So you want to build a SOC?

Lessons from the front line

Tim (Wadhwa-)Brown
Head Of Research, CX EMEAR Security Architecture
twadhwab@cisco.com / @portcullislabs

TALGEN-1013

Cisco live!
June 9-13, 2019 • San Diego, CA

Agenda
TLDR

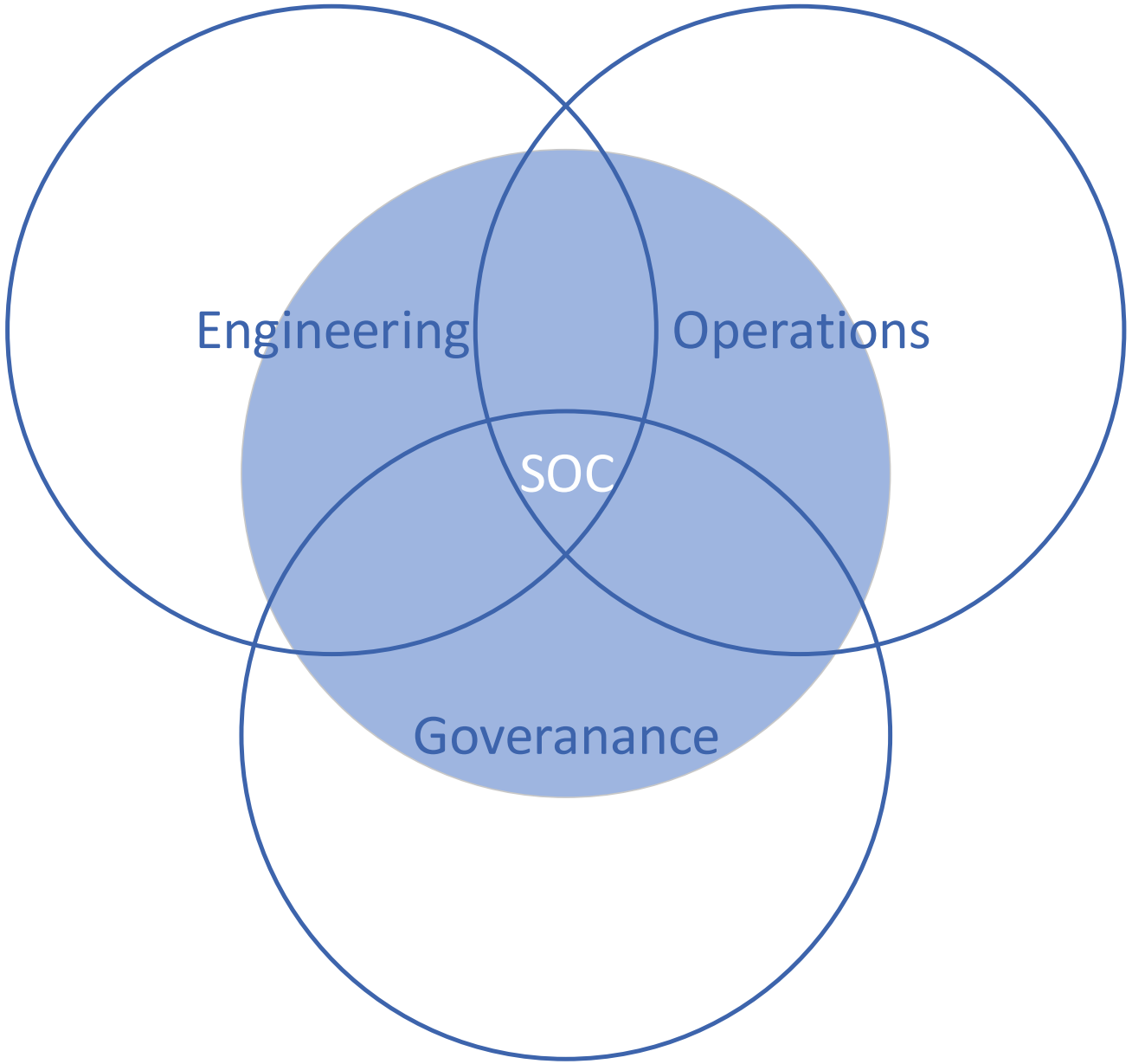
- What this session is not about
  - Building a SOC in 60 minutes
- What this session is about
  - Briefing you on some of what Cisco sees on the front line
    - From customer engagements
    - From our telemetry
  - What are some of the challenges of operating a SOC?
  - Suggestions on things Cisco have seen work
    - Foundations for your Security Operations team
    - Security intelligence and technical considerations
  - Reminding you of the importance of actionable telemetry

Introduction

The starting premise

- 15 years ago, I was sitting on the other side of the fence
  - Senior Security Operations Analyst
  - Working for a retail bank
- Problem
  - We wanted to know when our engineers ran sudo and why
- Solution
  - RCS and KSH for building and deploying systems and policies – DevSecOps
  - HIPS & RBAC events fed into SQL Server – SIEM
  - BAU processes and SQL queries to review events – Threat hunting

Who here works in a SOC?



