

Advancing detective controls and capabilities

CIO Leadership Academy
Applied Learning Project

Aldwin Maloto

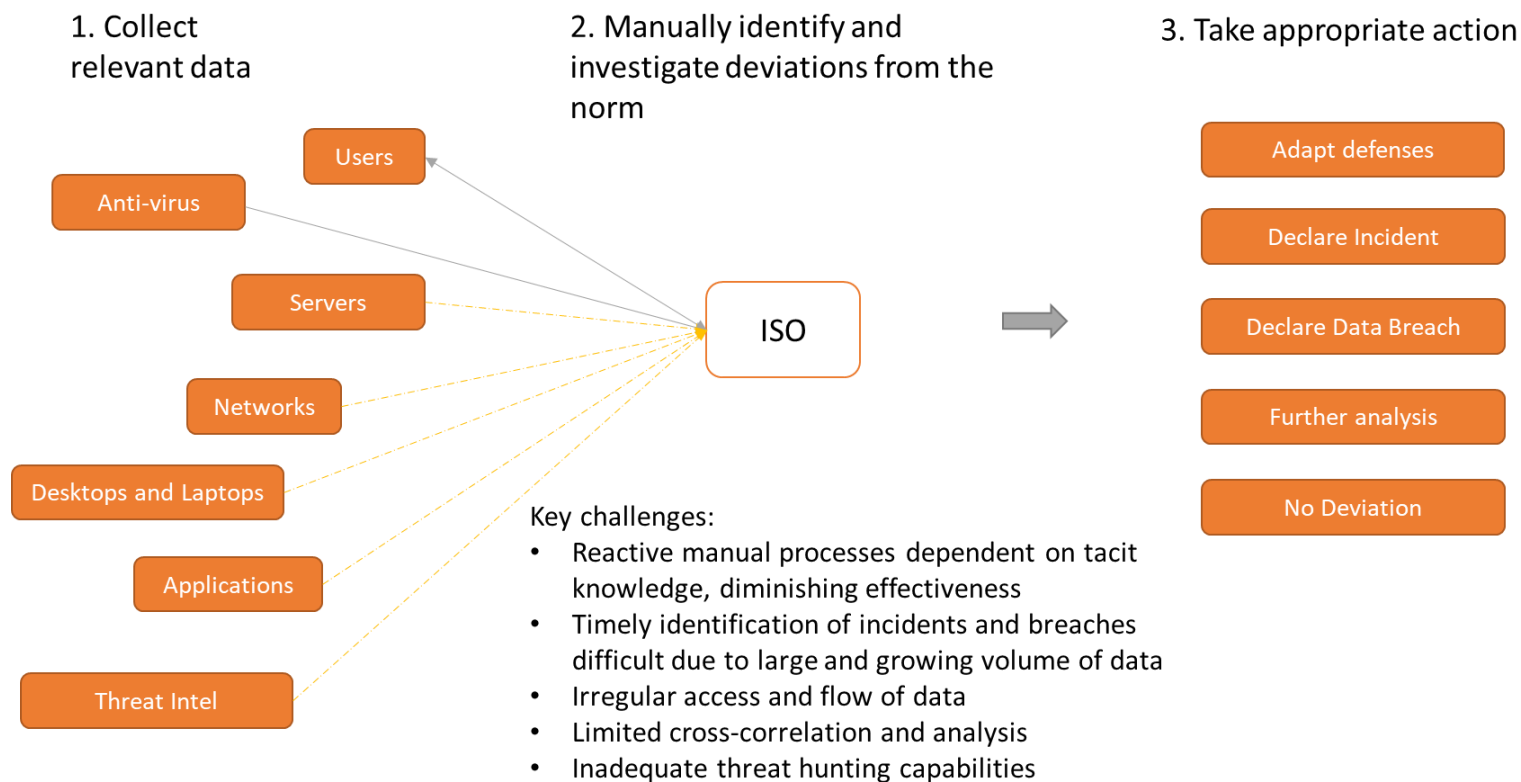
May 9, 2023



Problem statement:

Current detective controls and capabilities are lagging and do not fully support institutional needs

