Brian Smith, CTO & Founder
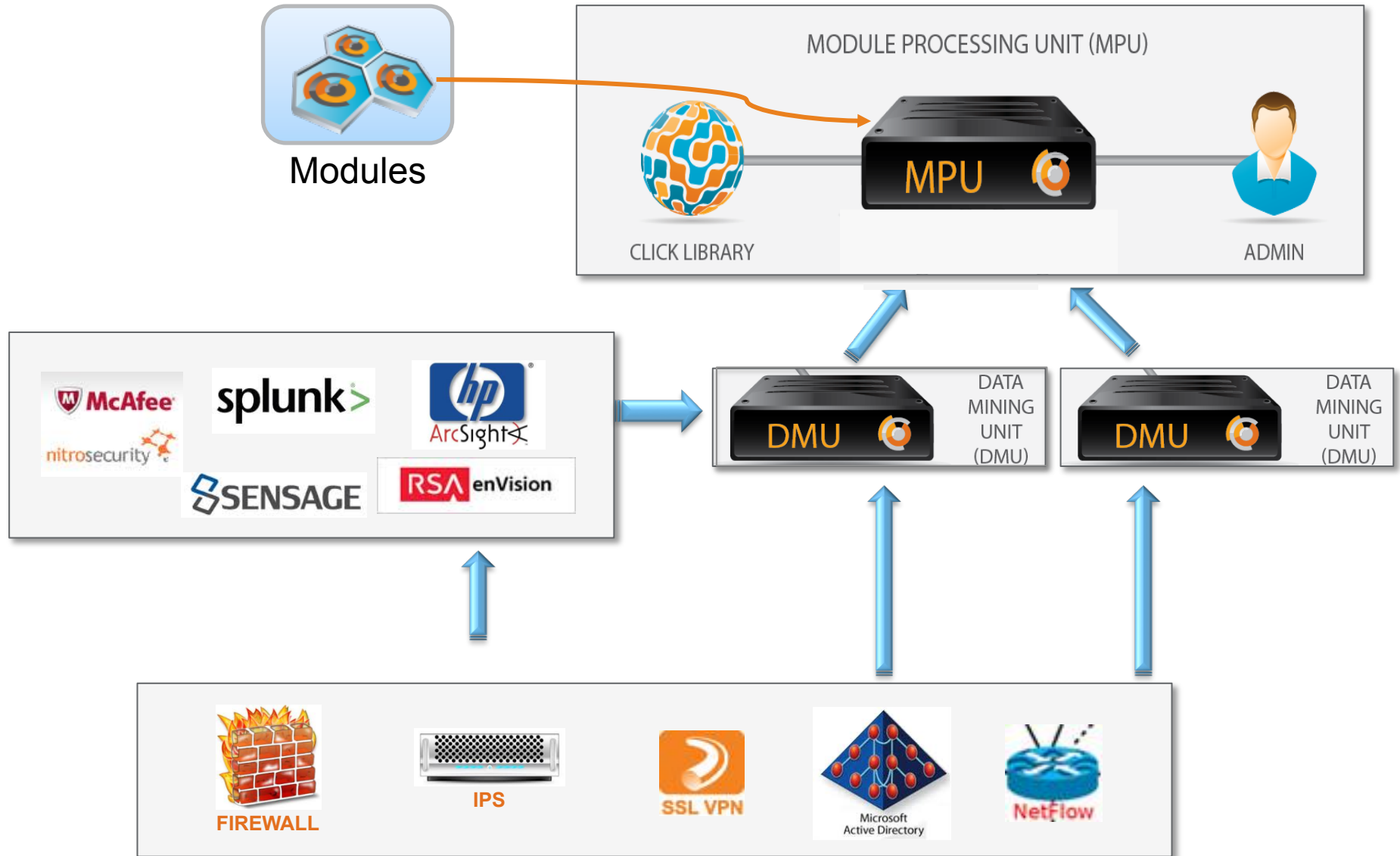
www.clicksecurity.com

It's Not Working!

- Firewall
- IDS/IPS
- Anti-X
- Vulnerability Scanner
- Identity Access and Management
- Web Application Firewall
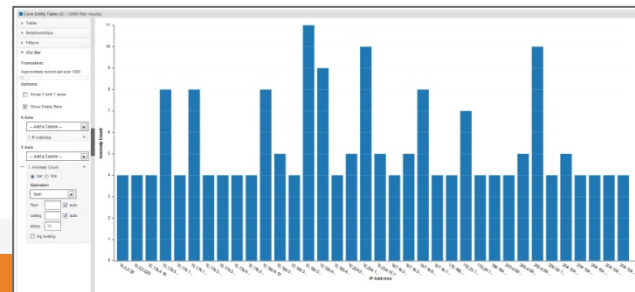- Patch Management
- Proxy
- …