SOC =

Engineering + Operations + Governance

Introduction

whoami

- Tim (Wadhwa-)Brown
  - 14+ years at Portcullis (and now Cisco)
  - Head Of Research & Security Architect, CX EMEAR Security Architecture
    - Ex-NCSC CHECK Team Leader (9 years)
    - CREST Registered Threat Intelligence Analyst
    - CREST Practitioner Intrusion Analyst
    - ISO 27001 LA
- >150 CVEs to my name
  - Covering Windows, Linux, AIX and Solaris platforms
    - Userland through to kernel
  - Most recent research: Where 2 Worlds Collide: Bringing Mimikatz et al to UNIX, Black Hat Europe 2018

A year in review, what did Cisco see on the front line?

A year in review

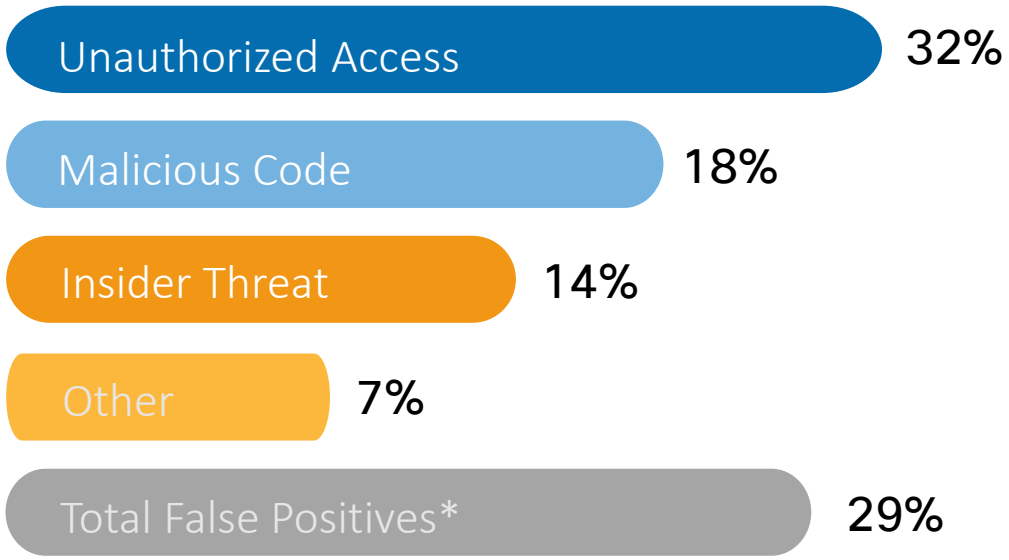
- *Customer engagements*
- *At scale*
- *Challenges of operating a SOC?*

What do you need to prepare for?

A year in review

Customer engagements

- *Pressure for immature sectors to mature at pace*
- *High level of dependency*
  - Dependencies aren't always well aligned to security capability requirements
- *Doing "simple" things is hard*

