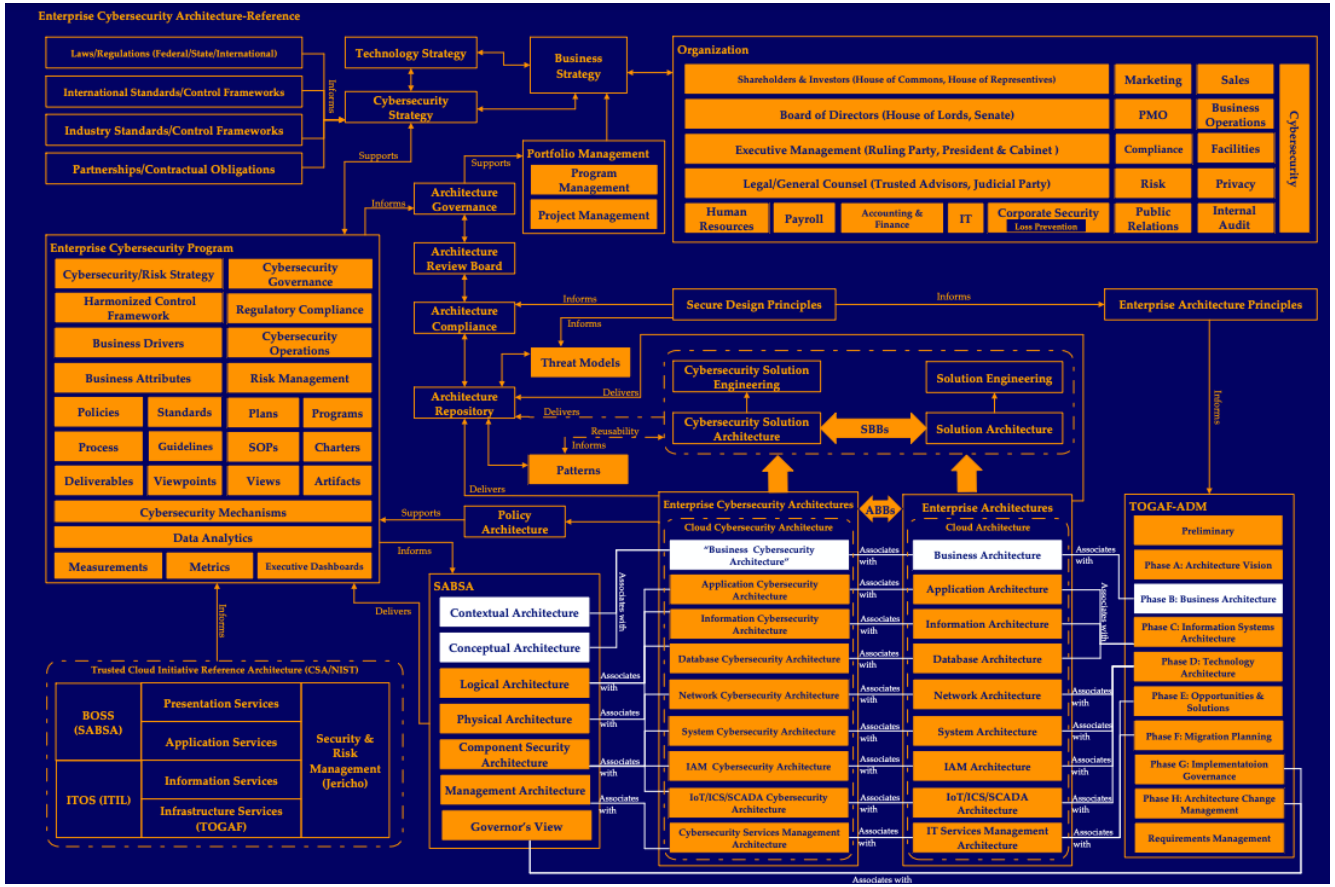
Security Split: Divorcing Your Stack

Presented by Alissa Torres

Security Practitioner | Antisyphon Instructor

Security Tool Migration Agenda

“I am **not** an engineer. And I am definitely **not your** engineer.”



Thank you, James J Fisher! https://www.jamesjfisher.org/esa/files/ref_arch_001.pdf

Why we can’t have nice things

Defining the problem

Security Tool Migration Suffers from Inadequate Planning

- Security stack stakeholders often dramatically underestimate the immensity, scope of security tool replacement.

