The Role of Internally Developed Open Tools as a Core Technology for an MSSP

Dr. Toto A Atmojo, CISSP, CISA

www.defenxor.com

About me: Dr. Toto A Atmojo, CISSP, CISA

Career:

- CEO of Defenxor since 2015
- 20+ years of career on IT Security Industry

Education:

- Computer Degree : STIMIK Perbanas
- Master Degree:
  - Master of Computer Science : Budi Luhur University
  - Master of Communication Studies : The London School of PR
  - MBA: Gadjah Mada University
- Doctor of Research in Management: Binus University
- Accelerated Management Program: National University of Singapore

CISSP
CISA Certified Information Systems Auditor
50th Year of ASEAN-Japan Friendship and Cooperation

Introduction of Defenxor

- Established in Q4-2015 as 100% Indonesia company (No foreign expertise)
- IT Security company that focusing on 3 pillars
  - Managed Security Service
  - IT Security Consulting
  - IT Security Integrator

- Our SOC by Numbers:
  - Total customers: >70 organizations
  - Concurrent customers: >60
  - Biggest Organization by EPS: >30K EPS
  - Total concurrent EPS managed by our SOC: > 300K EPS
  - Total concurrent assets (IP of servers, Container & VM): > 10K IP
  - SOC Operation Personnel: 60+

