27 NOVEMBER, 2016

Penetration Testing in Financial Institutions

COINS PH.D. STUDENT SEMINAR 2016

OLEKSANDR KAZYMYROV, TECHNICAL TEST ANALYST

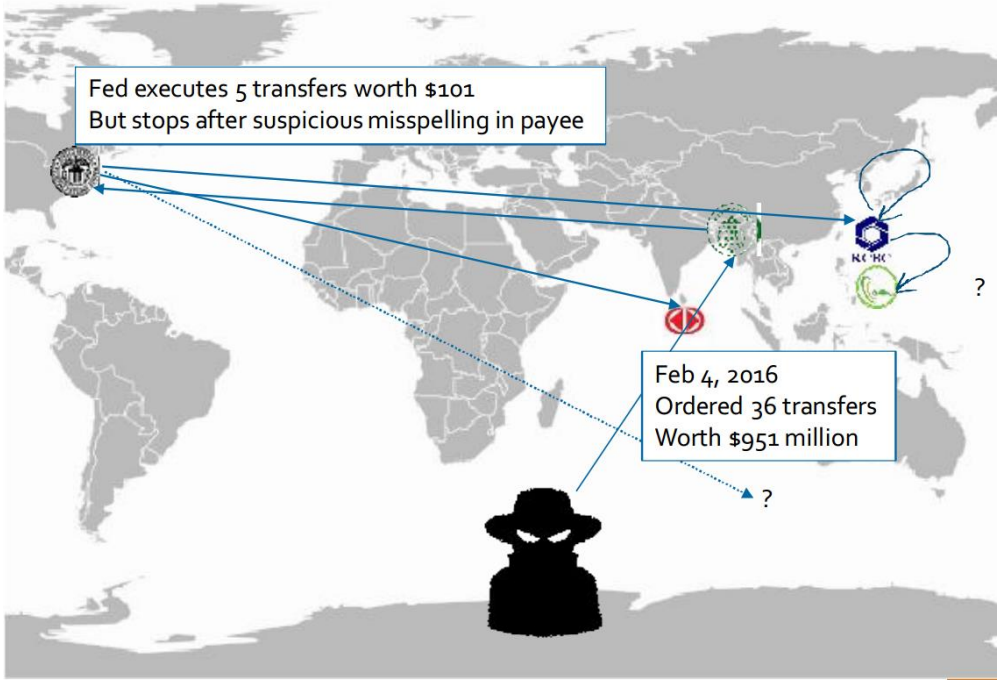
EVRY

How the SWIFT Hack Went Down and How to Benefit from the Lessons Learned

Agenda of the webinar :

- The sophisticated techniques used during the SWIFT hack, affecting the network, operating system, application and database layer.
- Key strategies and technologies to put in place for attack prevention and proper response.
- How Carbon Black can help you to implement the right level of protection and monitoring for different classes of systems.

Source:
https://www.carbonblack.com/webinars/swift-attack/



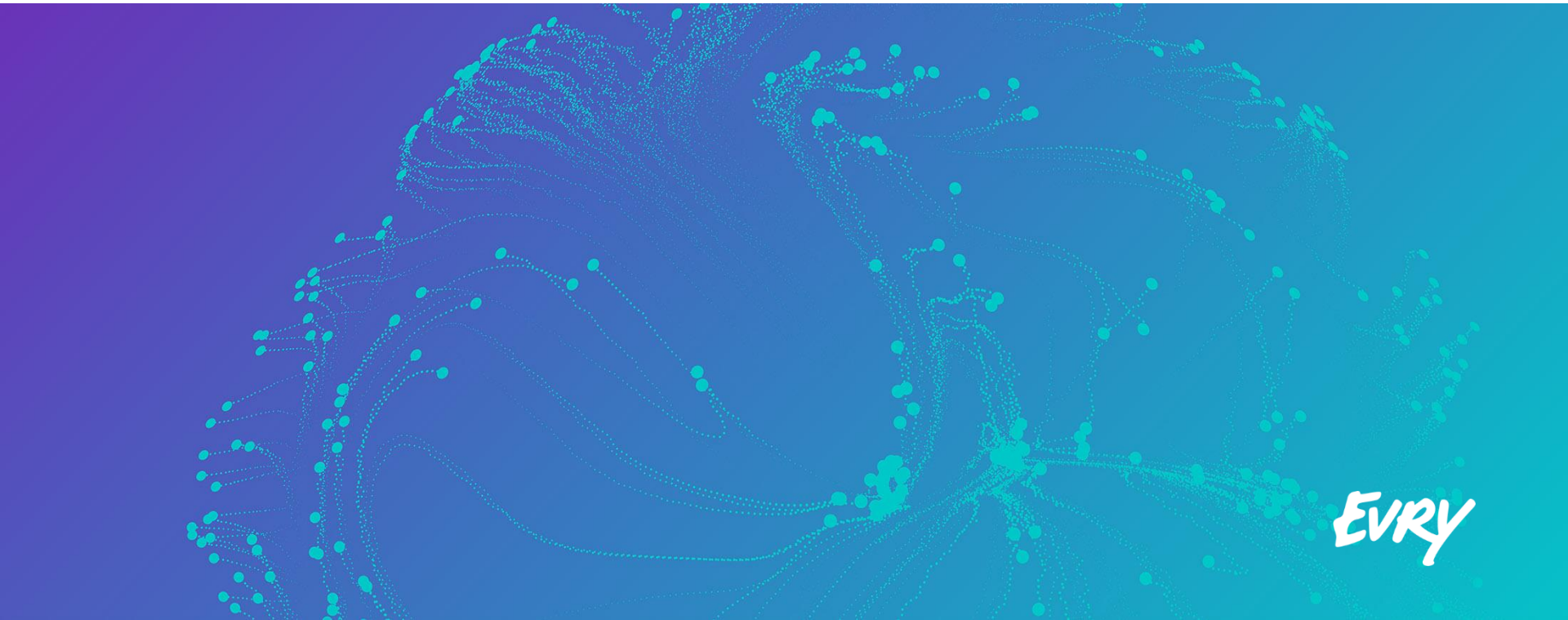
Agenda

- Chapter I – Brief Introduction
- Chapter II – What Is Penetration Testing?
- Chapter III – Pentest in Financial Institutions
- Chapter IV – Security Incidents
- Chapter V – Summary

EVRY

Brief Introduction

CHAPTER I



Who am I?

