Technology Evaluations:

Finding the Right Solutions for Your SOC

Part 1: How to Build a SOC

Montance® LLC

CYBRARY | FOR TEAMS

Introductions

Amanda Davi

Director of Business Development

Cybrary

Chris Crowley

Consultant, Author of SOC-Class.com

Montance® LLC

Overview

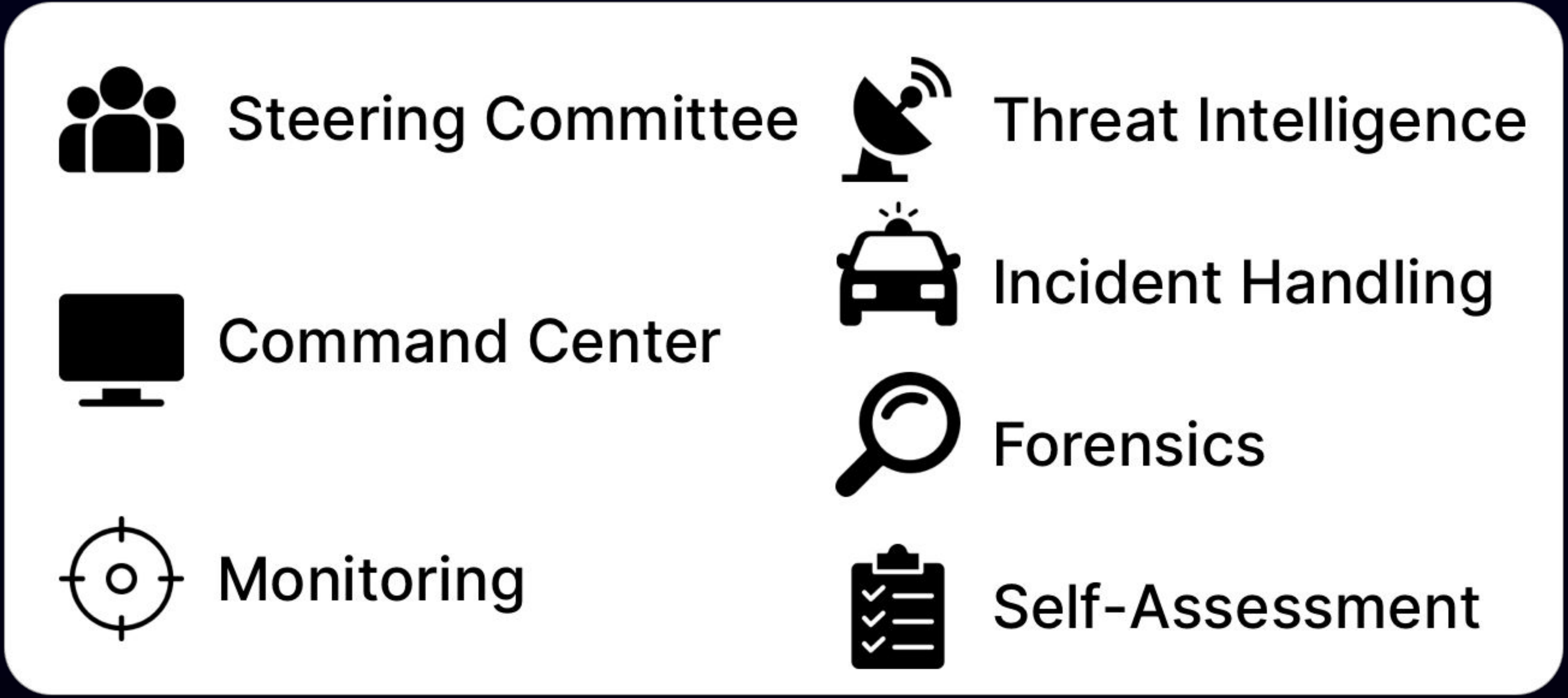
- Start of the second series
  - Deep dive on technology
  - Depends heavily on the framework discussed in our previous series
  - Hint: Go watch those if you haven’t already

