SecOps, SIEM, and Security Architecture Use Case Development

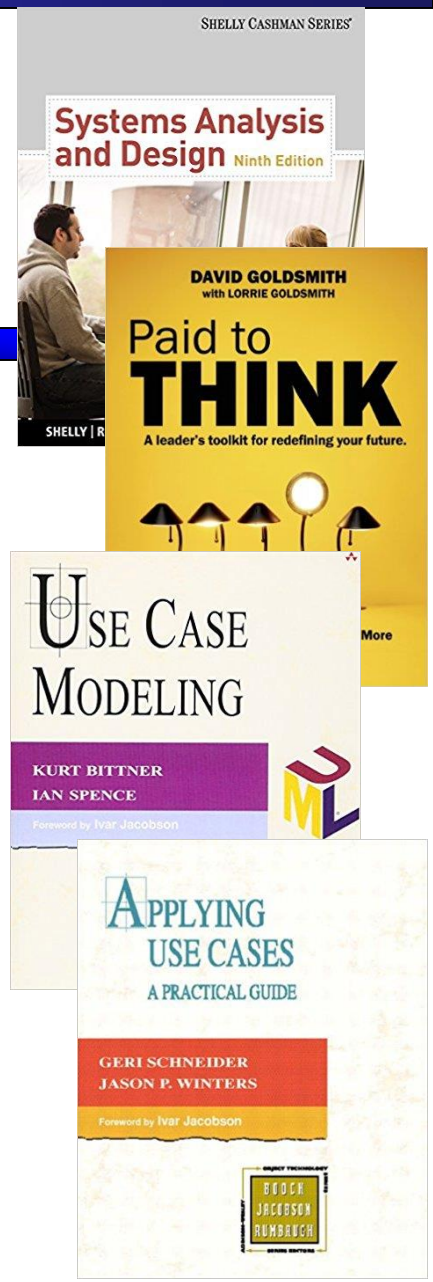
Don Murdoch, GSE #99
Asst. Director, Institute for Cyber Security,
Regent University, Virginia Beach, VA

Author, Blue Team Handbook: Incident Response

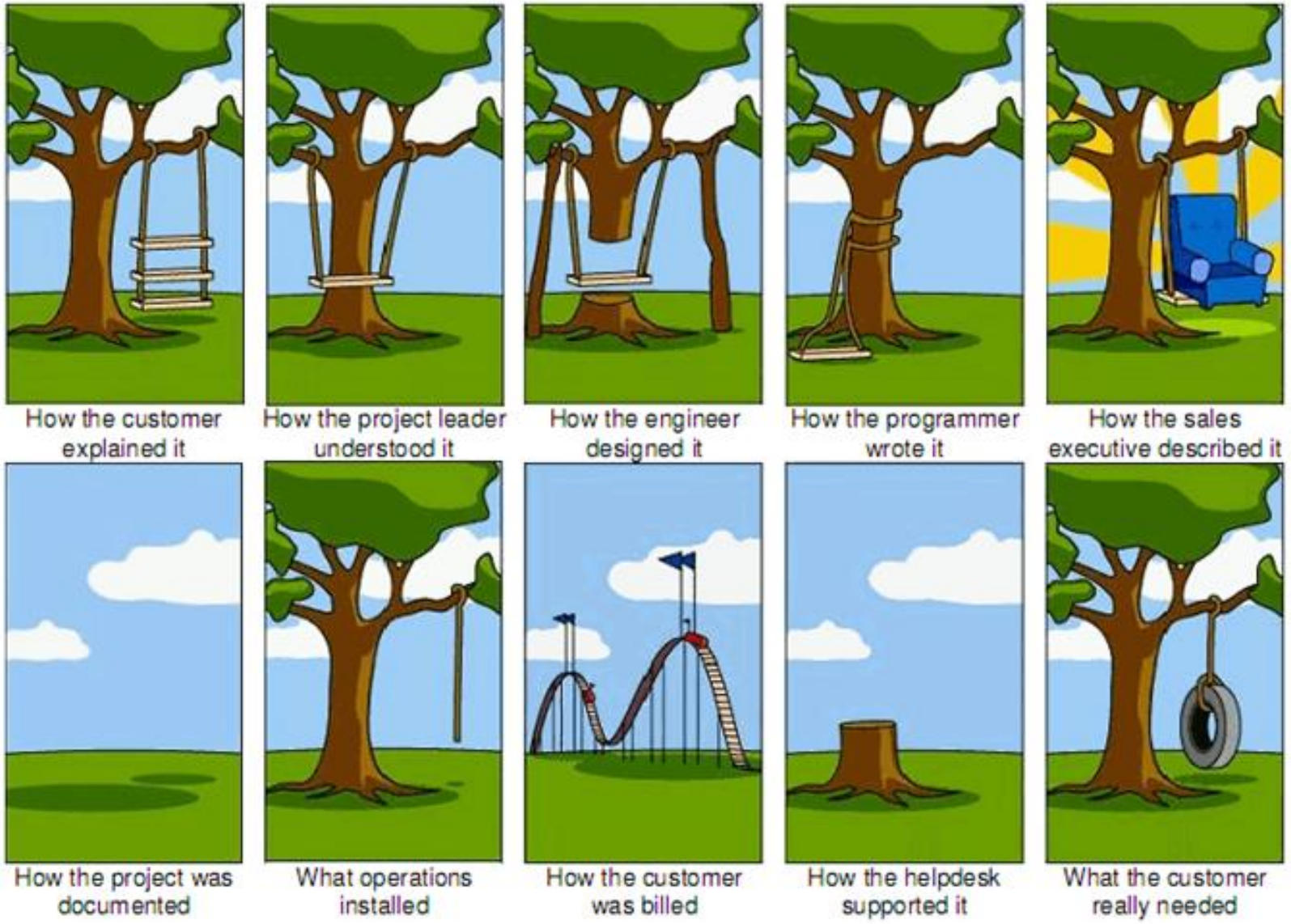
Latin "sapere aude" means "Dare to Be Wise"