Education

Candidate of Engineering Sciences in Information Security

KHNURE, Ukraine

Ph.D. in Cryptology

University of Bergen, Norway

Additional

Certificates

- Certified Ethical Hacker
- Certified Encryption Specialist

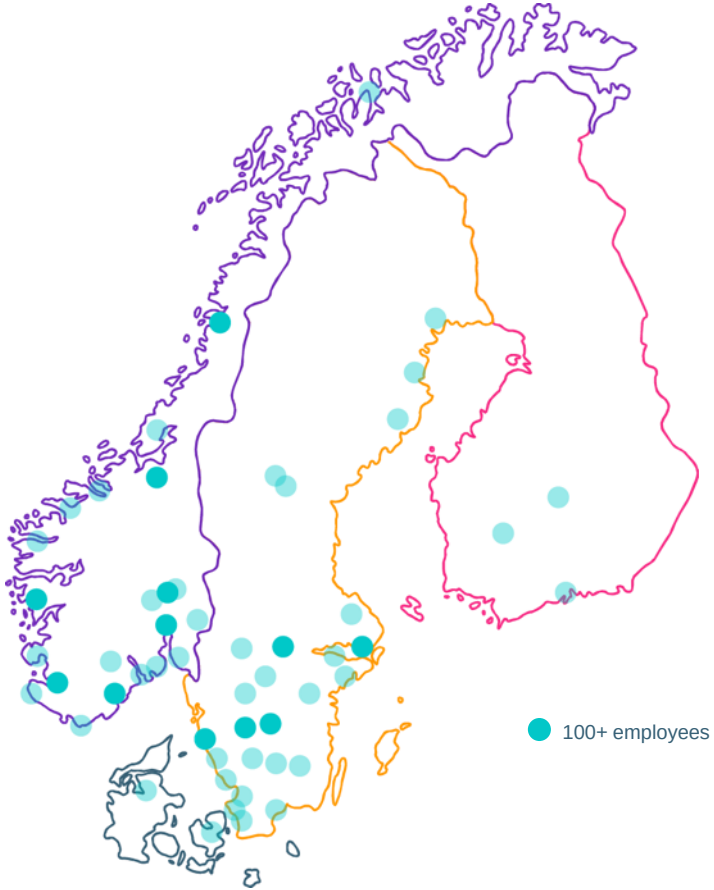
Standards

- DSTU 7624:2014
- DSTU 7564:2014

EVRY
– Nordic Champion

- 50 towns and cities with capacity to deliver
- 11 regional offices with specialist competencies
- 10.000 employees

