

SIEM: GOLDEN GOOSE OR MONEY PIT ?

Igor Volovich, CISSP,CISM,CISA,CRISC,CIPP

Scott Sattler, CISSP,CISM,CISA,CRISC,CCNP,CFE

In this session

- SIEM 101 – a quick primer
- Capabilities vs. technologies
- Common SIEM pain points
- Key concepts for a happy SIEM
- Getting SIEM wrong
- Doing SIEM right
- Sensory instrumentation approach
- SIEM service deployment models
- Q & A Session

SIEM functional components

THREAT & VULNERABILITY MANAGEMENT PROCESSES (TVM/CSIRT)

Preparation

Analysis

Eradication

Recovery

Detection

Containment

Debrief

RETENTION

VISUALIZATION

ALERTING

REPORTING

ANALYTICS

EVENT/DATA CORRELATION

EVENT/DATA AGGREGATION

EVENT/DATA COLLECTION

SENSORY DATA SOURCES

ENDPOINT SYSTEMS

NETWORK SYSTEMS

SECURITY SYSTEMS

CMDB/CONFIG

APP INFRASTRUCTURE

IDENTITY/ACCESS

VULNERABILITY MGMT

DATA INVENTORY

SIEM pain points

- Too much data – not enough intelligence
- Very quantitative – “need more people to examine events”
- Quality of detection, analysis unknown
- Complex platforms are difficult to manage
- ROI hard to measure, harder to achieve/show
- Vendors oversell and under-deliver
- Most issues are NOT technology failures
- Customer expectations unrealistic
- Vendor attitude is “fire-and-forget”

Key concepts

- Objectives are primary, tradecraft secondary
- Focus on capabilities, not tools
- SIEM as a service in your enterprise
- First, know your (platform's) purpose
- Second, have a plan
- Look for “Indicators of Compromise”
- Anything can be a sensor!

How to get it wrong

- Forget strategy – let's just collect stuff
- Not sure what to log – let's collect it ALL!
- Look, a magic box - stuff goes in, qualified actionable security alerts come out!
- It's too noisy, this platform sucks
- It's too quiet, we must be impregnable
- It's too difficult, let's just outsource
- I thought we were getting “security-compliance-reporting-alerting” in a box?

Getting it wrong, part II

- Setup is a “Five-day Quick Start” – that’s it
- Finally, our long-awaited log dump is here!
- Wait, we need “people” to run this thing?!
- Hey, what’s this button here do?
- I know we didn’t buy it for this, but...
- Vendor also said it could bake tasty pies
- It’s ok, we’ll just hire a consultant to tune it
- Why can’t I have your log data?
- Executive buy-in – what’s that?

