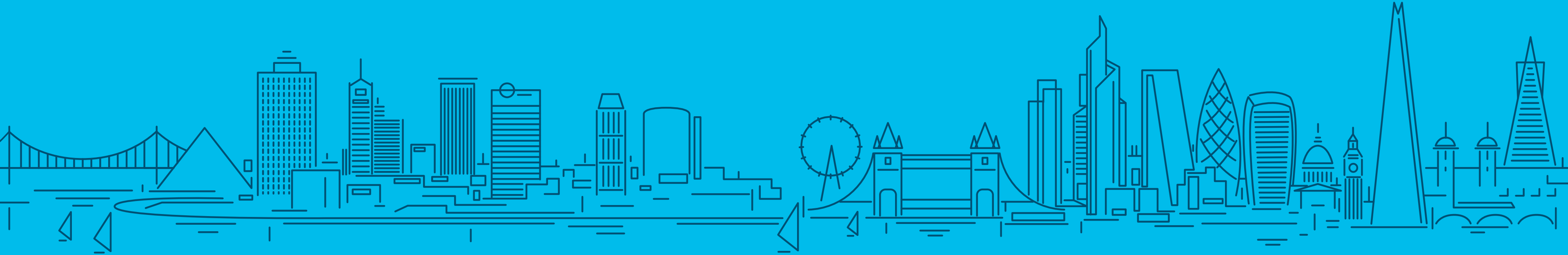


# The importance of logs

## You won’t see what you don’t log^Waudit

Tim (Wadhwa-)Brown
CX EMEAR Security Architecture
August 2018

# Introduction

# Introduction

- TLDR
- # whoami
- # cat .plan

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# TLDR

- What this talk is not about
  - Building a SOC in 30 minutes
- What this talk is about
  - Why logging goes wrong
  - How to start to plan your logging requirements
  - Case studies
  - Where to go next

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# # whoami

- Tim (Wadhwa-)Brown
  - Background in telecoms and financial services sectors
  - 14+ years at Portcullis (and now Cisco)
  - ~12 years as a CREST consultant
  - Head Of Research, CX EMEAR Security Architecture
- >120 CVEs to my name
  - Covering Windows, Linux, AIX and Solaris platforms
  - Userland through to kernel
- Current focus is operational security

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# # cat .plan

- Background
- Common failings
- The “what” of auditing
- Case studies
- Recommendations
- Conclusions

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

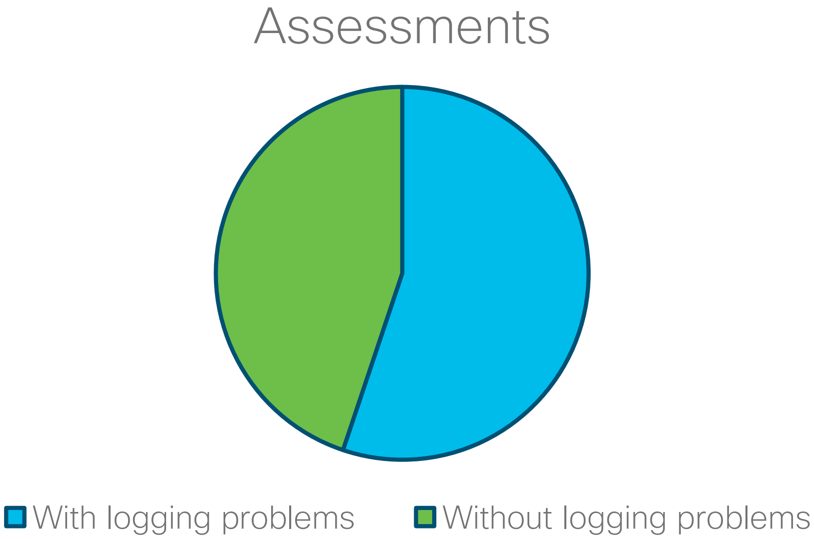
# Background

# Slow response is expensive

- Average breach identification time is in excess of 6 months
- 50% of businesses suffered breaches with a financial impact greater than $500,000

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Ineffective or missing logging is a real problem



Source: Cisco Security Advisory EMEAR assessment reports (2017)

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

> *“In over 50% of cases, logging will be insufficient to determine root cause, identify actions or attribute the actor.”*

IRR consultant

# Why does this matter?

- We’re expected to give expert guidance from both a blue and red team perspective
- Our customers want to mature their security posture from a defensive standpoint
- The first two questions after every breach are “how?” and “when?”…
  - …followed by “are they still active?”