Women	Age	Universum
26%	39yrs	#4

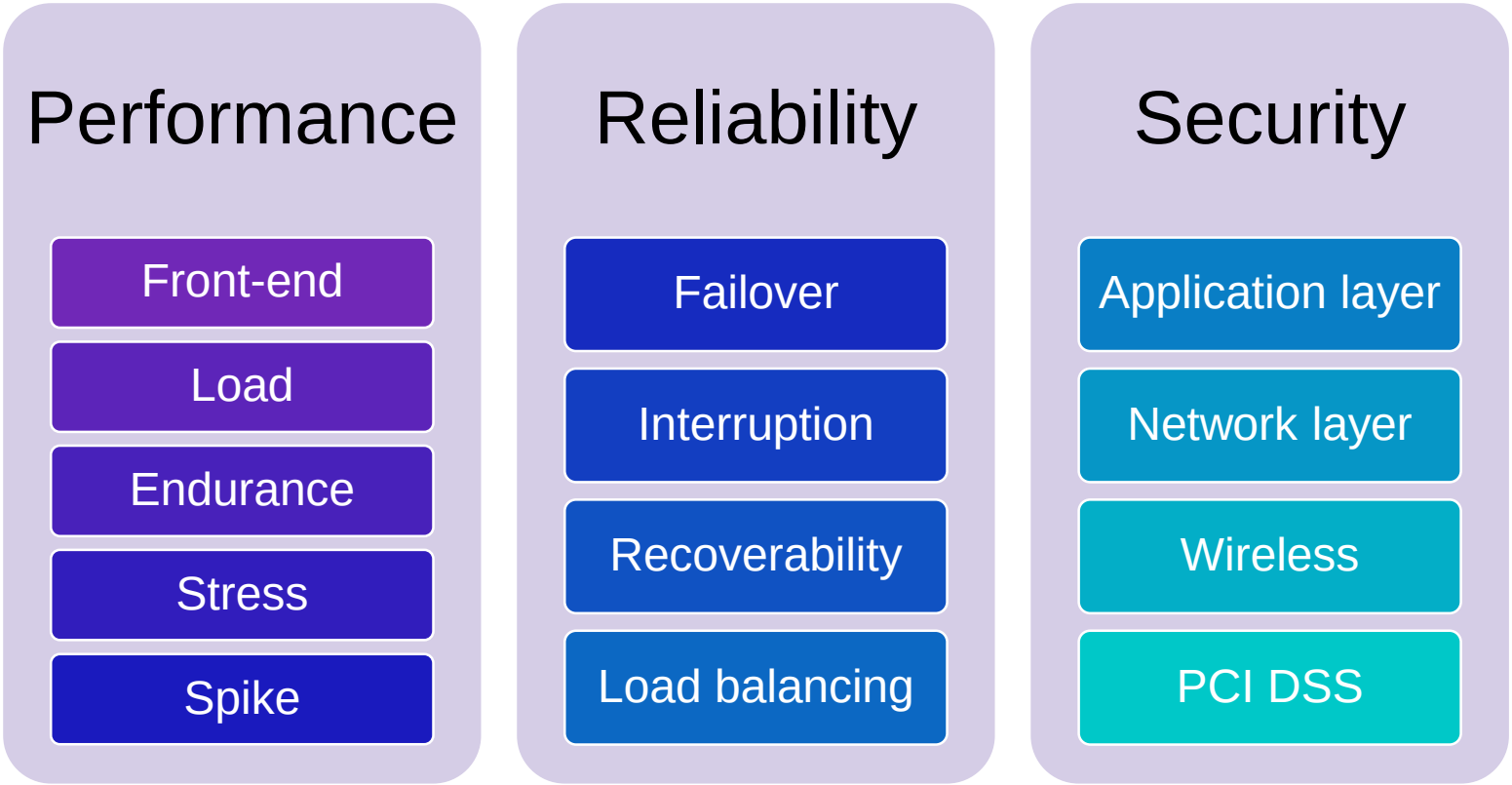


EVRY GROUP - Geographic distribution

Nordics

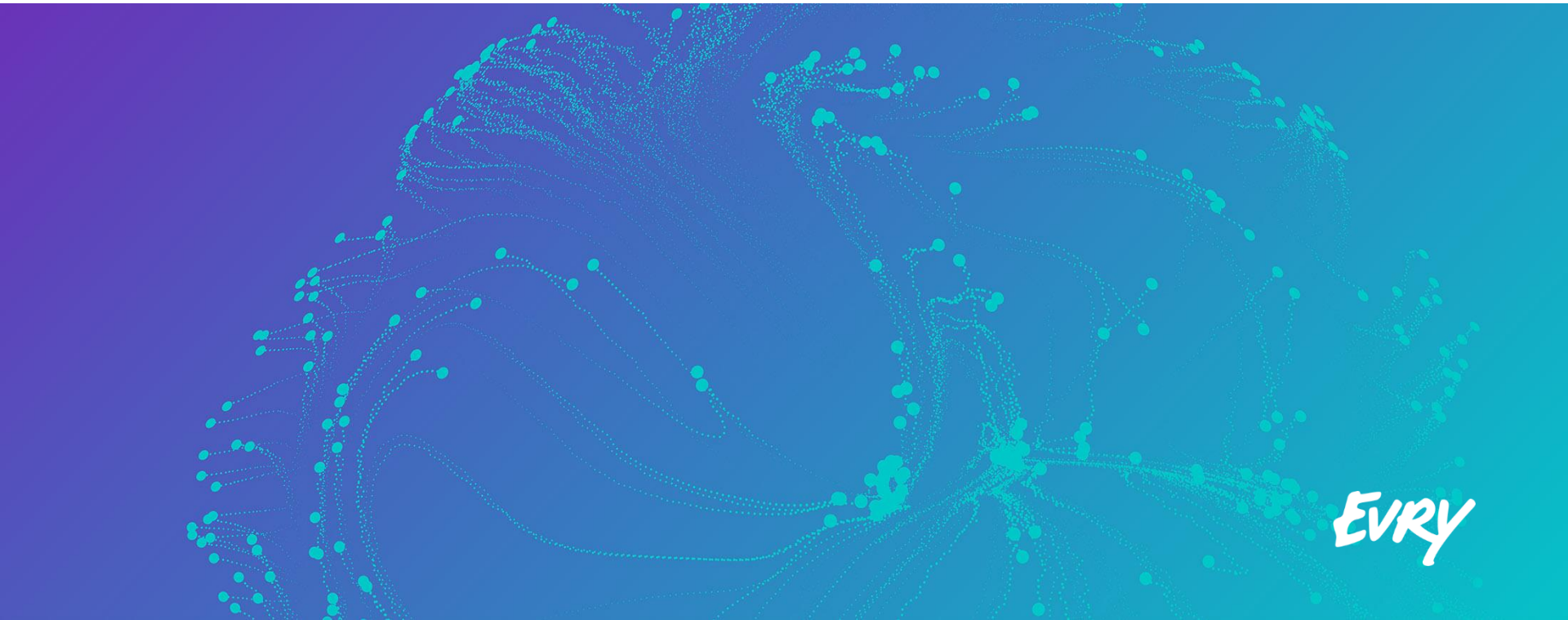
Rest of the World (Global Delivery)

NFT Department



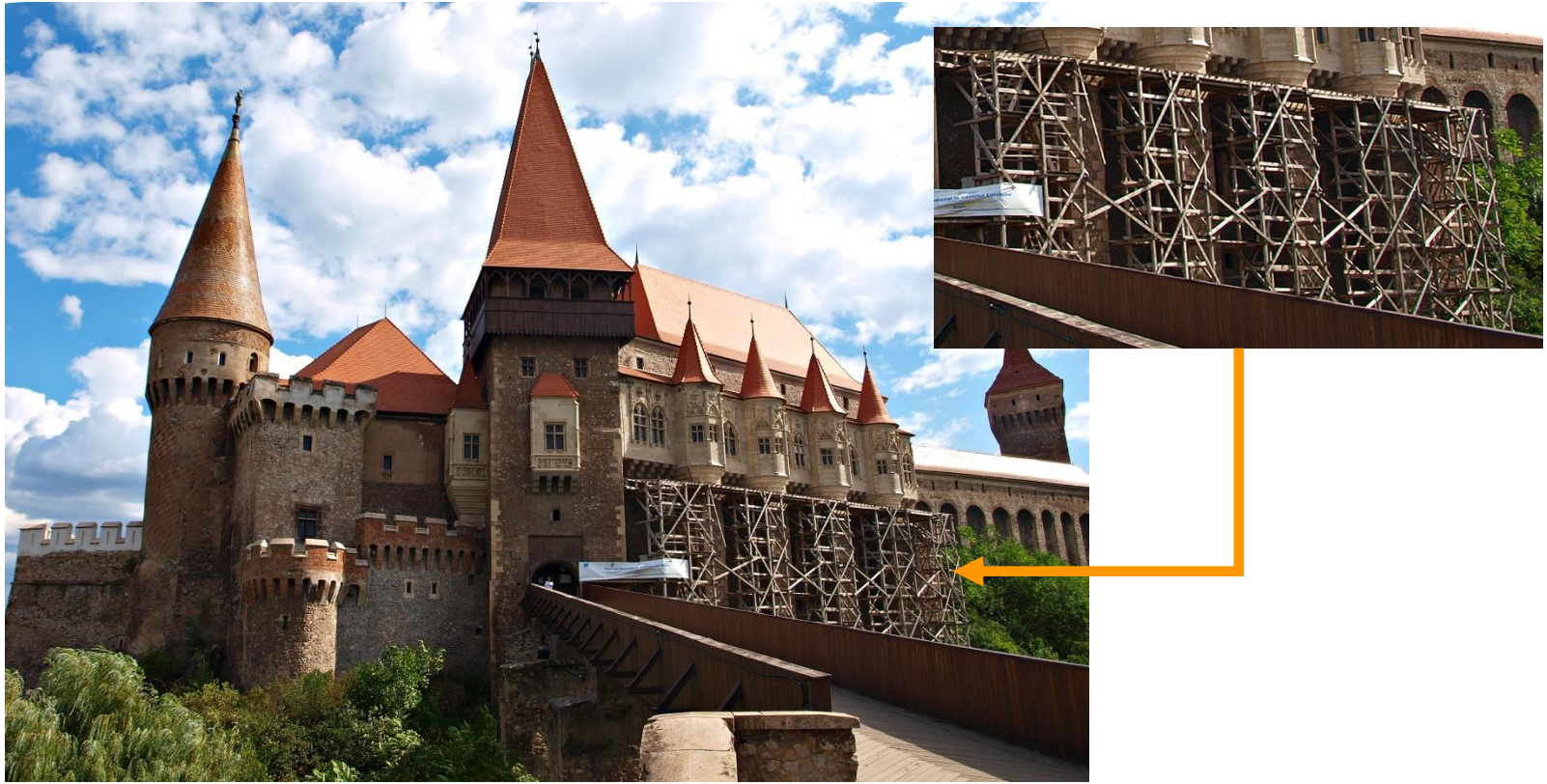
What Is Penetration Testing?