Session Agenda

- Requirements development in support of SecOps/SecArch focused use cases
- Define the security operations use case development process and key considerations
- Provide real life examples from a SIEM platforms and custom implementations



Requirements – Spot the need vs. feature



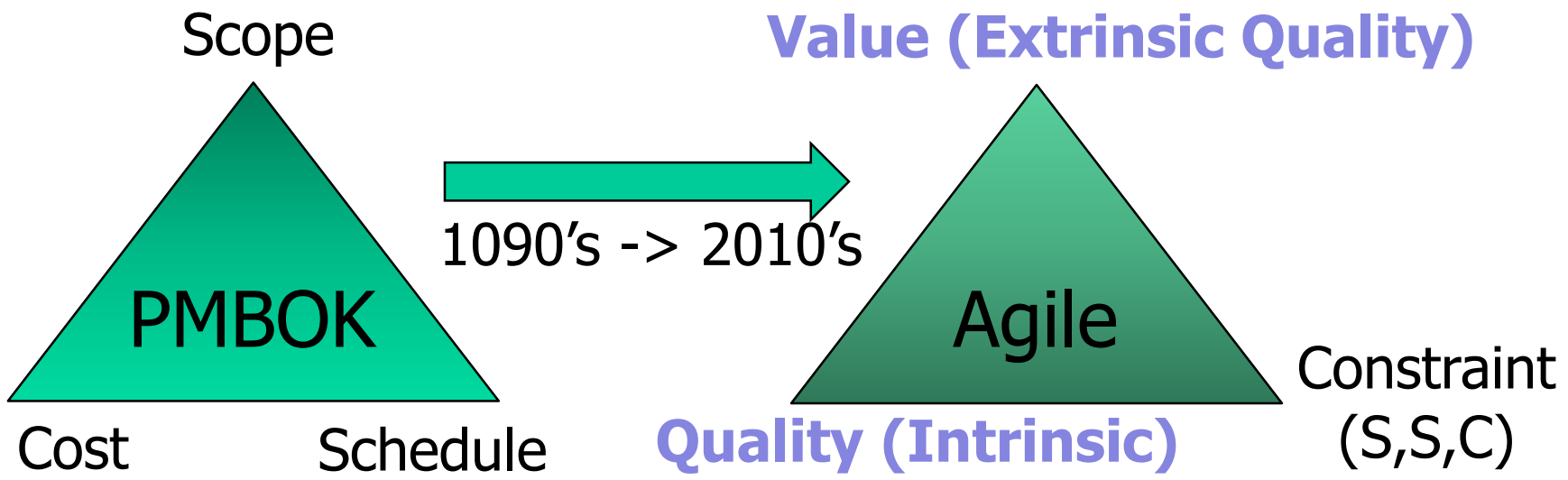
Needs: Things that the stakeholders believe that the system needs to do; problems that they need to have solved.

