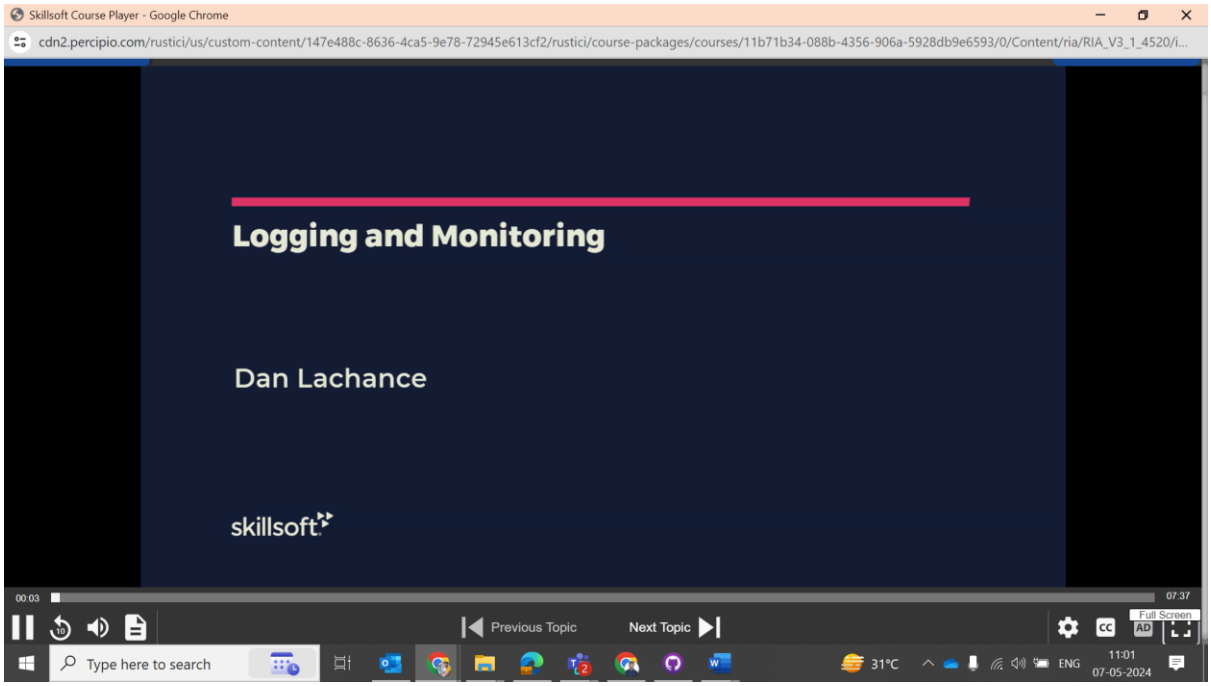

Skillsoft Course Player - Google Chrome
cdn2.percipio.com/rustici/us/custom-content/147e488c-8636-4ca5-9e78-72945e613cf2/rustici/course-packages/courses/11b71b34-088b-4356-906a-5928db9e6593/0/Content/ria/RIA_V3_1_4520/i...
Logging and Monitoring
Dan Lachance
skillsoft
00:03
07:37
Previous Topic
Next Topic
Full Screen
Type here to search
31°C
ENG
11:01
07-05-2024

Monitoring

Host Monitoring

- Bash/PowerShell script
  - Scheduled cron jobs
  - Windows task scheduler
  - Regular expression pattern matching
- Windows event viewer logs
  - Event severities
  - Event IDs
  - Log subscriptions
- Linux system logs
  - Syslog-ng log forwarding

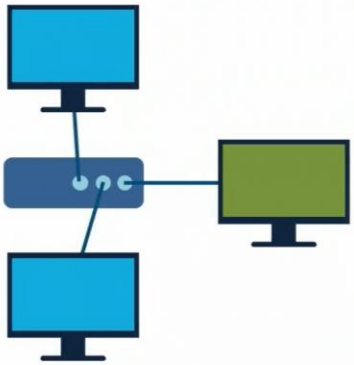
Device Monitoring

- HTTPS/SSH connectivity
- Network isolation
- SNMP v3
  - Encrypted
  - MIBs
  - Traps
  - Change community read/write strings

Application Monitoring

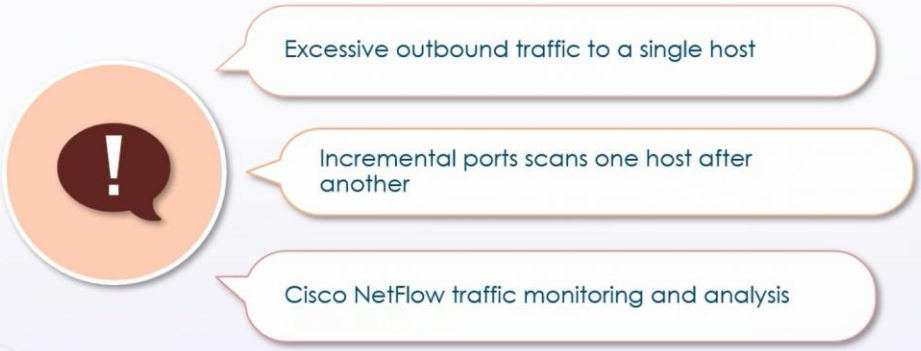
- Performance metrics
- App and web server Logs
- Unencrypted temporary index files for search
- Web Application Firewall (WAF) alerts
- Auditing alerts