50th Year of ASEAN-Japan Friendship and Cooperation

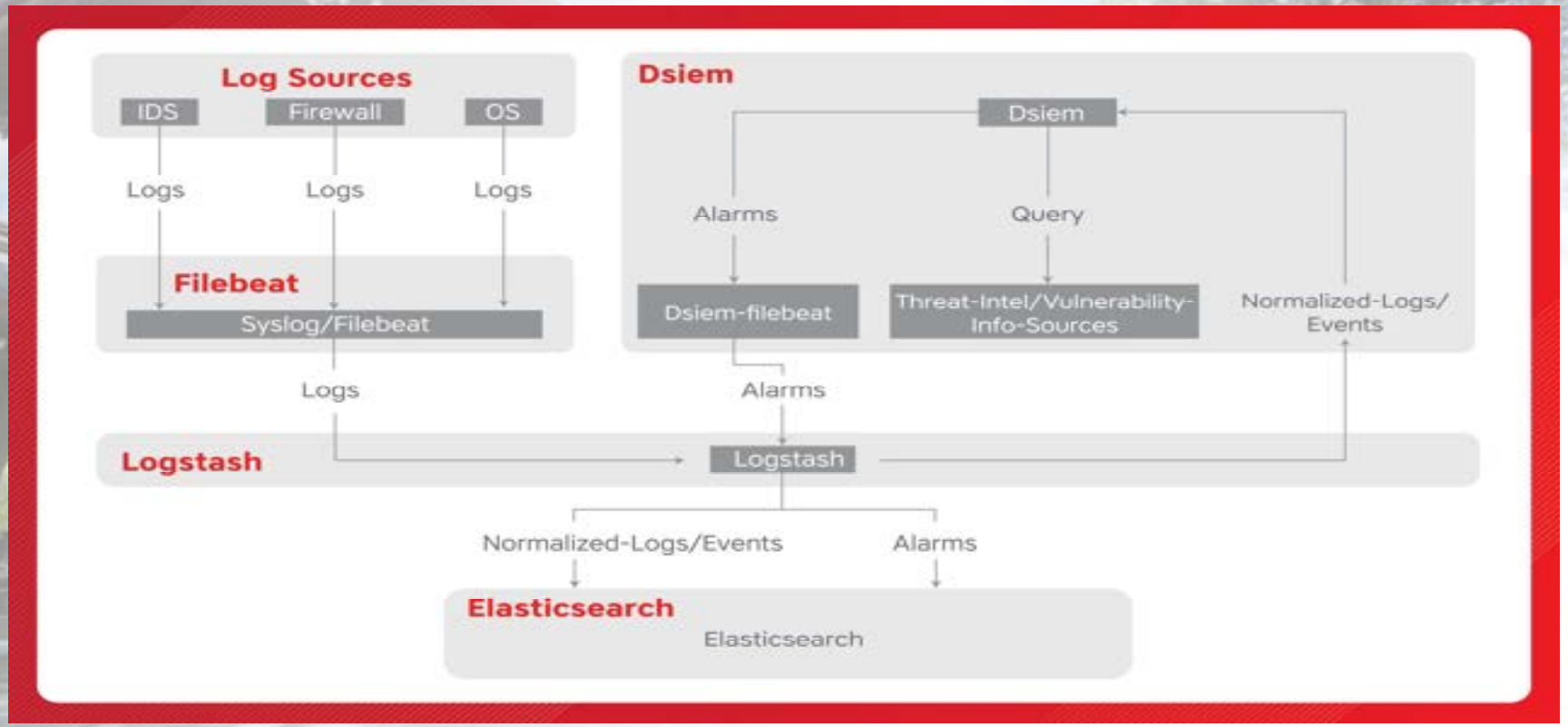
The Background & Needs

- Background:
  - Developing MSSP business need solid and stable SIEM tool as a core
  - SIEM also need to be connected to many operational technologies (case management, personnel's performance monitoring, etc)
- Needs:
  - Open standard tools that compatible with wide range of Technologies
  - Stable & reliable technology
  - Open for further development
  - Self dependencies

Meet our SIEM: DSIEM

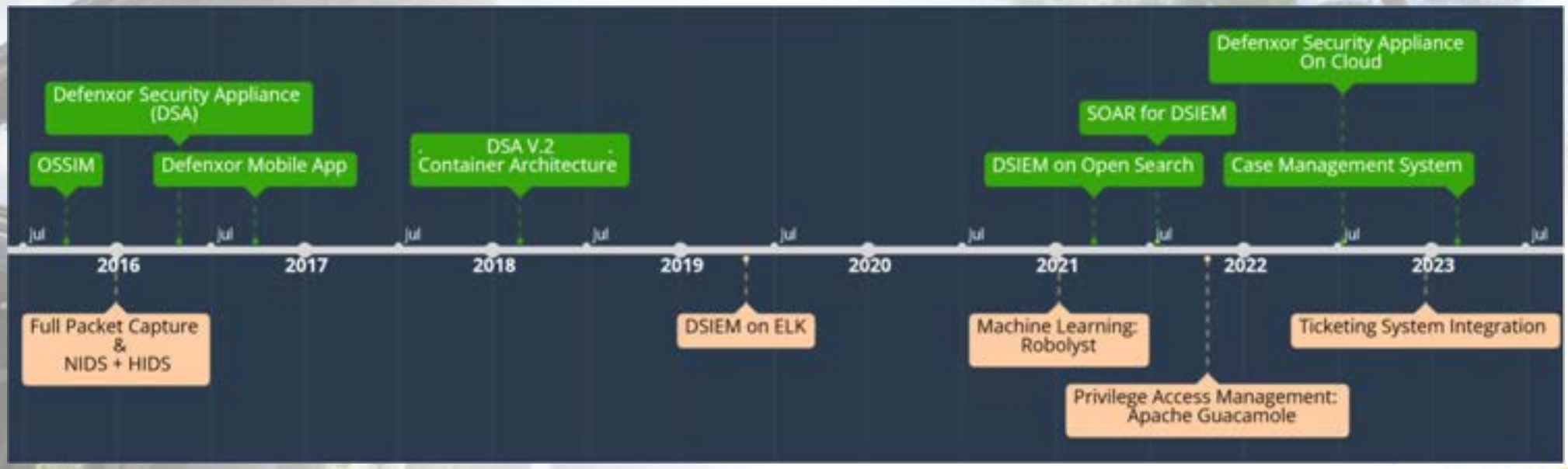
- OSSIM-style correlation engine for ~~Elastic stack~~ Open Search
- OSSIM-style correlation and directive rules, bridging easier transition from OSSIM.
- Produces risk-adjusted alarms
- Dsiem performs event correlation on all incoming Normalized Event based on its configured directive rules
- Enriches alarms with vulnerabilities and threat intelligence info
- Cluster mode for horizontal scaling
- It’s free and Open: GPLv3.
- You can download, use and contribute freely: www.dsiem.org