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Common failings

# Common failings

- Time is a rarely understood domain
- Logs grow (and grow and …)
- We’re still using syslog for the most part
- Logging is passive, auditing is active
- People miss (and don’t miss) what they don’t understand
- Knowing what “good” looks like is hard
- Every failed security check should result in an audit event

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Time is a rarely understood domain

- TZ=Europe/London?
  - Ideally logs and events should always be timestamped against UTC

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Logs grow (and grow and …)

- They may not be collected
- They almost certainly aren't processed
- You may well need to agree a suitable retention period
  - Check local regulations in case there is a legal minimum

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# We're still using syslog for the most part

- If we're lucky there may be remote ingestion using a SIEM agent
  - Often times there isn't
- And sometimes, the ingestion leverages syslog which is an insecure protocol
  - There's a question of integrity and attestation

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Logging is passive, auditing is active

- Logging often relies on defaults
  - It’s really for debugging in many cases
- Auditing is rarely turned on
  - In cases where auditing is available, it’s may not be ingested into the SIEM
- Configuring and enabling auditing involves thinking about TTPs and the IOCs they leave behind

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# People miss (and don’t miss) what they don’t understand

- IOCs are often missed
  - Would you spot a brute force attempt on an internal web application?
- Exceptions are left unhandled
  - Wouldn’t you want to know why a service keeps on crashing?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Every failed security check should result in an audit event

- Perhaps not but…
  - Humans aren’t the best at correlating ad-hoc events
  - Every attempt to brute force a vulnerability might look different but audit events tied to the root cause can be measured, benchmarked and SIEMs can be set to trigger alarms on thresholds

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# The “what” of auditing

| Source | Category | Urgency | Events | Use case |
|---|---|---|---|---|
| DHCP | User/device attribution | High | IP assignments | Trace victims |
| VPN | User/device attribution | High | IP assignments | Trace victims |
| 802.1x | User/device attribution | High | IP assignments | Trace victims |
| DNS | User/device attribution | High | DNS lookups | Identify C2 |
| Firewall | User/device attribution | High | Blocked and successful connections | Trace victims |
| Email | Email activity | High | Message routing with headers and subjects | Discover campaigns |
| Proxy | Network activity | High | Blocked and successful connections | Identify C2 |
| OS auditing | System activity | Medium | Authentication, configuration changes and security events | Identify breaches |
| AntiVirus | System activity | Medium | Malware discovery and removal | Identify contained breaches |
| Vulnerability scans | Vulnerability status | Medium | Vulnerability attribution | Attribute attack to vulnerability |
| AD authentication | User/device attribution | Low | Authentication and authorisation | Identify lateral movement |
| Netflow | Network activity | Low | Connections from enterprise to data center | Investigate access |