- Overall taxonomy
  - High-level taxonomy
  - How the parts go together
  - Start into the details of the technologies

Recap
SOC-Class Model

My SOC “Reference Model”

Created for SOC-Class.com



Steering Committee

Command Center

Monitoring

Threat Intelligence

Incident Handling

Forensics

Self-Assessment

Technology Overview

Technology

- Visibility: weather, IT monitoring, threat intelligence, partner/dependency visibility
- Communication: status portals, email, chat, telephone
- Ops: ticketing, SOAR, dev/qa/stage of SOC operational systems
- Detection & Prevention: endpoint, network, infra-/extra-structure, correlation
- Storage: aggregation, long-term storage, destruction
- Deception: models, decoys, containment nets, honey-*, fake accounts and personas
- Analysis: code, hardware, baselining, mapping, correlation, scanning, forensics
- Do you have a list of all your tech, categorized, with gap analysis for future capability?
- Technology is only one part of maturity

Visibility (External Awareness)

Communication

Ops

Detection & Prevention

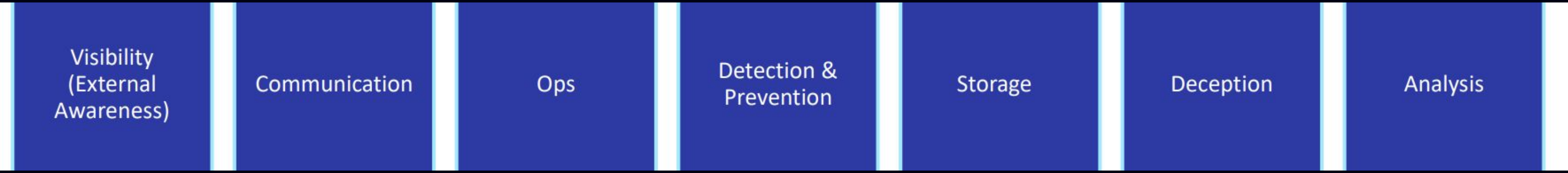
Storage

Deception

Analysis

Technology

- I advise organizations on security operations and assess maturity of SOCs
- I start with a “complete list” that I narrow based on drivers, needs, systems to defend
- Identify a budget-appropriate technology portfolio for organization and its culture
- Is open-source OK? Can McAfee/Kaspersky... be installed? (Legal/governmental alignment and prohibitions)
- Staff in place who are capable to deploy and maintain the tool
- Technologies should be compatible, effective, supported, secure, and fit into the operational capability of the organization



Visibility (External Awareness)

