SWANO

Plot your course

2023 Annual Conference

INFORMATION SECURITY IN LIBRARIES

IAN NOSEK, IT & SYSTEMS SUPPORT MANAGER

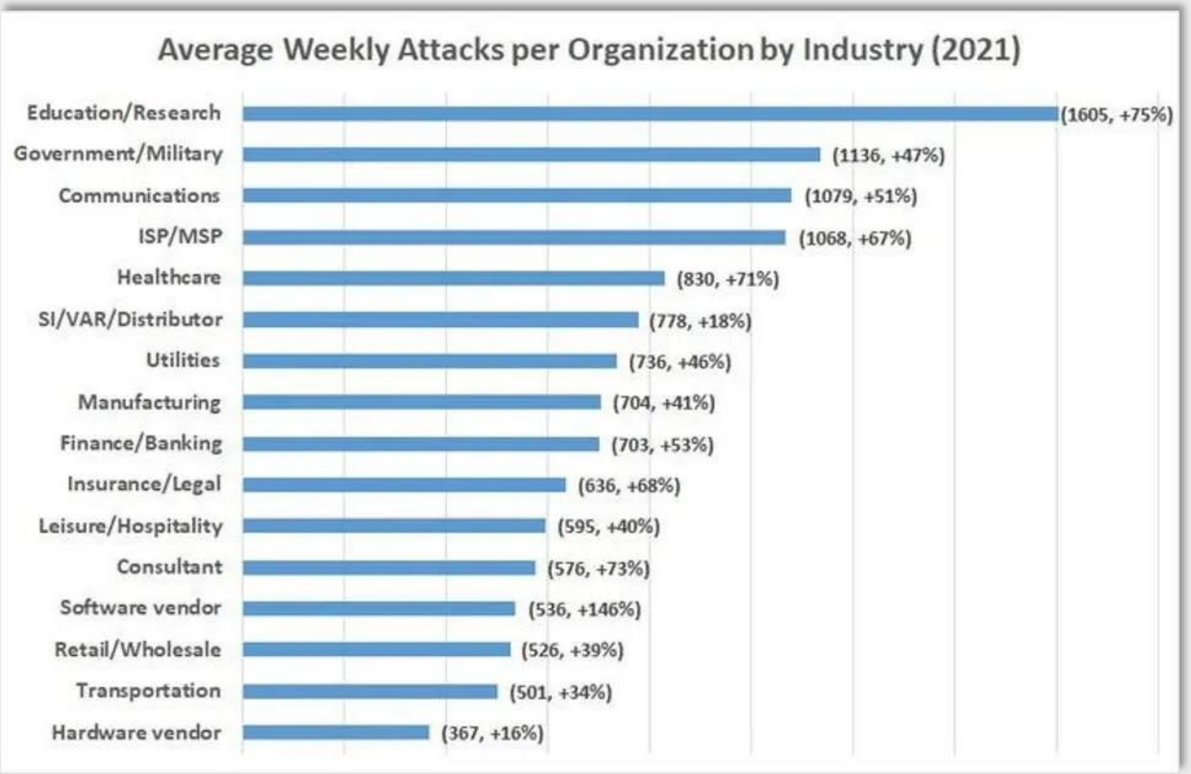
CRYSTAL VELA, UX CONSULTANT

VICKIE TOTTON, IT & SYSTEMS SUPPORT CONSULTANT

AHREN SIEVERS, SYSTEMS ADMINISTRATOR – IT & SYSTEMS SUPPORT

CYBERCRIME TRENDS

- Global cybercrime has increased over 400% since 2019
- 90% of attacks are targeted at employees, not technology
- 82% of attacks involve social engineering or phishing techniques
- 80% of data breaches involve exposure of PII
- Personally Identifiable Information: any data that could potentially identify an individual



HOW DOES SWAN SECURE ACCESS TO OUR SERVERS?

- Firewall rules limit access to SWAN Symphony server
- Library connections are encrypted through use Virtual Private Network (VPNs)
  - These connections protect all data transmitted between library and SWAN
- Vendors must sign off on SWAN’s Vendor Access Policy before onboarding begins
- Vendor IP addresses must be whitelisted before connection can be made
- Unless explicitly required for functionality, vendors have Read Only access

HOW IS SWAN PROTECTING THE DATA ON OUR SERVERS?

