OWASP
Open Web Application Security Project

Facing Security Monitoring: Hype, Challenges, Solutions

Alexios Fakos
alexios.fakos@owasp.org

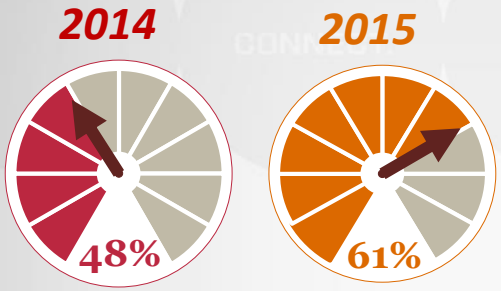
Johannes Schönborn
johannes.schoenborn@owasp.org

Agenda

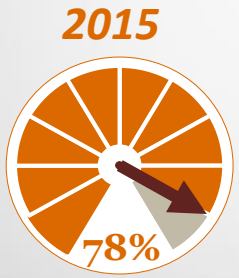
Hype

Hype or just your threat landscape?

% of global CEOs worried about Cyber Security



% of global CEOs saying Cyber Security is strategically important

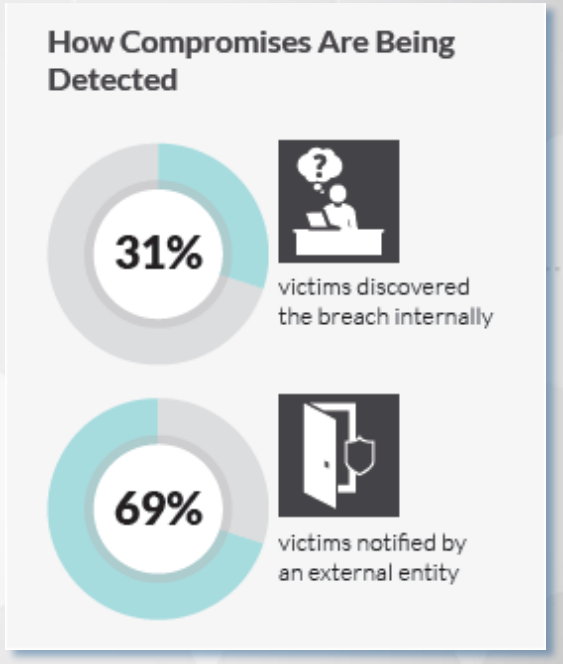


Source: Annual CEO Survey, PwC

95%
OF THESE INCIDENTS INVOLVE HARVESTING CREDENTIALS STOLEN FROM CUSTOMER DEVICES, THEN LOGGING INTO WEB APPLICATIONS WITH THEM.

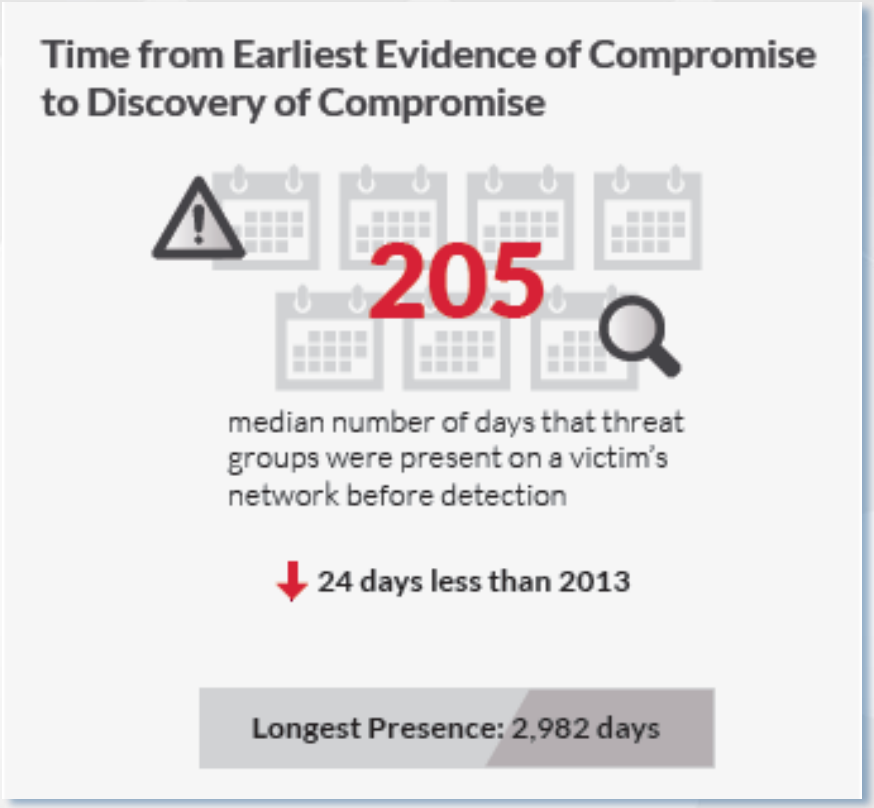
55%
THE TOP ACTION WAS PRIVILEGE ABUSE—AT 55% OF INCIDENTS—WHERE INTERNAL ACTORS ABUSE THE ACCESS THEY HAVE BEEN ENTRUSTED WITH.