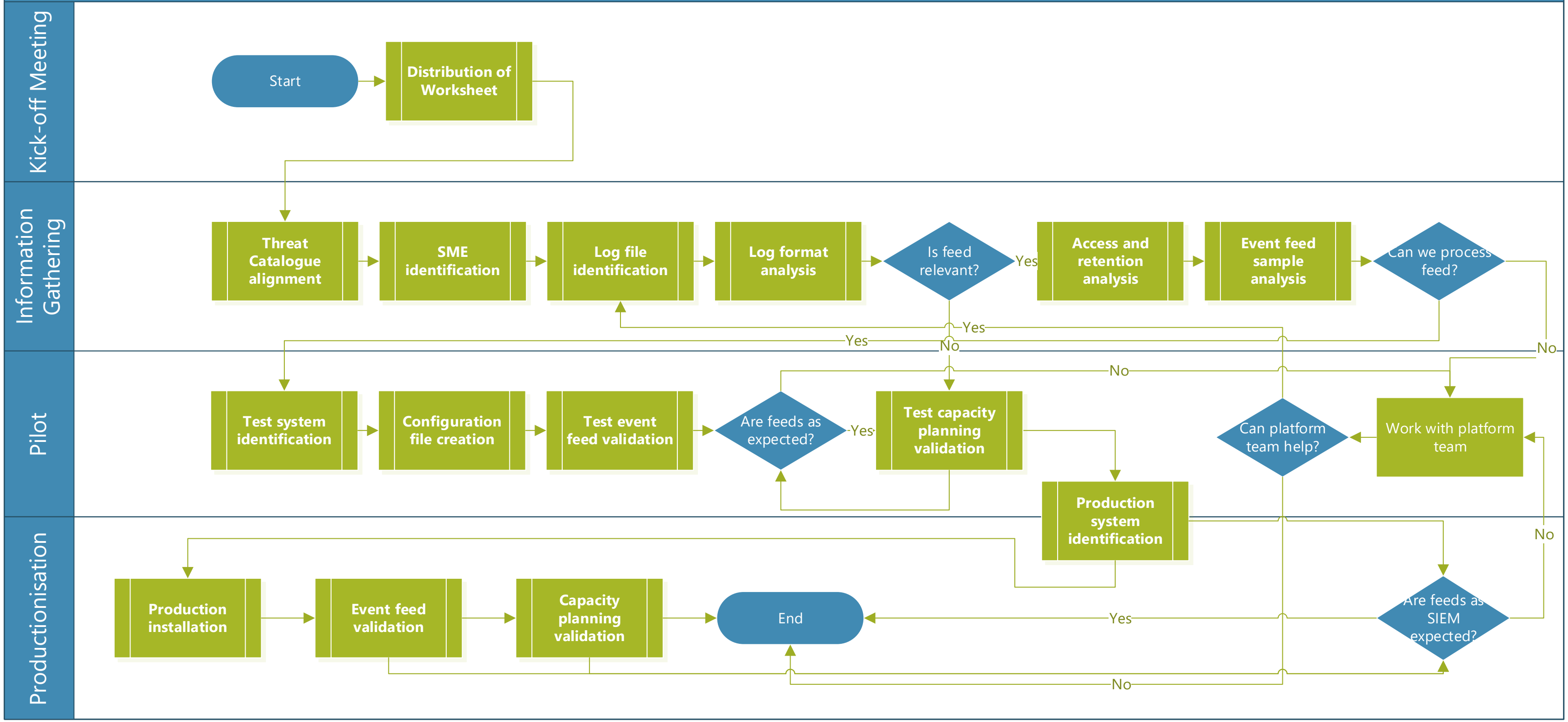
Source: Aaron Varrone, Cisco Security Incident Response Services (CSIRS)

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

| Key Considerations |
|---|
| Does the event meet legal requirements (no PII, etc)? |
| Validate that sensitive data has been randomised or removed (passwords, etc) |
| Ensure data is in the right format |
| Confirm event feed contains enough information to be useful (see Tab 4) |
| **Event Types** |
| Input validation failures |
| Change of privilege failures/successes |
| Authentication failure/successes |
| Session state changes |
| Suspicious behaviour and overuse |
| File uploads and writes |
| Access control failures/successes |
| Application and system errors |
| Any high-risk (those which may impact Confidentiality, Integrity or Availability (CIA) of the system) changes/administrative tasks |
| **Sensitive Data** |
| Personally identifiable information (PII) |
| Application source code |
| Session IDs |
| Access tokens |
| Passwords |
| Connection strings |
| Encryption keys and other master secrets |
| Bank account or payment card holder data |
| Data of a higher security classification than the logging system is allowed to store |
| Commercially-sensitive information |
| Information it is illegal to collect in the relevant jurisdictions |
| Information a user has opted out of collection, or not consented to e.g. use of do not track, or where consent to collect has expired |
| Consider replacing sensitive data with hashed equivalents in instances where these events need to be tracked |

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Event Feed Onboarding Process



Kick-off Meeting

Start

Distribution of Worksheet

Information Gathering

Threat Catalogue alignment

SME identification

Log file identification

Log format analysis

Is feed relevant?

Yes

Access and retention analysis

Event feed sample analysis

Can we process feed?

Yes

Yes

No

No

Pilot

Test system identification

Configuration file creation

Test event feed validation

Are feeds as expected?

Yes

Test capacity planning validation

No

Production system identification

Can platform team help?

Work with platform team

Productionisation

Production installation

Event feed validation

Capacity planning validation

End

Yes

Are feeds as SIEM expected?