- Migration of external SIP2 connections to encrypted TLS-SIP2
- Extracts and other data transmitted to vendors via SFTP
- Regularly scheduled database maintenance and patron data removal
- Patron’s reading history not visible to staff in Aspen while using Masquerade Mode
- BCA reports are scrubbed of PII or password protected if PII exists
- Patron PINs masked in system

SECURING SIP2 WITH TLS

- SIP2 is an industry standard for passing transactional data between server and client
- SIP2 data is passed in plaintext, potentially exposing Personally Identifiable Information
- Transport Layer Security (TLS) is an encryption method requiring the use of a key-pair to decrypt data
- TLS-SIP2 encrypts SIP2 data, rendering it unreadable without matching security key
- Libby, Hoopla, Kanopy, MeeScan, and several other vendors currently using TLS-SIP2 connections

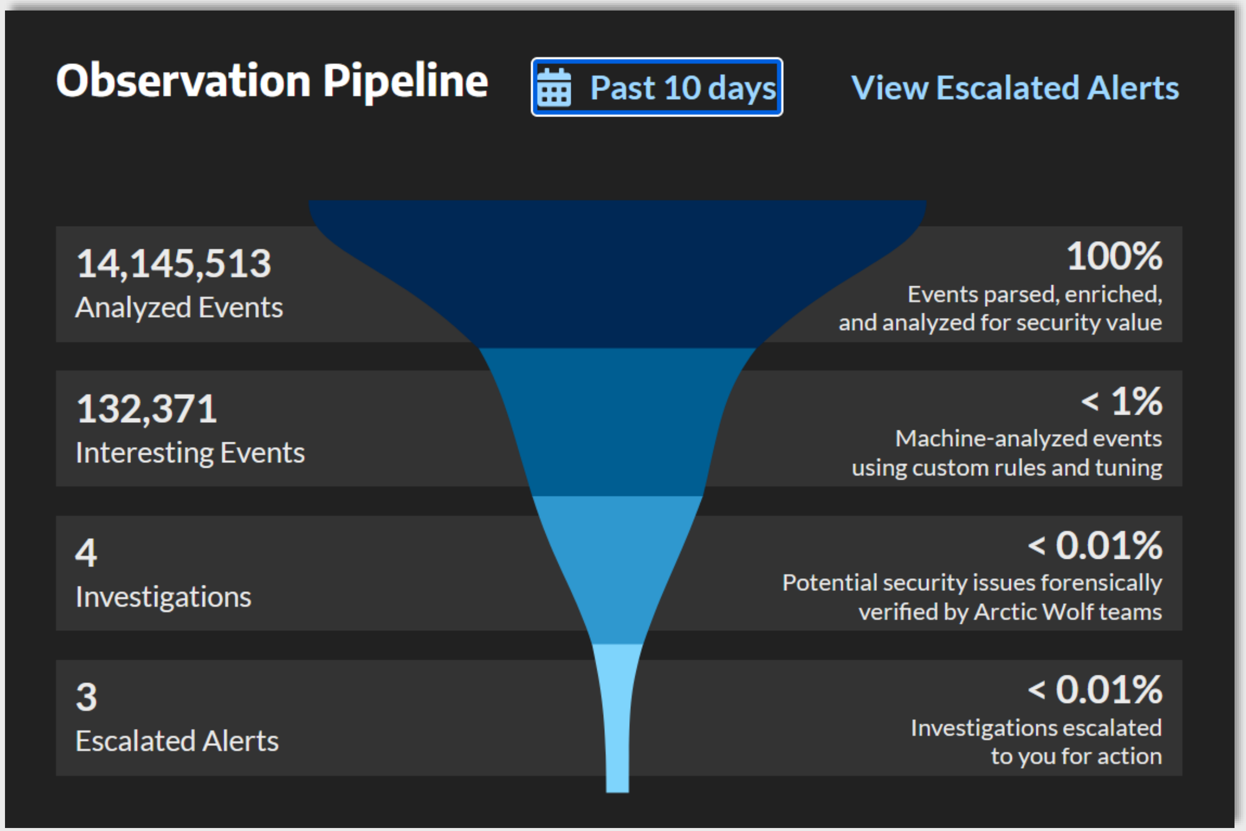
```
AOWMS|AA21140003533188|AENOSEK,IAN|
AQSWS|BZ0075|CA0000|CB0200|BLY| BV15.00
|BD800 QUAIL RIDGE DR WESTMONT IL 60559-6149
|BEian@swanlibraries.net|BHUSD|PD19830618|
PCSWS_STAFF|PEMALE|PFADULT|PG
```