2021 Stats from Panther Labs: It takes, on average, 6 months to deploy a SIEM.

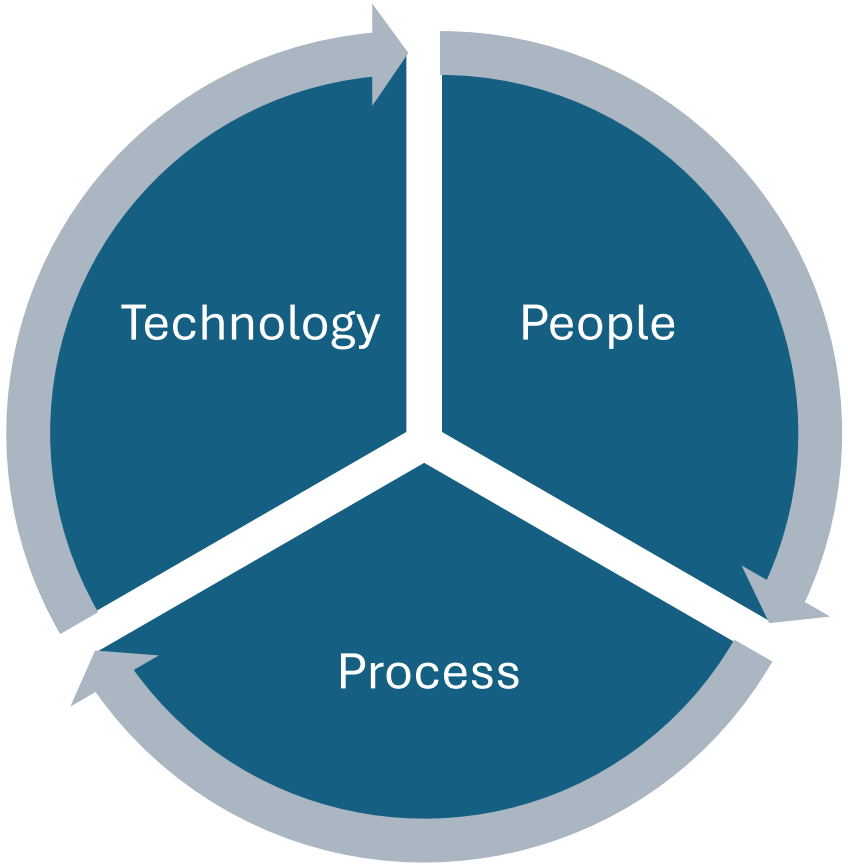
Unrealistic Expections - Buying into the Hype

- “When the SOAR gets here, we will integrate that…”
- “Our new tool will finally provide us with insightful metrics.”
- “When we onboard the new SIEM, we will be super heroes…”