Source: Verizon, 2015 Data Breach Investigations Report



Source: Mandiant, M-Trends® 2015: A View From the Front Lines

Median number of days before detection?



Source: Mandiant, M-Trends® 2015: A View From the Front Lines

5 Questions CEOs Should Ask About Cyber Risks

1. How Is Our Executive Leadership Informed about the Current Level and Business Impact of Cyber Risks to Our Company?

2. What Is the Current Level and Business Impact of Cyber Risks to Our Company?

What Is Our Plan to Address Identified Risks?

3. How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?

4. How Many and What Types of Cyber Incidents Do We Detect In a Normal Week?

What is the Threshold for Notifying Our Executive Leadership?

5. How Comprehensive Is Our Cyber Incident Response Plan?

How Often Is It Tested?

CFO, CISO, CEO, CIO

Source: https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

Solution

Risk Assessment Methodology

- Goals
  - Provide a quantitative view of risk
  - Align with the tools and capabilities that exist today
  - Provide specific and actionable mitigation recommendations
  - Align with industry standards
  - Utilize fewer resources
  - Standardize the results

Source: http://www.nist.gov/cyberframework/upload/cybersecurityframework_6thworkshop_chevron.pdf

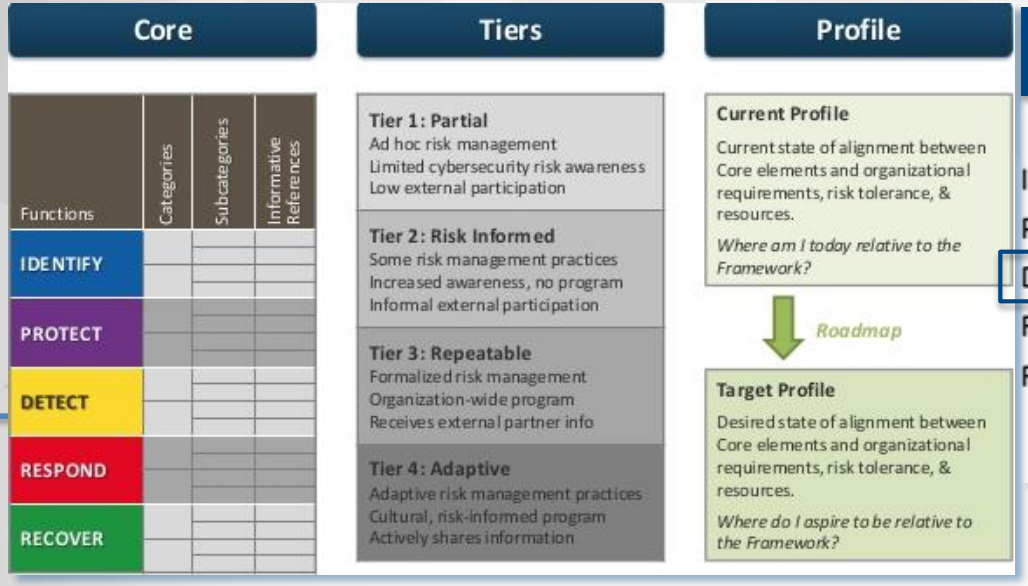
NIST Cybersecurity Framework

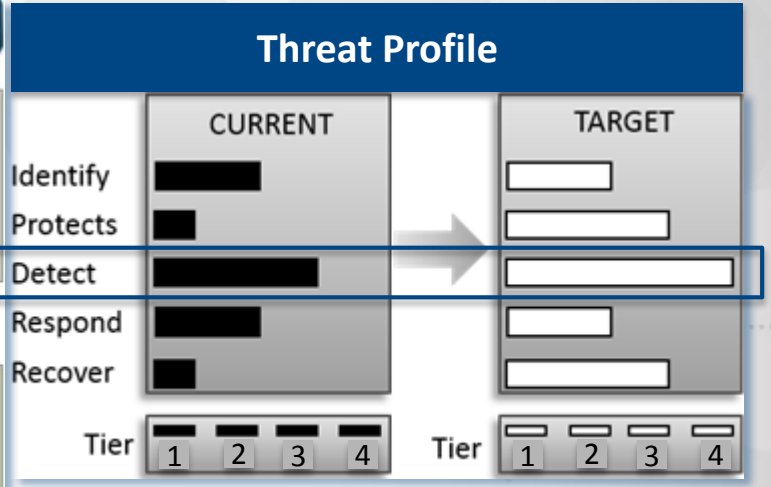
Building from standards, guidelines and best practices the Framework provides a common taxonomy and mechanism for organizations to:

1. Describe their **current** cybersecurity posture.
2. Describe their **target state** for cybersecurity.
3. Identify and **prioritize** opportunities for improvement within the context of a continuous and repeatable process.
4. **Assess progress** toward the target state;
5. **Communicate** among internal and external stakeholders about cybersecurity risk.

