AUBURN

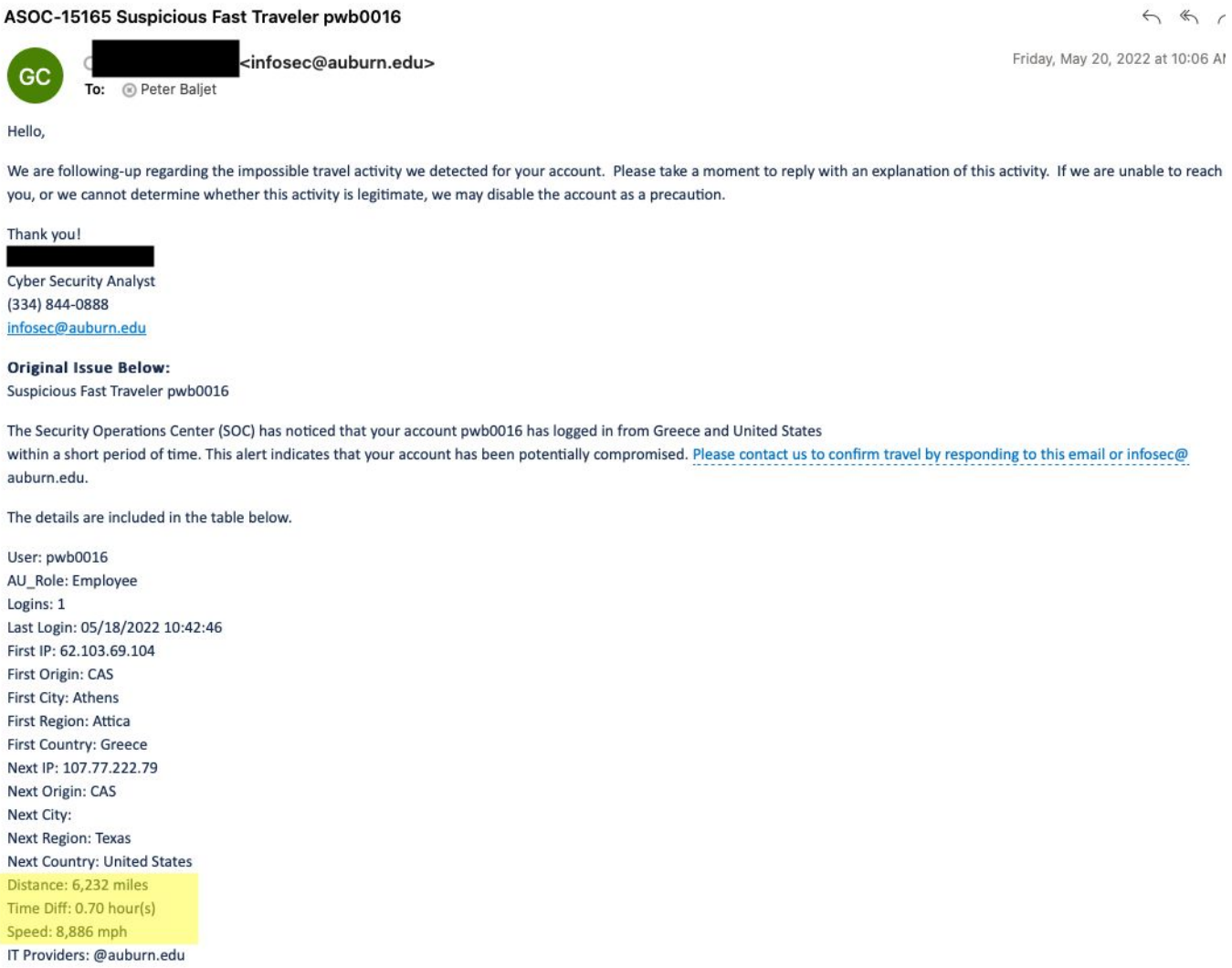
Security Logging & SIEM

Industry Drivers for Better Logging

AUBURN

- Rise in data breaches due to internal and external threats
- Rise in IT landscape spreading across traditional and cloud based infrastructure
- Attackers are smart and independent security tools are difficult to manage
- Faster detection and response to attacks and breaches
- Manage aggregating volumes of logs from multiple sources
- Meet stringent compliance requirements for auditing and non-repudiation

