Advancing detective controls and capabilities

CIO Leadership Academy
Applied Learning Project

Aldwin Maloto

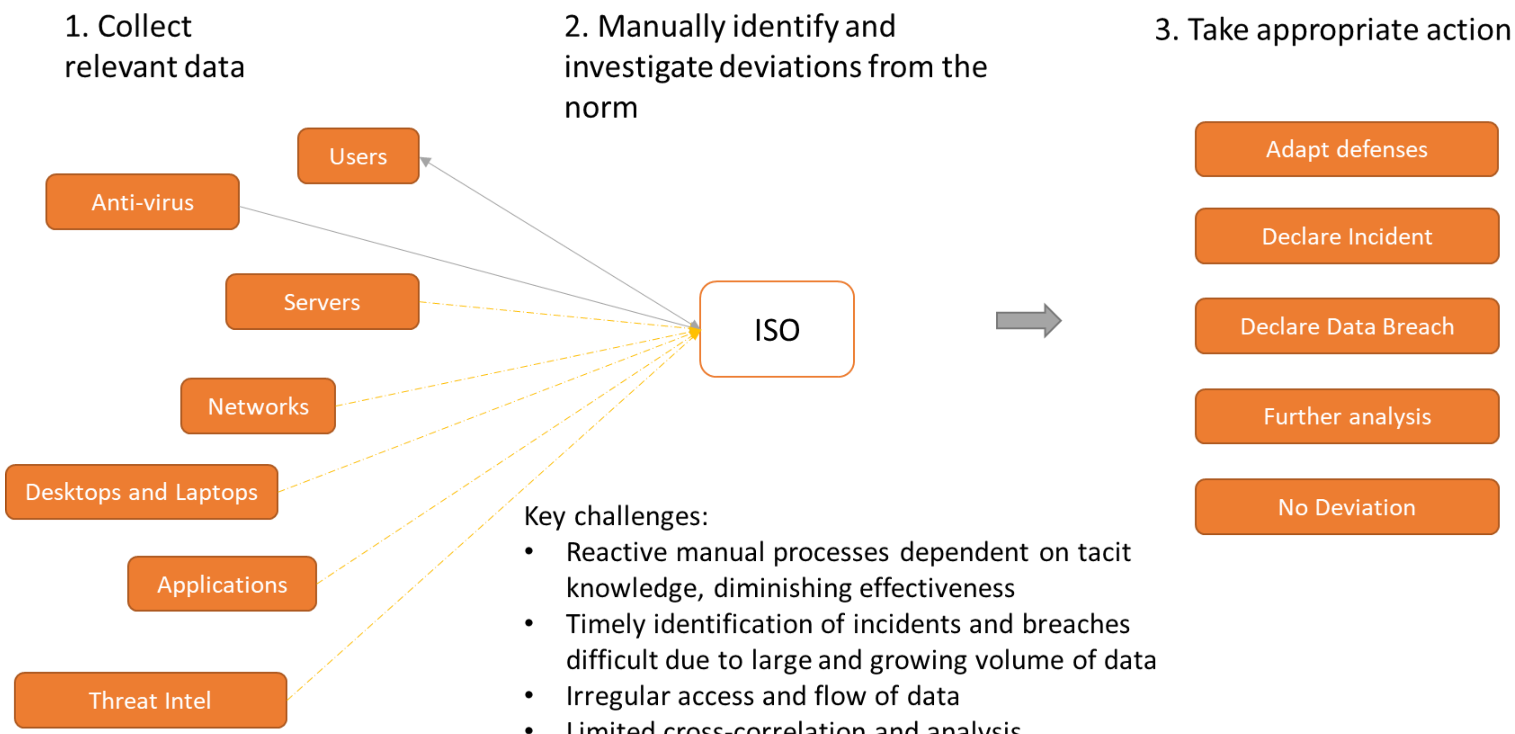
May 9, 2023

RIT

Problem statement:

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

Current State:



