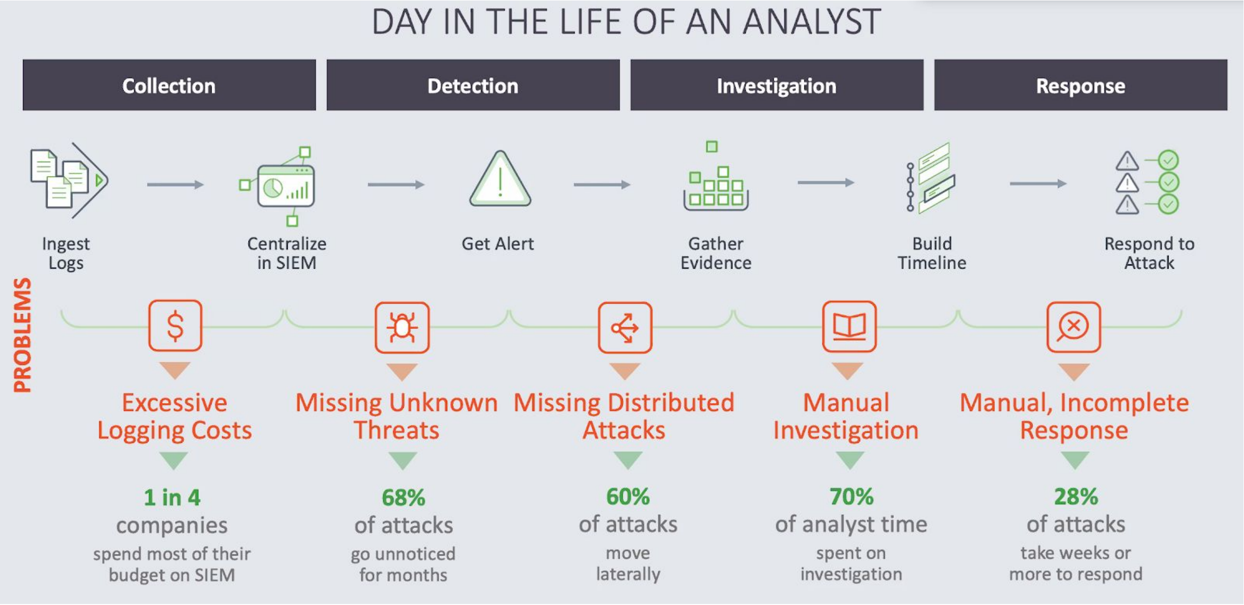
COMP 6448 - Week 8

Security Engineering Masterclass

Life of an analyst:

- Excessive logging costs. Most companies spend their budget on SIEM
- Lots of threats tend to go unnoticed for months.
- 60% of attacks move laterally.
- Analysts spend most of their time doing manual investigation on attacks.