Security Tool Migration Checklist

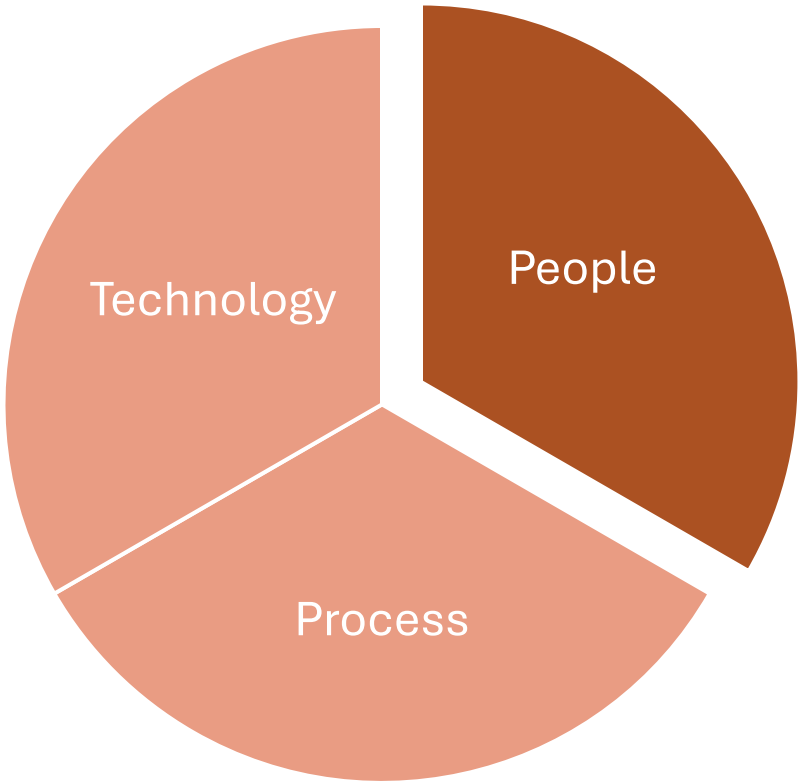
- What is the implementation scope? Migration phases?
- What is the migration timeline?
- Who are the stakeholders influencing the migration?
- Does the tool require development time for custom features?
- Do security stack integrations require secondary tool changes?
- Is Active Directory integration required for user access?
- Will the new tool replace a UI How was the legacy UI utilized?
- Will the new tool replace an existing log data source?
- Does internal engineers' workload allow for migration commit?
- Which team(s) will develop use cases?
- How will use cases be prioritized?
- Which use cases must be satisfied for minimal viable product?
- Which stakeholder(s) will hold acceptance verdict?
- How will secondary/tertiary teams be affected?
- What are the upskill training requirements?
- Does the new tool created additional legacy devices?
- Under what conditions can this project be deprioritized?
- What the risks of partial implementation?
- Are there licensing costs incurred for a warm handoff?

PPT Change Impact Assessment



++DATA, ORGANIZATIONAL SERVICE MODEL AND GOVERNANCE

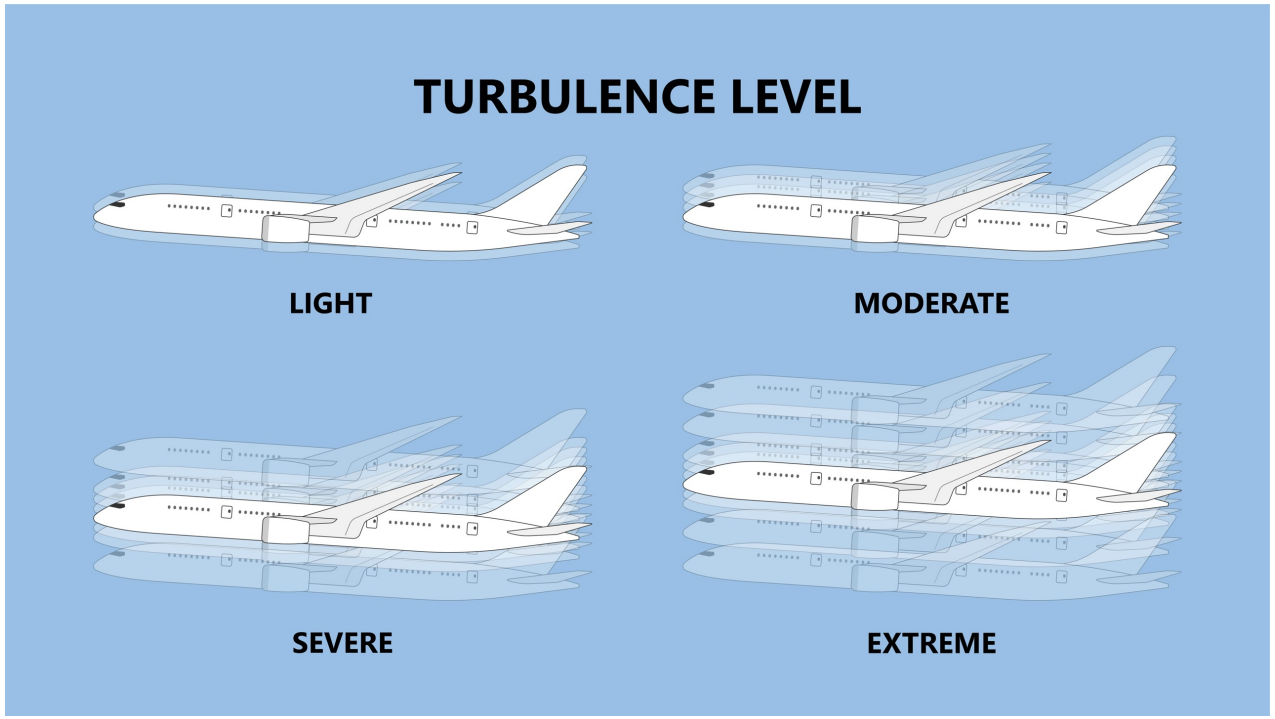
The Human Factor



- Human Errors
- Over-reliance on New Technology
- Disappointment due to Unrealistic Expectations
- Resistence to Change
- Technical Skills Gaps