Source: http://www.dhs.gov/using-cybersecurity-framework

The three parts and a rising question



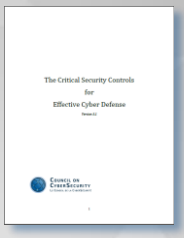


DE.AE	Anomalies and Events
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes

The ability to respond quickly and effectively to potential cyber attacks, but how to start?

Source: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

The Critical Security Controls for Effective Cyber Defense



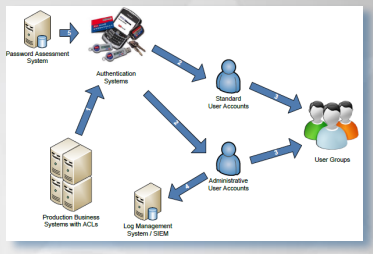
- Council on CyberSecurity was established in 2013 as an independent, expert, not-for-profit organization.
- Controls are in alignment with security standards and best practices.

- 20 Critical Security Controls focusing on
  - Prioritization (quick wins)
  - Procedures and tools that enable implementation and automation
  - **Metrics and tests to assess implementation status and effectiveness**
  - Guidance (how to)

Source: http://www.counciloncybersecurity.org/

Example CSC 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.



Effectiveness Metrics

- Does the system provide an inventory of all administrative accounts?
- Does the system report on the addition of new administrative accounts?
- How long does it take for administrators to be notified about user accounts being added to super user groups (time in minutes)?

612 minutes

Automation Metrics

- What percentage of the organization's elevated accounts do not currently adhere to the organization's password standard (by business unit)?

44%

- How many unauthorized elevated application accounts are currently configured on the organization's systems (by business unit)?

44%

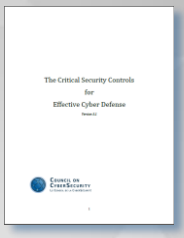
Effectiveness Test

Attempt to configure weak administrator passwords that are non-compliant with established policy.

Verify that the system does not allow weak passwords to be used.