DSIEM: OSSIM Style Event Correlation Engine for Open Search



50th Year of ASEAN-Japan Friendship and Cooperation

Our internal Open Tools timeline



50th Year of ASEAN-Japan Friendship and Cooperation

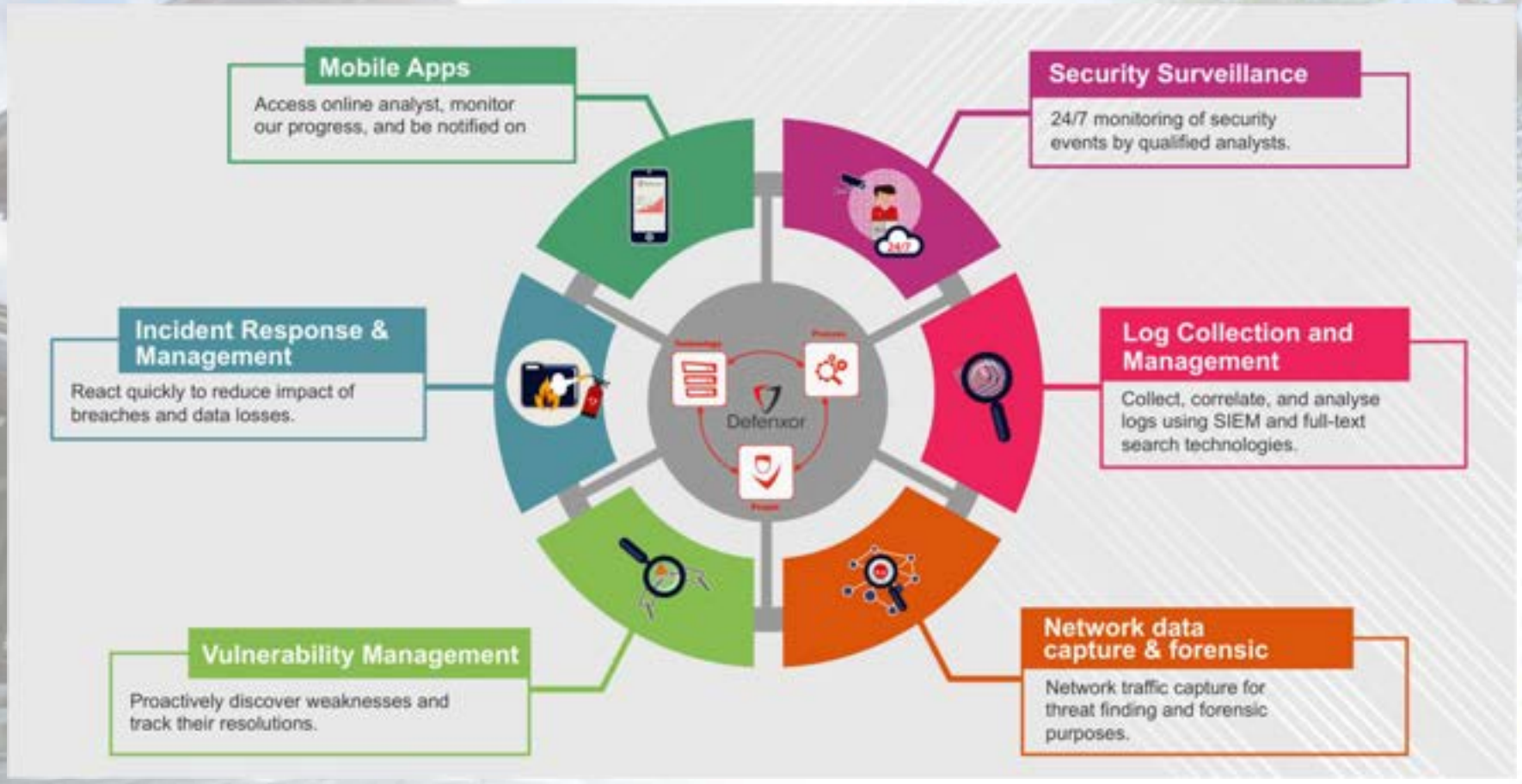
Usage of Open Tools at our SOC as MSSP

- Biggest Log Ingestion: > 30,000 EPS
- Largest clustering deployment: 10 stacks of appliances (1U)
- Concurrent SOC as a Service: > 60 Organizations
- Current deployment cases:
  - On-premise (Using our appliance)
  - Public cloud: Alibaba Cloud, AWS, Azure, GCP.
  - Private Cloud: Virtualization & Container based infrastructure

- **By using internally developed Open Tools, we can deliver our service while collaborating with global technology brands without being fully dependent on them.**

50th Year of ASEAN-Japan Friendship and Cooperation

Our MSS Service offering



50th Year of ASEAN-Japan Friendship and Cooperation

Thank You

Dr. Toto A Atmojo, CISSP, CISA

toto.Atmojo@defenxor.com

www.defenxor.com