Security Stack Changes: Impact on Stakeholders

- As changes to workflow become more significant, the likelihood of security operations **disruption** increases.
- Stakeholder roles & responsibilities often shift with the introduction of different tools
- Cost overruns affect other project funding

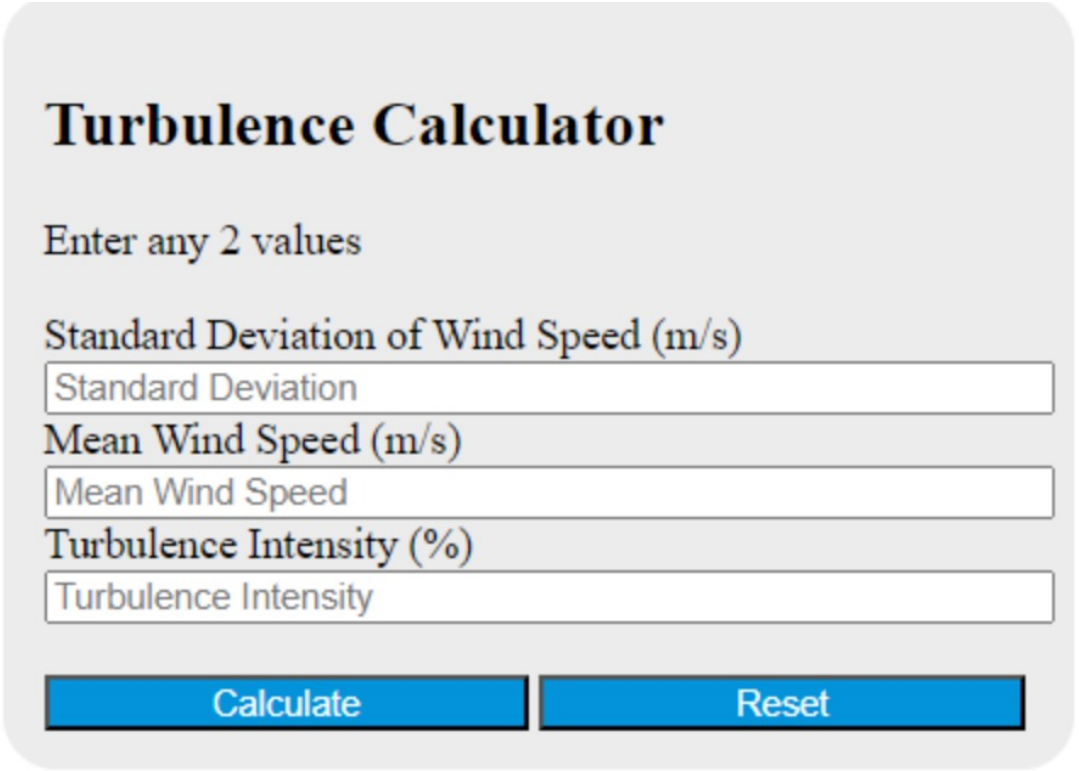


Creating Your Own Turbulence Calculator

Factors that matter

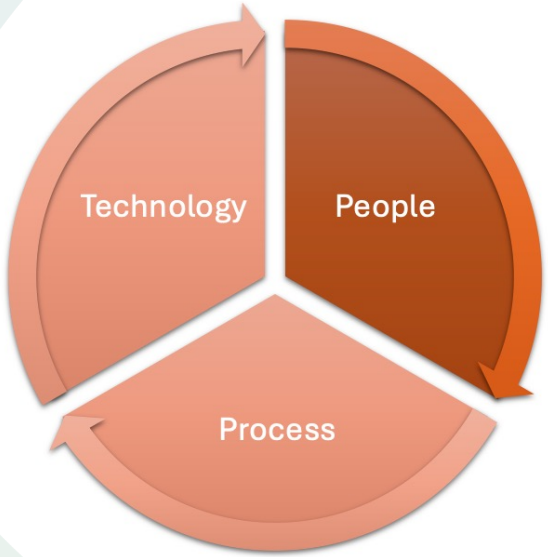
- Operational Tempo
- Implementation Timeline
- Staffing Levels
- Technical Savvy
- Operational Resilience
- Current Stakeholder Sentiment