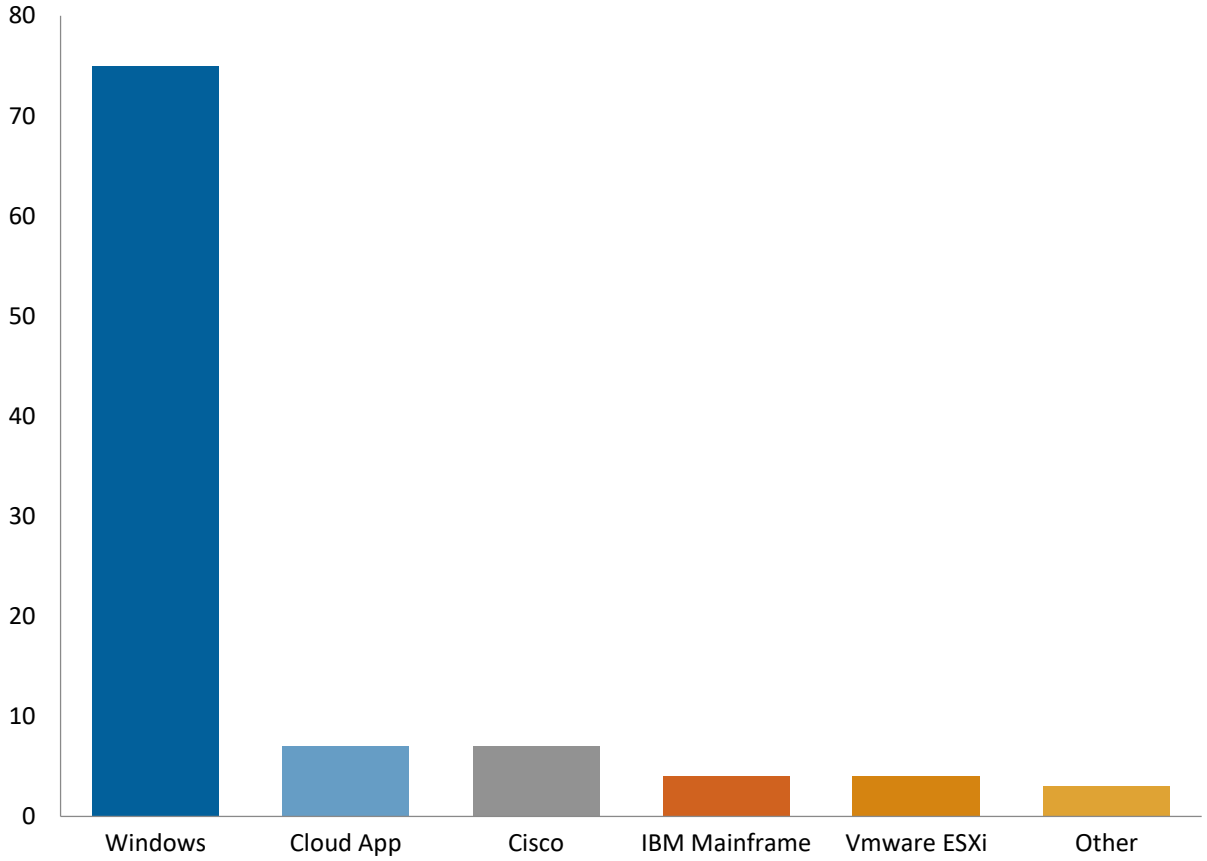


* false positive includes data from all investigation types

Customer engagements

Breach sources

Source: Cisco Security Incident Response Services (CSIRS), EMEAR, 2018



Customer engagements

Platforms

Source: Cisco Security Incident Response Services (CSIRS), EMEAR, 2018

At scale

Observations

- Increased use of encrypted traffic is making life harder for defenders
- Suspicious DNS traffic remains an effective indicator
- More generally, by frequency, suspicious traffic outbound > suspicious traffic internally > suspicious traffic inbound
- Microsoft's Exploitability Index combined with previous incidents such as WannaCry has helped to focus minds
  - *Interesting to see how quickly CVE-2019-0708 has been pounced on by both red and blue*

A year in review

Challenges of operating a SOC?

- *Governance*
  - *Benchmarking and KPIs*
- *Operations*
  - *Combining blue and red*
- *Engineering*
  - *The differences between legacy, enterprise and greenfield*
  - *Automation vs orchestration*
  - *Logging vs auditing vs telemetry*

Challenges of operating a SOC?

Benchmarking and KPIs

- *The industry needs to continue to move to build and operate the critical controls*
  - You should be benchmarking your capabilities against
    - CIS top 20 controls
    - ATT&CK for adversary simulation

Challenges of operating a SOC?

Combining blue and red

- Blue
  - Threat model
  - Build and operate critical controls
    - Hunt threats
- Red
  - Validate critical controls
    - Simulate threats
- Purple
  - Red and blue
  - Build muscle memory
  - Identify gaps

Challenges of operating a SOC?

The differences between legacy, enterprise and greenfield

- Enterprise
  - Endpoints, mail, file shares etc
  - Need to reliably deliver critical controls
- Legacy
  - Systems that generate revenue
    - May not be legacy at all
  - Need to integrate with service aligned platform and application teams
- Greenfield
  - Systems that you hope will generate you revenue in the future
  - Need to shift left
    - DevSecOps
    - CI/CD

Challenges of operating a SOC?

Automation vs orchestration

- Automation
  - Enables reliable delivery of critical controls
- Orchestration
  - Allows service aligned integration into wider organisation
- Both will help you scale but only orchestration allows scale outside of the technical space

Challenges of operating a SOC?

Logging vs auditing vs telemetry

- Logging
  - Events may be hidden in noise
  - Rules need to be configured
  - Requires Security Operations team to have first hand knowledge of event sources
- Auditing
  - Offers event-centric visibility, as defined by vendor
  - Policies may need to be configured
  - Enables behavioural IOCs for known threats
- Telemetry
  - Offers richer, API-centric visibility
  - Enables behavioural IOCs for “unknown” threats
  - Instrumentation may need to be developed
  - Agents will likely need to be deployed
  - Real-time threat awareness
  - May allow cross-application/cross-platform visibility