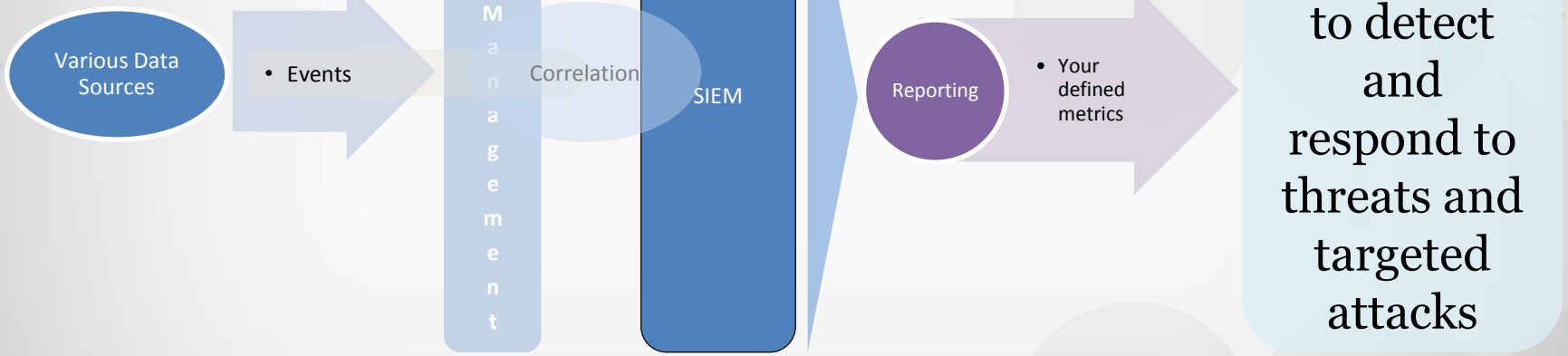
Source: http://www.counciloncybersecurity.org/

Dependencies



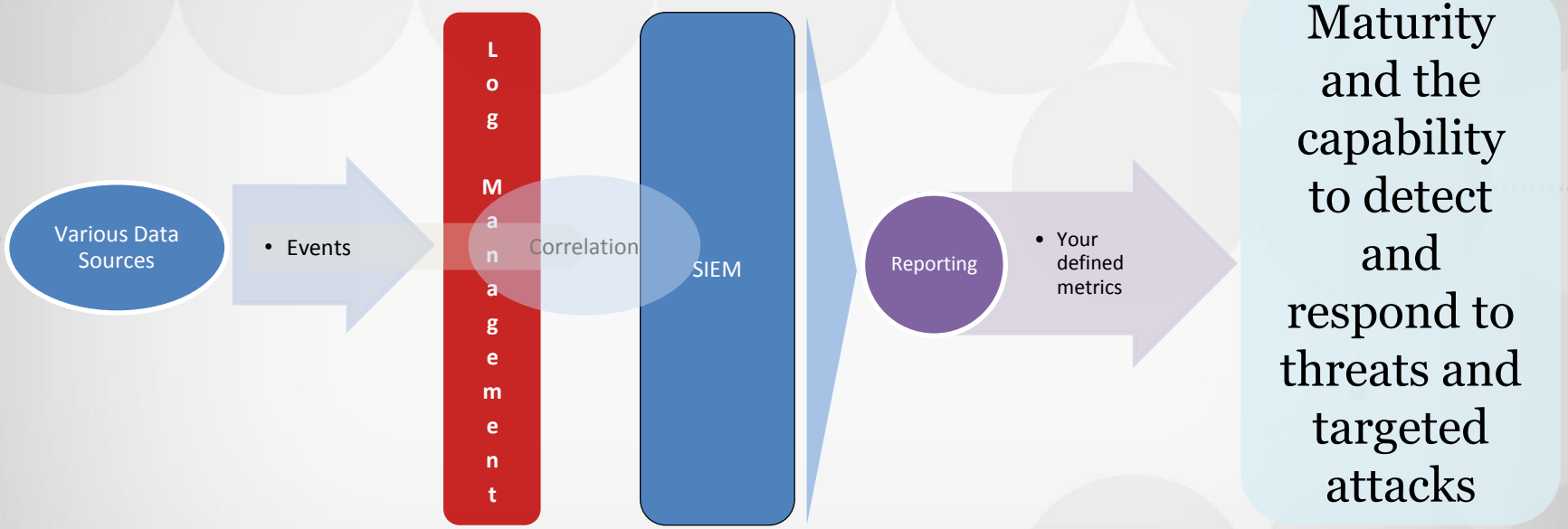
- Relevant Critical Controls for Continuous Monitoring
  - CSC 1: Inventory Of Authorized And Unauthorized Devices
  - CSC 2: Inventory Of Authorized And Unauthorized Software
  - CSC 4: Continuous Vulnerability Assessment And Remediation
  - CSC 12: Controlled Use Of Administrative Privileges
  - CSC 13: Boundary Defense (flow of information)
  - CSC 14: Maintenance, Monitoring, And Analysis Of Audit Logs
  - CSC 15: Controlled Access Based On The Need To Know
  - CSC 16: Account Monitoring And Control