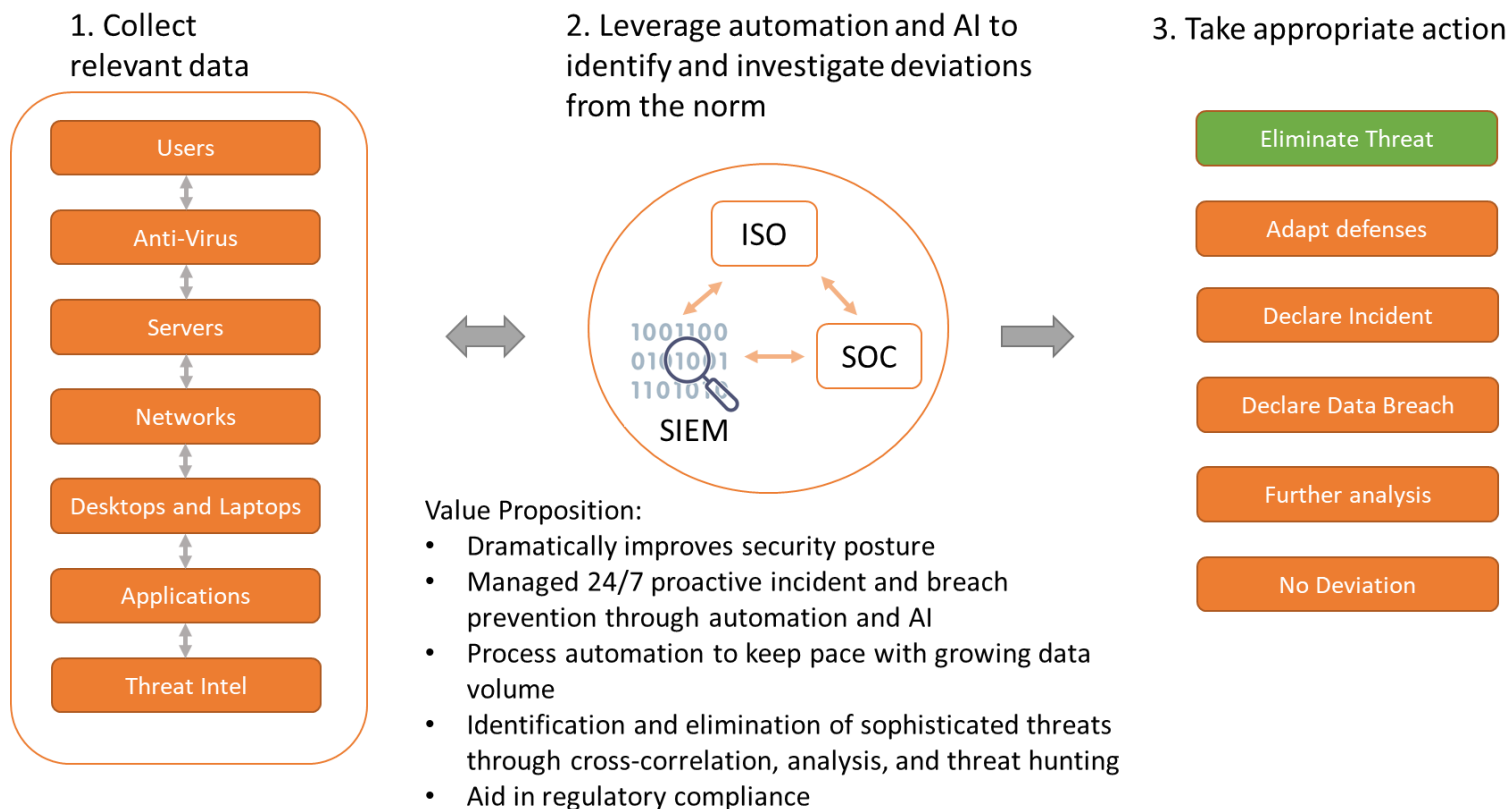
Current State:



Solution:

Advance detective controls and capabilities through the implementation of a managed next generation Security Information and Event Management (SIEM) Tool and Security Operations Center (SOC)

Desired State:



Stakeholders:

- **University Executive Leadership**
- **Sr. Leadership at Colleges and Business units**
- **Information and Technology Services**
- **Campus IT Administrators**
- **Information Security Office**
- **RIT Community**

Fostering Collaboration, Driving results



- **Creating and executing a shared vision**
- **Timeline**
- **Communication approach**
- **Collaboration tools**

Challenges

- **The Ask**
- **System owner buy-in**
- **Reporting limitations**
- **The second Ask**



Final Thoughts and Reflections

- **Trust is currency. Invest and build up your reserves**
- **Can't boil the ocean**
- **Have a good cat herder**

Questions?