CHAPTER II



Base Definitions

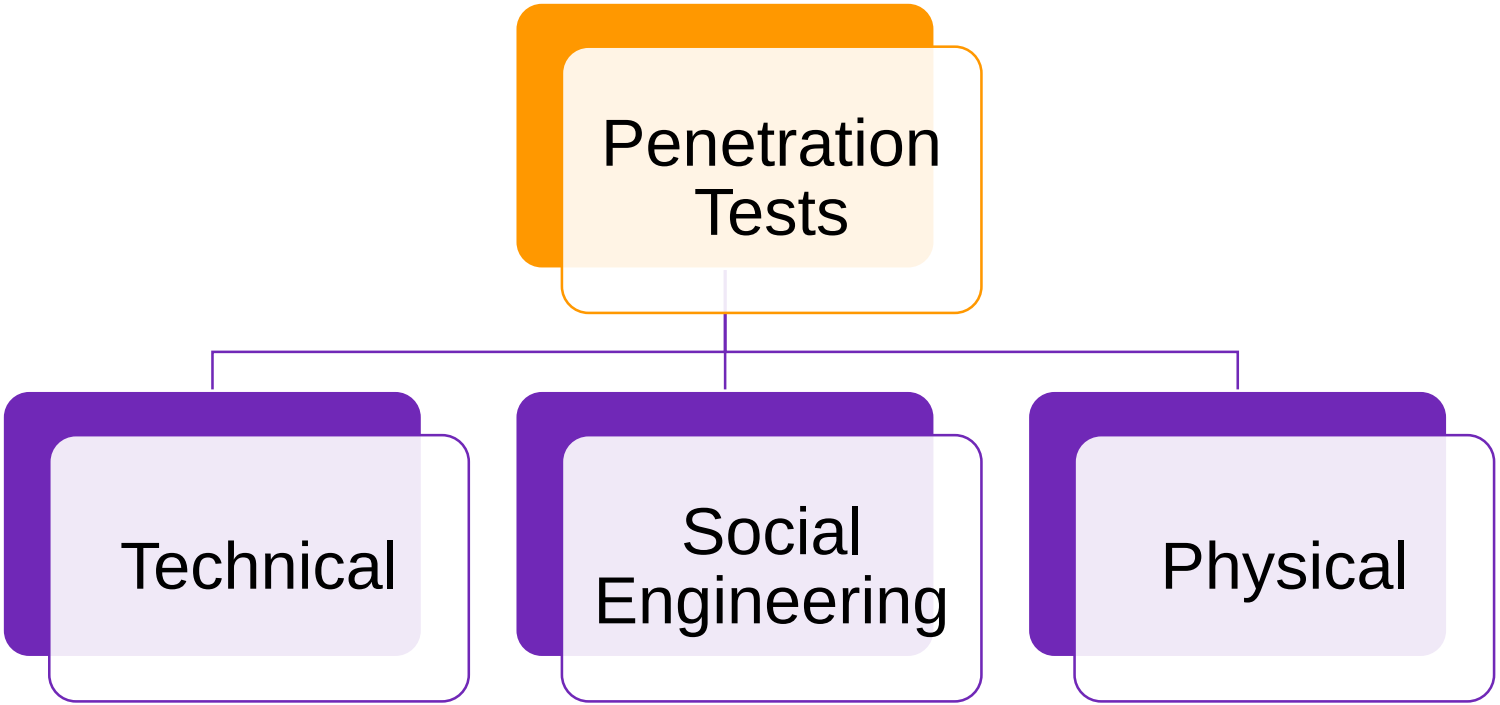
Vulnerability Scanning vs Penetration Testing



