BRICATA

SOARing into Netsec

With Carl Bolterstein

Objectives

- Introduction to Bricata
- Current methodologies of Network Hunting and Traffic Analysis
- Shortfalls of the current methods
- Introduction to SOAR
- Completing the loop on automated response – The Auto-Tagger
- Data Enrichment and what it means in your environment

The Bricata Solution

Unparalleled Network Visibility

Bricata lets you see everything that transpires on your network via high-fidelity metadata and SmartPCAP

Full-Spectrum Threat Detection

Bricata optimizes detection and minimizes false positives by employing multiple threat detection engines concurrently

True Threat Hunting

Bricata empowers you to thoroughly investigate detected threats and to hunt unknown threats that didn't generate an alert

Post-Detection Actions

Bricata stops threats on the network and generates required inputs to your downstream remediation tools

Current Methods of Analyzing Network Traffic

- In enterprise environments, the ground truth of the environment is in the data.
- Whether this data has come in the form of logs to network flows to full packet capture, it can provide value for security analysts.
- We will focus on the network flow and full packet capture data in our workflows today.

Alert and Data Sources

Where does it all come from?

Signature Driven Alerts

- Signature based detection systems have been with us for many many years
- They provide detection for threats based on criteria matching in the traffic

Message	ET FTP Outbound Java Downloading jar over FTP
Last Seen	19:47:04 11/15/19 -0500
Header	tcp $HOME_NET any -> $EXTERNAL_NET 21
Options	msg:"ET FTP Outbound Java Downloading jar over FTP"; flow:to_server,established; flowbits:isset,ET.Java.FTP.Logon; content:".jar"; nocase; fast_pattern; content:"RETR "; pcre:"/^[^\r\n]+\.jar/Ri"; classtype:misc-activity; sid:2016688; rev:3; metadata:created_at 2013_03_28, updated_at 2019_10_07;

Anomaly-based IDS

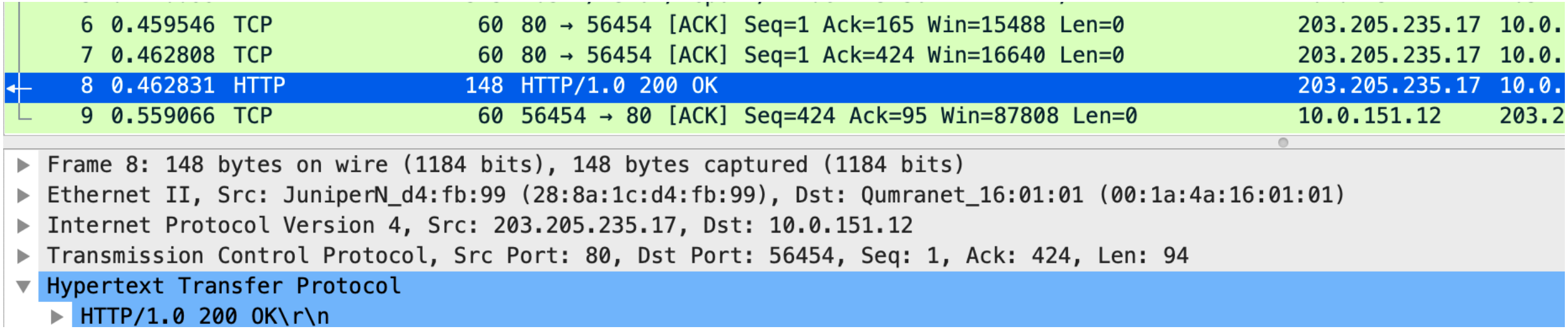
- Rather than relying on known-bad indicators of compromise such as signatures, heuristics search for potentially bad behaviors in the environment based on the data present.
- This allows the environment to baseline known-good traffic and attempt to find deviations from the baseline.

