Security Automation Standards:
What we need, why we need them

CHRIS SALTER

NSA IAD FUSION, ANALYSIS & MITIGATIONS

OCTOBER 2012

TWO ASPECTS

- Situational Awareness
- Command & Control

Automation: Welcome to Cyberspace

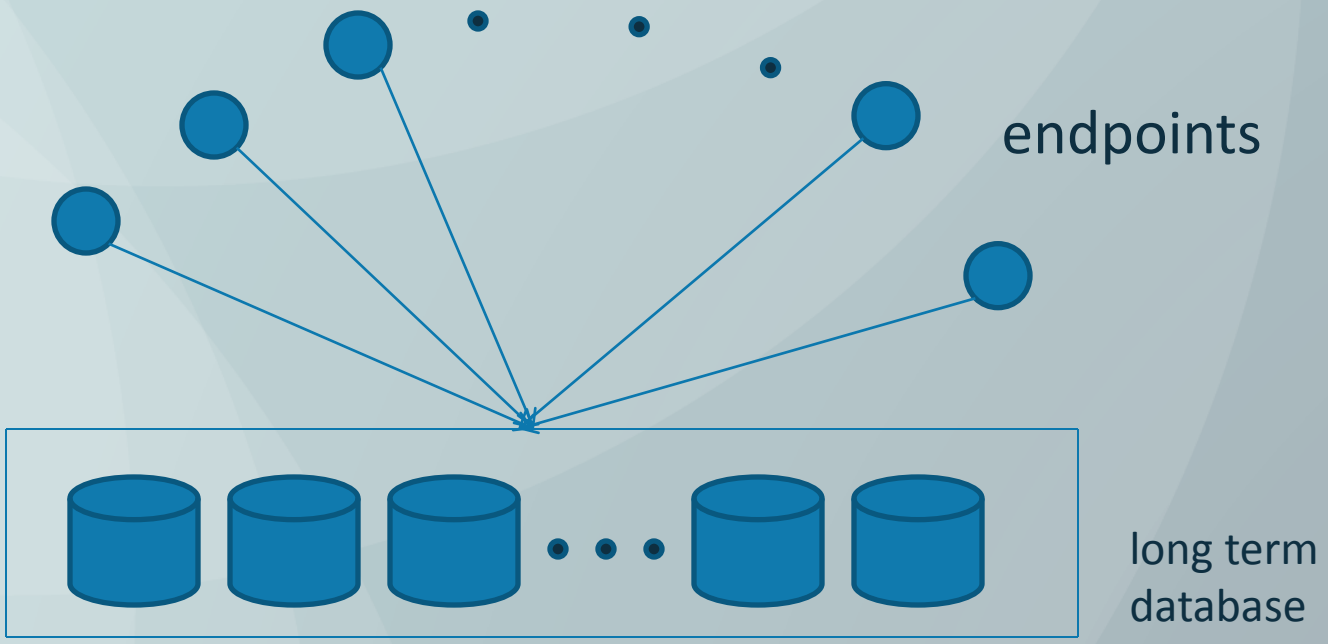
SOME DEFINITIONS

- Endpoint: every device assigned an IP address on your network
- Sensor: every device that reports behavior on the network
- All sensors are endpoints
  - Perhaps all endpoints should be sensors…

SITUATIONAL AWARENESS

- Is it healthy?
  - What is on the network?
- Is it compromised?
  - What is it doing?

WHAT IS ON OUR NETWORK?

