The best defense

- *Step -1*: Build solid security response procedures
  - Full scope close-out
- *Step 0*: Establish data collection / Instrument Network
  - Start with existing data
  - Improve based upon pain points

Identifying Pain Points

Monthly Retrospective of Alerts and Incidents

- *Sort by Type –*
- *Executable attachments*
- *Server Side Compromises*
- *Malicious Links*
- *Credential Re-Use*

THREATSTREAM®

Hunting Approaches

Personnel

Soc Analysts

Incident Responders

Dedicated Teams

Time Frame

Day per Week

Week per Month / Quarter

Longer engagements

Continual Hunting

Approach 1: Day per week

- Staff: SoC analysts and/or IR staff
- Tactics:
  - Indicator sweeps
  - Basic heuristic approaches
- Benefits:
  - Improve SoC staff proficiency
  - Identifying the “simple” stuff

Approach 2: Week per month / quarter

- Staff: SoC Staff and/or IR teams
- Tactics:
  - Improving and tuning data sources
  - Heuristics
  - General tactics in threat reports
- Benefits:
  - Improved posture against a *Pain Point*
  - New detection scripts
  - Improved skillsets and situational awareness

Approach 3: Longer Engagements

- Staff: IR Staff, Dedicated Hunting Teams
- Tactics:
  - Data Deep Dive
- Benefits:
  - Deep Situational Awareness
  - Establish a “Known Good” Baseline
  - Sets the stage for continual hunting

Server Side Compromise: Web Access and Error Logs

- **Search For RFI and LFI vulnerabilities**
  - rare client side IPs
  - Web host enumeration – cold fusion .cfm pages
    - File Owners – Administrator versus WWWService
- **Search for Web Shells**
  - via access.log
    - Tor and VPN IPs
  - via shell scripts
    - exec(variable)

Persistent Programs / Scheduled Tasks / Cron

- **SysInternals AutoRuns**
- **Scheduled Tasks**
  - Collect and review scheduled tasks
    - atN.job are suspicious
- **Crontab**

```
$ hostname = `/bin/hostname`
$ cr=`crontab –l`
$ echo $hostname,$crontab  >> /network_fileshare/cron_hunting.csv
```

Other Examples

Other Pain Points

- **HTTP C2 Channels**
    - Review Web Proxy
        - Entries lacking referer
- **HTTPS C2**
    - Suricata or Bro – review certificates.
        - Remove alexa top 1000 from censys.io
        - New certificates
- **DNS Covert channels**
    - DNS logs
- **Credential Re-Use**
    - Speed of Light – New Locations
- **Spear Phishing**
    - Email Spool

General Data Sources

- **Instrument End Points**
    - Osquery
    - Osxcollector

    - Sysmon – apply filters –
        - dump to data store
        - UF or Elastic Search

THREATSTREAM®

General Tactics

- **Least Frequency Occurrence**
  - The rare things are the interesting things
- **Cross Hosts**
  - Clients versus Server hosts
  - Organizationally significant Hostnames
- Organizationally significant Usernames

Happy Hunting

THREATSTREAM®

Aaron Shelmire | Sr. Security Researcher
2317 Broadway, 3rd Floor| Redwood City, CA 94063
Twitter: @ashelmire