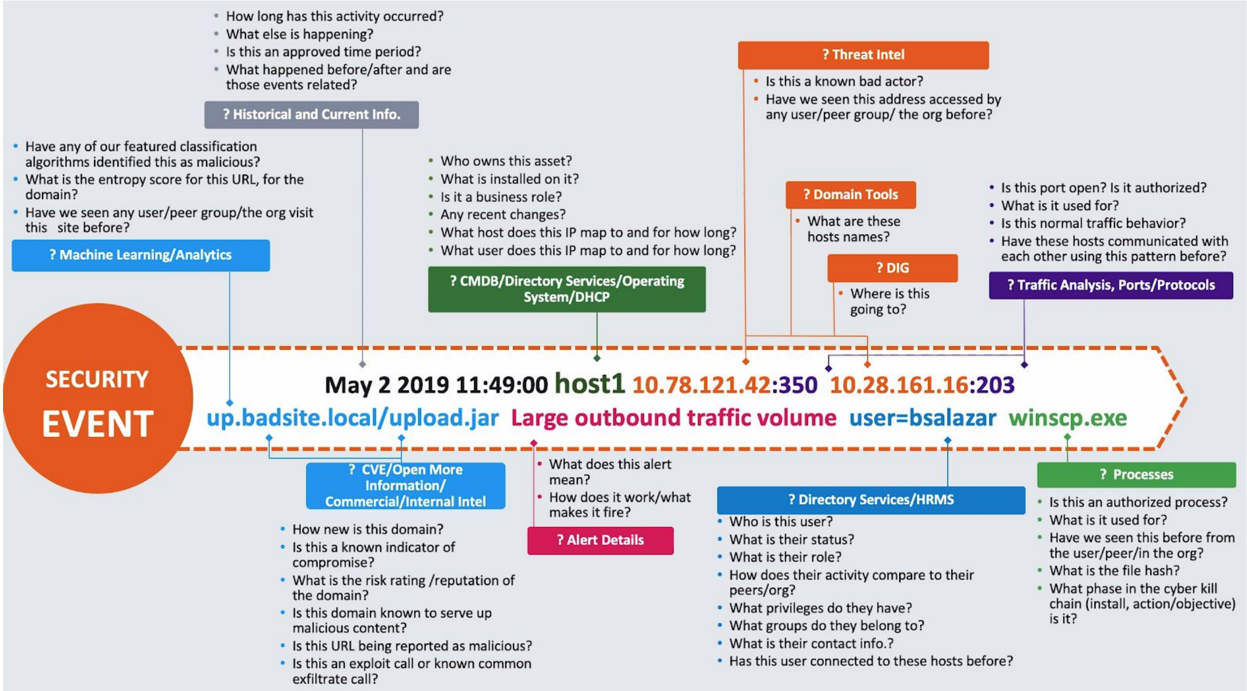
DAY IN THE LIFE OF AN ANALYST

Collection | Detection | Investigation | Response

Ingest Logs → Centralize in SIEM → Get Alert → Gather Evidence → Build Timeline → Respond to Attack

PROBLEMS

- Excessive Logging Costs — **1 in 4** companies spend most of their budget on SIEM
- Missing Unknown Threats — **68%** of attacks go unnoticed for months
- Missing Distributed Attacks — **60%** of attacks move laterally
- Manual Investigation — **70%** of analyst time spent on investigation
- Manual, Incomplete Response — **28%** of attacks take weeks or more to respond



SECURITY EVENT

May 2 2019 11:49:00 host1 10.78.121.42:350 10.28.161.16:203
up.badsite.local/upload.jar Large outbound traffic volume user=bsalazar winscp.exe

? Historical and Current Info.
- How long has this activity occurred?
- What else is happening?
- Is this an approved time period?
- What happened before/after and are those events related?

? Machine Learning/Analytics
- Have any of our featured classification algorithms identified this as malicious?
- What is the entropy score for this URL, for the domain?
- Have we seen any user/peer group/the org visit this site before?

? CMDB/Directory Services/Operating System/DHCP
- Who owns this asset?
- What is installed on it?
- Is it a business role?
- Any recent changes?
- What host does this IP map to and for how long?
- What user does this IP map to and for how long?

? Threat Intel
- Is this a known bad actor?
- Have we seen this address accessed by any user/peer group/ the org before?

? Domain Tools
- What are these hosts names?

? DIG
- Where is this going to?

? Traffic Analysis, Ports/Protocols
- Is this port open? Is it authorized?
- What is it used for?
- Is this normal traffic behavior?
- Have these hosts communicated with each other using this pattern before?

? CVE/Open More Information/ Commercial/Internal Intel
- How new is this domain?
- Is this a known indicator of compromise?
- What is the risk rating /reputation of the domain?
- Is this domain known to serve up malicious content?
- Is this URL being reported as malicious?
- Is this an exploit call or known common exfiltrate call?

? Alert Details
- What does this alert mean?
- How does it work/what makes it fire?

? Directory Services/HRMS
- Who is this user?
- What is their status?
- What is their role?
- How does their activity compare to their peers/org?
- What privileges do they have?
- What groups do they belong to?
- What is their contact info.?
- Has this user connected to these hosts before?

? Processes
- Is this an authorized process?
- What is it used for?
- Have we seen this before from the user/peer/in the org?
- What is the file hash?
- What phase in the cyber kill chain (install, action/objective) is it?

SIEM Capabilities:

- Collection:
    - Gather log information
- Operation

    - Compliance
    - Investigations
- Analysis
    - Gather different log sources and analyse

Entity Behaviour Analytics:

- Baseline typical users and analyse normal activity.
- E.g. looking at email activity, vpn activity, file activity.

