2020
Industry
Day

MOSAICS Data Requirements and Baselining Strategy

Robert G. Cole, John Jacobellis, Jennifer Trasti, Karen Shanklin
Sandia National Laboratories
Albuquerque, New Mexico, USA

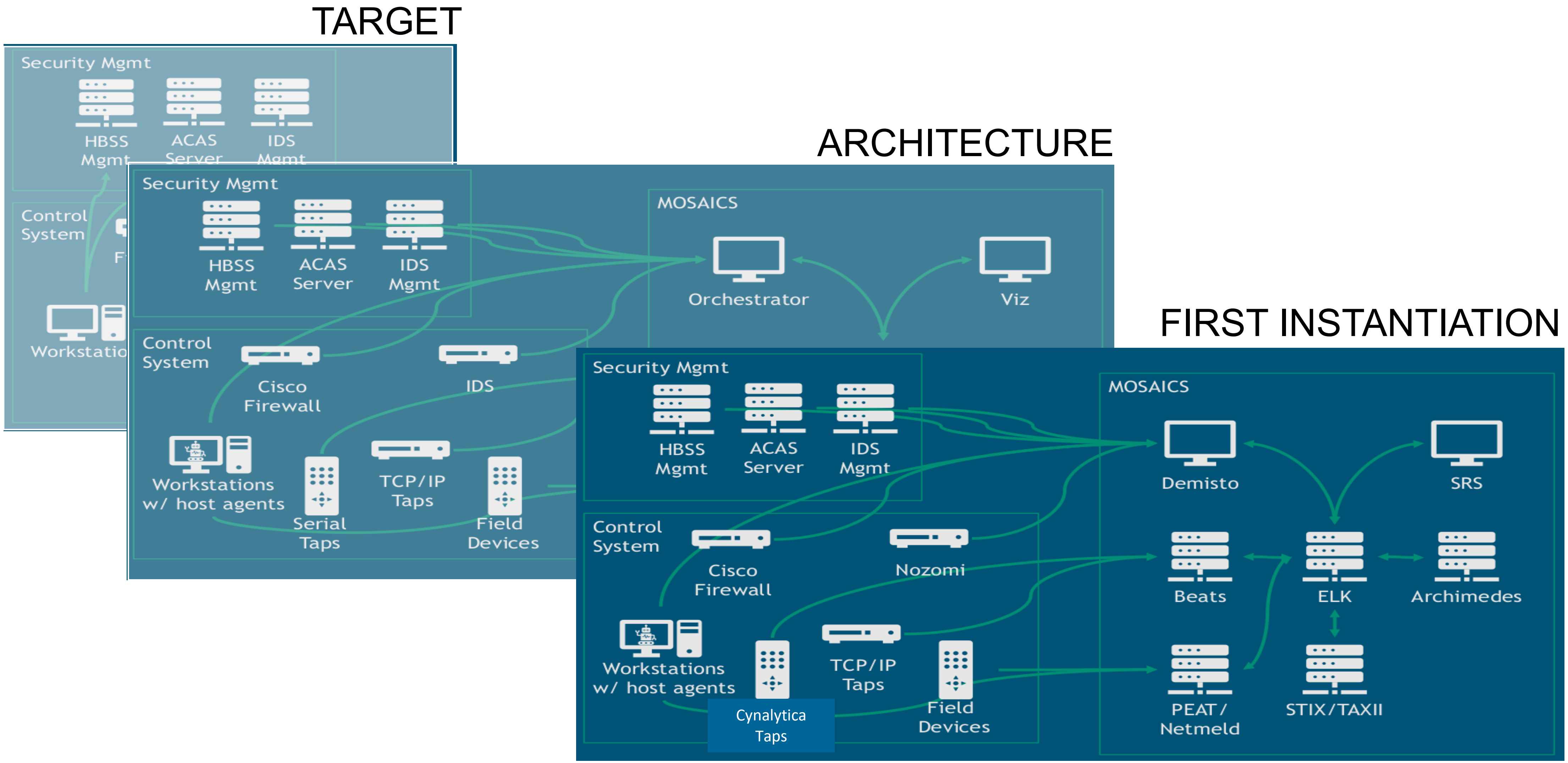
Contact: rcole@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2020-12104 PE

MOSAICS Data Requirements

Operational	Functional	Technical
O1.1 • Inventory IT and OT system devices and system components in the targeted environment. • Capability: Identify **O1.2** • Identify internal and external data flows and connections relative to the target environment. • Capability: Identify **O1.3** • Enable prioritization of components and system • devices. Capability: Identify	9 Functional Reqs	~58 Technical Reqs
O3.1 • Continuously monitor system components to detect indications of the presence of threat actor/anomaly. • Capability: Monitor	14 Functional Reqs	~111 Functional Reqs