Communication

Ops

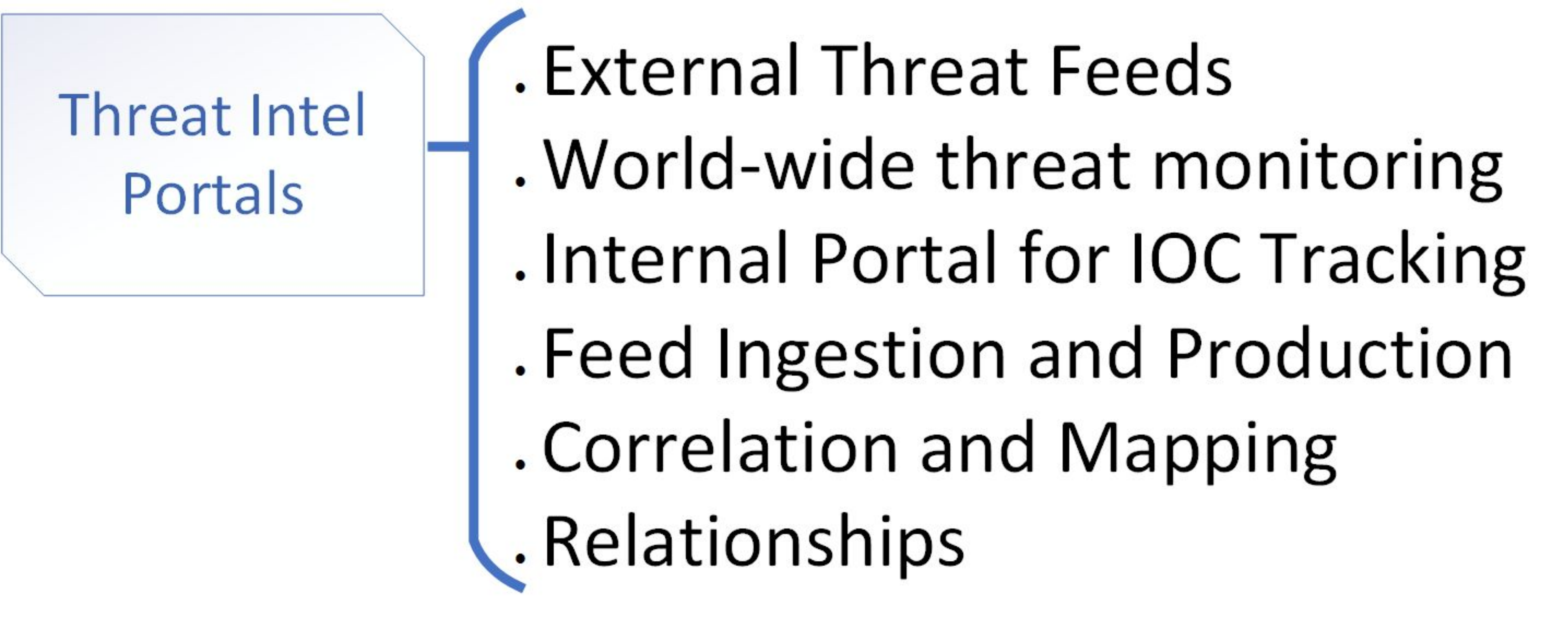
Detection & Prevention

Storage

Deception

Analysis

Visibility

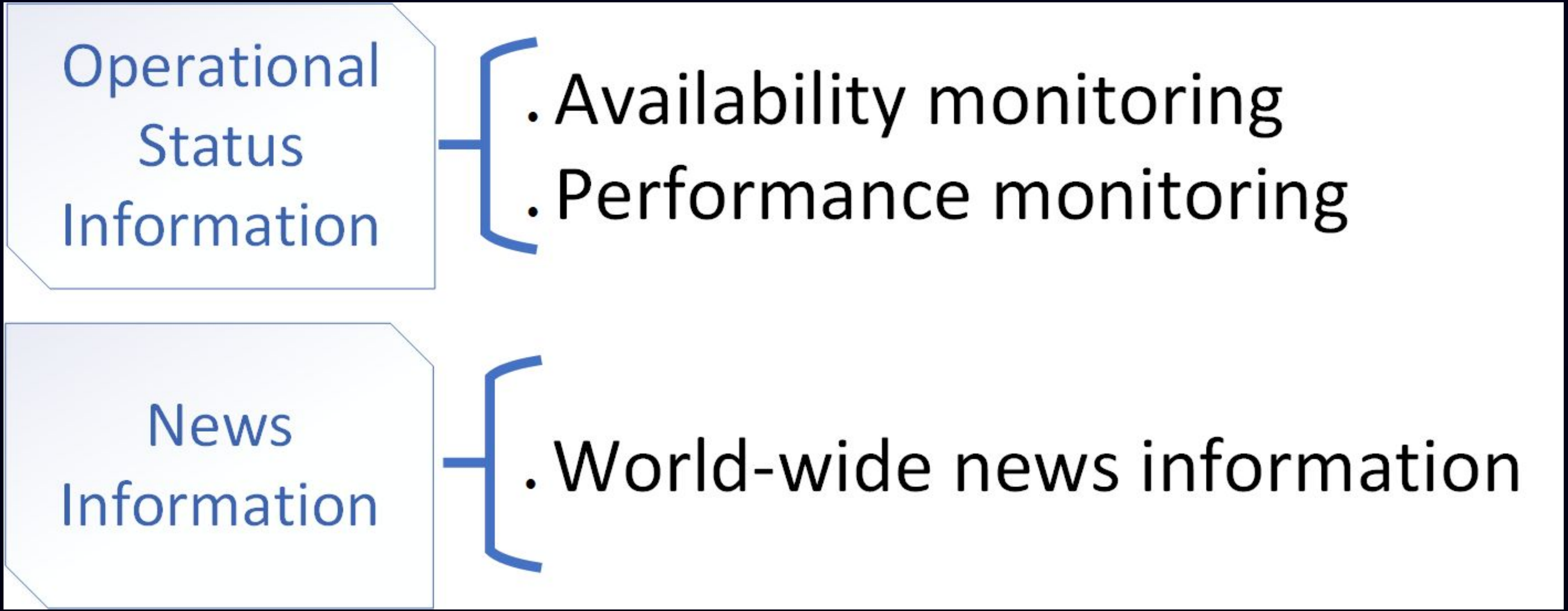


Threat Intel Portals

- External Threat Feeds
- World-wide threat monitoring
- Internal Portal for IOC Tracking
- Feed Ingestion and Production
- Correlation and Mapping
- Relationships

Visibility (External Awareness) | Comm-unication | Ops | Detection & Prevention | Storage | Deception | Analysis

- Threat Intel Portals
- Operational Status Information
- News Information
- Weather
- Internet Weather



Operational Status Information

- Availability monitoring
- Performance monitoring

News Information

- World-wide news information

Visibility (External Awareness) | Comm-unication | Ops | Detection & Prevention | Storage | Deception | Analysis

- Threat Intel Portals
- Operational Status Information
- News Information
- Weather
- Internet Weather

Weather

- Weather (Physical) Forecast

Internet Weather

- World-wide Internet Status

Care & Feeding

Keeping the Lights on Isn't Enough

- Many SOCs do little more than operate systems, never get to in-depth analysis
  - Poor budgeting
  - Misunderstanding of what the SOC is supposed to do by management (lack of management support)
  - Staff shortage, lack of empowerment, lacking clear boundaries of authority (results in overreach, then hesitance)
- Resolutions
  - Outsource the tool management if feasible