Features: Informal / imprecise statements of capabilities of the system used often for marketing and product-positioning purposes, as a shorthand for a set of behaviors of the system.

Requirements Development is Essential

- Software development goal
  - Develop [acceptable] quality software, on time and on budget that meets a real need
  - Satisfy Requirements, or the individual statements of conditions and capabilities to which the system must conform
  - *Use Cases express and show how to realize the requirements*
- Studies advise:
  - 50% of businesses experience IT [cloud] project failure (Innotas, 2013)
  - Only 16.2% of 8,360 software projects had ideal results (Standish, 2014)

The Maturing Iron Triangle



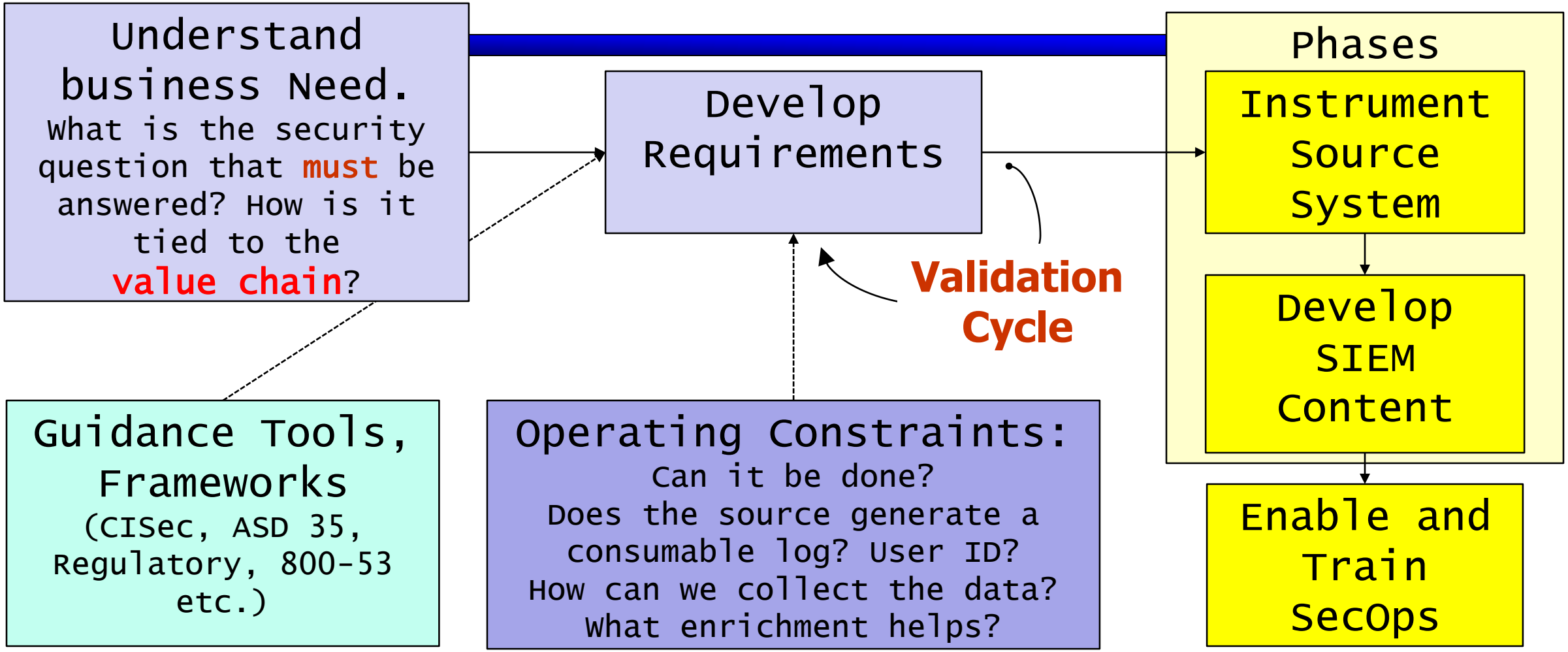
- Value- to the end user in terms of a deliverable product
- Quality- continuous delivery of value according to the customer's requirements
- Constraints- a traditional scope, schedule and scope