Network Metadata Collection

- Network Metadata was built on the concept that more information needed to be present for effective analysis beyond standard 5-tuple flow information
- Efficient, at scale collection and inspection of traffic is essential to this concept to provide the most value to security tools attempting to search for bad behaviors in a network

Packet Capture

- Full or selective packet capture enables security organizations to dig into the traffic on the network as deep as possible
- Enables the ability to search payload information in traffic compared to just collecting metadata information



Shortfalls

- With every detection or collection method, there are unavoidable shortfalls

Shortfall of Signatures

- Requires the signature to match exactly to a behavior that is previously known or found in the data manually
- Limited detection capability of traffic that has encrypted payloads
- Signatures are easily defeated by mutating or obfuscating malware

Shortfalls of Heuristics

- Prone to false positives out of the box due to the nature of determining a baseline against data the model is not aware of
- Computationally intensive workflow to build meaningful detections against the data
- Speed of detecting anomalous behavior is typically much slower than signature or deterministic detection methods as more data is required to be collected first

Network Metadata Shortfalls

- Volume of network metadata can quickly reach such a high level; it may start to diminish in value due to storage and computational costs
- Not all analytics take advantage of all metadata fields available
- The double-edged effect that while analysts have more data available, the human time needed to analyze or hunt inside this data grows too
- As networks grow in complexity and size, metadata systems are required to grow along with them in order to provide seamless visibility which can be easily overlooked due to cost

Packet Capture Shortfalls

- Storing vast quantities of packet capture on ever-growing network sizes can quickly spiral into a costly endeavor
- Pure cloud or hybrid cloud environments are not typically architected with traffic flowing in a concentrated manor through the edge of the network which can leads to gaps or no coverage of certain traffic
- Requires storing everything regardless of value on most typical packet capture systems
- Human analysis of raw PCAP consumes vast amounts of time due to the volumes present

Analyzing all the Things

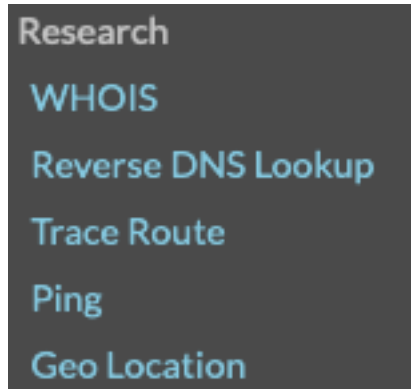
- Whether you are working from an alert in your system or hunting through metadata.. The thought process is the same;
- You want to determine if the behavior observed is bad or not, and what to do about it

Alert Triage

- Analyzing alerts that come into your environment are usually handled by a workflow
- This workflow may include items such as;
  - Hostname lookup in an IPAM or directory system
  - IP whois, reverse dns lookup
  - Endpoint interrogation with tools such as OSQuery
  - Log analysis from endpoints such as AV or EVTX output
  - Restrict access
  - System Isolation
  - Malicious file removed or quarantined

Data Enrichment in Cyber Security

- Data enrichment is an important key process in cyber security to help in providing the best value out of your environment
- These enrichments not only allow your analysts to make better decisions, but they can be leveraged in SOAR playbooks
- This can take many forms such as;
  - IP and Domain intelligence
  - Hostname resolution
  - DHCP mapping
  - Tactics, Techniques and Procedures (TTP) matching
  - MD5 lookup



Expanding the Hunt in Metadata

- After reacting to an individual system you can pivot out further to check for similar behaviors on the network
- This may include searching for destination IP addresses or DNS requests on a wider scope than the original endpoint
- Allows an analyst to build an enhanced picture of the activities surrounding an alert, rather than just reacting to the alert details