No

No

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Practice breeds confidence

- If a system is important enough to warrant a penetration test
- But you can’t tell when they…
  - Connected to the network
  - Began their Nessus scans
  - Ran Burp active scan against the admin interface
- You may not be collecting the right audit feeds…
  - Or you might not know where to look

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Document “good” and curate “bad”

- Figure out what audit events occur and when
- Benchmark them
- Institute BAU policies to check key audit events hourly, daily or weekly
  - Get into a habit
- Incidents are not the right time to be learning about your SIEM’s query language

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Case studies

# Case studies

- Have we improved in 15 years?
- Developing in-house
- Whose been sitting at my shell prompt?
- A little knowledge can be a dangerous thing
- The oldest server in the data center

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Have we improved in 15 years?

- 15 years ago, I was sitting on the other side of the fence
  - Senior Operational Security Analyst
  - Working for a retail bank
- Problem
  - We wanted to know when people ran sudo and why
- Solution
  - HIPS & RBAC events fed into SQL Server
  - BAU processes to review events

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Developing in-house

- Development house x are building a new application
- Threat modeling has identified where attacks are likely
- They didn't build auditing in
  - No way to determine what the normal cadence of password resets was and when there was a peak

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Whose been sitting at my shell prompt

- A system has been changed and rebooted
- It’s unclear by whom and under what circumstances
- Management are ready to throw a contractor under the bus
- The log server was full

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# A little knowledge can be a dangerous thing

- The admins have been subjected to a red team recently
- I’m there to do a penetration test
- They’re all fired up watching their event logs
- STOP! What’s making all those connections to “C$”
- Turned out it was cached connections being reactivated when they used the search bar
- 12 hours of my life I won’t get back

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# The oldest server in the data center

- The box has been compromised
- Data has been wiped
- Yay! They have logs
  - Both application and OS
  - The problem is that the application logs weren’t suitably granular (HH:SS)
- Boo! There is literally no documentation on what the logs actually mean
  - Reversing mainframe binaries is fun but wasteful
  - We eventually found an OS event in the logs that acted as a crib

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Have we improved in 15 years?

- I'll let you be the judge ☺

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Recommendations

# Recommendations

- Engagement
- Full stack auditing
- Threat modeling

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Engagement

- With procurement
  - Build requirements into the procurement process
  - In particular, consider SaaS and PaaS vendors and their ability to service your requirements – systems you don't own are a particular pain point when collecting audit event feeds
- With platform teams
  - Ensure that the correct value of "good" is known
- With application support teams
  - Ensure auditing is switched on
- With developers
  - Ensure that detective controls are included in functional requirements
  - Check that you're not reliant logs that are intended for debugging
  - Reject unknown exceptions

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Full stack auditing

- Auditing every element of the stack could improve visibility
  - Network
  - OS
  - Filesystem
  - Database
  - Application
  - Web server
  - User
- Get to know your SMEs

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Threat modeling

- From an defensive standpoint we should look at
  - Assets
  - Actors
  - Threats
  - Impact
- Where are the detective controls?
- Frameworks can help
  - Microsoft: STRIDE
  - MITRE: ATT&CK (TTP) and CAPEC (weaknesses)
- Does the solution help or hinder visibility?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Conclusions

# Conclusions

- What have we learnt?
- Next steps?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# What have we learnt?

- Logging and auditing are rarely done well
  - Logging is for developers
  - Auditing should be for operators
- Everyone gets breached, plan for it
- Wouldn’t it be nice to understand your environment
- Don’t take my word for it…
  - https://www.ncsc.gov.uk/blog-post/learning-love-logging

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Next steps?

- Configure
  - Windows Event Log
    - Microsoft are obviously the canonical source
  - Linux Auditd
    - There are some great publicly shared policies on GitHub for this
- Collect the audit event feeds
  - There are open source solutions out there that DON'T use syslog but which do allow for audit event feeds to be collected in a secure fashion
- Build auditing into your SDLC
- Examine the audit events and learn what "good" looks like

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Links

- NCSC
  - https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes
- Windows
  - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
  - https://github.com/SwiftOnSecurity/sysmon-config
- Linux
  - https://github.com/bfuzzy/auditd-attack
  - https://github.com/Neo23x0/auditd

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Questions?

twadhwab@cisco.com

cisco