Network Monitoring - SPAN Port Monitoring



- Packet sniffer station connected to switched port analyzer (SPAN) switch port
- All network traffic is visible

Common Network Traffic Analysis Security Indicators



Security Incident Detection and Response

Security Content Automation Protocol (SCAP)

Facilitates keeping up-to-date with everchanging cybersecurity threats

Automated

- Compare host/device/network security configuration against baselines
- Security policy compliance/violation
- Vulnerability management

Components

- SCAP content modules - NIST and other party acceptable security configurations (e.g. Federal Desktop Core Configuration)
- SCAP scanner - engine that compares security configurations against content modules

True and False Security Indicators

False positive

"There is malware on the system!"

It could be temporary app installation files, there really is no malware

True positive

"A network DDoS attack is in progress"

It is correct and is now happening

False negative

"The downloaded file is free from malware, no worries here."

The malware might use obfuscation or directive name replacement to prevent malware alerts

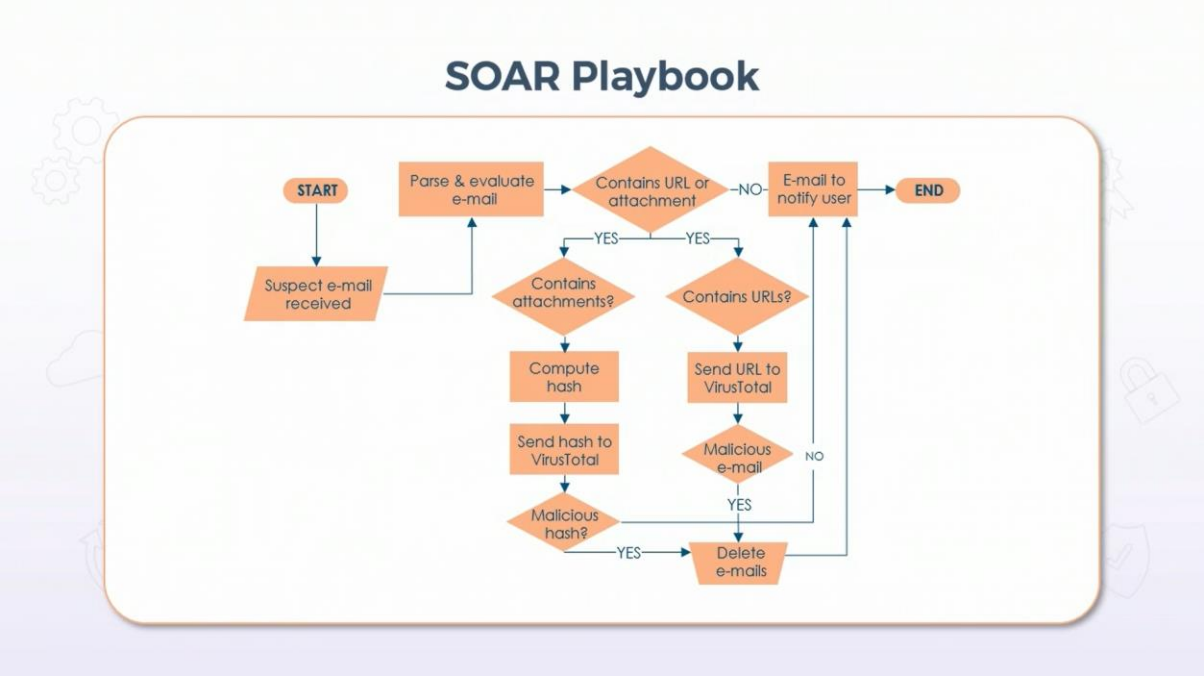
True negative

"Network traffic volume looks normal, no problem here."

Activity is determined to be acceptable, and it truly is

Security Information and Event Management (SIEM)

Security Orchestration, Automation and Response (SOAR)