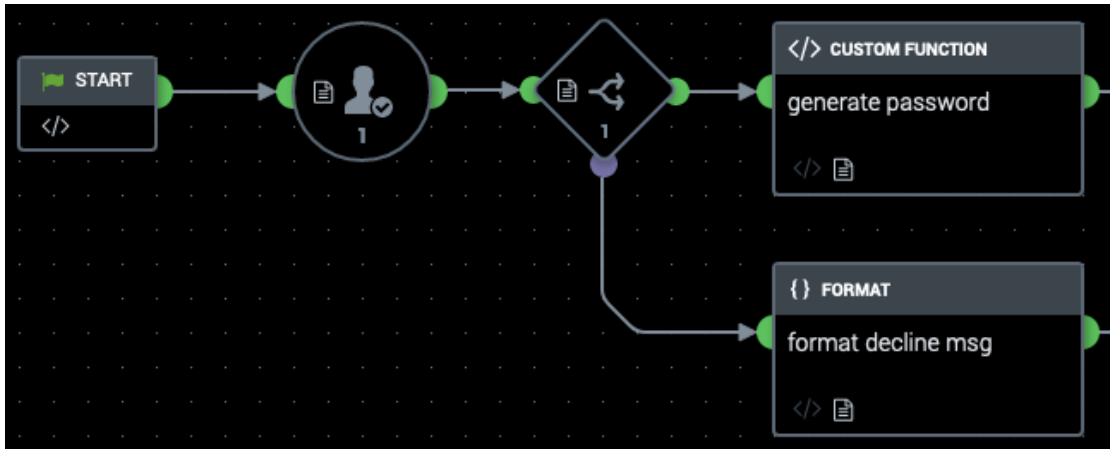
Bringing us into the future

- But how you ask do we bring ourselves into the future?

- I follow a simple mantra; automate everything I must do more than once
- This not only has the effect of making me more efficient, but allows for me to move past error prone manual workflows and concentrate on making my system do more by itself in an accurate, repeatable fashion
- Leveraging this in the security space brings us to Security Orchestration, Automation and Response

Security Orchestration, Automation and Response

- The concept of SOAR is new to the cyber security space, but it brings with it many welcomed ideas to help with the shortfalls plaguing security teams everywhere
- With the ability to automate tasks typically carried out manually this brings not only speed and efficiency, but wider integration with typically disparate systems to provide the best outcome from triaging alerts