Target picture



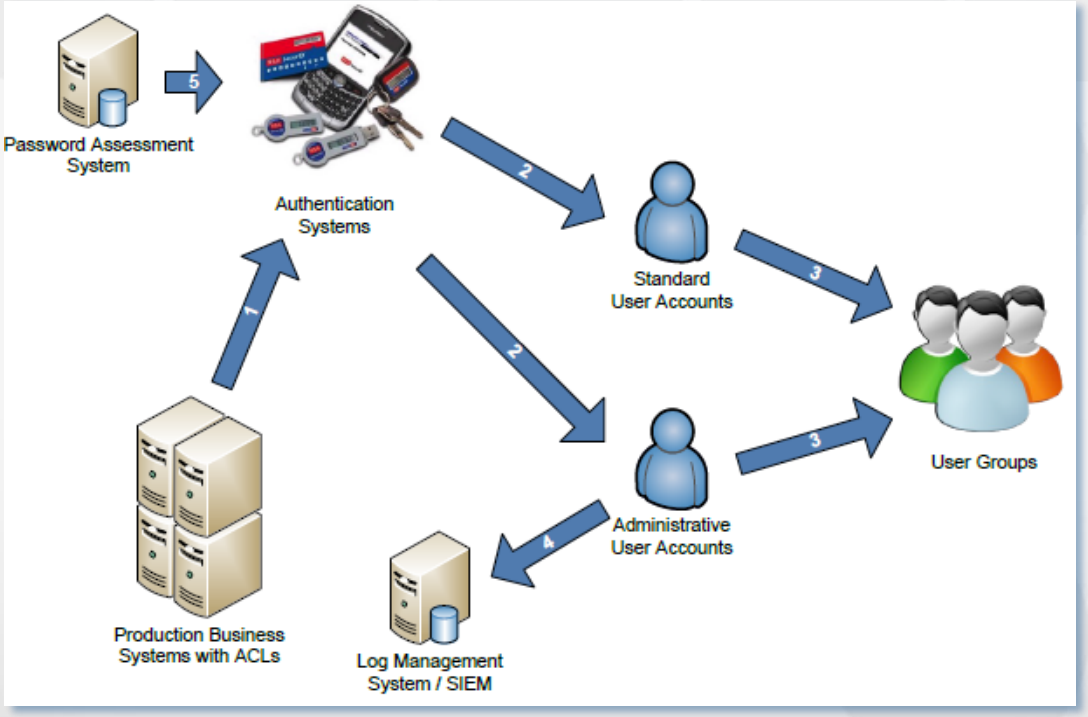
Challenges

Target picture



Example CSC 12: Controlled Use of Administrative Privileges

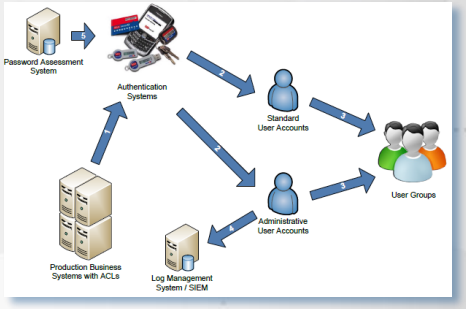
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.