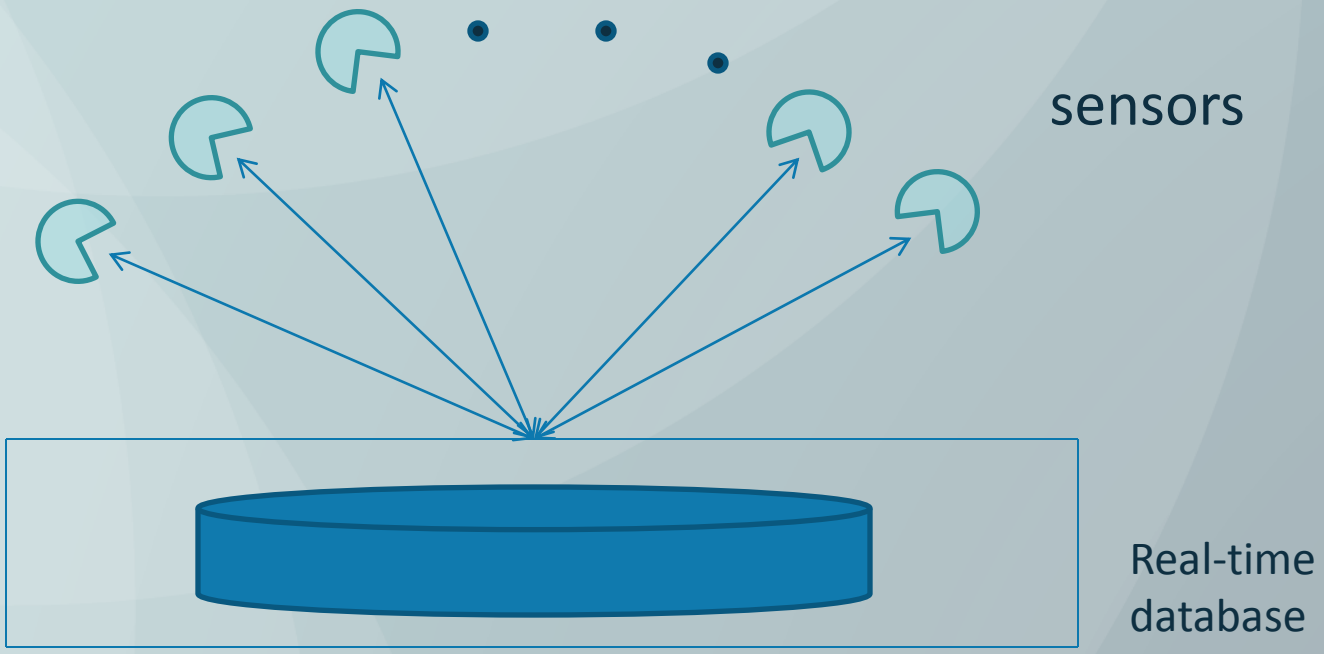


Configuration and Asset Management Dashboard

VULNERABILITY DISCOVERED IN A PRODUCT

- Which hosts
- Which versions
- Which patches
- Which configurations

WHAT IS HAPPENING ON OUR NETWORK?



Operational Dashboard

VULNERABILITY EXPLOITED ON A HOST

- Checksums on files
- Ports open on host
- Unexpected connections

COMMON OPERATING PICTURE

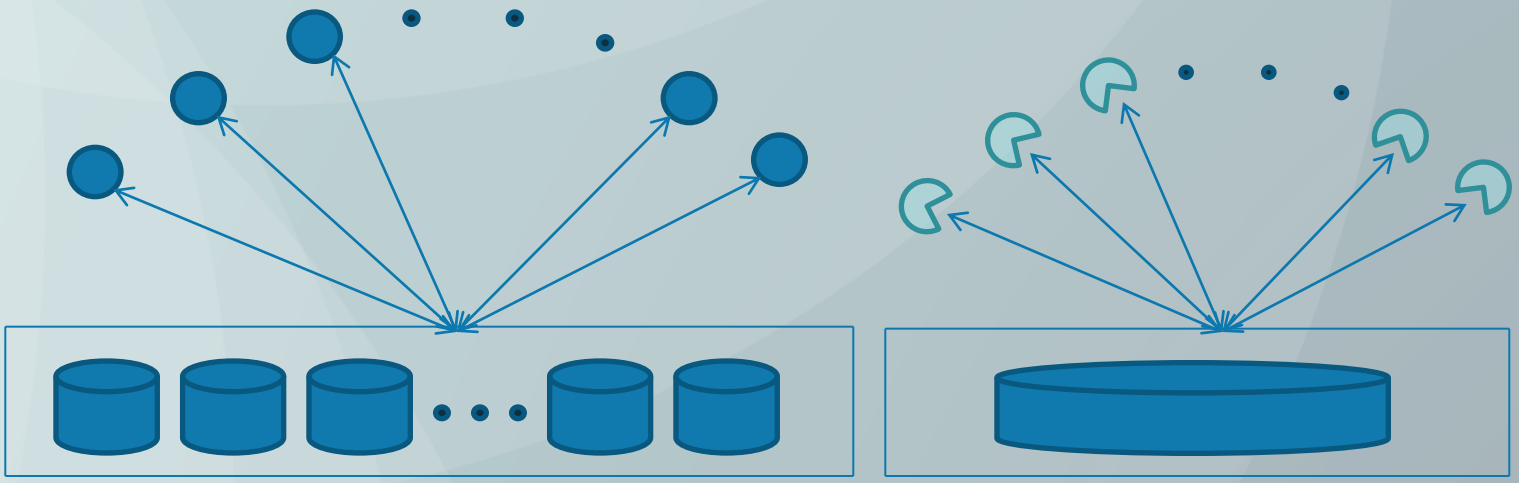
Dashboard
(How vulnerable are we?)

