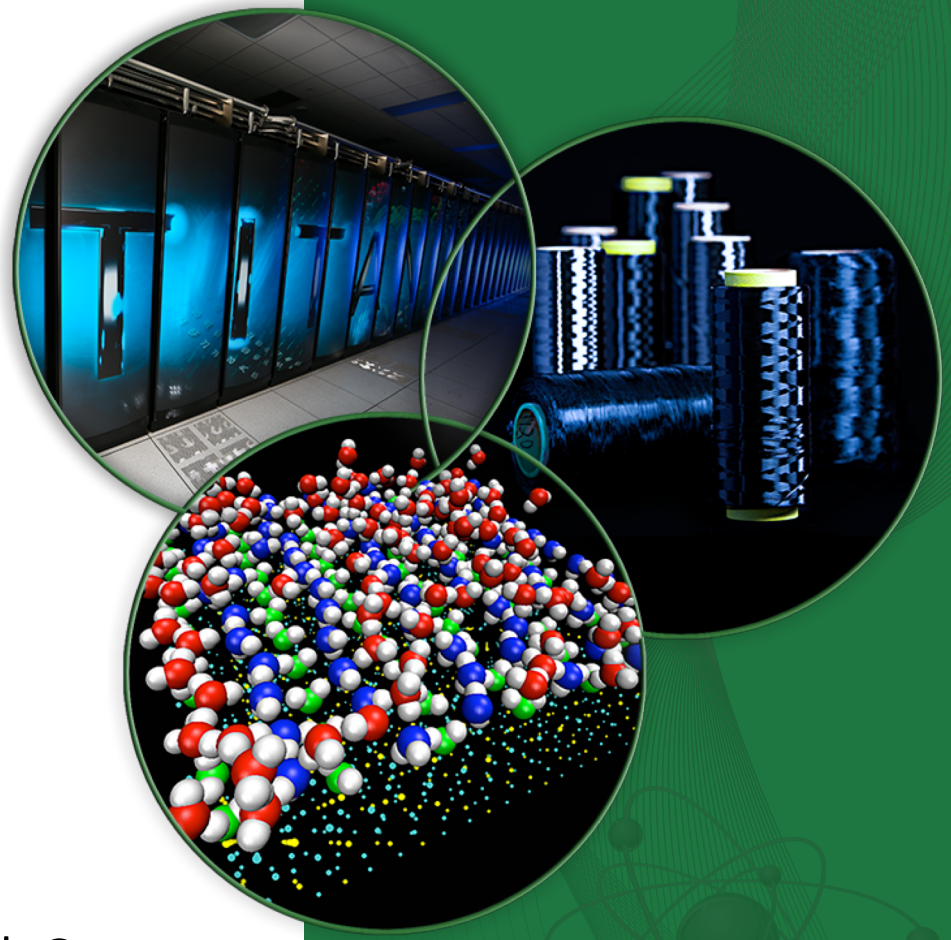
# AKATOSH

## Automated Forensic Analysis and Cyber Incident Verification



**Jared M. Smith**
Principal Investigator
smithjm@ornl.gov

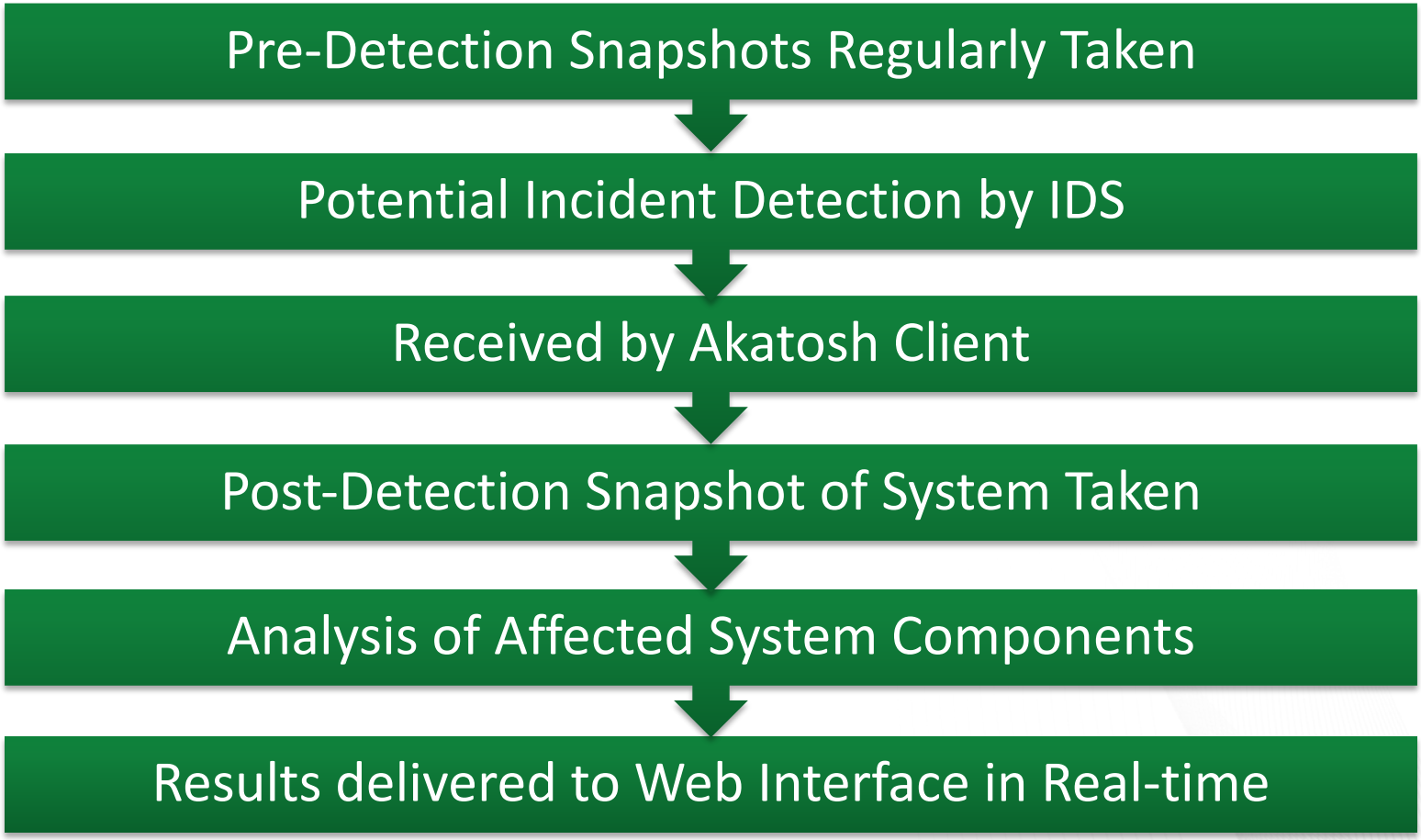
**Elliot Greenlee**
Security Researcher
egreenle@vols.utk.edu