PII Exposed:

- Name
- Gender
- Birthdate
- Home Address
- Email Address
- Barcode/PIN

MANAGED DETECTION AND RESPONSE

- Managed Detection and Response (MDR)
  - 24x7 Cloud, network & endpoint monitoring
  - Dedicated security team investigates and alerts us to incidents and helps with remediation and analysis.
- Managed Security Awareness
  - Phishing simulations
  - Interactive training sessions
- Incident Response JumpStart
  - Incident Response plan development assistance
  - Up to $1M in recovery funds following a breach



Observation Pipeline

14,145,513
Analyzed Events

100%
Events parsed, enriched, and analyzed for security value

132,371
Interesting Events

< 1%
Machine-analyzed events using custom rules and tuning

4
Investigations

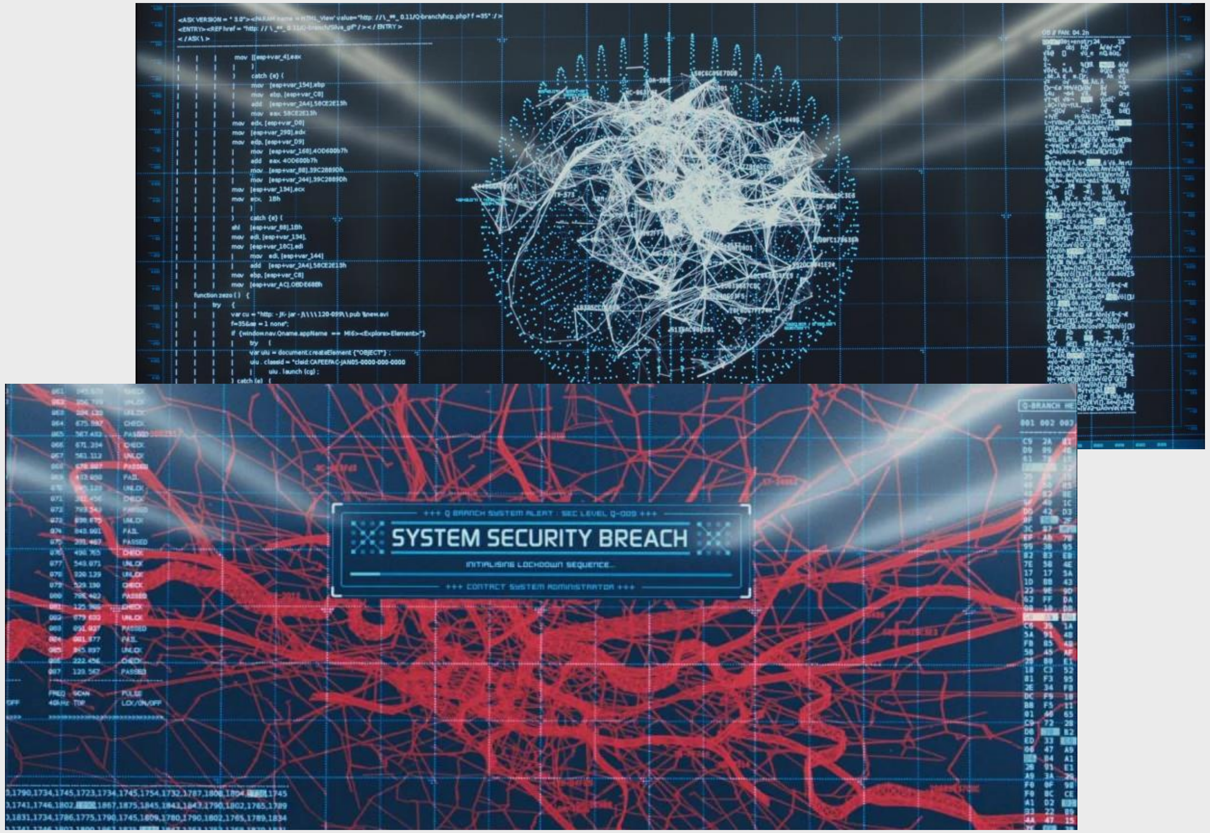
< 0.01%
Potential security issues forensically verified by Arctic Wolf teams