COMMAND AND CONTROL

- Remediation
  - Change setting
  - Patch
- Response
  - Drop connection

How quickly?

COMMAND AND CONTROL

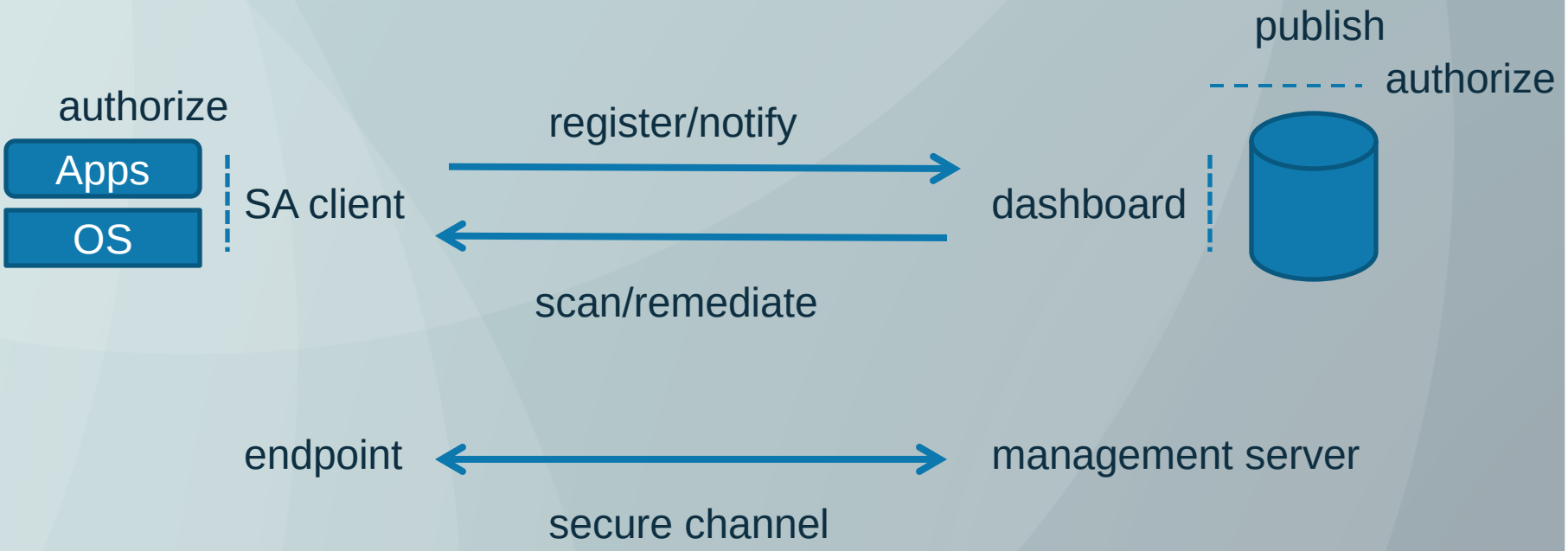


Operations Center

SECURITY AUTOMATION MACHINERY

- Schemas: express information in a common language
- Protocols: exchange information and commands between *authenticated* parties
- Interfaces: expose information and accept instructions from *authorized* parties

DIFFICULT TO DO RIGHT



HAVE TO HAVE STANDARDS

- To be available for all platforms and work with all types of products
- Work in concert (interoperate and share information as needed)
- Ensure only authorized parties (human and software) are privy to sensitive information and can remediate endpoints and respond to a threat

SECURITY AUTOMATION GOALS

- Every host, every user, every application accounted for
- Every sensor (IDS, Firewall, VPN, etc.) able to share, observe and consume information about security critical states and events
- Instruct devices to be in compliance (change settings)
- Instruct infrastructure how to respond (filter, drop, etc.)
- Ability to share threat information that can be understood and acted on by another party's security automation tools

TAKEAWAY

- Standards take patience, but potential payoff is tremendous
- Questions?

Forward. Thinking.