Foundations for your Security Operations team

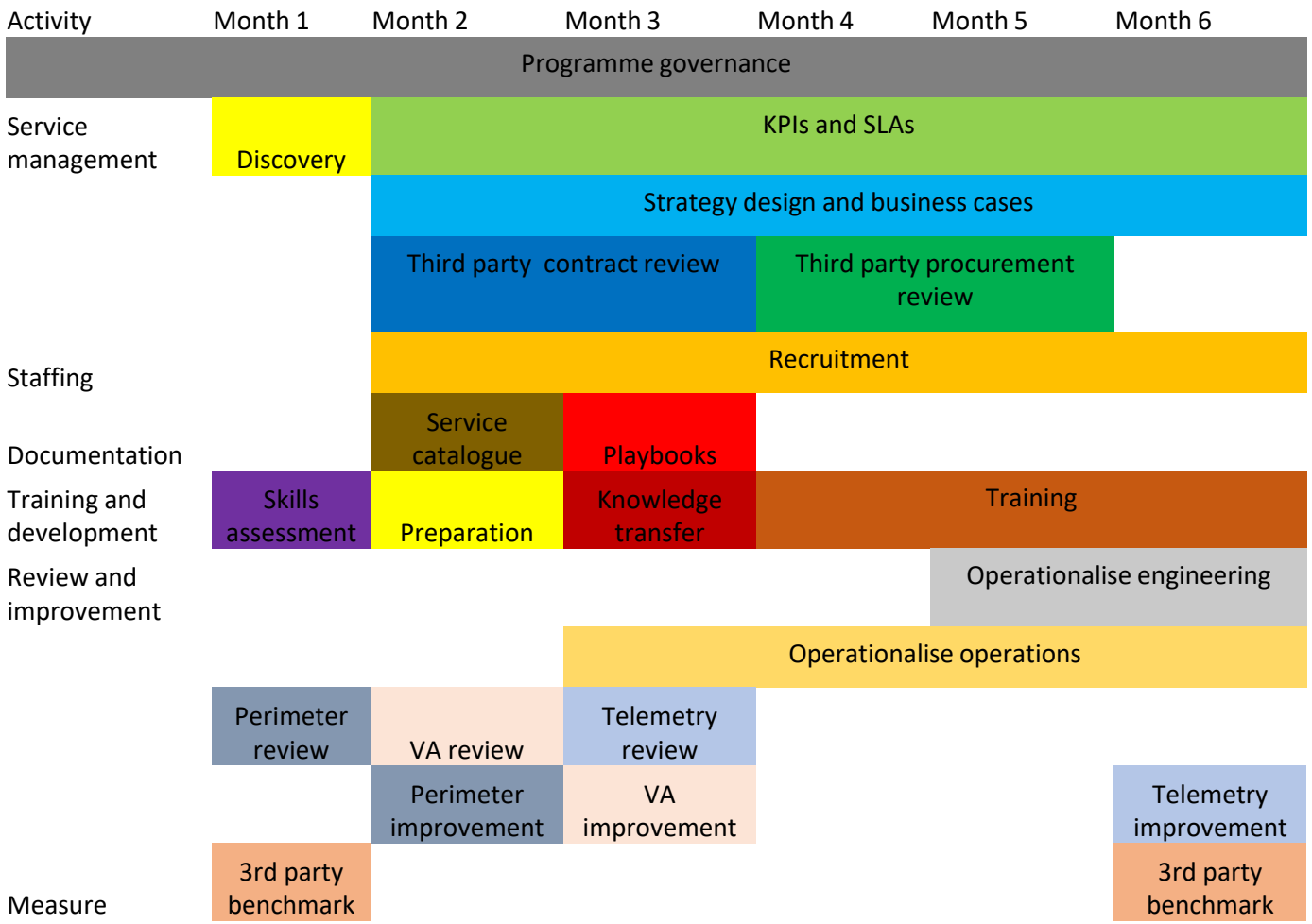
Foundations for your Security Operations team

- *Align to service catalogue*
- *Plan your first 6 months*
- *Define KPIs*
- *Build a culture*

Foundations for your Security Operations team

Align to service catalogue

- Identify customers and service providers
- Define lines of service
- Define and categorise services
- Identify gaps in capability
- Build operational capability
- Gauge acceptance
- Publish to staff and customers
- Operate
- Leverage KPIs for continual improvement



Foundations for your Security Operations team

Plan your first 6 months

Foundations for your Security Operations team

Define KPIs

- Why are you spending all this money?
  - Legislation
  - Reputation
  - Culture
- *Which one matters to the C-suite and why?*
- There are other metrics…
  - Employee motivation
  - Evaluating your MSSPs
  - Hidden costs

Foundations for your Security Operations team

Build a culture

- Organisationally
  - Leverage existing tooling to enable effective intelligence collection and processing
    - Application support teams, NOCs etc have lots of fun toys
    - You **will** need
    - **Ticketing**
    - **Document management**
    - **Revision control**
- Internally
  - Hire operators who understand the business user base
  - Hire engineers who understand app sec
  - Build, operate and benchmark critical controls
  - Build effective processes
  - Automate everything
  - Remember: Every second-line analyst started as a first-line analyst

Security intelligence and technical considerations

Security intelligence

- *What is intelligence?*
- *How should you be using it?*
- *Why focus on telemetry?*
- *How can you improve your telemetry?*
- *The “what” of telemetry*

Security intelligence

What is intelligence?