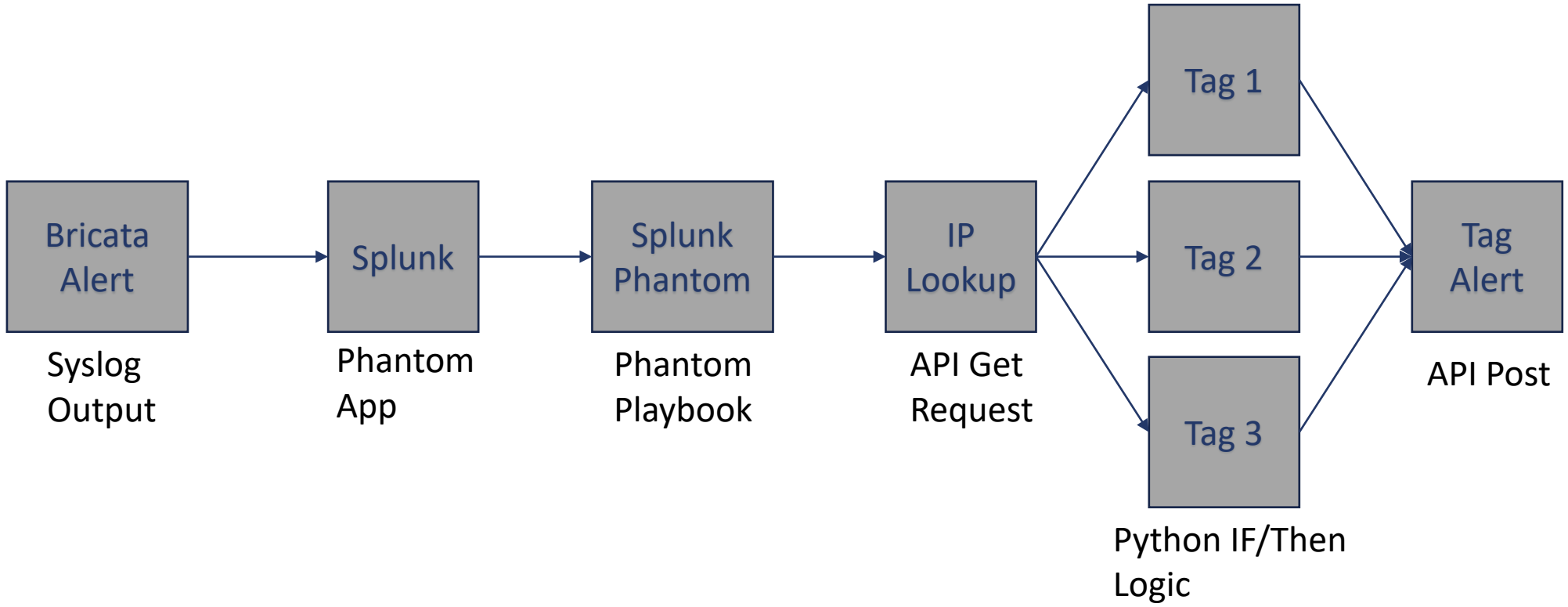


Automation Use Case: The Auto-Tagger

- Starting with a simple premise, I decided to build out a playbook in Phantom to provide me with further context around alerts by tagging various ip addresses back in my Bricata system
- This not only is a task that I didn't want to do manually, but provided me with the ability to lookup this IP address during the execution to change the tag if it matched a threat list
- This lookup traditionally was done manually through different lists spread across a wide number of different systems containing piles of IPs

Auto-Tagger Playbook

- Flow of my playbook

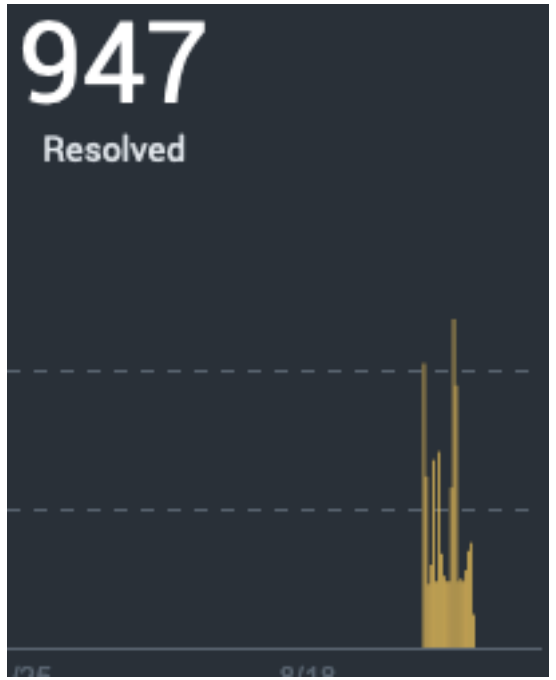


Value Driven Workflow

- With the ability to automate workflows, we can then think about what is the most value we can drive from data we are attempting to enrich
- These use cases can range from reducing the mean time to detection and response, to reducing the volume of alerts that human analysts must work through
- Previously disparate systems and endpoints can be brought together to provide a complete picture of the security posture of an environment in a dynamic way rather than static information
- This also helps adapt security systems for the disposable nature of cloud and container-based systems

Endless Possibilities

- With the amount of actions able to be taken, the possibilities for responding to alerts with a SOAR platform can be functionally endless
- Playbooks are best thought of as an extension of the existing resources in your environment rather than a replacement
- Traditionally siloed data environments can be bridged together to assist in reacting quicker to security threats rather than spending time and resources on manual tasks



Final Thoughts

- Traditional security event response is not all bad
  - It got us to where we are today, and is a good baseline for improvement
- Security Orchestration, Automation and Response should be on the forefront of your future way of thinking
  - Automate the mundane
  - Build the ability to interact with everything available
- Bring context to the table with data enrichment
  - Keep your systems integrated with each other to best enable your environment to provide the best data available while empowering your analysts to make the best decisions

Thank You

cbolterstein@bricata.com