Systems Security Research Team
Cyber and Information Security Research Group
Oak Ridge National Laboratory

ORNL is managed by UT-Battelle
for the US Department of Energy

OAK RIDGE National Laboratory

# PROCESS OVERVIEW



# INCIDENT RESPONSE IS HARD

- Incident response is **critical**, but **costly and time-consuming**
- Time to discovery and mitigation can be **months to years**
- IDSs have **high false alert** rates, which means we often ignore many alerts

**$4 Million**

average cost of recovering from security breach in 2015
(Study of 383 companies by IBM)

**205 days**

to discovery of incident in 2015
(Study of incidents responded to by Mandiant)

# SECURITY INCIDENTS ARE INEVITABLE

To help mitigate incidents when they do happen:

**Akatosh** assists in **detecting, verifying, analyzing, and recovering** from security incidents and breaches by providing **situational awareness** and automating forensic analysis for **IT infrastructure**.

# AKATOSH

# OUR APPROACH

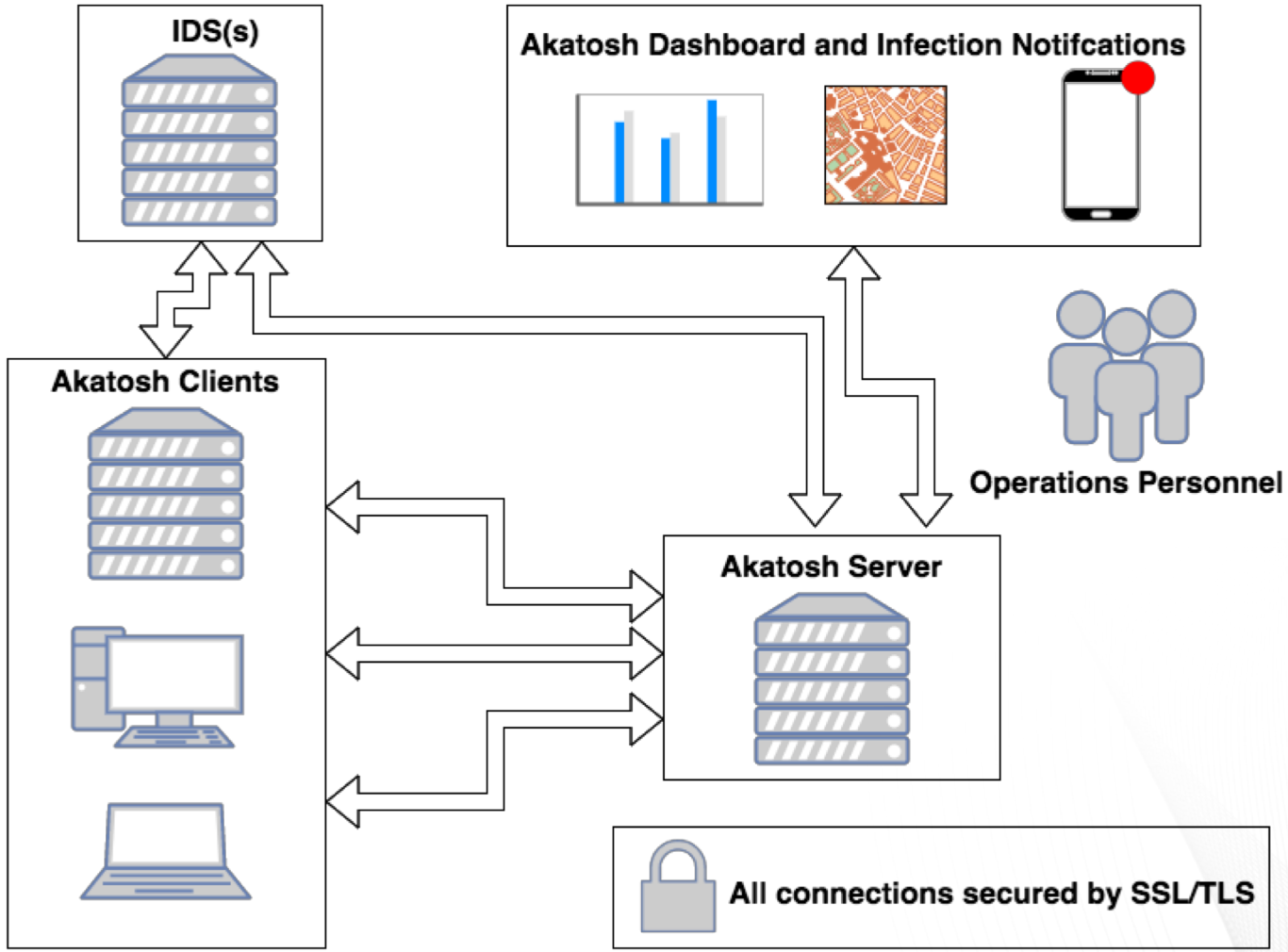
- Akatosh **collects baseline memory images** from Windows, Mac, and Linux clients over time, pulling out **client state changes** between baseline images with images taken immediately after any existing IDS **connected to Akatosh** sounds an alarm

- We do this by installing **small software agent** with low attack surface on clients, which coordinates with the server that performs the actual diffing of baseline and post-alert images