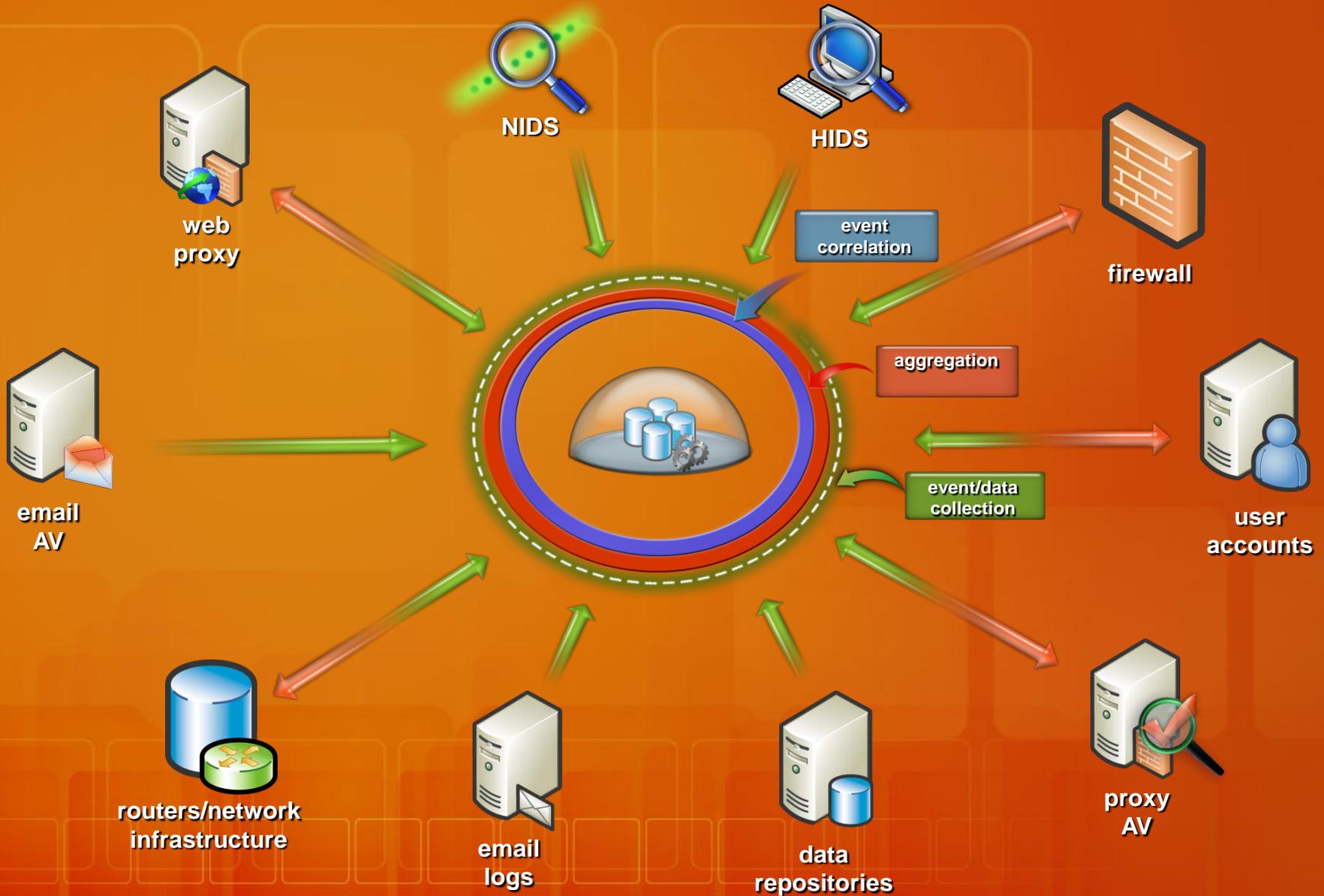
How to get it right

- Focus on *capabilities*, not flashy gimmicks
- Assess your monitoring objectives
- Know your environment and data mapping
- Capture and mature existing processes
- Set clear goals for platform implementation
- Invest time into vendor/platform selection
- Recognize commitment of self-run SIEM
- Is self-hosted/self-managed for us?
- Talk to your CFO: CAPEX or OPEX?

Sensory instrumentation

- Develop use cases to inform your source selection process
- Determine event/data acquisition constraints
 - Parsing ability
 - Event rates
 - Payload fidelity
- Don't collect just because you can
- Focus on *protection target*, not infrastructure
- Smart sensors = intelligent events