Looking for anomalies (not correlations):

- Look for abnormalities by group and country
- E.g. It might be normal to interact with Chinese or Russian entities if from marketing.
- Look for sessions, not events

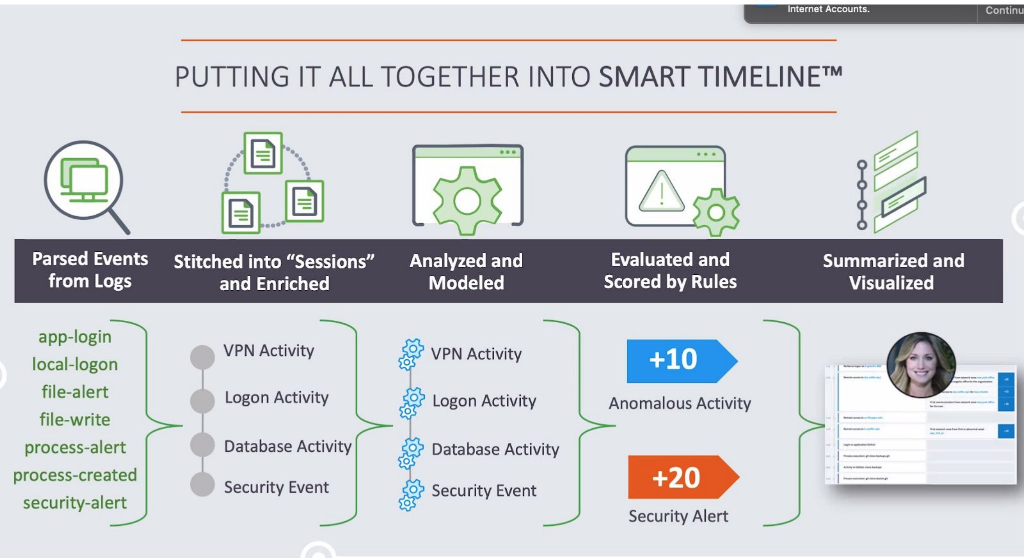
Typical anomalies and alerts:

- Suspicious logon. E.g. suspicious logon from abnormal country, strange time of day or network.
- Abnormal amounts of data uploaded
- Security alerts from symantec
- First account management activity.
- Abnormal file access for group
- Abnormal VPN location.

Advanced Analytics:

- Advanced analytics engines take infrastructure, activity and security logs with contextual data to create a smart timeline.
- Contextual info: e.g. who their manager and coworker are.
- Logs → Events → Sessions → Models → Rules
    - Events are normalized from logs. Extracting user/host info, alert ID, IP addresses etc
    - Events are stitched into a daily session
    - Sessions are modelled for baselining users/entities
    - Rules:
        - E.g. Black and white rules: is this website malicious?
        - Anomalous behaviour.
- Sessions:
    - Can start with an event: e.g. logon, vpn access, entering the building (ID cards)
    - Finishes at the end of the day or four hours of inactivity, or vpn logout.
- Models:
    - Can take around 4-6 weeks
    - Three types:
        - Numerical
            - Gamma distribution
            - E.g. amount of email sent on a daily basis
        - Time of week: Numerical clusters to time
            - E.g. login times
        - Categorical: for string data

        - E.g. collecting data for countries from which a user connects to vpn
    - Models can be represented visually with histograms.
    - Rules are not triggered until a confidence level is given to that model.
- Risk scores:
    - Gather event data, mark as trigger anomalies and apply an anchor score. Use data science adjustments (bayesian scoring). The bayesian allows the AI to adapt to analysts' choices.
- Smart timeline:
    - Compile all of the above into a smart timeline.



Internet Accounts.

Continu

PUTTING IT ALL TOGETHER INTO SMART TIMELINE™

Parsed Events from Logs

Stitched into "Sessions" and Enriched

Analyzed and Modeled

Evaluated and Scored by Rules

Summarized and Visualized

app-login
local-logon
file-alert
file-write
process-alert
process-created
security-alert