1. Collect relevant data

2. Manually identify and investigate deviations from the norm

3. Take appropriate action

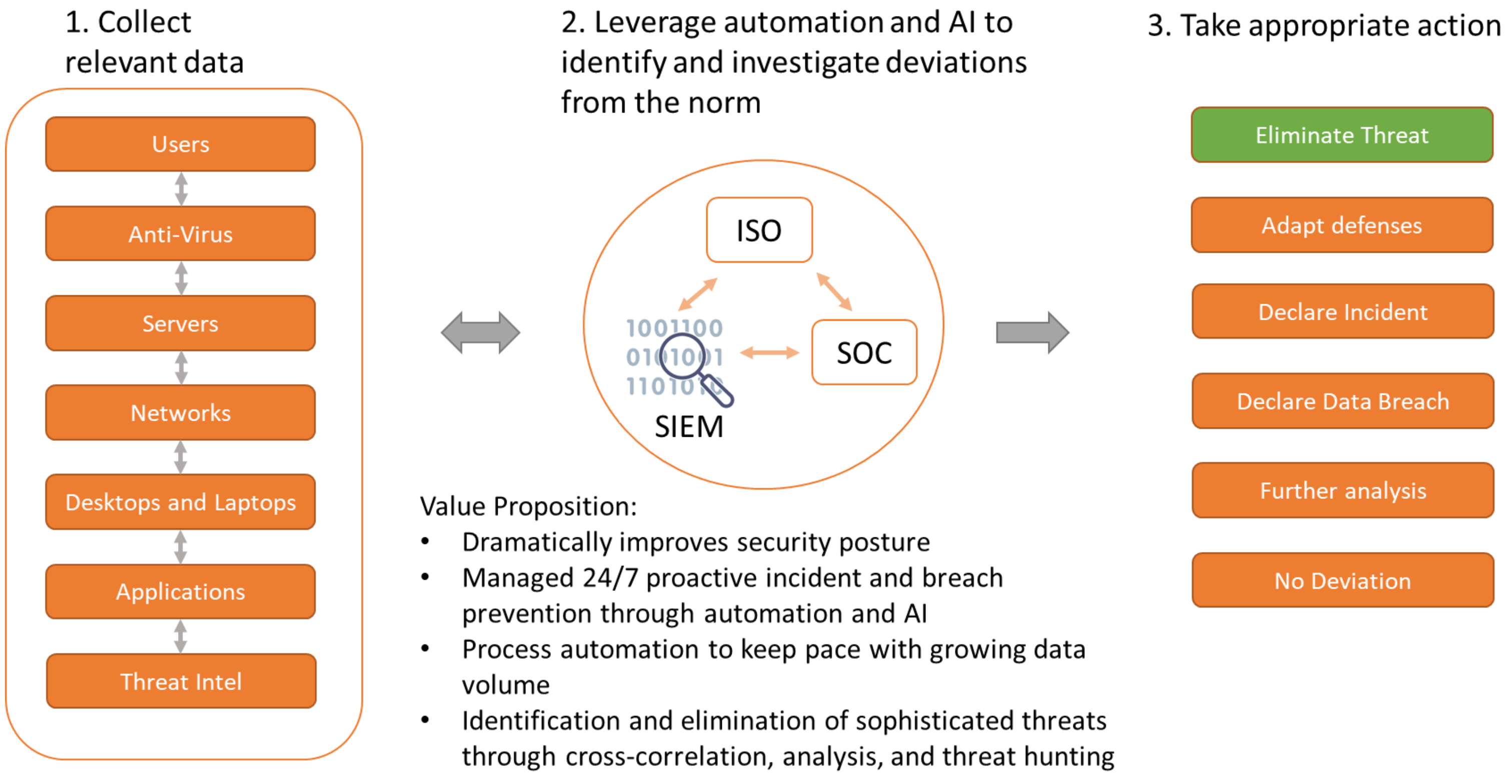
Key challenges:

- Reactive manual processes dependent on tacit knowledge, diminishing effectiveness
- Timely identification of incidents and breaches difficult due to large and growing volume of data
- Irregular access and flow of data
- Limited cross-correlation and analysis
- Inadequate threat hunting capabilities

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:



1. Collect relevant data

- Users
- Anti-Virus
- Servers
- Networks
- Desktops and Laptops
- Applications
- Threat Intel

2. Leverage automation and AI to identify and investigate deviations from the norm

3. Take appropriate action

- Eliminate Threat
- Adapt defenses
- Declare Incident
- Declare Data Breach
- Further analysis
- No Deviation

Value Proposition:

- Dramatically improves security posture
- Managed 24/7 proactive incident and breach prevention through automation and AI
- Process automation to keep pace with growing data volume
- Identification and elimination of sophisticated threats through cross-correlation, analysis, and threat hunting
- Aid in regulatory compliance

Stakeholders:

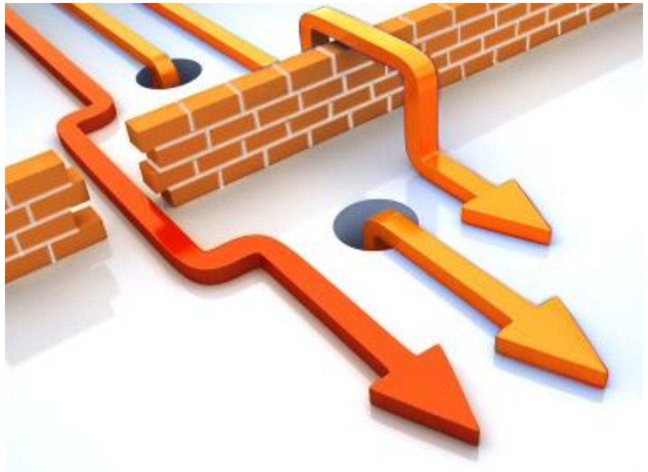
- University Executive Leadership
- Sr. Leadership at Colleges and Business units
- Information and Technology Services
- Campus IT Administrators
- Information Security Office
- RIT Community

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?