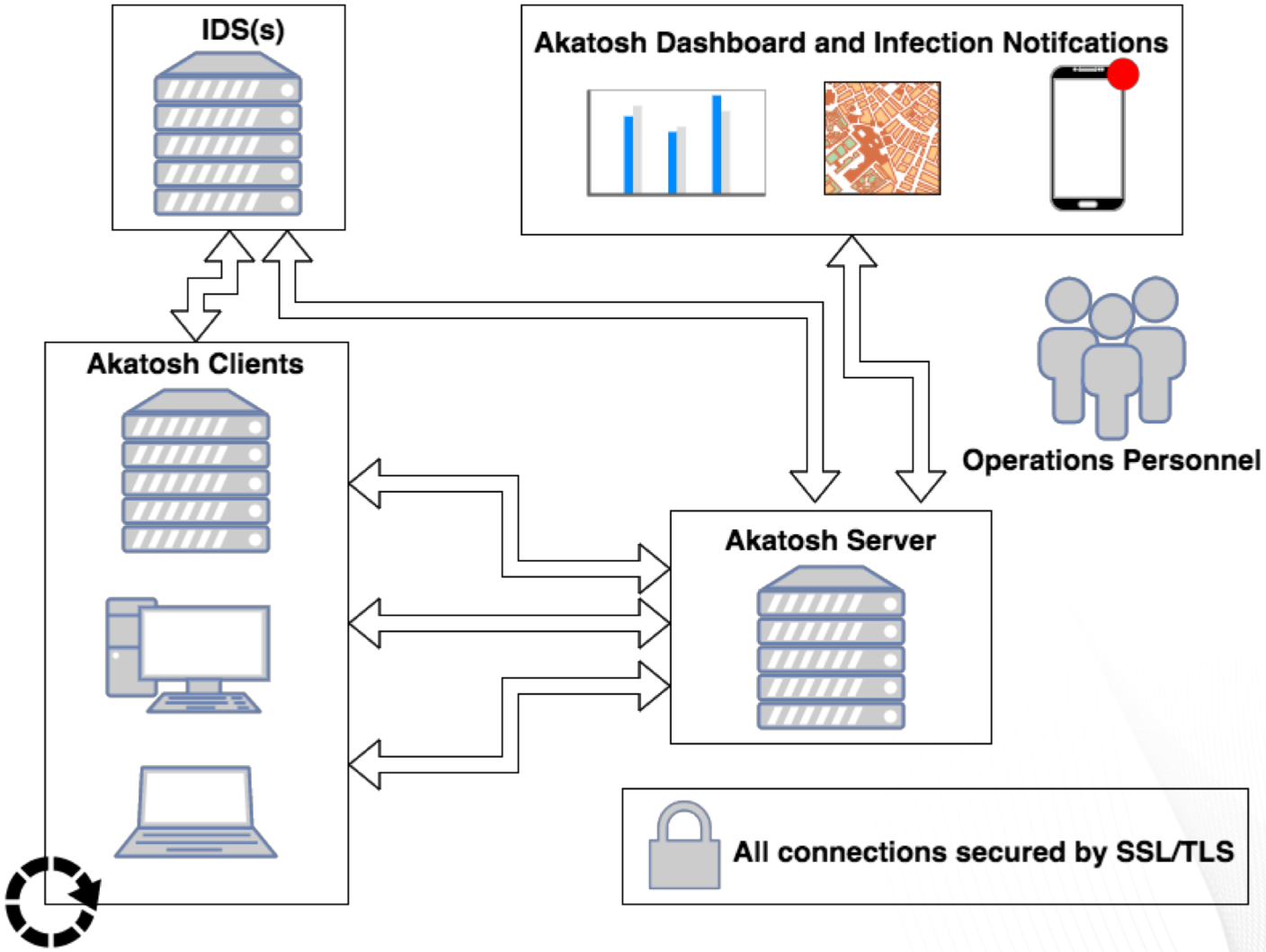
- Akatosh then provides **enhanced context to existing IDS alerts** of high priorities through a dashboard based on the analysis done

- This helps to indicate **true compromises** and highlights affected components to **assist in recovery** of your machines in the case of a real infection or IT need