Source: https://www.knowledgehut.com/blog/agile-management/agile-project-management-triangle-a-golden-product-in-organizations

Use Cases Defined

- Definition:
  - Actions or steps that define the interactions between a role and a system to achieve a specific goal. Roles are outside.
  - Actor: a person or things that interact with the system
  - Use Case: Things of value the system provides to its actors
- SecOps: Use cases define the flow of data and how the Security Team interacts with the system to monitor and detect adverse conditions

SIEM/SecOps Process



SecOps Use Case Template

- Name
- Purpose
- Problem Statement
- Requirement Statement(s)
- Design Specification
- Security Operations Notification Process and Key Data
- Incident Response / Investigation Process for the Analyst
- Use Case Component Names
- Use Case Component Names
- Use Case Data Source Descriptions
- Data Analysis – Go Diamond
- Kill Chain Analysis
  - Traditional KC
  - ICS Specific KC
- Audit support
- Assumptions / Limitations
- Alternatives to this Use Case

Be Wise Up Front (1/2)

- Name – placeholder in the library, control tie in
- Purpose
  - To describe a specific use case for topic X and explain how the UC will be satisfied by system Y
- Problem Statement
  - Describe the business objective / process / problem
  - Provide direction without stating a solution
  - Ideally, it expresses a solvable problem

Be Wise Up Front (2/2)

- Requirements
  - Correct, unambiguous, and feasible
  - Must support the use case – in scope
  - Ideally, requirements communicate priority.
  - Measurable or verifiable in some way which will manifest through the source data and actions that the system will take.
  - **Testable** (design of experiment)

Use SMART Design Specifications

- Specific – target a specific area.
- Measurable – quantify an indicator of progress.
- Assignable – specify who, what, where
- Realistic – state what results can realistically be achieved, given available resources
- Time-related – specify when the result(s) can be achieved.

- Because Use Cases need to be successful too!

Sec Ops Team Notification – Key Actors

- Ensure that all necessary data arrives to the SoC
  - Enrichment is important for SoC analyst success
  - Automate as much as possible for rapid review
- Provide process guidance for content context
  - A note to explain the "attribute"
  - Define further analyst investigation paths / opening move to shorten the MTTD (detect)