- Results from your security assessments
- Vulnerability research
- Stories in the press
- IOCs
- Telemetry from your network

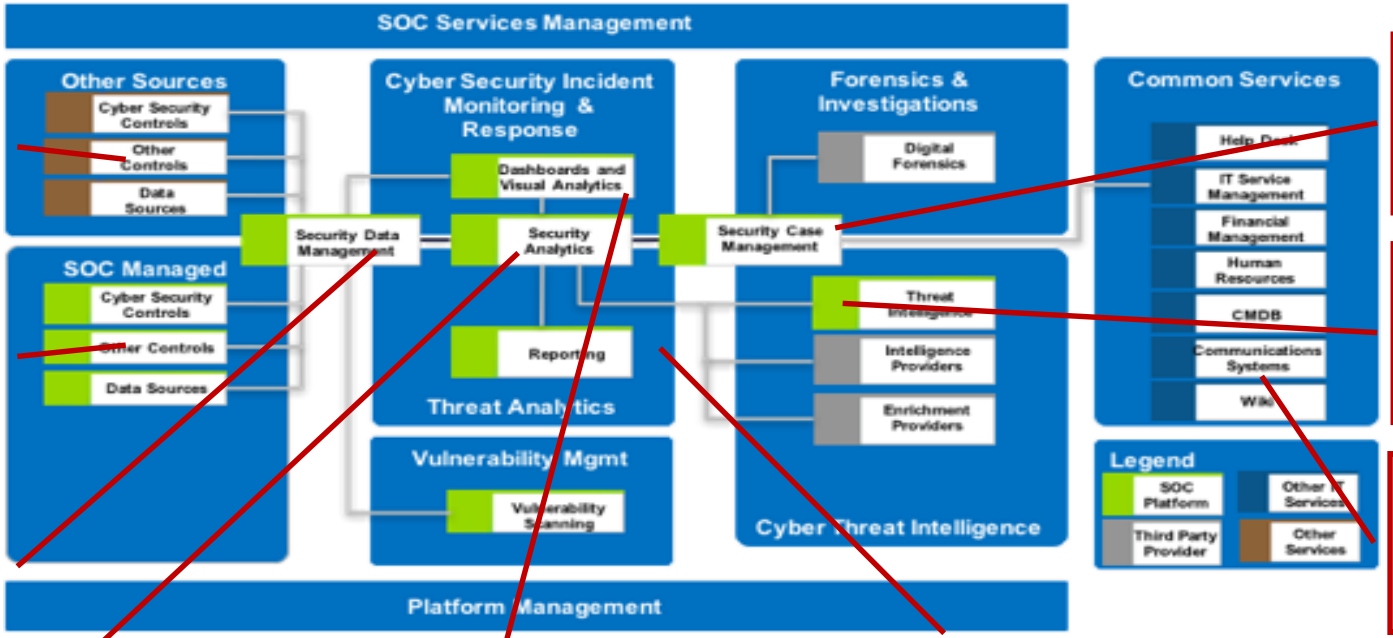
Security intelligence

How should you be using it?

Data sets, including telemetry and attribution data, from outside the SOC

Data generated by SOC managed controls and sources

Data management across the lifecycle



Current intra- and cross-SOC workflow

Higher-confidence threat intelligence production from collected intel sources

Use and integration of key enterprise services

Real-time and historical analytics, including alerting, query and cross-platform integration

Effects on flow and operational rhythms by standard and custom views

Value to consumers provided by current reporting, including self-service and automation

Why focus on telemetry?

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*

Source: Cisco 2018 Annual Cybersecurity Report

“In well over half of response cases, logging will be insufficient to determine root cause, identify actions or attribute the actor.”

Source: CSIRS consultant, EMEAR

Why focus on telemetry?

Why should this matter to you?

- Boards are waking up to the need to recognise the need to mature their security posture from a defensive standpoint
  - If you can't do telemetry right, then how are you going to deliver other critical controls?
    - It's a good canary in the coal mine for technical capability
- The first two questions after every breach are "how?" and "when?"...
  - ...followed by "are they still active?"
  - *Logs tell you this!*

Why focus on telemetry?

Case studies

- Networking device
- Recent red team engagement
- In-house development
- Mainframe
- Have organisations improved?

Telemetry is the hub of Security Operations

The importance of telemetry

Why telemetry fails

- Governance
  - Insufficient capabilities
- Engineering
  - Unsynced time and/or multiple time zones
  - Lack of centralised visibility
  - Poorly engineered ingestion
  - Capacity and growth
  - Poor configuration
- Operations
  - Unfamiliarity with application stack
  - Lack of ground truth
  - Every failed security check should result in an audit event

Technical KPIs?