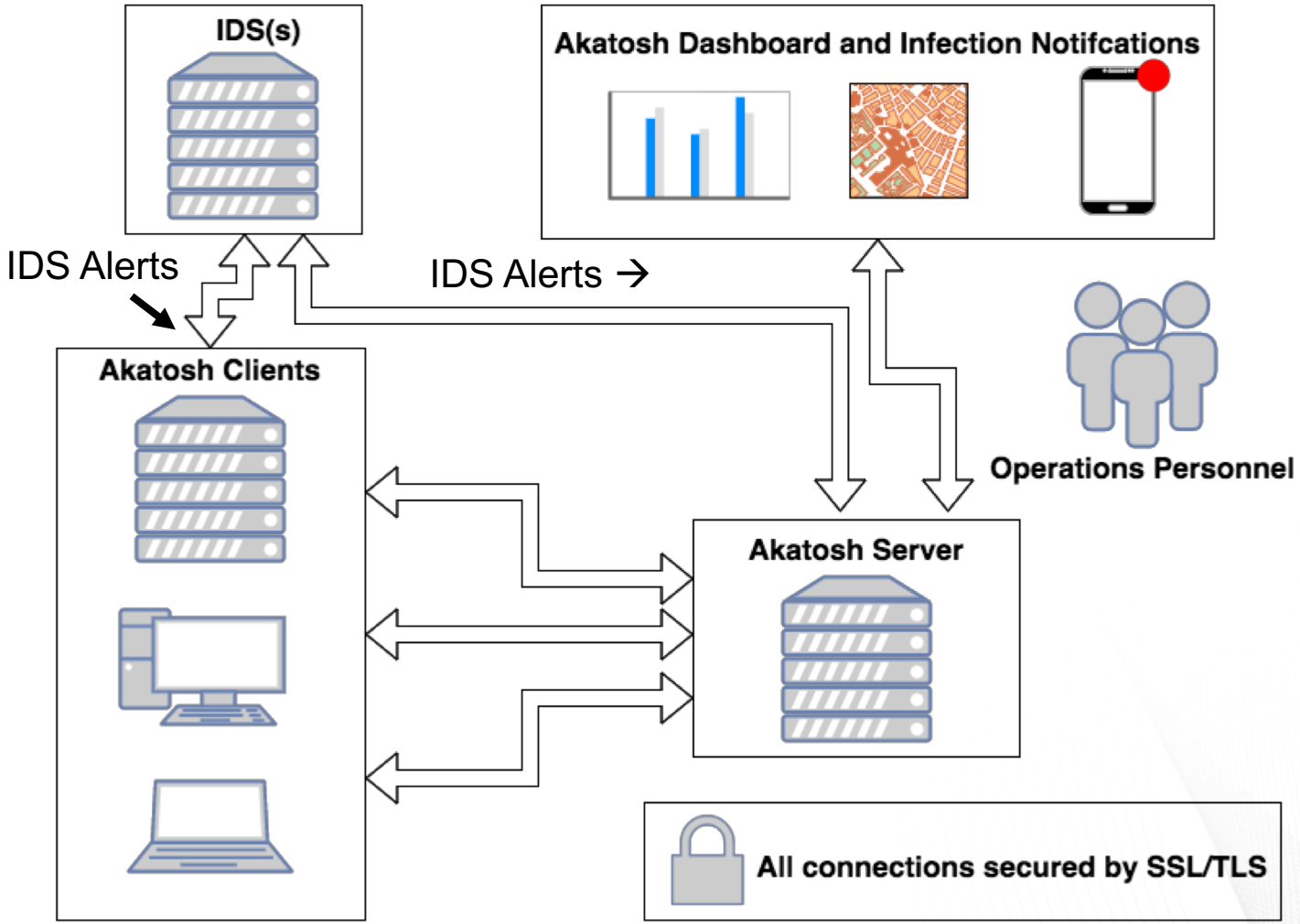
# OUR APPROACH



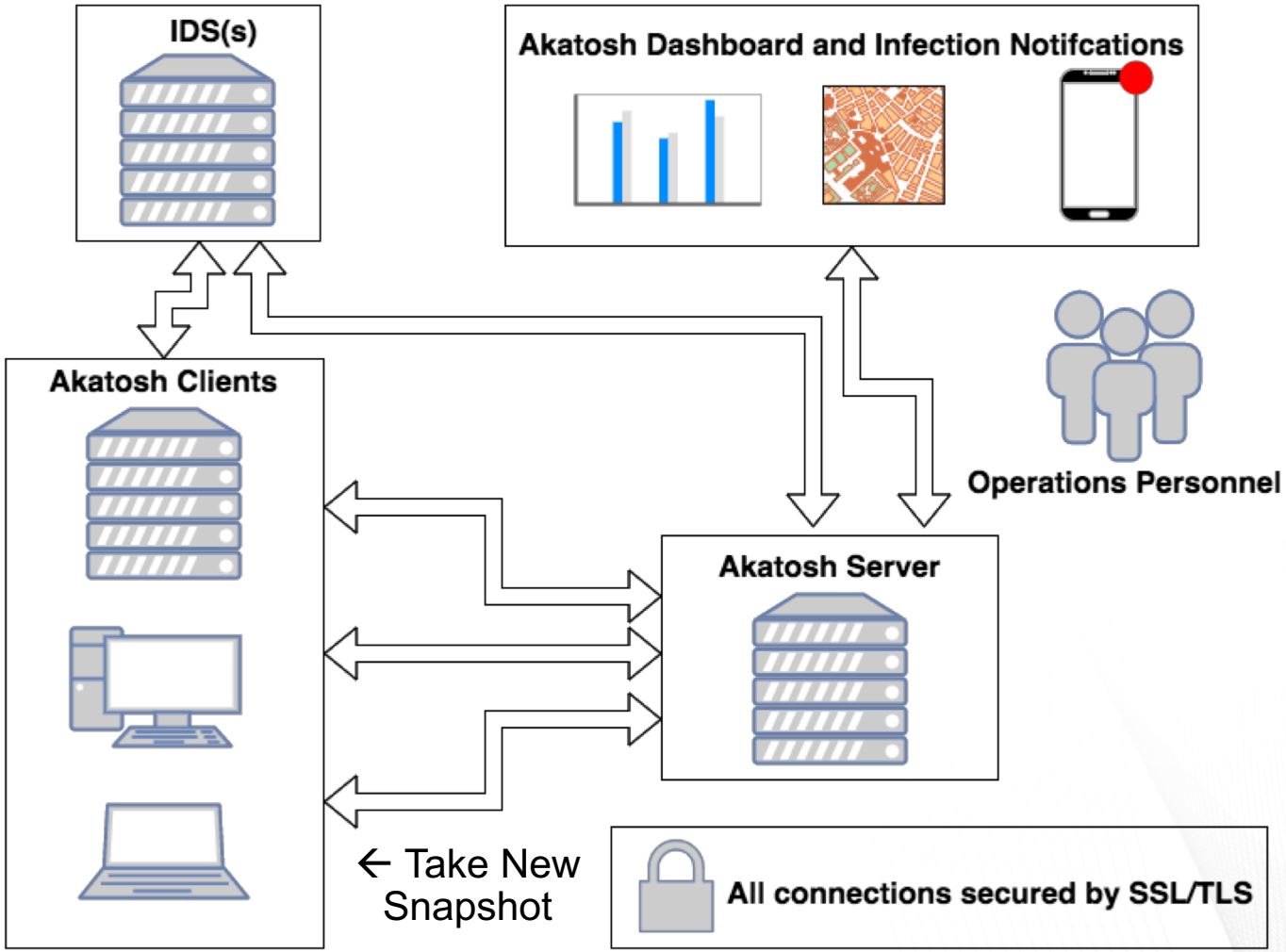
# OUR APPROACH



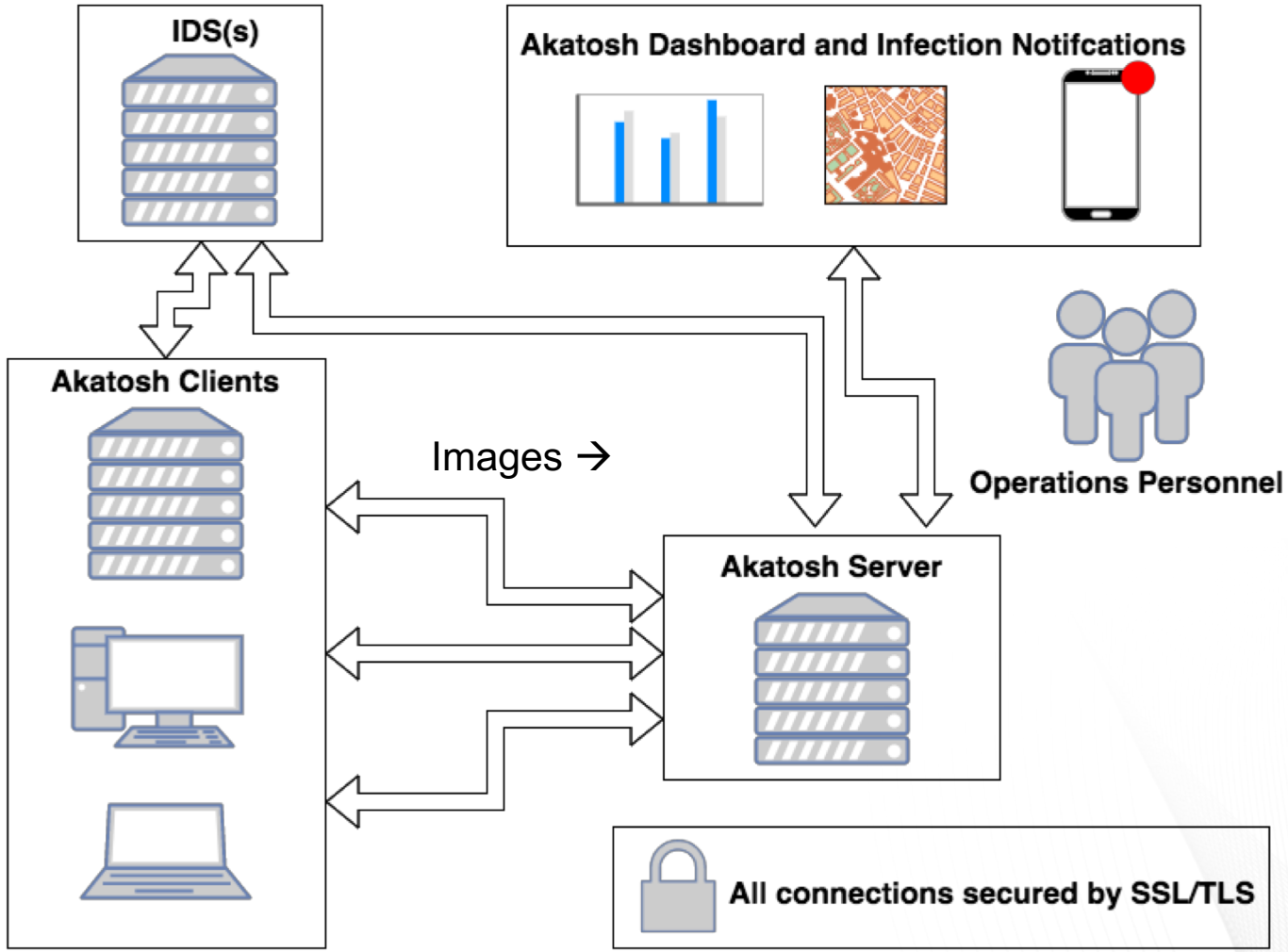
# OUR APPROACH



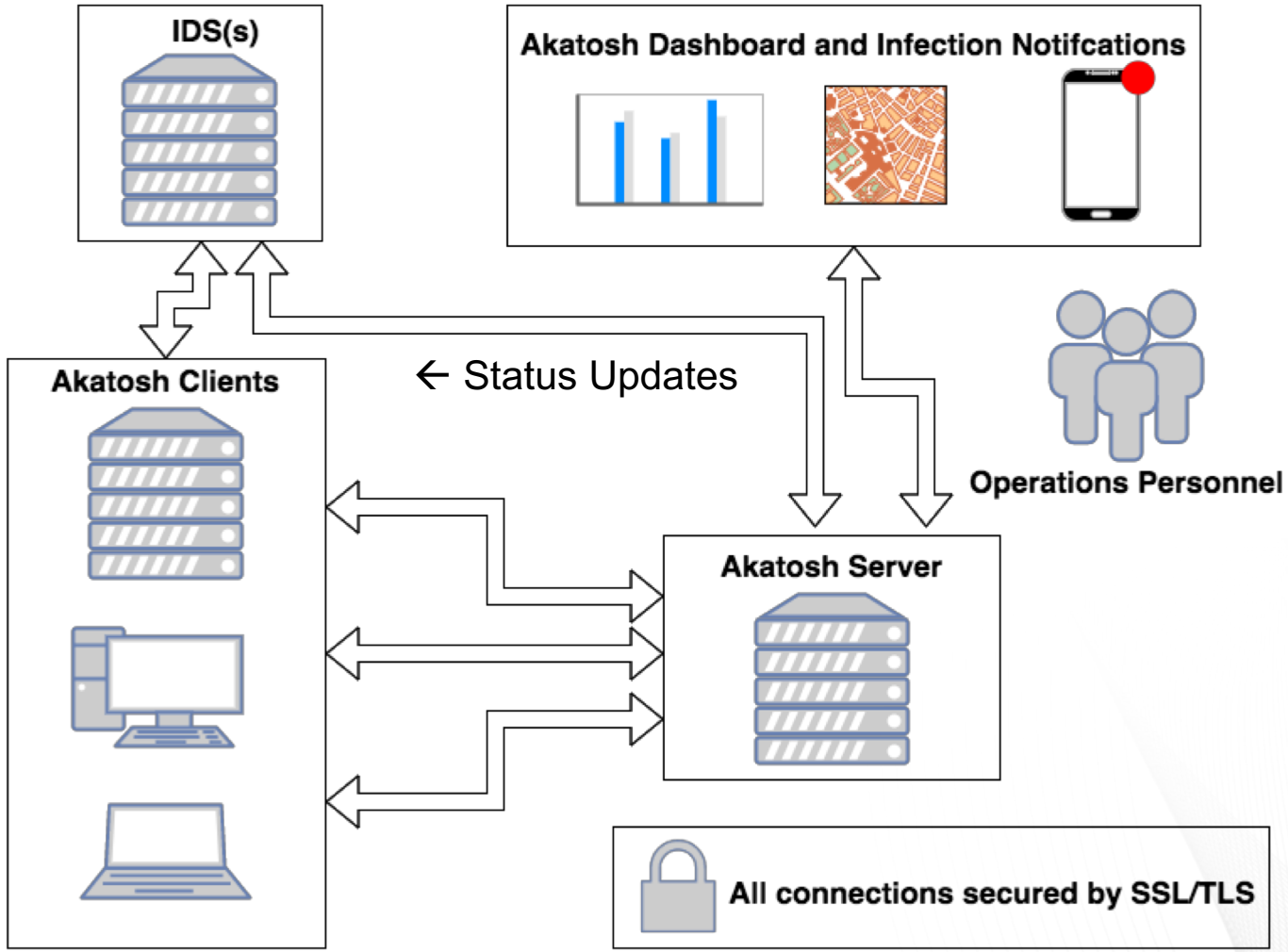
# OUR APPROACH



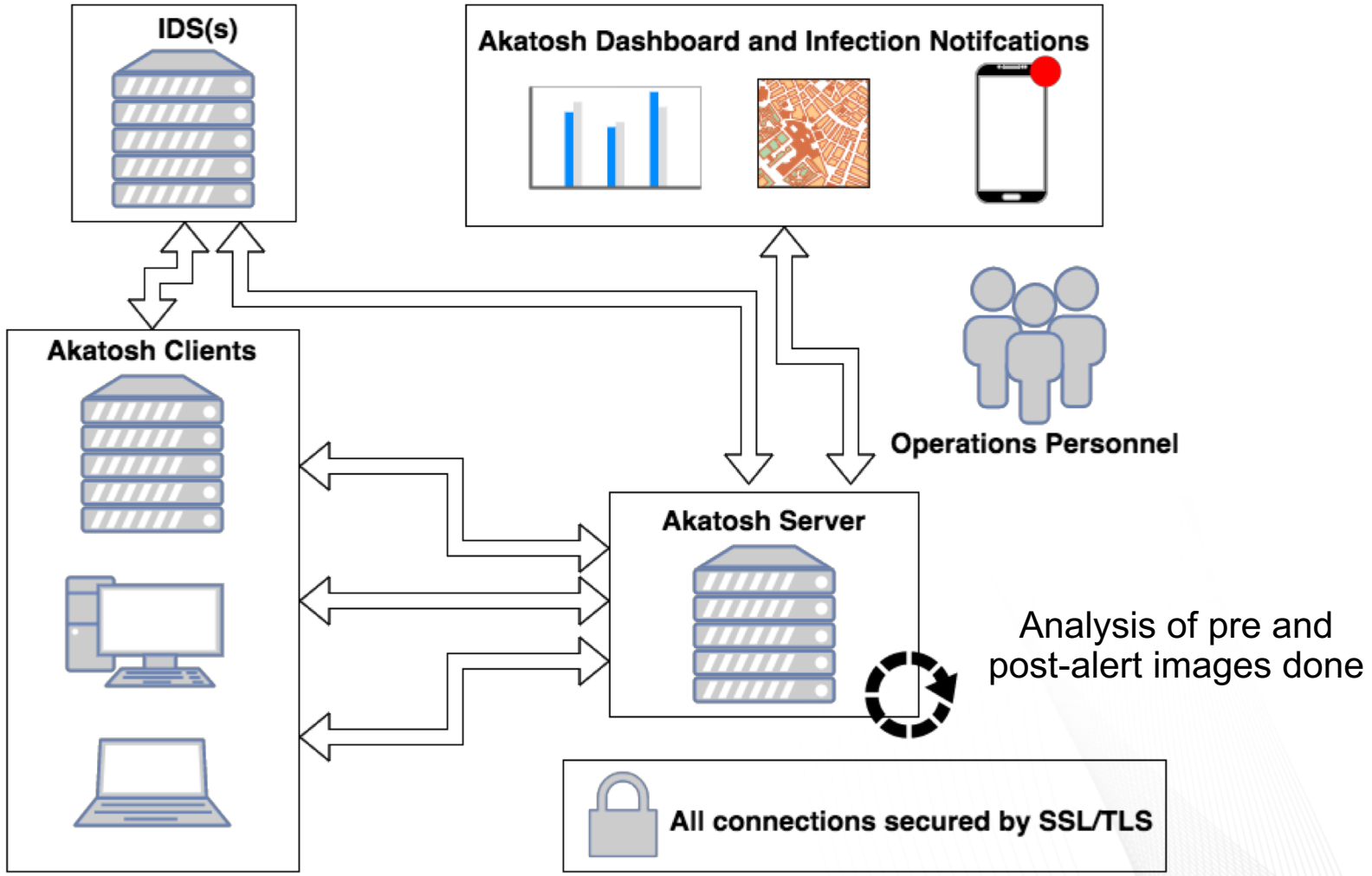