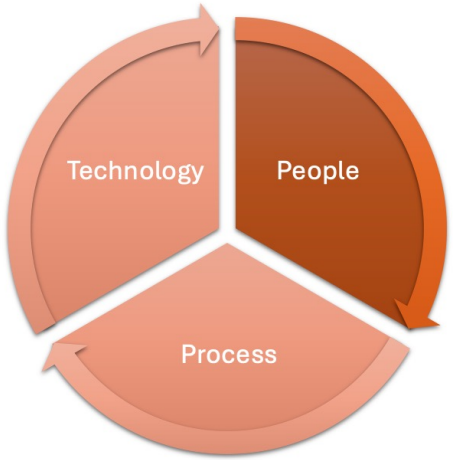
** Capture current & future states for all operational stakeholders*



Key Role:
Security Analyst

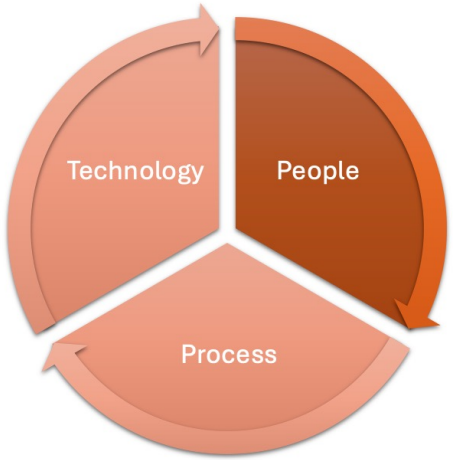
- Primary User == Primary Stakeholder
- Change raises **stress levels** in an already stressed out environment.
- Increased stress may lead to tool rejection.
- **Muscle memory** takes time to build.
- Anticipate **metrics** skew initially.
- Define the **analyst's** MVP.





Key Role: Detection Engineer

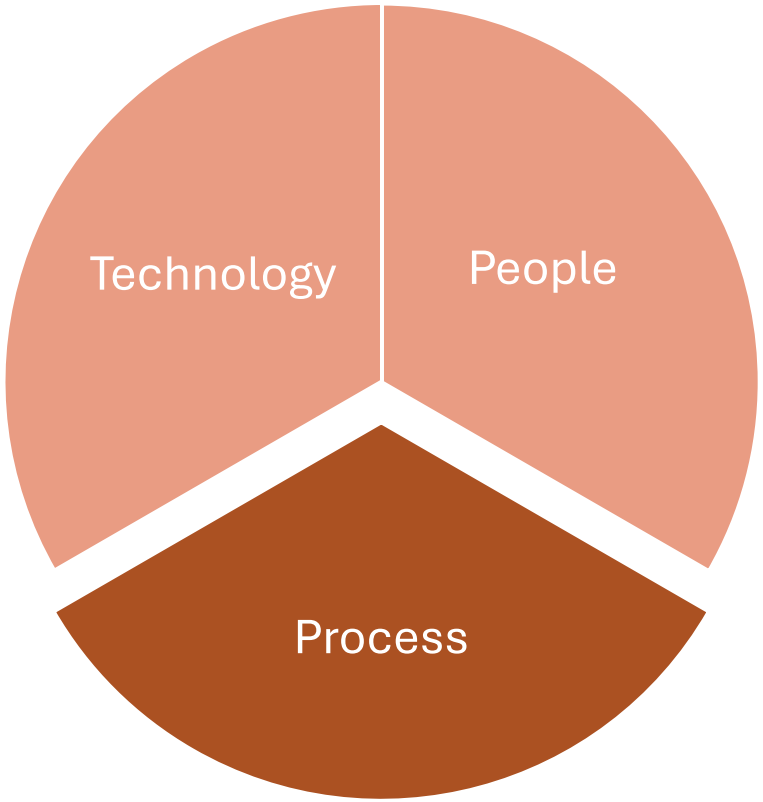
- Upskilling may require additional training in detection rule conversion
- Must identify apples-apples & apples-pears baked-in detection logic



Key Role: Tool Engineer

- Upskilling will require more than asynchronous training
- BakeIn the Verification Process
- Ensure long-term funding to security technology implementation

Operational Process Changes



How does it work?