The importance of telemetry

How can you improve your posture?

- Ensure that you're risk focused
- Ensure that you consider the full stack
- Engage with the enterprise

Don’t wait for a breach!

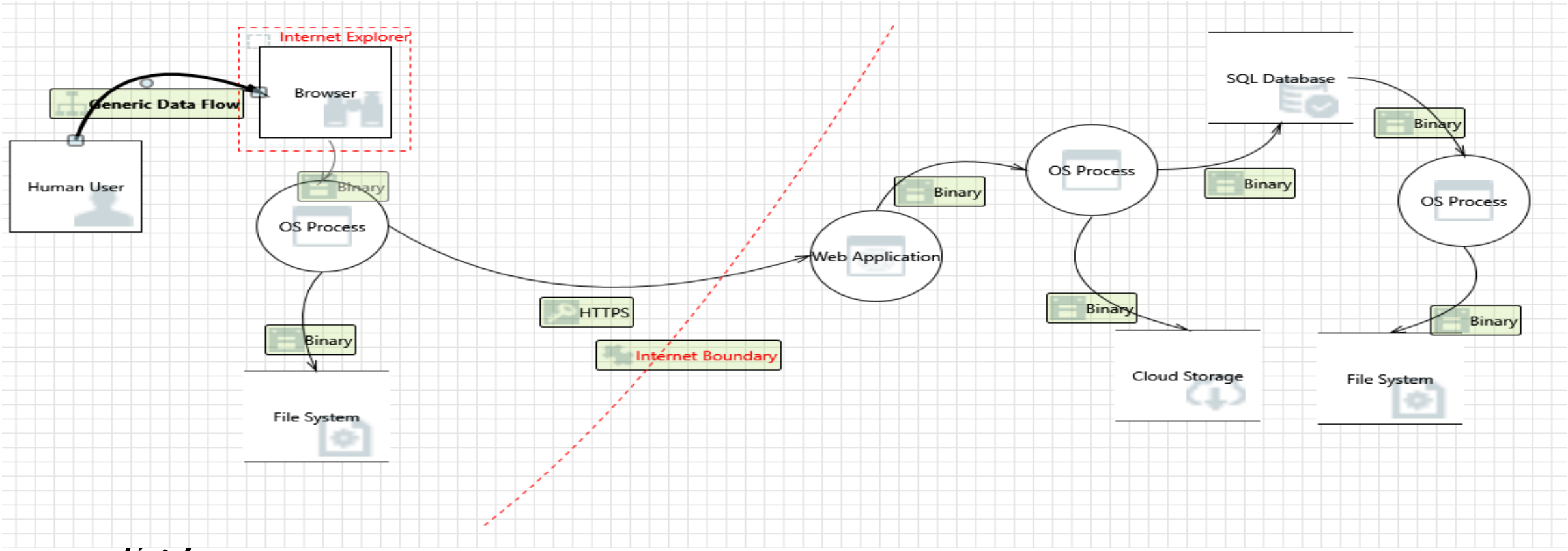
How can you improve your posture?

Ensure that you're risk focused

- From an defensive standpoint
  - Assets
  - Actors
  - Threats
  - Impact
- Where are the controls?
- Frameworks can help
  - Microsoft: STRIDE
  - MITRE: ATT&CK (TTP) and CAPEC (weaknesses)

How can you improve your posture?

Ensure that you consider the full stack



How can you improve your posture?

Engage with the enterprise

- With procurement
  - Build critical control 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
- With platform and application support teams
  - Ensure that the correct value of "good" is known
  - Ensure critical controls are switched on
- With developers
  - Ensure that critical controls are included in functional requirements
  - Check that you're not reliant on logs that are intended for debugging
  - Reject unknown exceptions

The “what” of telemetry

Practice breeds confidence

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

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

The “what” of telemetry

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

Conclusions

- What have you learnt?
- Key takeaways?
- Next steps?
- How can Cisco help you?
- Where do Cisco's products deliver critical controls?

Conclusions

What have you learnt?

- *What Cisco sees on the front line*
  - Telemetry needs to improve
- *The challenges to a modern SOC*
  - Digital transformation will change how we do things
- *Suggestions on things Cisco have seen work*
  - Plan
  - Document
  - Measure
- *The importance of actionable telemetry*

Conclusions

Key takeaways?

- Everyone gets breached: *Build and operate your systems to ensure resilience and aid recovery*
- *You need to be able to both configure and interpret your environment*

Security Operations isn't enough

(You need Security Engineering and Governance too =))

Conclusions

Next steps?