# OUR APPROACH



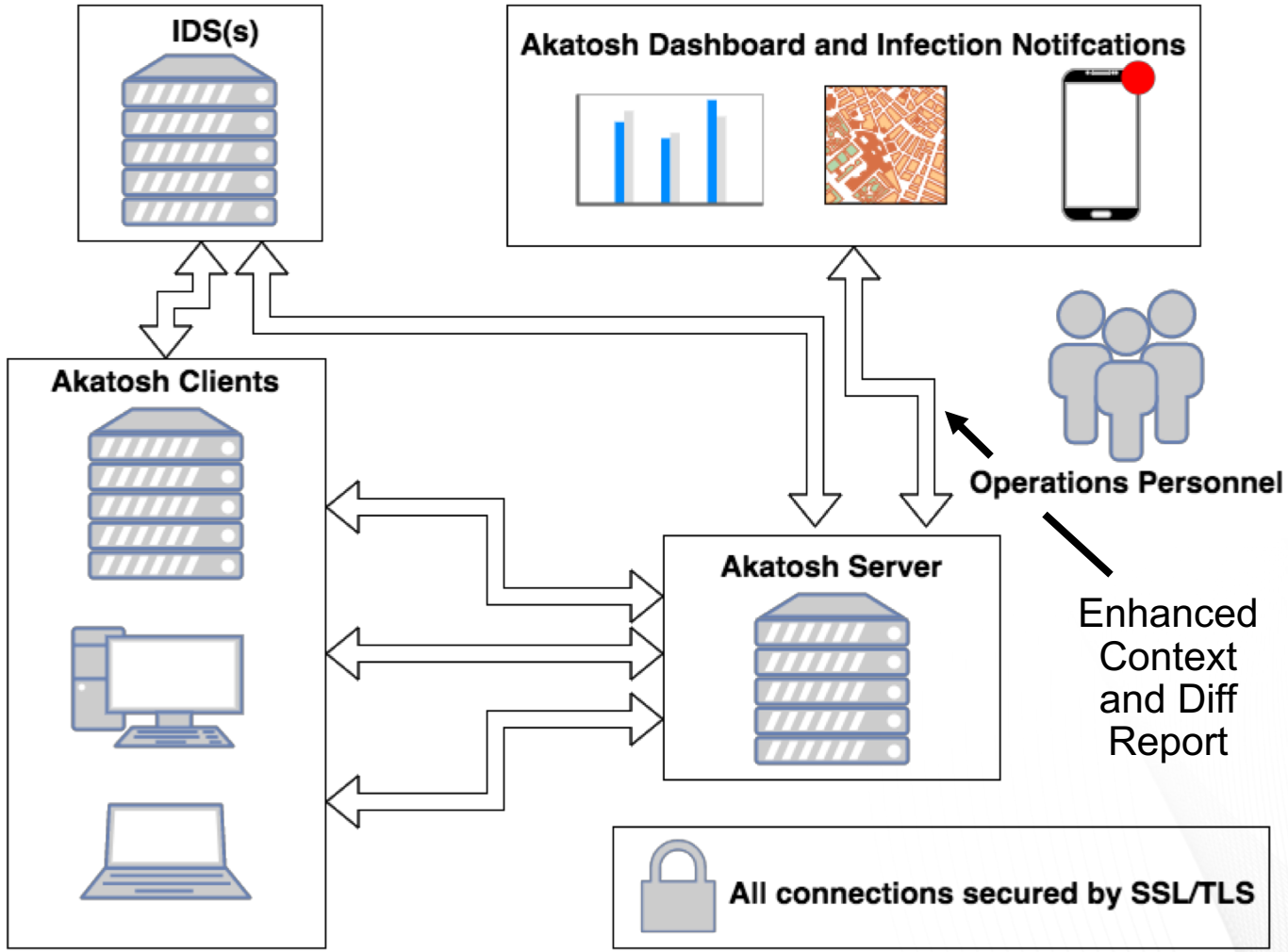
# OUR APPROACH



# OUR APPROACH



# OUR APPROACH



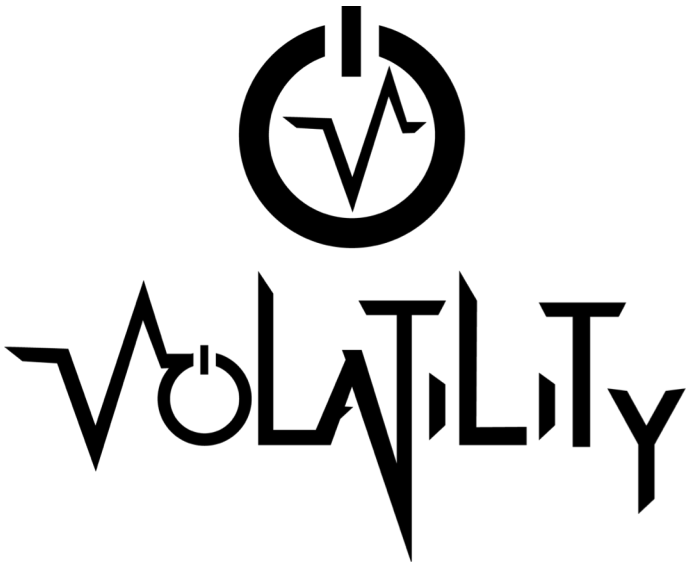
# DIFFING RESULTS

- Akatosh will “diff” prior and post-IDS alert states to tell operators what **exactly** changed on the system in real-time