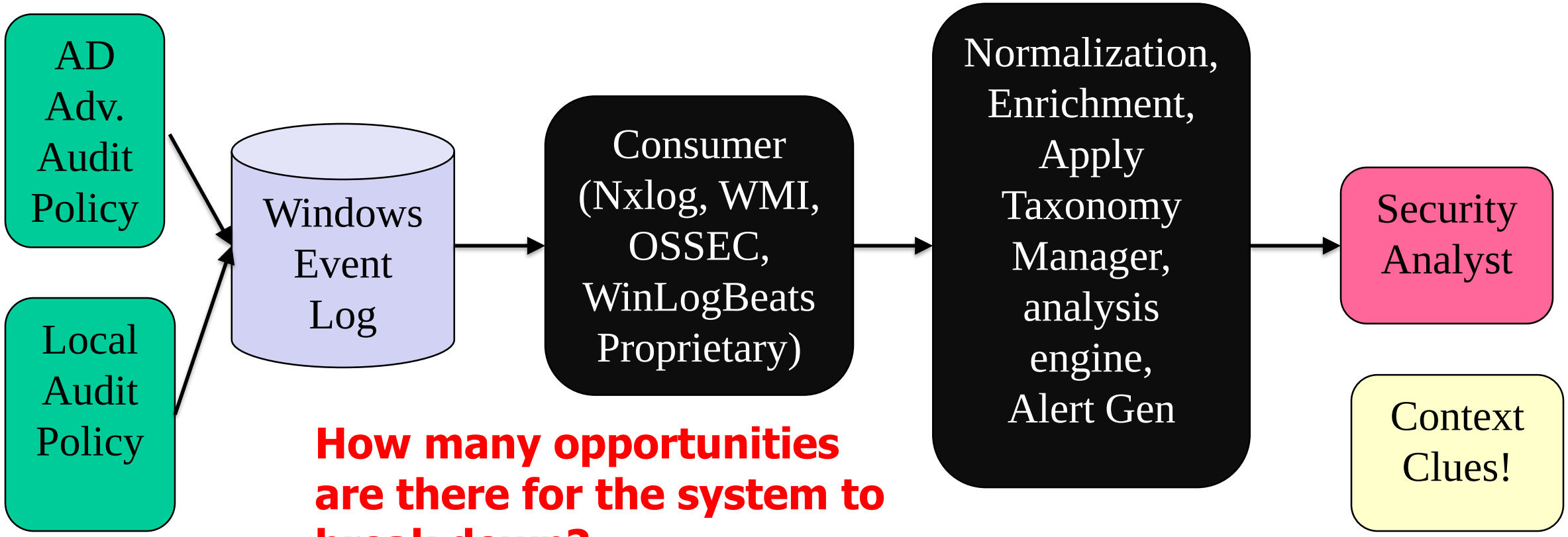
Component Names – Maintenance

- Document the Use Case components for the "entire system"
  - Data feeds, plug ins, configuration files, parsers, normalizers
  - Device names
  - Rules, lists, directives, enrichment/reference sources
  - Content components such as internal lists, dashboards, output reports, etc.
- This section is *critical* for "debugging"

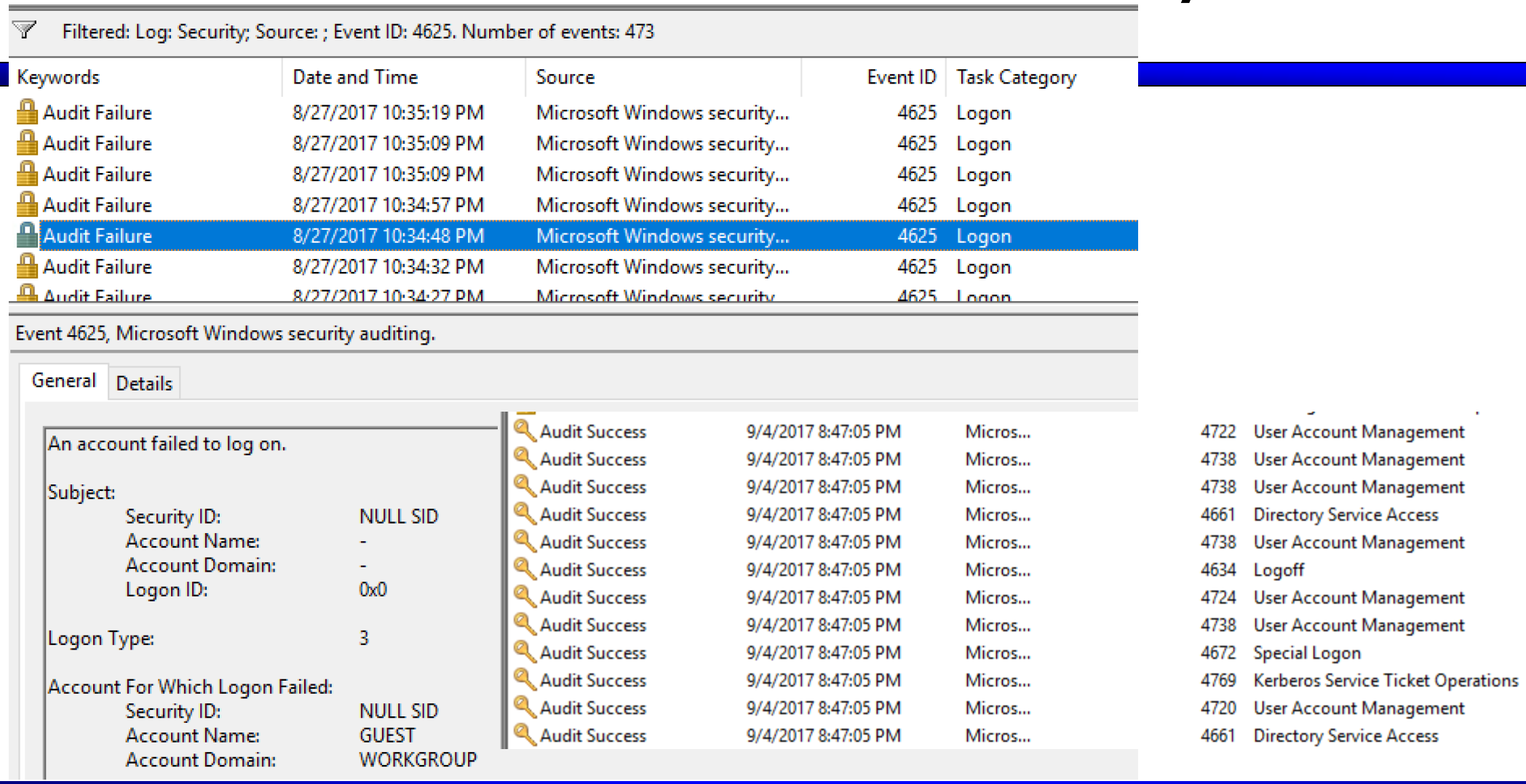
Example UC's for Account Misuse and ALCE's