- Build a plan to improve your Security Operations and Security Engineering capabilities
  - Get to know and love NIST 5 functions and CIS top 20 controls
  - Benchmark your current capabilities
  - When you build your business cases, don't forget to include the engineering effort to uplift the operational capability
    - Black boxes aren't magic and tuning them isn't free
- If you've not already done so
  - Configure Windows Event Log and Linux's Auditd
  - Examine the audit events and learn what "good" looks like

Conclusions

How can Cisco help you?

- Cisco Security SOC Advisory
  - Help with planning
- Cisco Security Incident Response Services (CSIRS)
  - Help with breaches *(even on z/OS)*
- Cisco Security Red Team
  - Benchmark your SOC and IR capabilities
- Cisco Security Architecture
  - Let us engineer your operational capability
- Cisco Talos
  - The world's biggest private intelligence platform
- Cisco product…

Thank you

Learn more about Cisco's Security Services at
https://cs.co/security-advisory

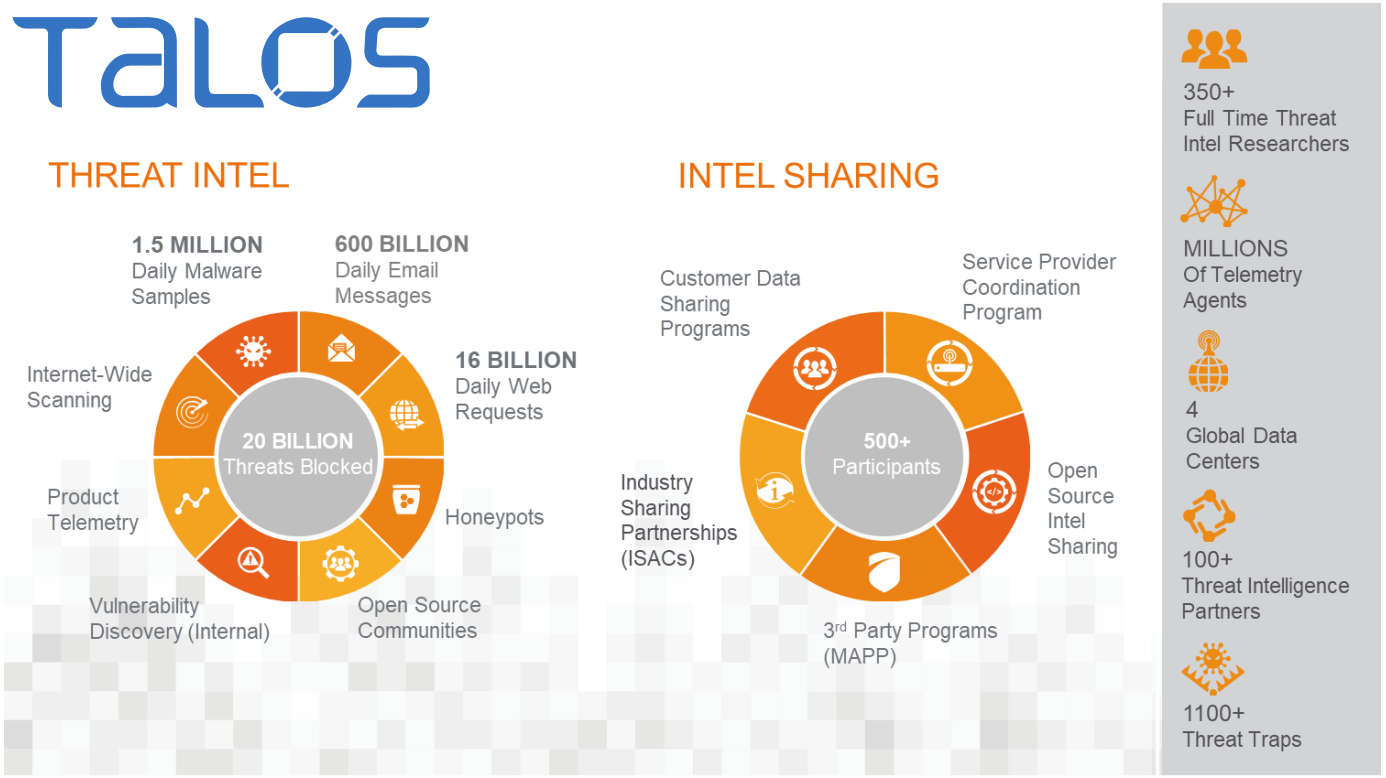
Bonus material

Introduction

Just another penetration tester^W^Wsecurity researcher?