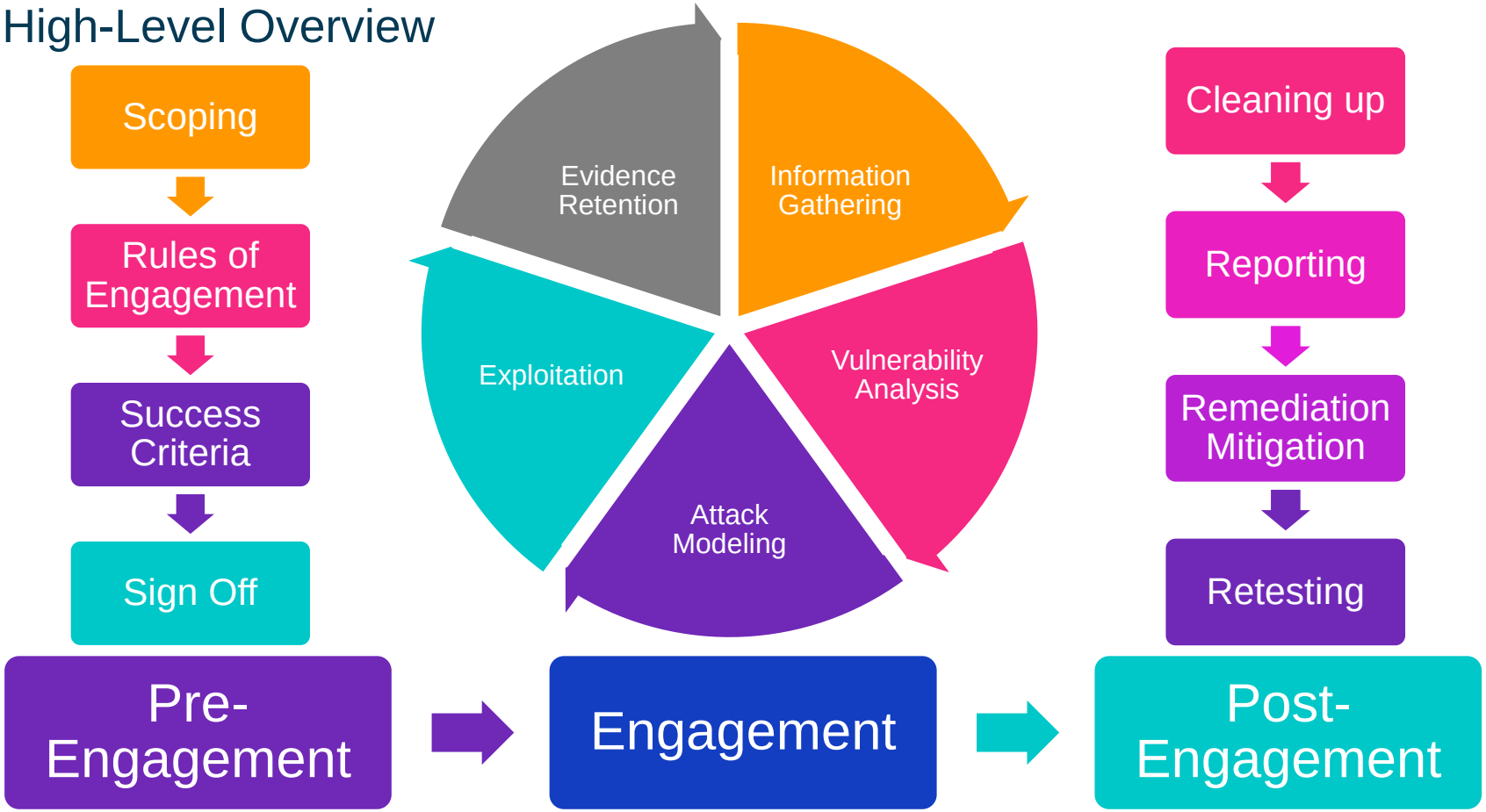
Corvin Castle in Transylvania

Source: https://en.wikipedia.org/wiki/File:Hunyad_Castle_TB1.jpg

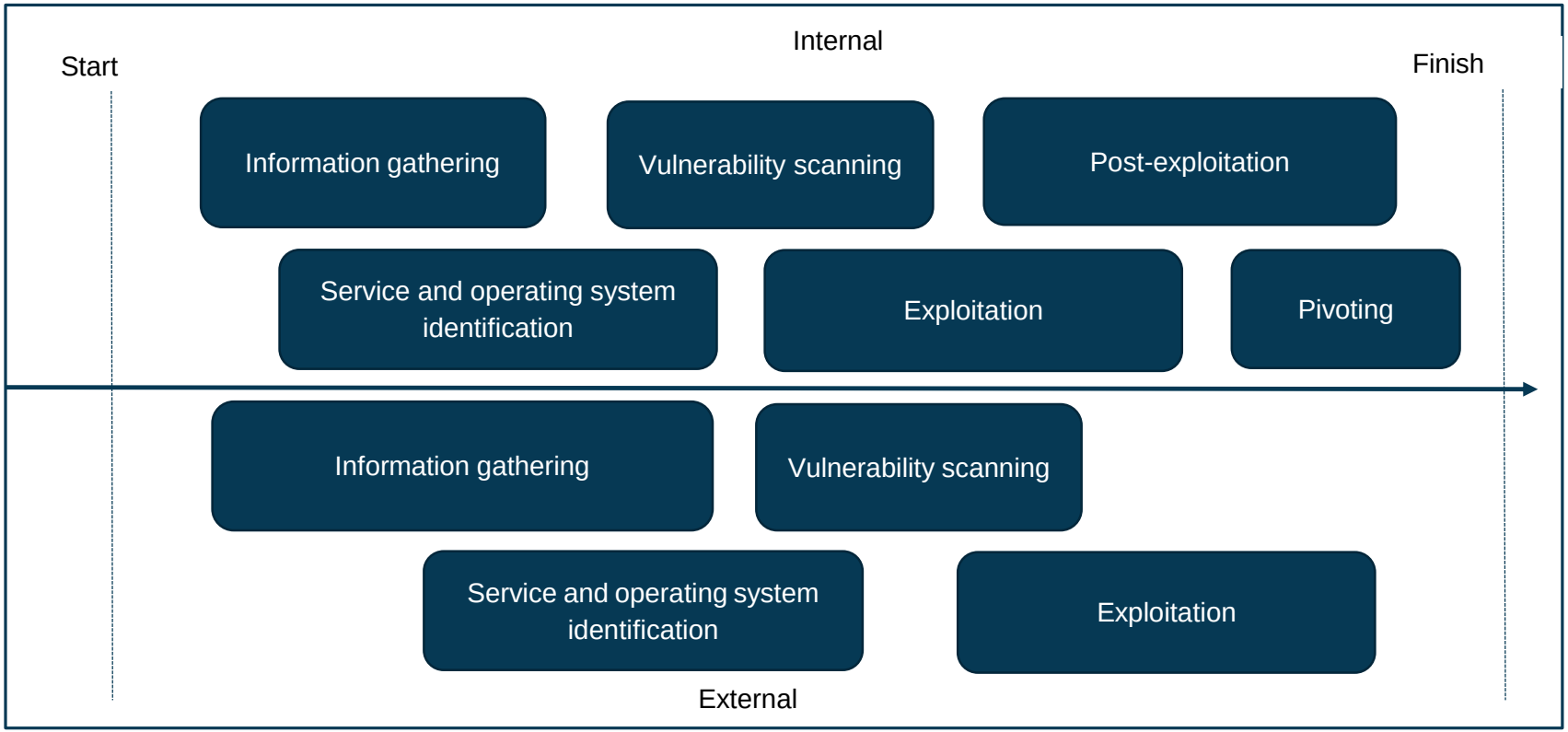
Types of Penetration Tests