Mitigating Monitoring Deficiencies

Dan Lachance

skillsoft

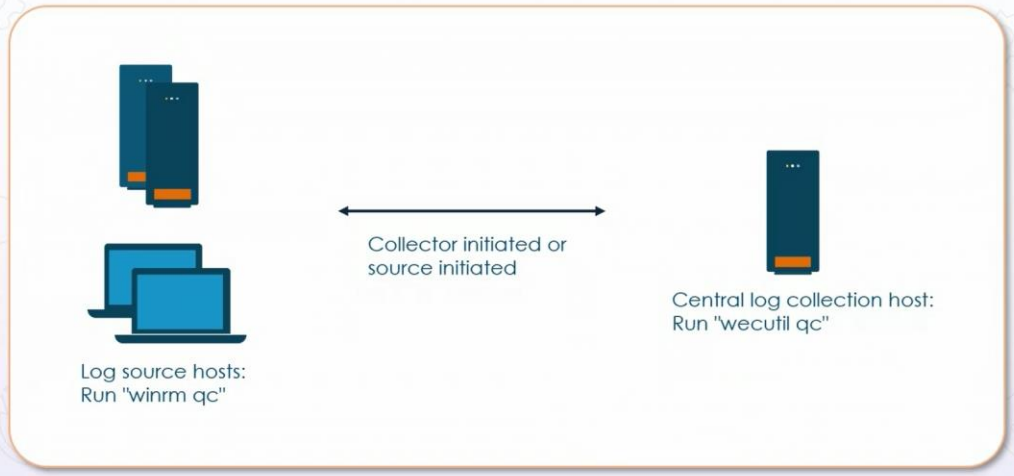
Mitigating Monitoring Deficiencies

You can't secure what you don't know about

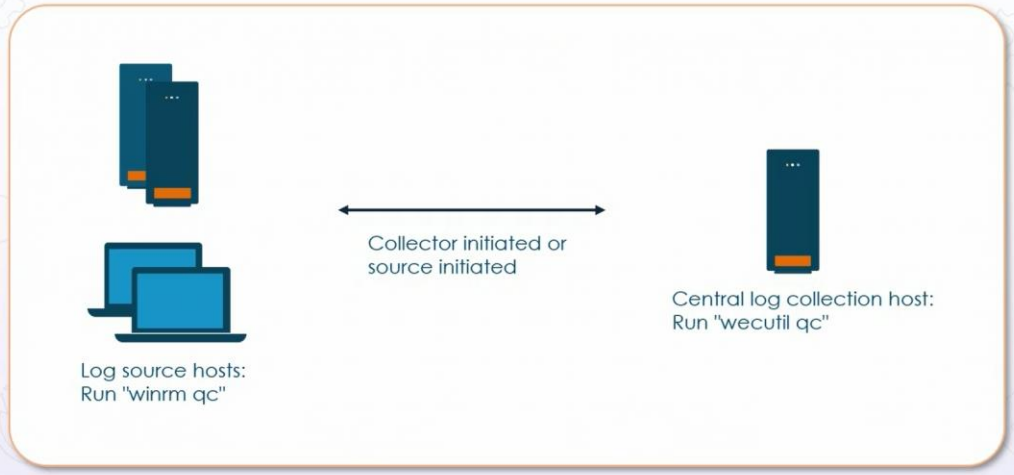
Log Forwarding

- **Sends a copy of some or all log events to a different logging host**
- **Commonly used for honeypots**
- **Should be used for everything**
  - User stations
  - Servers
  - Network infrastructure devices
  - Web servers
  - Specific web applications

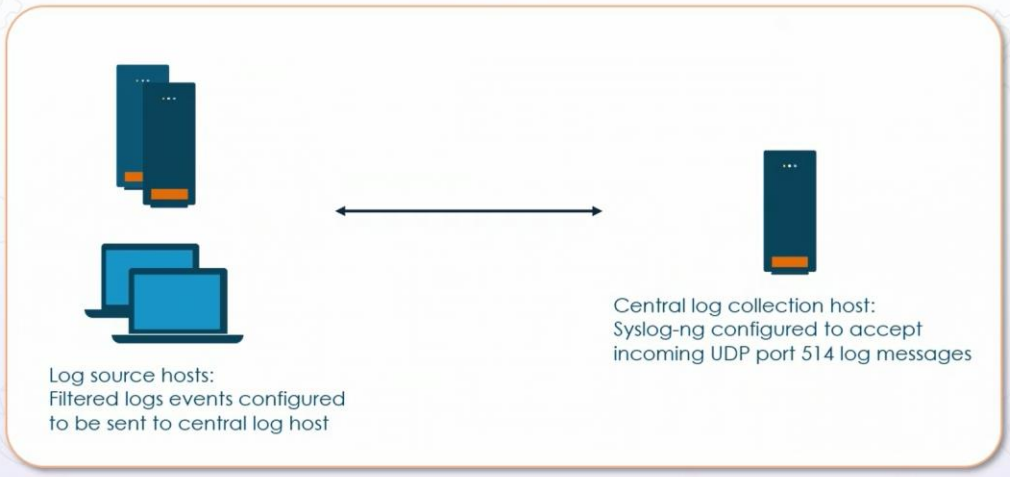
Windows Log Forwarding - Event Subscriptions



Windows Log Forwarding - Event Subscriptions



Linux Syslog Forwarding



Centralize Log and Activity Collection

- Sources
  - Intrusion detection and prevention sensors
  - Network traffic analyzers
- Target
  - SIEM and SOAR solutions using machine learning (ML) algorithms for threat detection

Timely Event Notification

Notification via SMS, e-mail, phone call

Potentially stop attacks in progress

Centralized SIEM and SOAR solutions can reduce incident response time