Anything can be a sensor

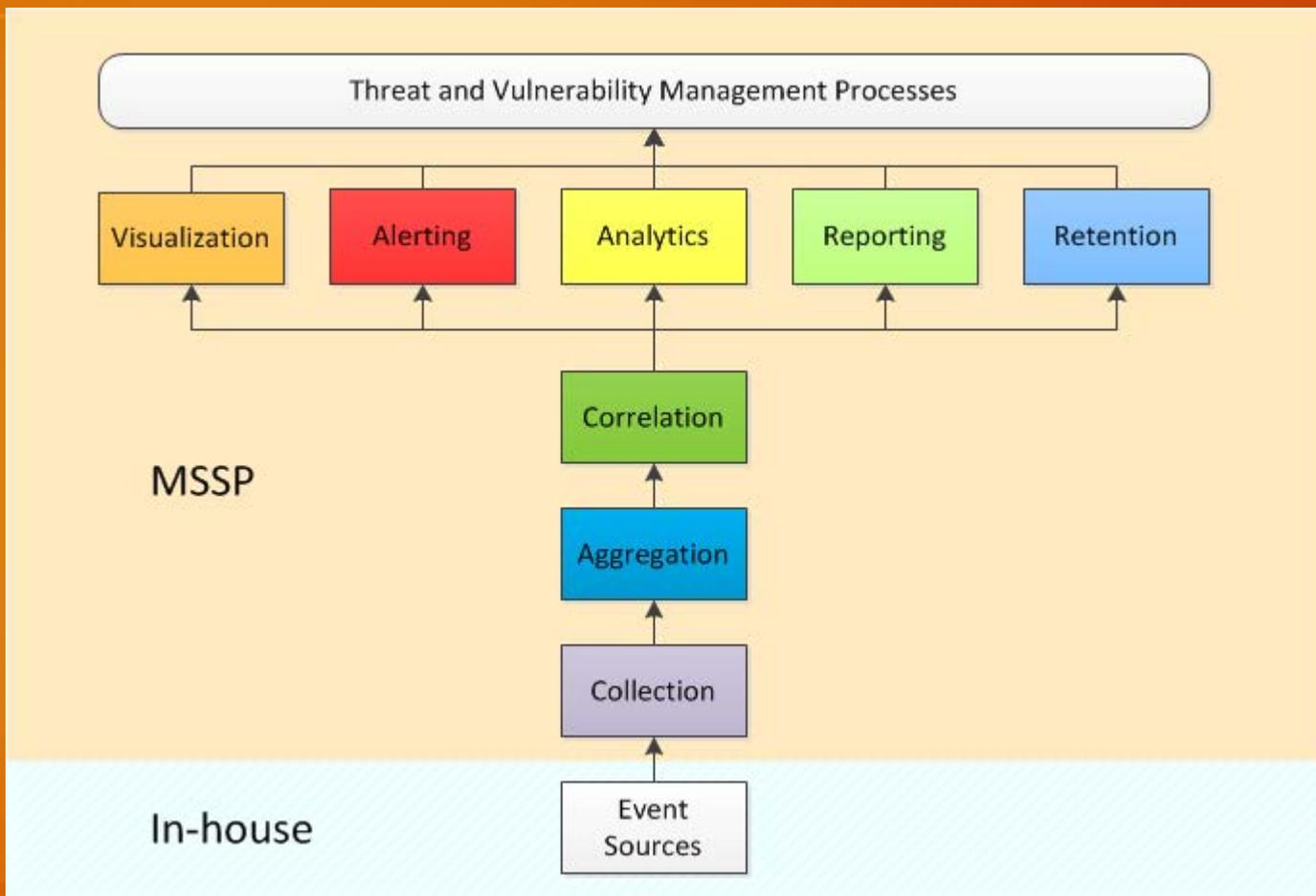


Intelligent sensors - rich data

- Data Loss Prevention (Vontu)
- Next-Gen Firewalls (PaloAlto)
- Endpoint security agents (Bit9, CyberArk)
- NAC technologies (ForeScout)
- Purpose-built platforms (FireEye, Damballa)
- Web App Firewalls (Imperva)
- VPN/RAS systems (Juniper, Citrix)
- Wireline solutions, IPS (Netwitness, Solera)
- Identity Management systems