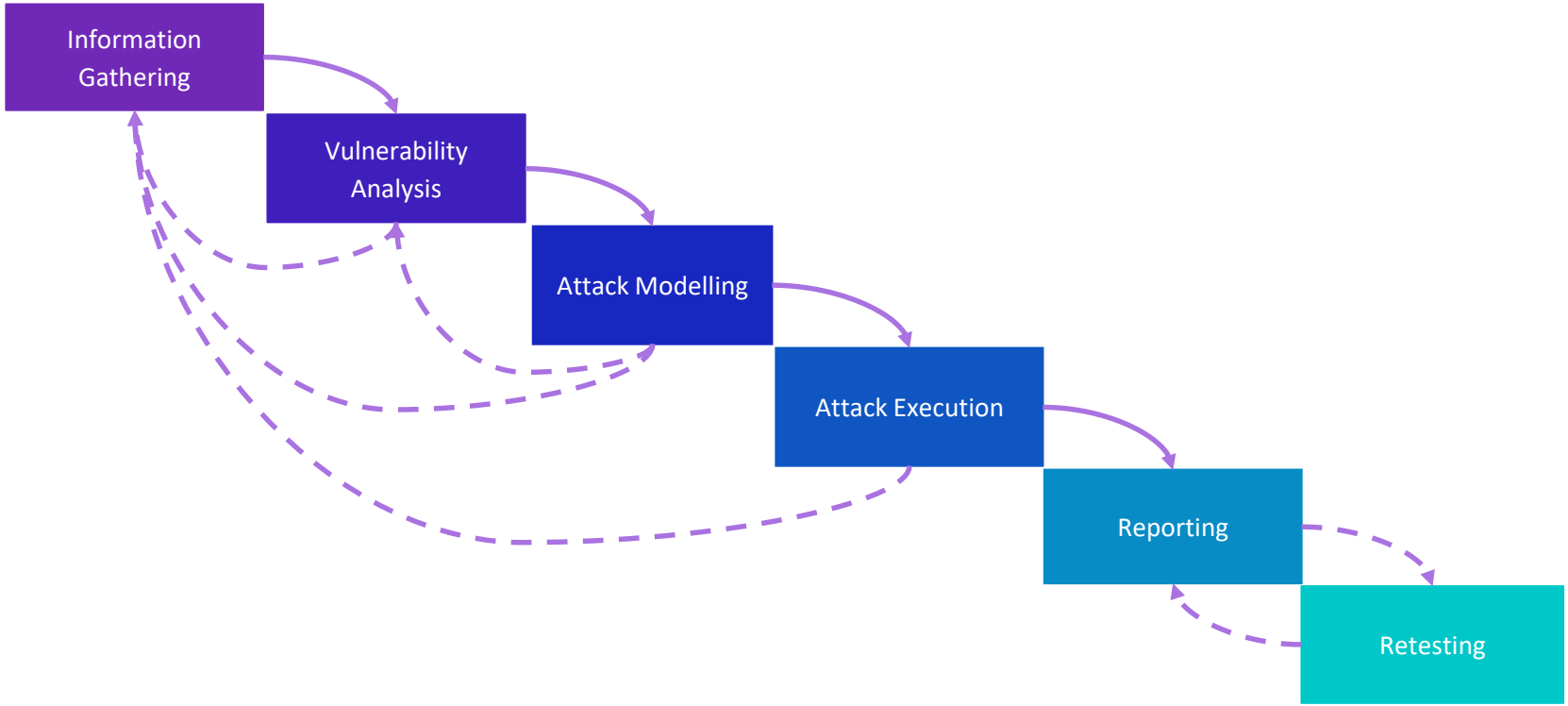
High-Level Overview



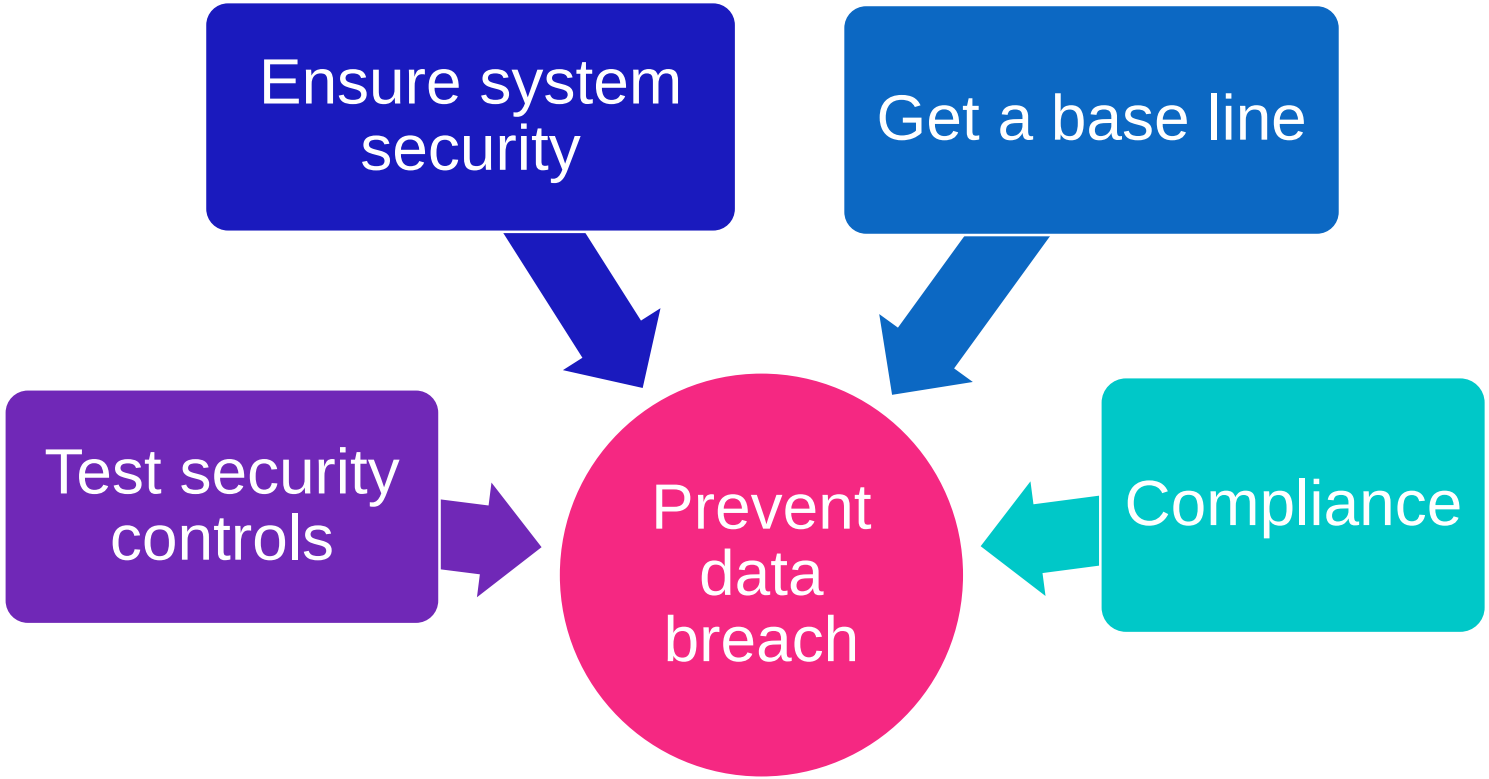
Timeline of a Penetration Test



Workflow of a Penetration Test

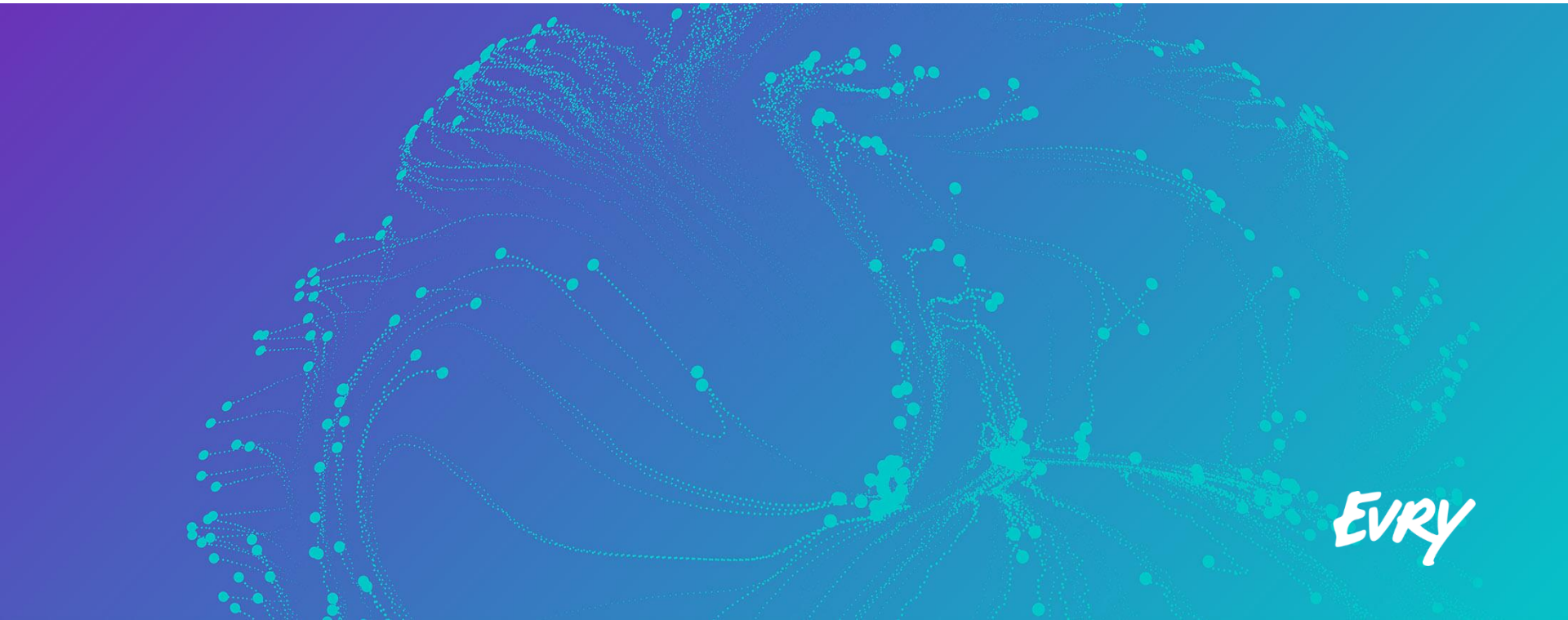


Why conduct a penetration test?