- Modifications to data collection, access controls, platform auditing
- Changes in baked-in security detections

Where did go?

- Dashboard changes
- New data entry requirements
- Shift in automations

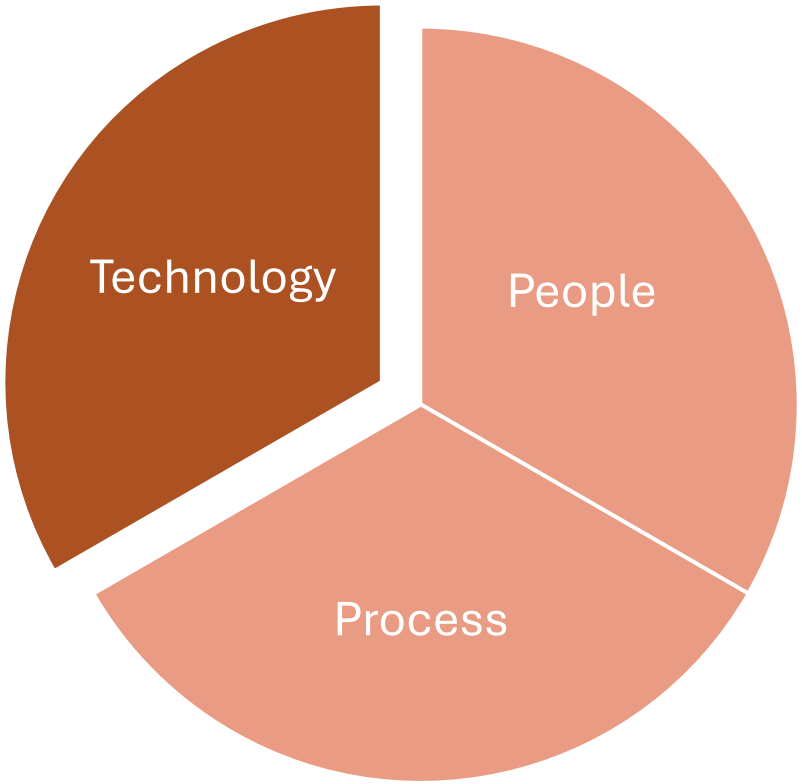
Now how do I investigate?

- Revamp your playbook decision trees
- Anticipate redundant tool capabilities that may allow deviation in ”playbooks”

Migrating Detection Content

- Evaluate current log data sources. Can any be dropped?
- Evaluate current detections. Don’t migrate those with little value.
- Limited **window of opportunity** to build active detection library from the ground up.
- Can the content even be migrated? Use Sigma? Some converters exist.
- Along the way, verify rule fidelity. Verify log coverage.
- Remember to recreate “Silent Log Alerts”!
- Implement a **warm hand-off** with an extended outboard/onboard phase.

Technology Considerations



- Prioritize Use Cases, Integrations
- What to take, what to leave
- Compatibility Issues
- Potential for revised definition of “legacy”
- Plan beyond MVP (Minimal Viable Product)
- Avoid Project Abandonment

Migrating your SIEM

- Identify custom detection content
  - which detections are actively useful/produced results over the last year.
- Identify current SOC processes
- Design and Plan New Use Cases per OS, product, threat
  - Prioritize!
  - MS recommends a focus on detections that would enforce 90% true positive on alert feeds. Those with high false positive rates will most likely take lower priority.
- Validate detections, log retention

MoSCow Methodology

- Identify use cases for new security tool
- Then **categorize & prioritize**:
  - Must-have
  - Should-have
  - Could-have
  - Won’t have (at least not right now)
- Failure to structure a migration roadmap will most probably lead to delays in implementation.
- With significant delays,chances of abandonment increase.