- Provides feedback on changes in the system from
  - New and recently exited processes
  - Changed/new files
  - Network connections
  - Loaded kernel libraries
  - User sessions
  - Much more…

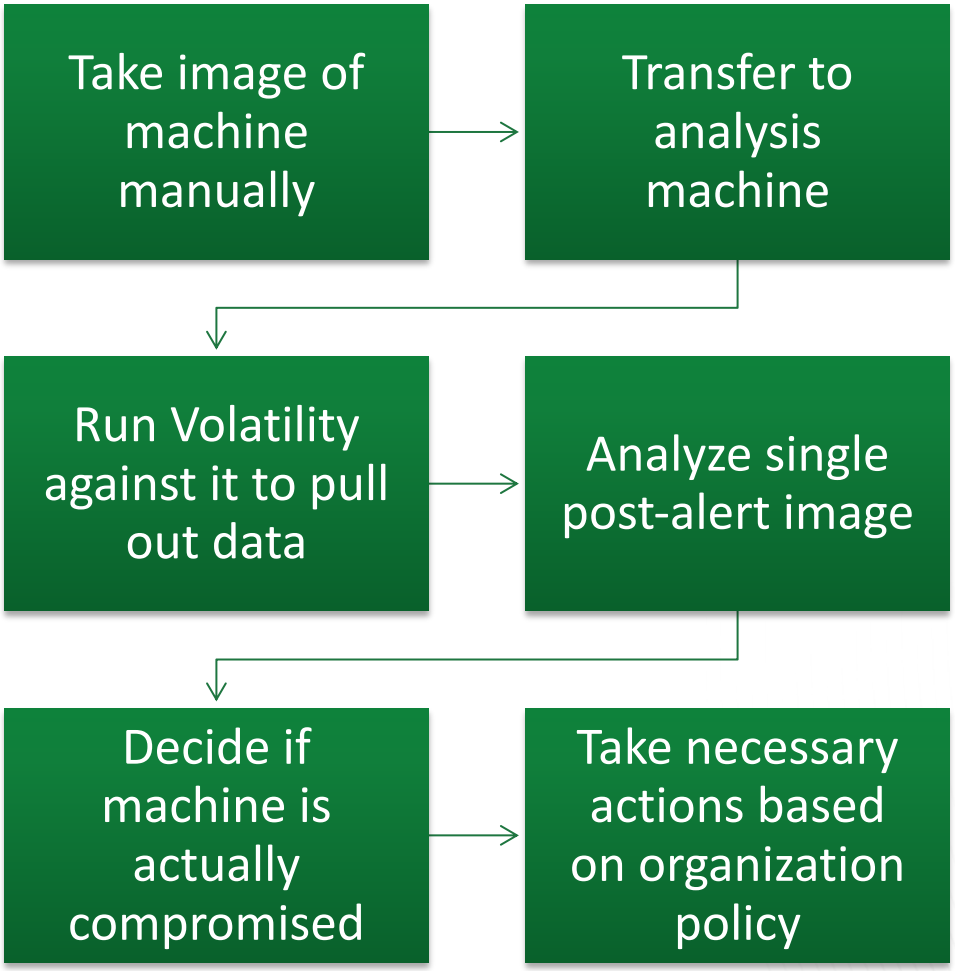
# POWERED BY OPEN SOURCE

- Akatosh's image analysis is powered by Volatility, the de facto open source forensic analysis framework
- Used by the FBI, Mandiant, FireEye, Google, DOE, and more…
- Raw images extracted from hosts by Akatosh clients **can be analyzed independently** by Volatility