Pentest in Financial Institutions

CHAPTER III

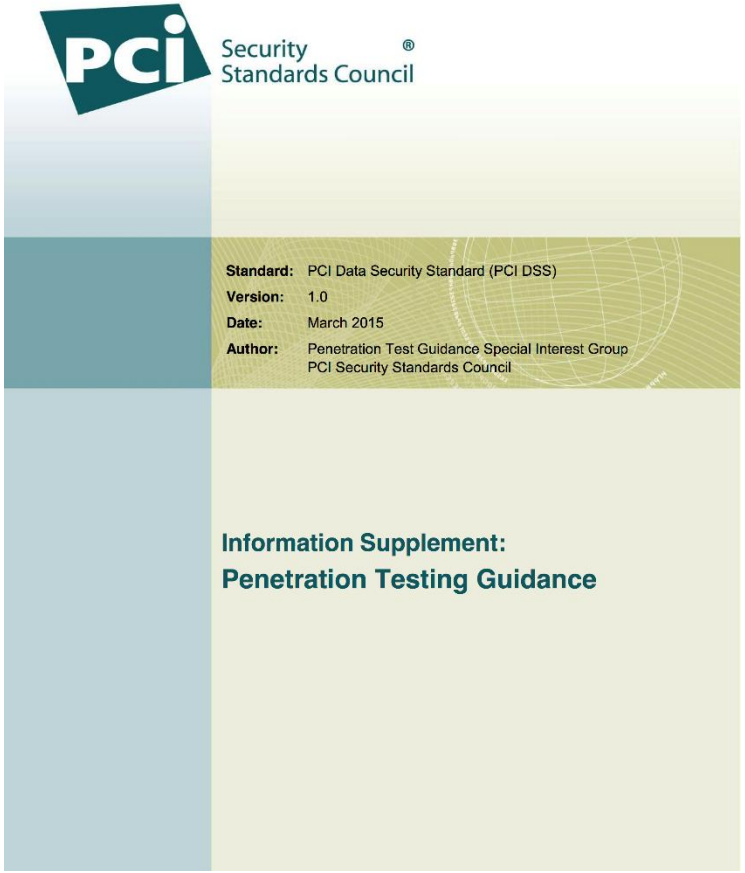


PCI DSS

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 3.2
April 2016



PCI DSS: What? When?

Requirement 11.3.1

- *“Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).”*

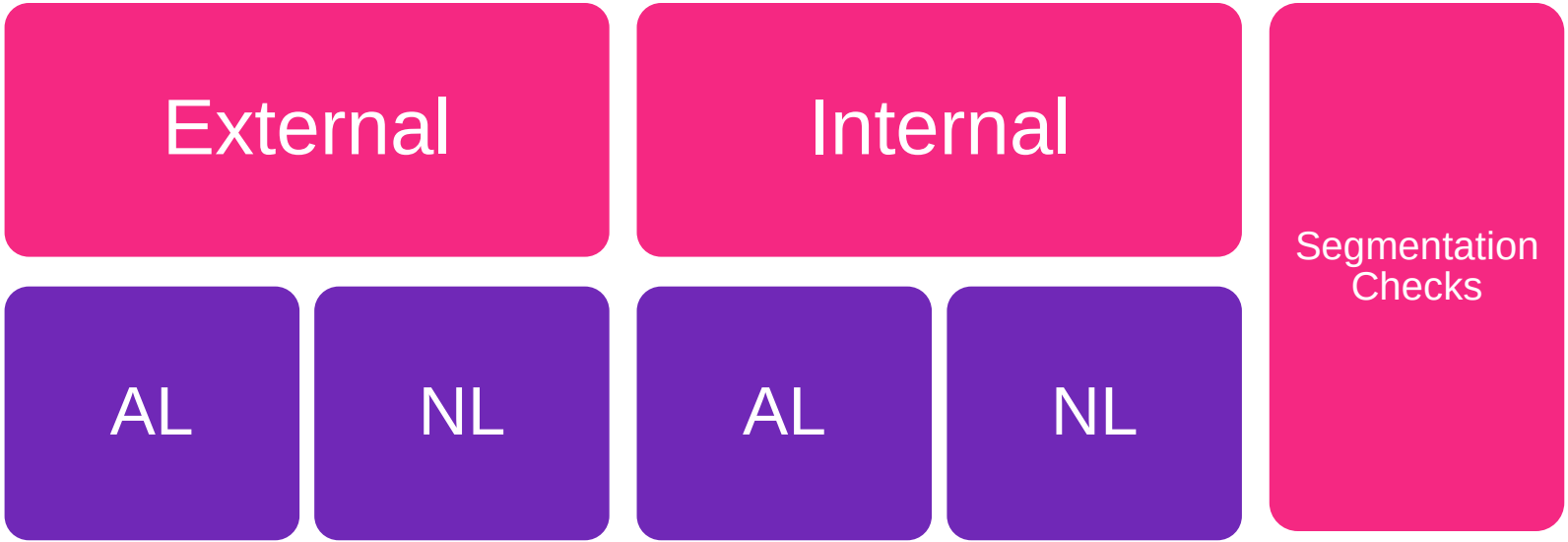
Requirement 11.3.2

- *“Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).”*

Penetration testing Guidance: How?