Avoid SIEM deployment delays

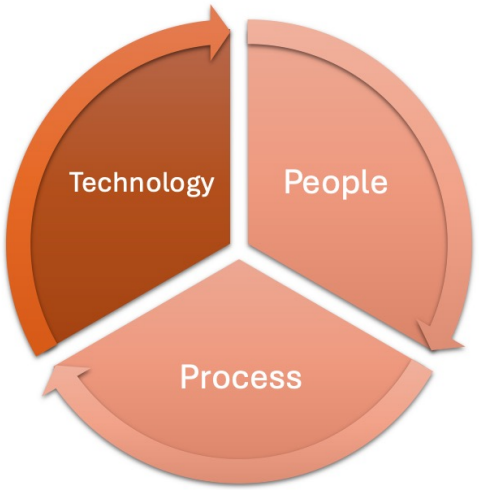
- Identify legacy security tool user base (some stakeholders may surprise you!)
- Define success. Titrate this into reasonable milestones.
- Invest in upskilling your engineers and analysts before, during and after migration
- Ensure adoption of standardized event format (Common Event Format (CEE by Mitre)
- Identify (and potentially cull) strategic and well-configured data sources
- Document configuration decisions and keep up to date

Security Product Abandonment

Abandonment factors parallel other customer rejection behaviors

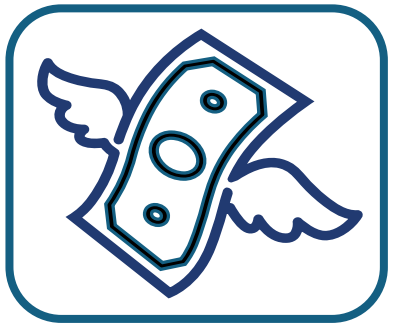
"Most Common Reasons for Shopping Cart Abandonment"

- Mandatory Account Creation -> MFA fatigue
- Long or confusing checkout process -> Laborious data entry
- No discounts or promo codes to use -> No enrichments!
- Unexpected shipping costs -> Cost per query
- Longer than expected delivery times -> Slow query processing…
- Ambiguous return and refund policy -> Low fidelity alerts. Poor ROI.
- Lack of desirable payment options -> Report features are lacking



Security Product Abandonment

Primary User Rejection



Implementation Project Defunded

External Delays (AD Integration, Arch Change)

Steep Learning Curve

Deprioritized

Vendor Feature Due Out

Steps to Prevent Abandonment

Secure these Operational Commitments

- Adequate Time for Tool Baseline Phase
- Continued Automation Support (or Upskilling for Internal Dev)
- Support for Optimizations (from both Vendor and Engineering)
- Guardrails on Metrics during Detection Baselining
- Drive Additional Data Sources

Automation Redrafting

- Recreating automations
- EDR isolation - is it gonna screw up your ability to perform additional triage?

Security Tool Migration Checklist

- What is the implementation scope? Migration phases?
- What is the migration timeline?
- Who are the stakeholders influencing the migration?
- Does the tool require development time for custom features?
- Do security stack integrations require secondary tool changes?
- Is Active Directory integration required for user access?
- Will the new tool replace a UI How was the legacy UI utilized?
- Will the new tool replace an existing log data source?
- Does internal engineers' workload allow for migration commit?
- Which team(s) will develop use cases?
- How will use cases be prioritized?
- Which use cases must be satisfied for minimal viable product?
- Which stakeholder(s) will hold acceptance verdict?
- How will secondary/tertiary teams be affected?
- What are the upskill training requirements?
- Does the new tool created additional legacy devices?
- Under what conditions can this project be deprioritized?
- What the risks of partial implementation?
- Are there licensing costs incurred for a warm handoff?

Additional Resources

- Microsoft. (2024, 11 March). Plan your migration to Microsoft Sentinel. https://learn.microsoft.com/en-us/azure/sentinel/migration
- Hubbard,D. & Seiersen, R. (2023). *How to Measure Anything in Cybersecurity Risk*. John Wiley & Sons, Inc.
- People Centricity. Transforming Together Monthly, The Importance of Assessing Change Impacts. (2023, 9 August). https://www.linkedin.com/pulse/importance-assessing-change-impacts-people-centricity/

Contact Info:

Alissa Torres

atorres@sibertor.com

@sibertor