VPN Activity
Logon Activity
Database Activity
Security Event

VPN Activity
Logon Activity
Database Activity
Security Event

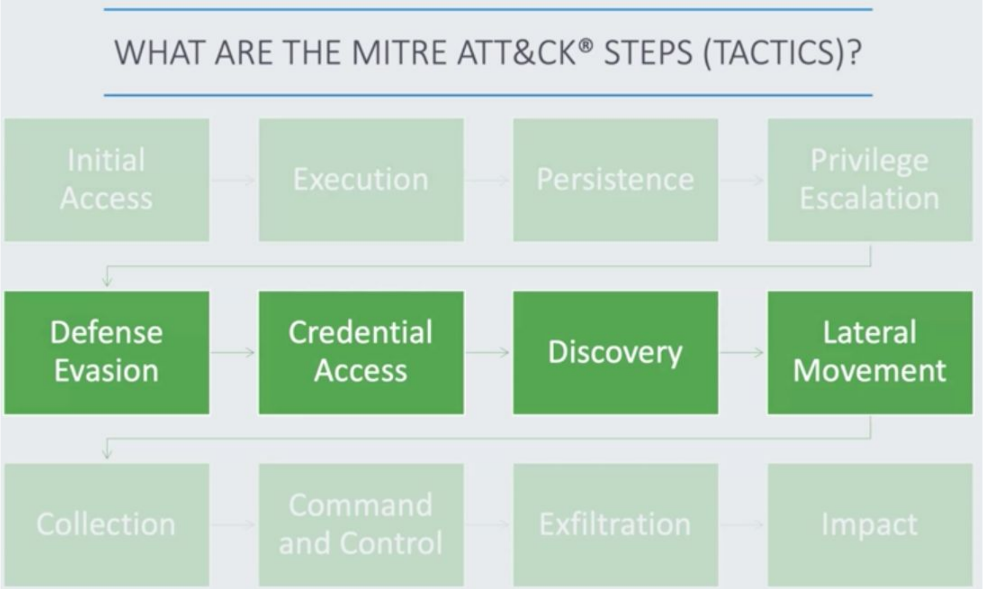
+10
Anomalous Activity

+20
Security Alert

Models and Frameworks:

- ATtack is useful because:
    - It provides common vocab
    - Red team testing
    - Labelling intel
    - Team testing and assessment
- Mitre:
- ATT&CK: Tactics, techniques and common knowledge

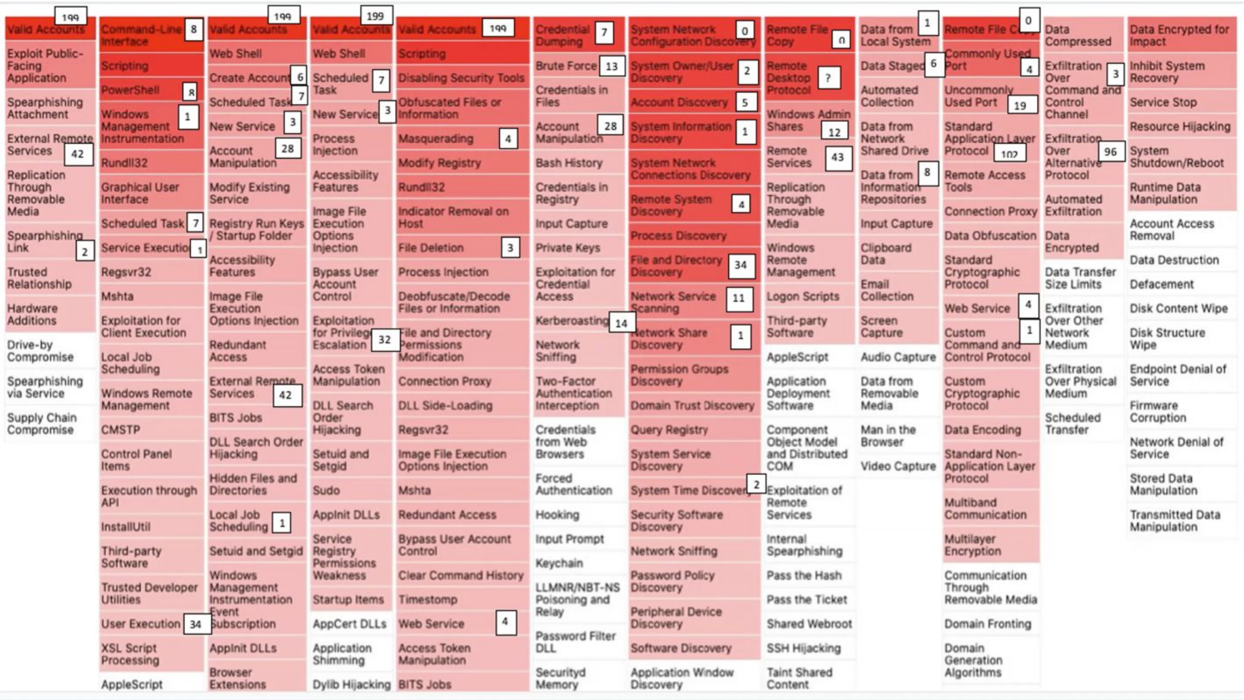
Mitre Tactic Steps:



WHAT ARE THE MITRE ATT&CK® STEPS (TACTICS)?

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

The dark red indicates that these vulnerabilities are common out in the wild. See Charles' attachment.