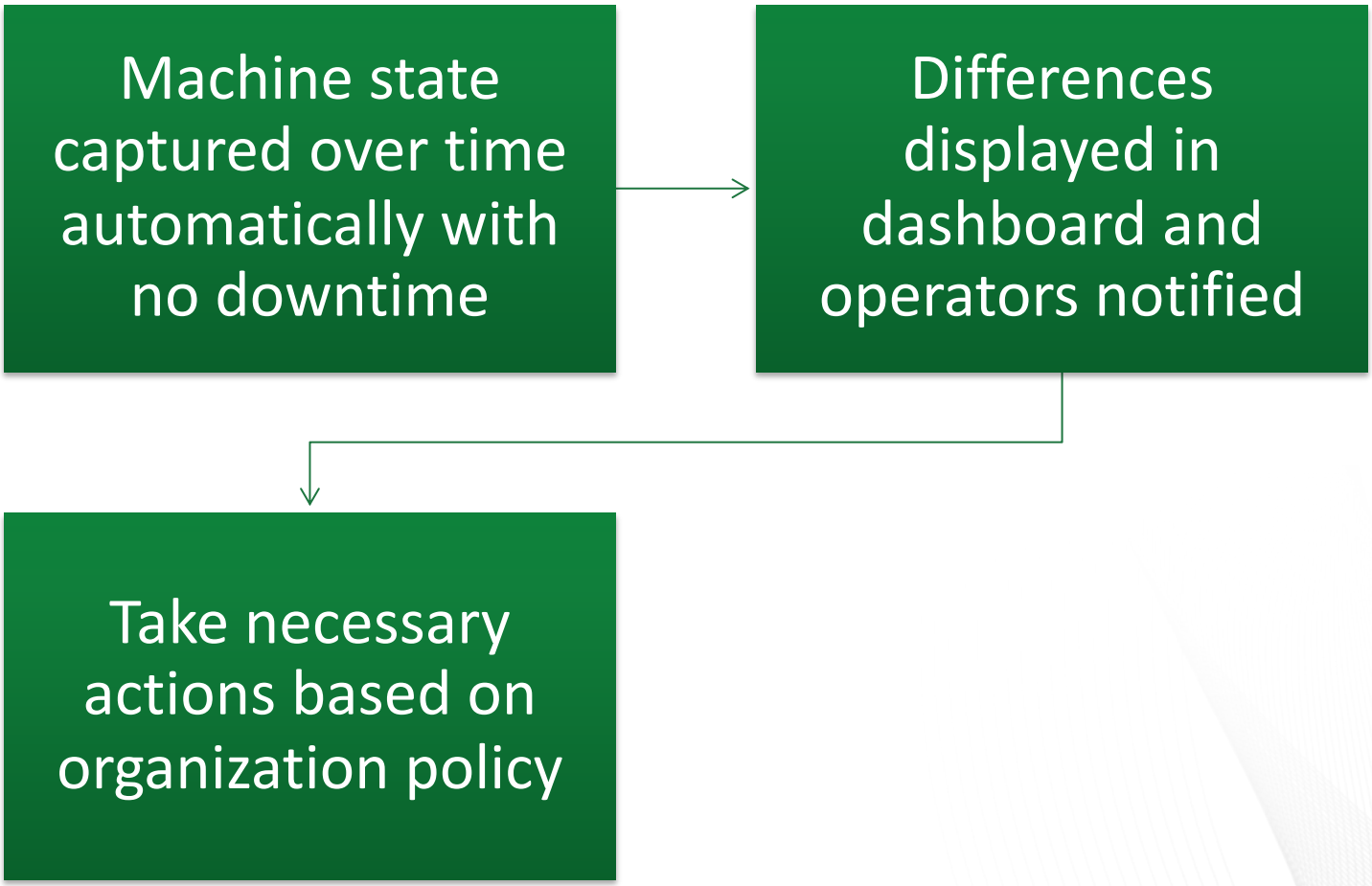


# WITHOUT AKATOSH

## With Only Volatility or Similar Tool



# WITH AKATOSH



# EXTENDING AKATOSH

- Can extend Akatosh to work on new machine architectures by providing memory capture tool with memory layout of new systems
- Allows Akatosh to be adjusted to work on systems beyond Windows, Linux, and Mac
- Proprietary OSes, PLCs, SCADA/ICS, etc.

# BENEFITS

- Reduces incident response time and cost
- Cuts time to discovery and mitigation
- Integrate with any existing security infrastructure
- Minimal performance impact and no downtime
- Highly configurable

# USE CASES

- Incident response teams use diffs to avoid complex manual analysis
- Security analysts can get deeper context on security incidents
- SOC operators can quickly determine if an IDS alert represents an actual problem
- IT teams can use historical data to solve support tickets

# DIFFERENTIATING FACTORS

- Existing systems do not scalably capture full on-host memory, network, and filesystem snapshots and index them for use by analysts
- Integration with existing IDS/SIEM systems enables analysts to get insight into the true impact of attacks on infrastructure **as they happen**
- Existing network-based host-forensic tools can never capture the full extent to which individual hosts are affected by incidents

# EVALUATION

# PERFORMANCE & STATS

- ~30 seconds to image and transfer a 16 GB machine
  - Nothing saved on the client's disk
- ~40% of original memory size encrypted and stored on the server's disk (due to lossless compression)
  - i.e. For a 16 GB RAM VM, we only save less than 8 GB, and it still has all the state!
- When the client images a host, no noticeable slowdown
- Client source is less than 130 lines of code

# TESTING SETUP

- Historical state collection on Windows, Linux, and Mac
- Differential state analysis on Windows, Linux, and Mac
- Currently scales to 120+ Linux and Windows clients, constantly deploying more in an internal CISR data center

# VALIDATION

- Analysis component of Akatosh validated on several pieces of malware
  - DarkComet Trojan
  - NJRat Trojan/Reverse Shell
  - Stuxnet
  - Currently running Akatosh through 1000s of additional samples of recent malware
- **Identified all affected system components** on the endpoints with the infection
  - Detected spawned malicious processes
  - Libraries loaded by malware
  - Network connections made

# STATUS

# IP STATUS

- Patent Pending (U.S. Provisional Patent Application 62/432,929 completed on 12/2016)
- Non-Provisional Patent Application in progress, to be submitted before 12/2017
- Code Copyrighted
- Available for licensing

# UPCOMING PILOTS

- **MITRE**
  - Planned pilot in Q4 2017-Q1 2018 on a military network of 100+ Red Hat Enterprise Linux clients
- **Assured Information Security (AIS)**
  - Planned pilot in Q4 2017-Q1 2018 to DHS 3rd-party contractor to functionally validate Akatosh, evaluate all claims, and perform a red-team
- **DOE HQ**
  - Working to deploy Akatosh to a set of internal machines
- **ORNL ITSD Network Operations Center**
  - Future potential to deploy Akatosh to 1000's of Windows, Mac, and Linux user machines and servers

# FUTURE WORK

# ARCNET

- **ARCNET:** Akatosh for Operational Technology (OT) and Critical Infrastructure (Energy Delivery Systems, SCADA, and ICS devices)
  - **Requirements:** Low resource availability on client machines, very diverse and radically different machine architectures
  - **Potential Targets:** RTUs, PLCs, Proprietary OSes, etc.
  - **Status:** initial work funded through DOE Cybersecurity for Energy Delivery Systems (CEDS) Program

# MARA

- **Mara:** Akatosh for Cloud Environments
  - **Requirements:** Larger memory space to analyze, higher resource availability (potentially offload processing to clients), high scalability is critical from the start
  - **Potential Targets:** Amazon Web Services, Amazon GovCloud, Microsoft Azure, Google Cloud Platform, on premise datacenters, hybrid clouds, etc.
  - **Status:** seeking funding

# THANKS!

PI Contact: Jared M. Smith

Voice: +1 (865) 274-3800

Email: smithjm@ornl.gov