Security Operations Center



ASOC-15165 Suspicious Fast Traveler pwb0016

GC [redacted]<infosec@auburn.edu>

Friday, May 20, 2022 at 10:06 AM

To: Peter Baljet

Hello,

We are following-up regarding the impossible travel activity we detected for your account. Please take a moment to reply with an explanation of this activity. If we are unable to reach you, or we cannot determine whether this activity is legitimate, we may disable the account as a precaution.

Thank you!

[redacted]
Cyber Security Analyst
(334) 844-0888
infosec@auburn.edu

Original Issue Below:
Suspicious Fast Traveler pwb0016

The Security Operations Center (SOC) has noticed that your account pwb0016 has logged in from Greece and United States within a short period of time. This alert indicates that your account has been potentially compromised. Please contact us to confirm travel by responding to this email or infosec@auburn.edu.

The details are included in the table below.

User: pwb0016
AU_Role: Employee
Logins: 1
Last Login: 05/18/2022 10:42:46
First IP: 62.103.69.104
First Origin: CAS
First City: Athens
First Region: Attica
First Country: Greece
Next IP: 107.77.222.79
Next Origin: CAS
Next City:
Next Region: Texas
Next Country: United States
Distance: 6,232 miles
Time Diff: 0.70 hour(s)
Speed: 8,886 mph
IT Providers: @auburn.edu

SIEM Tools

AUBURN

- SIEM - “Security Information and Event Management”
  - Gathering, analyzing and presenting information from technology infrastructure and identity and access management applications.
- Two main capabilities
  - **Security Information Management** - collecting of security related information from a variety of IT infrastructure sources.
  - **Security Event Management -** Events generated based up executing business rules, artificial intelligence, or monitoring dashboards.
- Key Objectives
  - Collect audit logs for security and compliance
  - Identify threats and possible breaches
  - Conduct investigations and provide evidence

