.”

- **Malware Information Sharing Platform (MISP)** - [https://www.misp-project.org](https://www.misp-project.org)
  - “A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.”

- **Critical Stack** - [https://intel.criticalstack.com](https://intel.criticalstack.com)
  - Build custom intel lists from various public feeds

  - Convert between intel formats

- **Ssh-auditor** - [https://github.com/ncsa/ssh-auditor](https://github.com/ncsa/ssh-auditor)
  - Scan for weak SSH passwords on your network

- **US-CERT Announcements** - [https://www.us-cert.gov](https://www.us-cert.gov)
  - Release IOCs for current threats

- **REN-ISAC** - [https://www.ren-isac.net](https://www.ren-isac.net)
  - SES(curtailed public and private member intel), Passive DNS, Daily Watch Report