MOSAICS Architecture



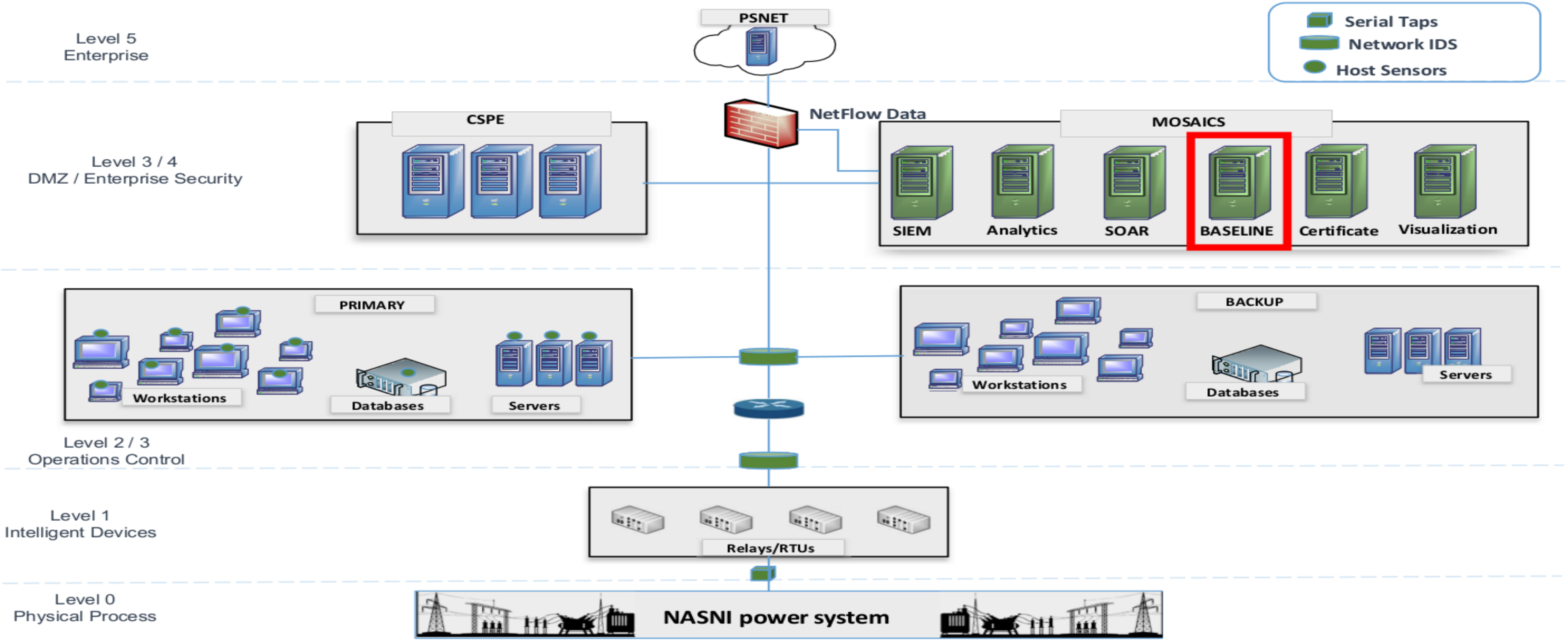
TARGET

ARCHITECTURE

FIRST INSTANTIATION

MOSAICS Prototype

MOSAICS
2020
Industry
Day



SNL

Baselining in MOSAICS

1. Baseline Tool – GOTS IT passive and active network mapping through network device config parsing and active scanning
    - Address, host OS, ports/processes, ….

    a) Process Extraction and Analysis Tool (PEAT) – GOTS OT Device interrogation tool
    - Logic, firmware, vendor information, …

    b) VEDAR – GOTS OT analytics
    - Passive packet collection using elastic Packetbeats
    - OT packet deep packet inspection
    - OT specific analytics
2. Nozomi – COTS network IDS

    Passive IT and OT mapping and analytics

3.Cynalytica – COTS serial taps

    a) Passive serial taps

    b) OT analytics engine

4. Host Sensors

    a) Elastic Winlogbeats

    b) Cisco NetFlow packet flow collection

Potential Improvements in MOSAICS Data Modeling

1. Improved integration among the various data sources

    Open up interfaces for better data sharing

2. Security baseline

    Incorporation of security scans for improved Baseline

3. Open interfaces on ICS devices for ease of information extraction