3
Escalated Alerts

< 0.01%
Investigations escalated to you for action

MANAGED DETECTION AND RESPONSE

- Detection
  - Movies vs. Reality
  - Combing through logs is tedious.
    - Typically only happens *after* a breach or incident.
  - Reactive
    - IT only looks through logs when there’s an issue.
- Response
  - Proactive
    - Logs are constantly being ingested and scanned.
  - Zeroes us in on the exact nature of the issue with less hunting through various systems and scrolling through log files.
  - Recent Example


+++ Q BRANCH SYSTEM ALERT · SEC LEVEL Q-005 +++
SYSTEM SECURITY BREACH
INITIALISING LOCKDOWN SEQUENCE...
+++ CONTACT SYSTEM ADMINISTRATOR +++

PROTECTING PATRON PRIVACY ON THE FRONT LINES

How would you help a patron at the desk without a library card?

- Ask for photo ID
- Photographs in a patron record to ensure identity
- Ask patron to write down address, email, birthdate & shred paper

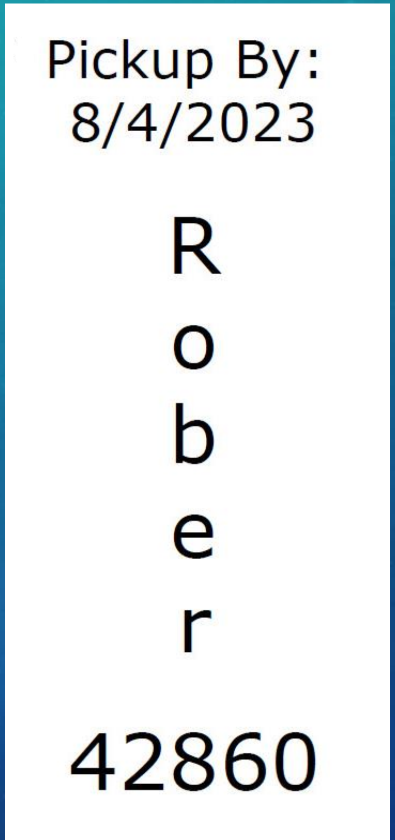
How would you help a patron with their PIN?

- Keypad for patron to enter PIN
- At registration enter last 4 digits of phone number and urge the patron to change it in Aspen
- Assist patron at a public OPAC in resetting/changing PIN

PROTECTING PATRON PRIVACY ON THE FRONT LINES

How do you protect your patrons hold information?

- Closed hold shelf
- Hold wrappers do not have full name or card number
- Flip item so spine is not face out.



Pickup By:
8/4/2023

R
o
b
e
r

42860

Pro Tip!

Do not leave title information in a voicemail

HOW CAN YOU HELP?

- Subscribe to SWANcom for important announcements and communications!
- Update passwords on a regular basis
  - Follow Managing Passwords & Logins guidelines
  - Use a password manager tool if possible
- Submitting support tickets with SWAN
  - Do **not** include PII or passwords in tickets!
  - Edit screenshots to redact sensitive information

HOW CAN YOU HELP?

- Password protect BLUEcloud Analytics report subscriptions if they contain PII
- Enable PIN for 3rd party vendor connections
  - Self-Check
  - Scheduling Software
- Limit the PII collected and retained
  - Do not use open forms for collection, e.g. Google Forms
  - Create a retention policy and delete files
    - Self-Check Logs
    - Scheduling Software

OTHER WAYS TO PROTECT ACCESS TO INFORMATION

Open a support ticket when offboarding library staff. SWAN can help!

What is included in SWAN offboarding?

- Reset passwords in
  - WorkFlows
  - BLUEcloud Analytics
- Unsubscribe from
  - SWANcom
  - The Current
- Remove access to
  - SWAN support site
  - SWAN Community Forums (posts remain)
  - SWAN Online Learning

ANY QUESTIONS?

Contacting SWAN Support:
Email: help@swanlibraries.net
Phone: 844.SWANLIB (844.792.6542)