- Answer is in the Logs, but…
  - Where to start?
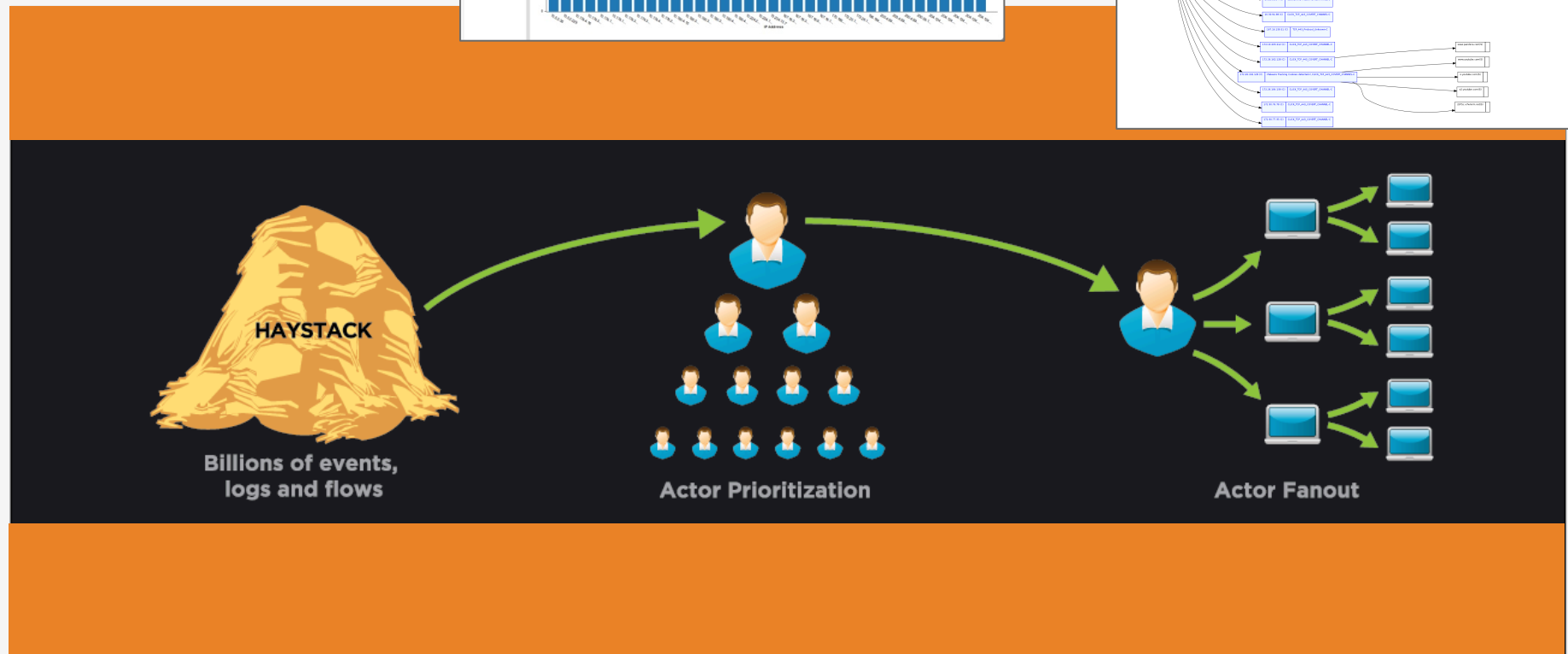 - What questions to ask?
  - What to look for?

Click Tool

Modules

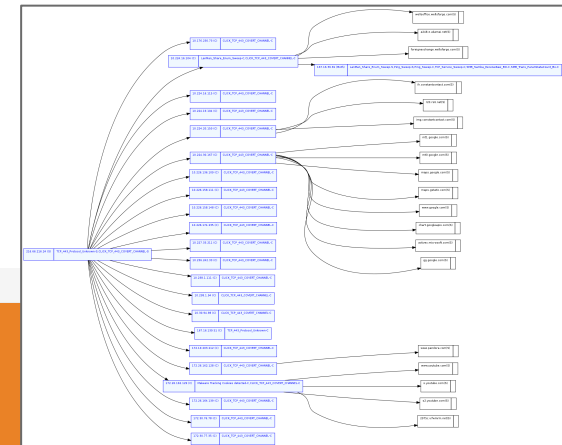MODULE PROCESSING UNIT (MPU)

MPU

CLICK LIBRARY

ADMIN

McAfee
splunk>
hp ArcSight
nitrosecurity
SENSAGE
RSA enVision

DMU — DATA MINING UNIT (DMU)

DMU — DATA MINING UNIT (DMU)

FIREWALL
IPS
SSL VPN
Microsoft Active Directory
NetFlow

4

Module Example: Actor Core

High Anomaly Actors

Actor Context Graph

HAYSTACK

Billions of events, logs and flows

Actor Prioritization

Actor Fanout

Demo Time!

Thank You!

bsmith@clicksecurity.com

http://www.clicksecurity.com