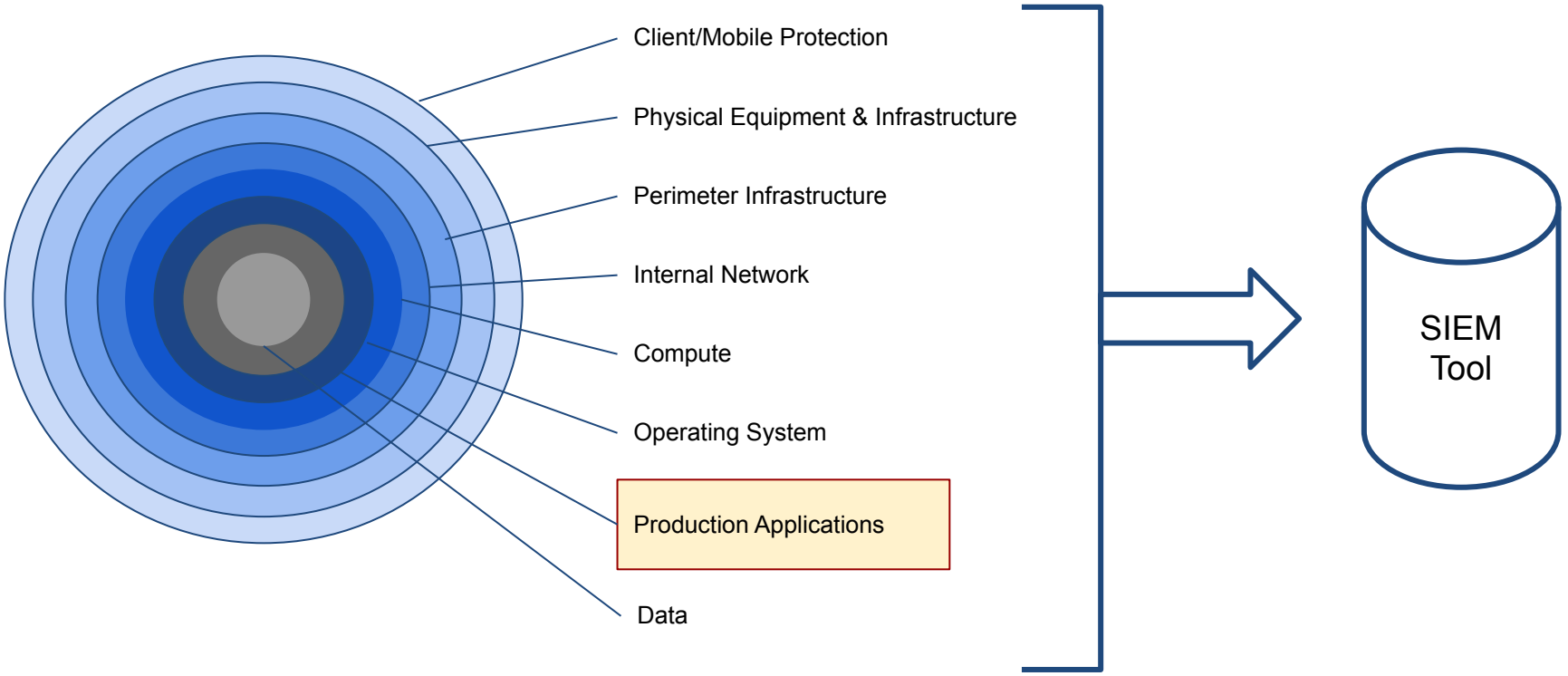
SIEM Tools

AUBURN

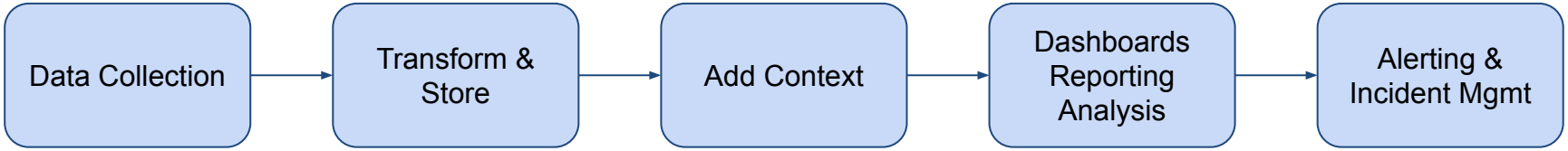
- Typically incorporates a **Log Management** tool
  - Handles large volumes of typically text based log messages. Examples are a access logs, audit records, audit trails, event-logs, etc.
  - Capabilities are log ingestion, centralized storage & compression, data life cycle, log search, categorization, and reporting.

- Used by Security Operations Centers (SOC)

Logs Generated from a IT Infrastructure



SIEM Process Flow



- Application
- Geo Location
- User Details
- Data Details

SIEM Key Capabilities

AUBURN

- **Centralized Log Collection**
- **Real Time Event Correlation**
  - Proactively addressing threads based on rules or AI across system components
- **User Activity Monitoring**
  - Both human and API access (system to system)
- **Log Retention**
  - Non-repudiation - logs can not be tampered with
- **IT Compliance Reports**
  - Need for reports such as PCI DSS, FISMA, SOC2, HIPAA
- **Change Management Integrity**
  - files, applications, infrastructure; send alerts when system changed or accessed
- **Log Forensics**
  - Track down attackers or determine impact of a breach
- **Dashboards**
  - Present data in a human readable format.

AUBURN UNIVERSITY