- Not exactly..
  - I've worked in multiple Operational Security roles
    - Managed service provider – security analyst
    - Lottery operator – security architect
    - High street retailer – security engineer
  - I'm also
    - An occasional CSIRS participant
    - Responsible for initiating OpenVAS (the open source Nessus fork) project
    - Advisor to UK HMG's NCSC Security Research Information Exchange programme
    - Co-owner of an ISP offering last mile connectivity and hosting services

TALOS



A year in review

At scale

Task	Type	Day	LOE	Done
Start creating flags and rules in Outlook	Personal	1	-	
Document onboarding	Leadership	10	-	
Review patching policy	Engineering	10	5	
Review password policy	Engineering	10	5	
Review email access	Engineering	10	5	
Review web access	Engineering	10	5	
Review DNS access	Engineering	10	5	
Engage with change management	Governance	10	2	
Document risks	Governance	10	2	
Schedule regular meetings with team	Leadership	10	12	
Engage with risk owners	Governance	20	2	
Prioritise risks	Governance	30	5	
Engage with procurement	Governance	30	2	
Map your external assets	Operations	30	5	
Fix critical risks	Engineering	30	10	
Review architecture	Engineering	30	5	
Decide document repository	Leadership	30	-	
Decide code repository	Leadership	30	-	
Organise external VA	Operations	30	3	
Attend CAB	Engineering	30	5	
Develop IR requirements	Operations	30	5	
Review joiners and leavers process	Governance	30	2	
Define service catalogue	Leadership	60	3	
Engage with PMO	Engineering	60	2	
Review endpoint policy	Engineering	60	5	
Develop operational requirements	Engineering	60	5	
Schedule regular meetings with platform support teams	Engineering	60	4	
Review team and capability	Leadership	60	2	
Define KPIs	Leadership	90	2	
Develop documentation	Leadership	90	-	
Identify critical control gaps	Engineering	90	3	
Organise internal VA	Operations	90	3	
Develop training plan	Leadership	90	5	
Identify engineering requirements	Engineering	120	2	
Document application list	Operations	120	-	
Document platform list	Operations	120	-	
Document third parties	Operations	120	-	
Schedule regular meetings with application support teams	Engineering	120	2	
Define SDLC requirements	Engineering	150	5	
Set up centralised logging capability	Engineering	180	5	
Review team and capability	Leadership	180	1	
Document SDLC requirements	Engineering	180	7	
Document engineering requirements	Engineering	180	5	
Develop bug bounty program	Engineering	180	5	
Enable secure DNS	Engineering	180	7	
Enable secure email with DMARC	Engineering	180	7	
Review third parties	Governance	180	7	
Start budget planning	Leadership	180	3	
Organise external VA	Operations	180	2	
Organise internal VA	Operations	180	2	

Foundations for your Security Operations team

Start your task list

Why focus on telemetry?

Basic Cyber hygiene

- Logging is…
  - Number 6 on CIS list of “basic” controls
  - Key to the Detect and Respond phases from the NIST 5 functions
  - *Incident response without logging is “challenging”*

Case studies

Networking device

- 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
- Maturity: Low

Case studies

Recent red team engagement

- Everything was being treated as bad
- 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
- Maturity: Low

Case studies
In-house development

- Development house x are building a new application
- Threat modelling 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
- Maturity: Low

Case studies

Mainframe

- 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
- Maturity: Medium

Case studies

Have organisations improved?

- 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
  - RCS and KSH for building and deploying policies – DevSecOps
  - HIPS & RBAC events fed into SQL Server – SIEM
  - SQL and BAU processes to review events – Threat hunting
- Maturity: High

Common failings
Insufficient capabilities

- 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

Common failings

Unsynced time and/or multiple time zones

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

Common failings

Lack of centralised visibility

- A single pane of glass is the holy grail
  - More likely you'll end up with a SIEM of SIEMs
- If not...
  - How will your analysts have visibility?
  - How will you know if something has failed?

Common failings

Poorly engineered ingestion

- 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

Common failings

Capacity and growth

- The events 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

Common failings
Poor configuration

- 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 may not be ingested into the SIEM
  - Configuring and enabling auditing involves thinking about TTPs and the IOCs they leave behind

Common failings

Unfamiliarity with application stack

- 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?

Common failings

Lack of ground truth

- Only partially useful if you don’t know what audit events occur and when
  - This requires benchmarking
    - 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

Further 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
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

The “what” of telemetry

Further considerations

Conclusions

Where do Cisco's products deliver critical controls?

- Cisco Stealthwatch (Recon, Persistence)
- Cisco Talos (Staging)
- Cisco web and email (Launch)
- Cisco FirePOWER Next-Generation IPS (NGIPS) (Exploitation)
- Cisco Advanced Malware Protection (AMP) (Installation, Persistence)
- Cisco Umbrella (C2)
- Cisco Cognitive Threat Analytics (C2)
- Cisco Identity Services Engine (ISE) and Cisco TrustSec (Persistence)

Conclusions

Baseline controls

- NIST 5 functions
  - https://www.nist.gov/cyberframework/online-learning/five-functions
- CIS top 20 controls
  - https://www.cisecurity.org/controls/cis-controls-list/

Conclusions

Doing logging and telemetry right

- NIST
  - https://csrc.nist.gov/publications/detail/sp/800-92/final
- 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