Source: http://www.counciloncybersecurity.org/

Solution Path – Logging

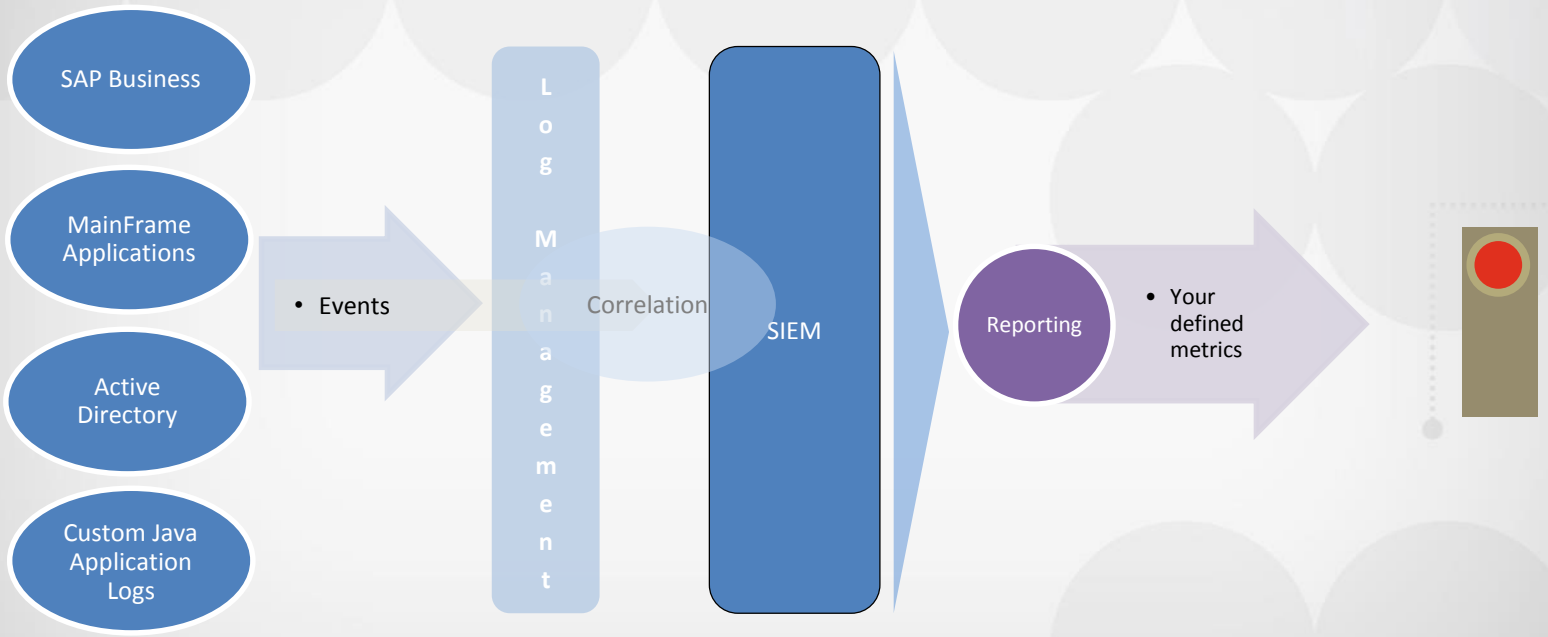
- Administrative Privileges in applications:
  - Does your application log these?
  - How does your application log these?
    - Who
    - What
    - Where
    - When
  - Does the logging provide (near) real time monitoring? Or do you get application logs once each six hours?



Source: http://www.counciloncybersecurity.org/

Our target picture again

Does the system provide an inventory of all administrative accounts?



Source: http://www.counciloncybersecurity.org/

Use Case Approach

- Use Cases
  - Business Use Case VS System Use Case
  - Create Business Use Cases for existing controls if applicable

- System Use Case

  Track successful logins

- Business Use Case

  Track successful logins, that are not automated scripts etc. and correlate against existing business processes

Use Case Approach

Objective	Details	Output	Data Sources

CSC12: Controlled Use Of Administrative Privileges	• Successful Admin Login
	• Collect exiting Support Tickets for Admin
	• Prevent False positives:
	  • Automated scripts
	  • Logins from machines XYZ
	  • Logins from service ZYX
	  • Logins around 3.30 am each Wednesday night
		• Reports
		• Alerts
		• KPI
			• OS
			• Databases
			• Applications
			• Network Devices
			• Ticketing Systems

Summary

Summary

- Use your Risk Assessment Methodology to identify
  - Capability and maturity regarding your appropriate security controls
  - Take your time for metrics and how to evaluate security controls
- Think big but start smart and small
  - Identify KPIs you need for your desired maturity level
  - Identify Applications and Infrastructure you need do deliver information into your LM/SIEM for evaluation for these KPIs
  - Assess readiness of these components to actually deliver this information

Questions?

CONNECT. LEARN. GROW.

Thank you for your attention!