  - Consistently convey the SOCs responsibility as analytical and threat-focused, with monitoring and incident handling responsibility
  - Develop great engineered programs for automated detections (develop use cases)
  - Also hunt: ad hoc, sloppy, but structured and progressively more repeatable in structure, enabling progressively more creative and unstructured hunting

Conclusion

Conclusion

- Today, we started into the Montance® Technology Taxonomy I use to organize technology for security operations.
- In our next two programs we'll cover:
  - The rest of the taxonomy: Communication, Ops, Detection & Prevention, Storage, Deception, and Analysis
  - Orchestrating and automating technology to develop effect data use and technology selection criteria

Let's Connect

Amanda Davi

adavi@cybrary.it

linkedin.com/in/amanda-davi

www.cybrary.it/business

Chris Crowley

chris@montance.com

mgt517.com/linkedin

www.soc-class.com

Resources

- Cybrary SOC Career Paths
  - SOC Analyst Level 1
  - SOC Analyst Level 2
  - SOC Analyst Level 3
- Montance® SOC-Class: Online in December
  - https://soc-class.com
- SOC Survey Key Findings and Results Video Series : https://soc-survey.com
- Maximizing Security Operations, on-demand 4-part series
  - Part 1: The Role of a SOC
  - Part 2: SOC Architecture and Management
  - Part 3: SOC Staffing and Incident Response
  - Part 4: Enhance SOC Capability and Maturity

Thanks For Joining Us!