Valid Accounts 199
Exploit Public-Facing Application
Spearphishing Attachment
External Remote Services 42
Replication Through Removable Media
Spearphishing Link 2
Trusted Relationship
Hardware Additions
Drive-by Compromise
Spearphishing via Service
Supply Chain Compromise

Command-Line Interface 8
Scripting
PowerShell 8
Windows Management Instrumentation 1
Rundll32
Graphical User Interface
Scheduled Task 7
Service Executio 1
Regsvr32
Mshta
Exploitation for Client Execution
Local Job Scheduling
Windows Remote Management
CMSTP
Control Panel Items
Execution through API
InstallUtil
Third-party Software
Trusted Developer Utilities
User Execution 34
XSL Script Processing
AppleScript

Valid Accounts 199
Web Shell
Create Account 6
Scheduled Task 7
New Service 3
Account Manipulation 28
Modify Existing Service
Registry Run Keys / Startup Folder
Accessibility Features
Image File Execution Options Injection
Redundant Access
External Remote Services 42
BITS Jobs
DLL Search Order Hijacking
Hidden Files and Directories
Local Job Scheduling 1
Setuid and Setgid
Windows Management Instrumentation Event Subscription
AppInit DLLs
Browser Extensions

Valid Accounts 199
Web Shell
Scheduled Task 7
New Service 3
Process Injection
Accessibility Features
Image File Execution Options Injection
Bypass User Account Control
Exploitation for Privilege Escalation 32
Access Token Manipulation
DLL Search Order Hijacking
Setuid and Setgid
Sudo
AppInit DLLs
Service Registry Permissions Weakness
Startup Items
AppCert DLLs
Application Shimming
Dylib Hijacking

Valid Accounts 199
Scripting
Disabling Security Tools
Obfuscated Files or Information
Masquerading 4
Modify Registry
Rundll32
Indicator Removal on Host
File Deletion 3
Process Injection
Deobfuscate/Decode Files or Information
File and Directory Permissions Modification
Connection Proxy
DLL Side-Loading
Regsvr32
Image File Execution Options Injection
Mshta
Redundant Access
Bypass User Account Control
Clear Command History
Timestomp
Web Service 4
Access Token Manipulation
BITS Jobs

Credential Dumping 7
Brute Force 13
Credentials in Files
Account Manipulation 28
Bash History
Credentials in Registry
Input Capture
Private Keys
Exploitation for Credential Access
Kerberoasting 14
Network Sniffing
Two-Factor Authentication Interception
Credentials from Web Browsers
Forced Authentication
Hooking
Input Prompt
Keychain
LLMNR/NBT-NS Poisoning and Relay
Password Filter DLL
Securityd Memory

System Network Configuration Discovery 0
System Owner/User Discovery 2
Account Discovery 5
System Information Discovery 1
System Network Connections Discovery
Remote System Discovery 4
Process Discovery
File and Directory Discovery 34
Network Service Scanning 11
Network Share Discovery 1
Permission Groups Discovery
Domain Trust Discovery
Query Registry
System Service Discovery
System Time Discovery 2
Security Software Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Software Discovery
Application Window Discovery

Remote File Copy 0
Remote Desktop Protocol ?
Windows Admin Shares 12
Remote Services 43
Replication Through Removable Media
Windows Remote Management
Logon Scripts
Third-party Software
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Pass the Hash
Pass the Ticket
Shared Webroot
SSH Hijacking
Taint Shared Content

Data from Local System 1
Data Staged 6
Automated Collection
Data from Network Shared Drive
Data from Information Repositories 8
Input Capture
Clipboard Data
Email Collection
Screen Capture
Audio Capture
Data from Removable Media
Man in the Browser
Video Capture

Remote File C 0
Commonly Used Port 4
Uncommonly Used Port 19
Standard Application Layer Protocol 102
Remote Access Tools
Connection Proxy
Data Obfuscation
Standard Cryptographic Protocol
Web Service 4
Custom Command and Control Protocol 1
Custom Cryptographic Protocol
Data Encoding
Standard Non-Application Layer Protocol
Multiband Communication
Multilayer Encryption
Communication Through Removable Media
Domain Fronting
Domain Generation Algorithms

Data Compressed
Exfiltration Over Command and Control Channel 3
Exfiltration Over Alternative Protocol 96
Automated Exfiltration
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

Data Encrypted for Impact
Inhibit System Recovery
Service Stop
Resource Hijacking
System Shutdown/Reboot
Runtime Data Manipulation
Account Access Removal
Data Destruction
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Network Denial of Service
Stored Data Manipulation
Transmitted Data Manipulation