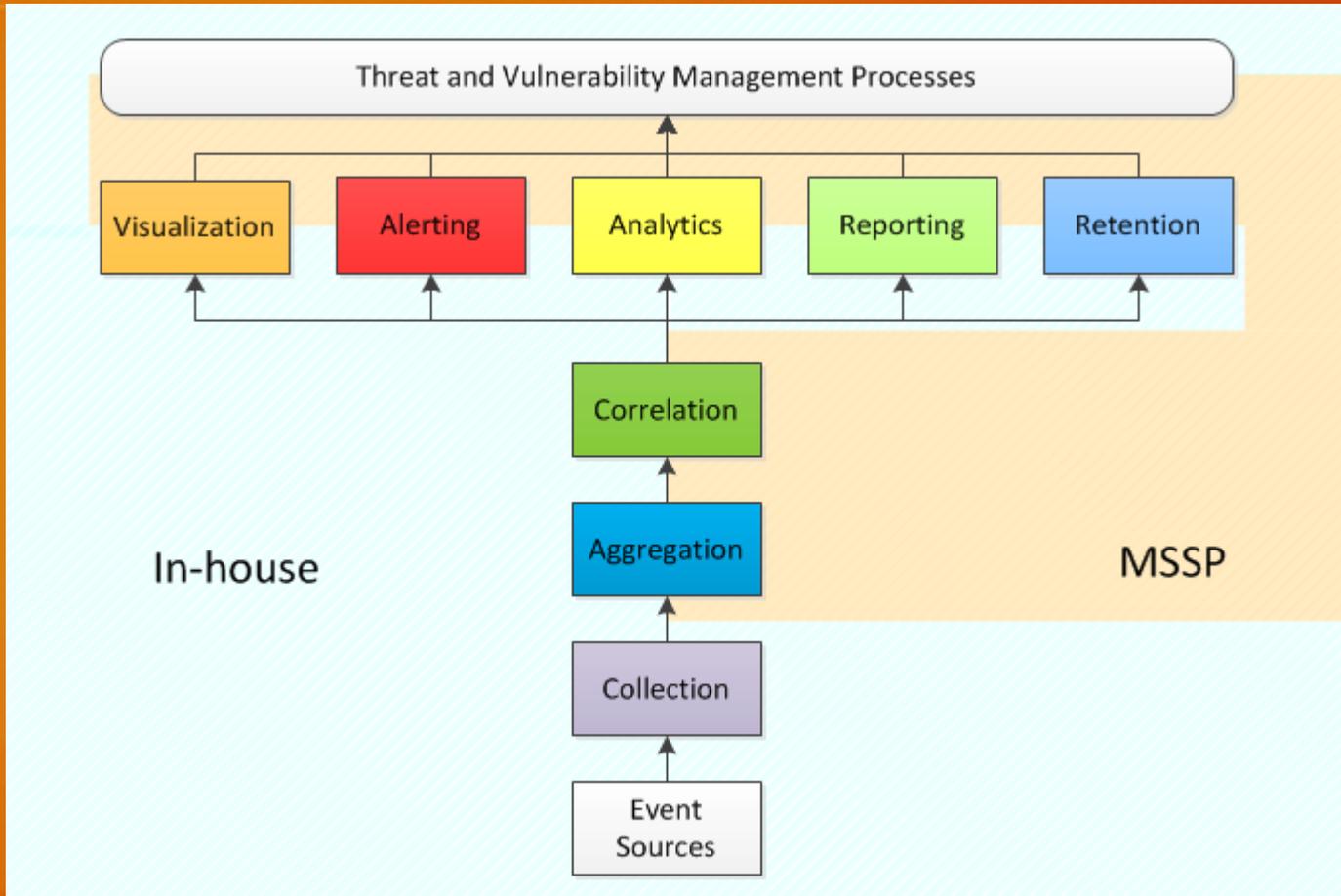
Deployment Options

Self-hosted, MSSP-managed



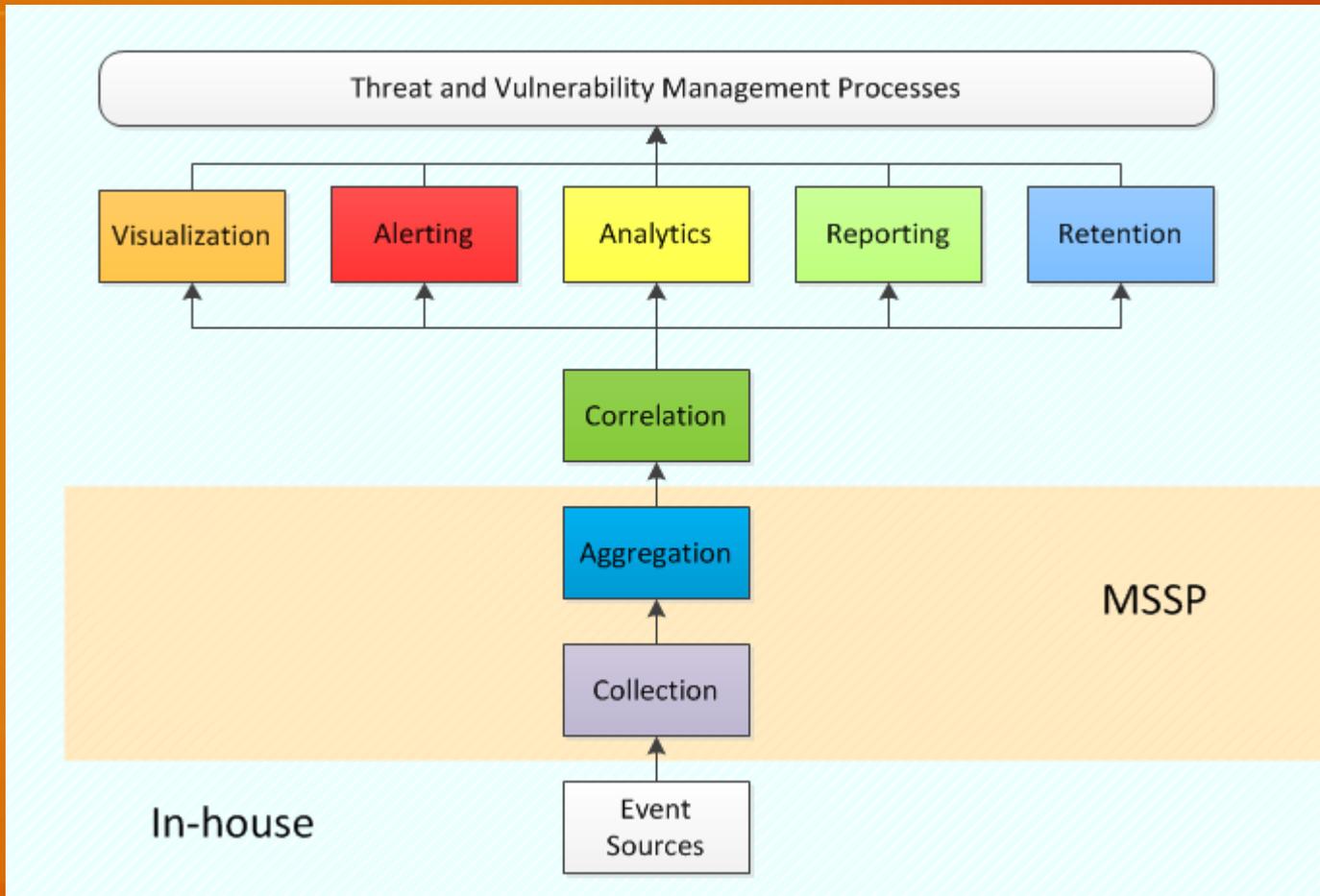
	CI	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■							
MSSP		■	■	■	■	■	■	■

Self-hosted, jointly managed



	CI	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■	■	■	■	■	■	■	■
MSSP		■	■	■	■	■	■	■

Cloud, self-managed



	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house			■	■	■	■	■	■
MSSP	■	■						

Q & A

igor@securelabs.net

scott@securelabs.net

No SIEMs were hurt in the making of this presentation.

Thank You!