- Audit Logon and Account Logon
  - AD DDGPO, DDC GPO, Local GPO – is this thing on?
  - Log reader – every X Seconds, read and forward
  - Alert notification must be able to parse and identify the condition
- Constituent system policy - "defer" to the central directory for account name and needs to log attempts
- Privileged "security context" (group) changes

Data Process – Windows Event Logs

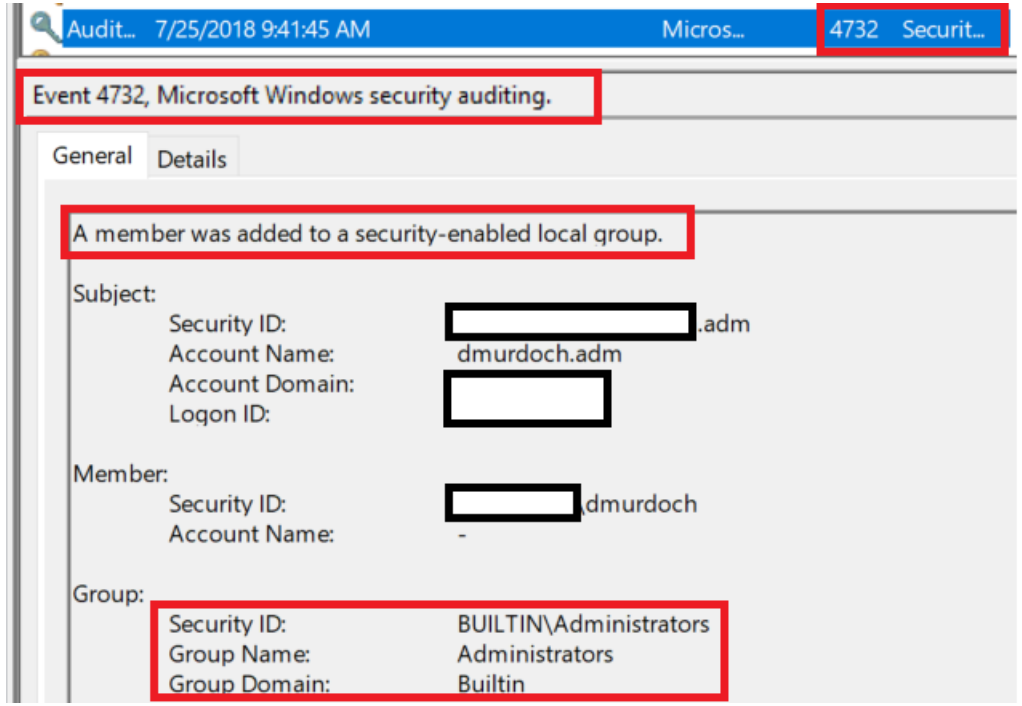


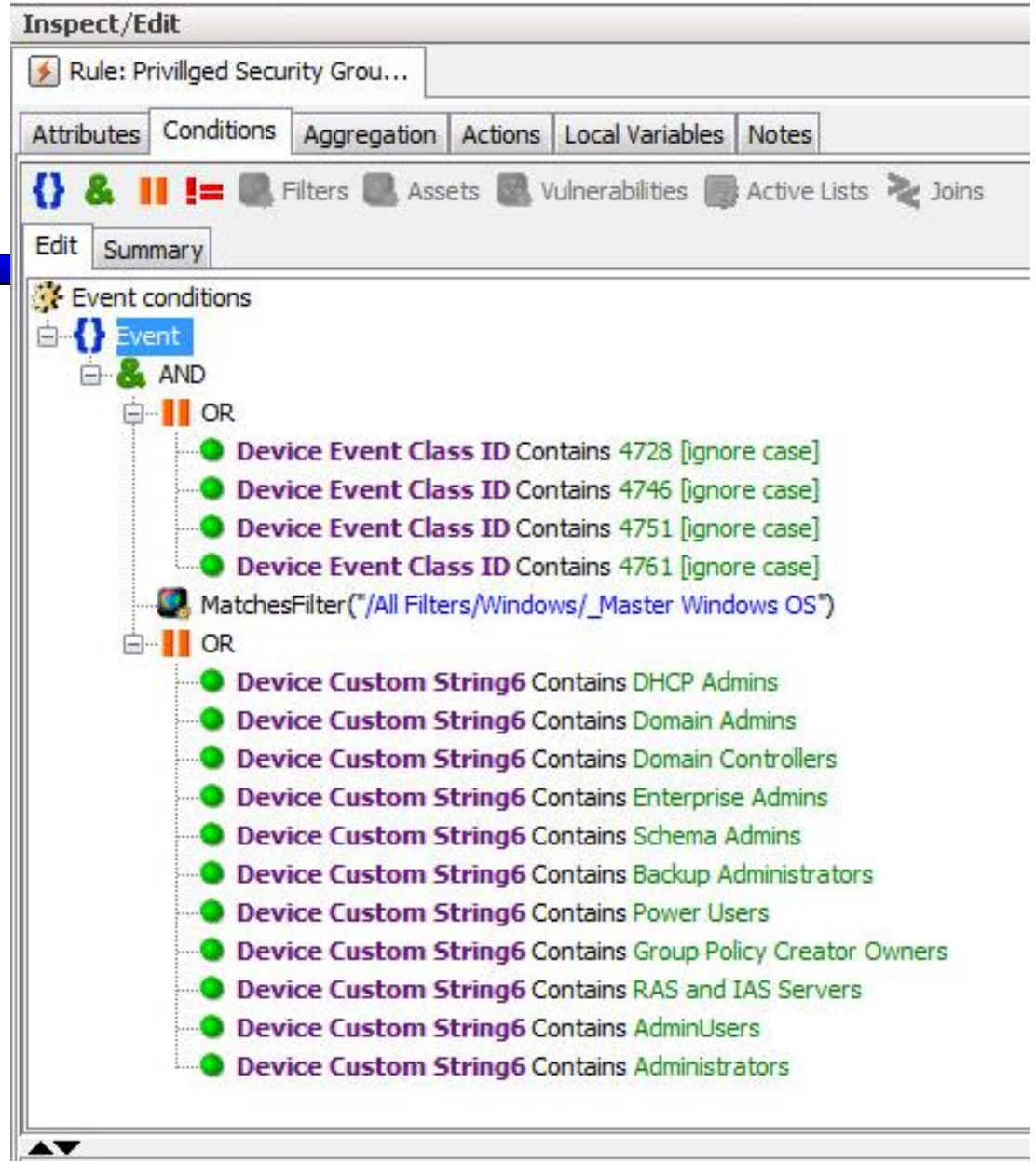
Instrument and test the system!



SIEM Example - Privileged Group Changes

Can you find the gap?





4728: A member was added to a security-enabled global group

How “we” spent 204 hours or $13,872 to “monitor PeopleSoft HCMS and FIN”

- Multilevel security rights/roles model – 67 pages
- Design 17 conditions to satisfy Financial Controls
  - 17 select’s that rolled into one, 17 unit tests, meetings..
  - 24 page BRD, 70+ page DD, 17 step test plan, 6 Stored procedures and collectors, rights, deployments (Q,D,P) with change control
  - Custom collector codebase – one per environment - multiple dashboards, two email notifications, audit report
  - Ensure you ***predict prod impact*** because Dev and QA will not mimic production while you design/develop

Hundreds of Other Use Cases

- Accounts not conformant to standards or in use in a constituent system but not defined in the central directory
- Successful brute force
- Local A/V event followed by outbound URL to suspicious IP and a PDF file open on the PC
- Proxy says “Suspect site”, then AV event, then ‘first IP use without prior DNS lookup’

Thank you!