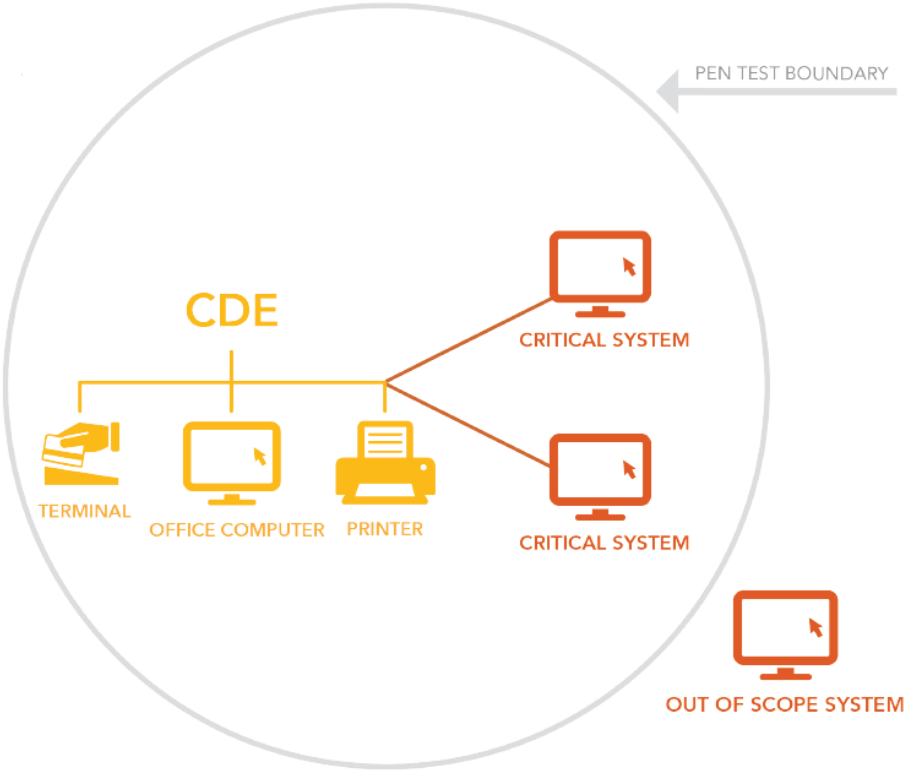
Penetration Testing Components	Qualifications of a Penetration Tester	Penetration Testing Methodologies	Penetration Testing Reporting Guidelines
• Understanding of the different components that make up a penetration test and how this differs from a vulnerability scan including scope, application and network layer testing, segmentation checks, and social engineering	• Determining the qualifications of a penetration tester, whether internal or external, through their past experience and certifications.	• Detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement.	• Guidance for developing a comprehensive penetration test report that includes the necessary information to document the test as well as a checklist that can be used by the organization or the assessor to verify whether the necessary content is included.

PCI DSS Penetration Testing



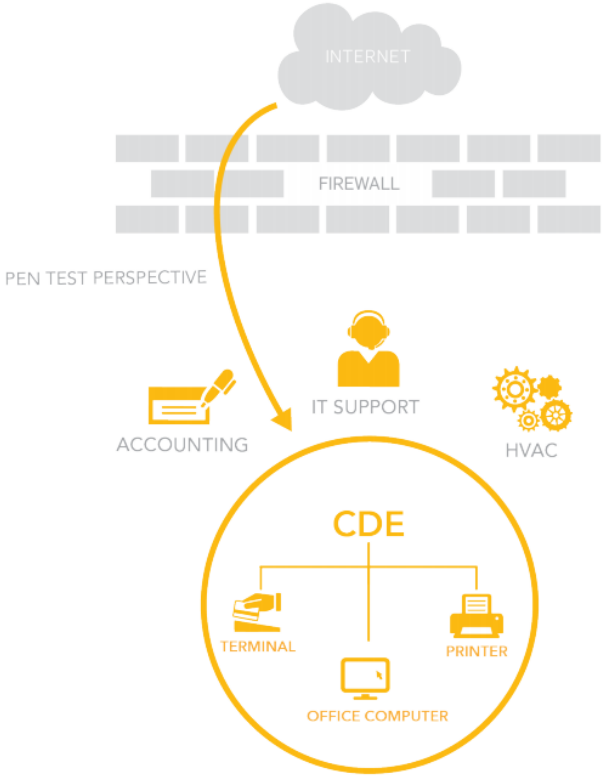
EVRY

Cardholder Data Environment (CDE)

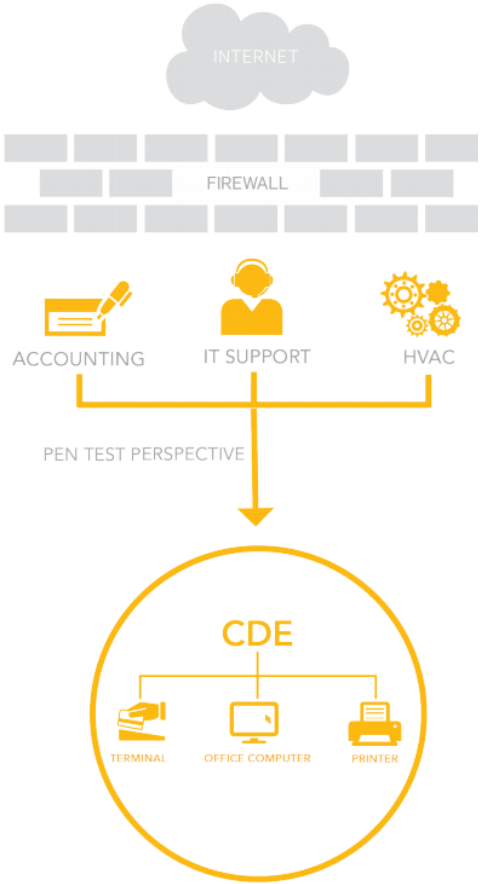


Source: https://www.securitymetrics.com/static/resources/orange/new-penetration-testing-requirements-explained.pdf

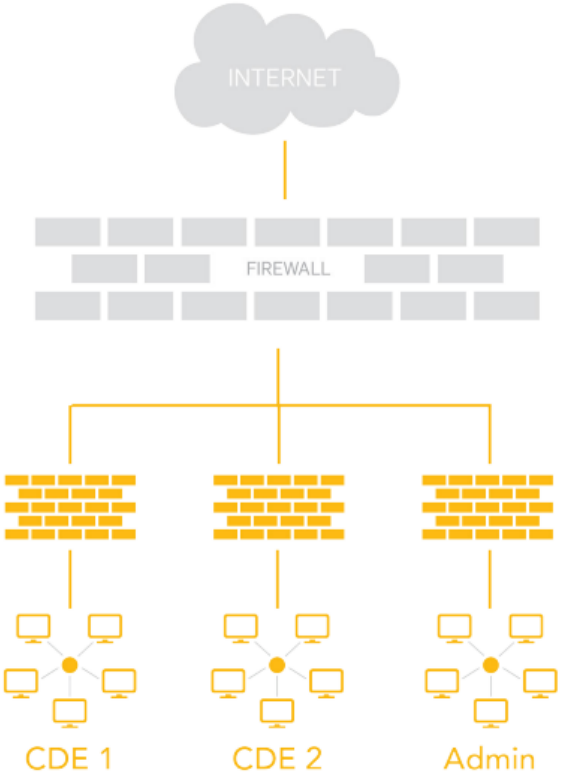
Scope for PCI DSS Pentest



External



Internal

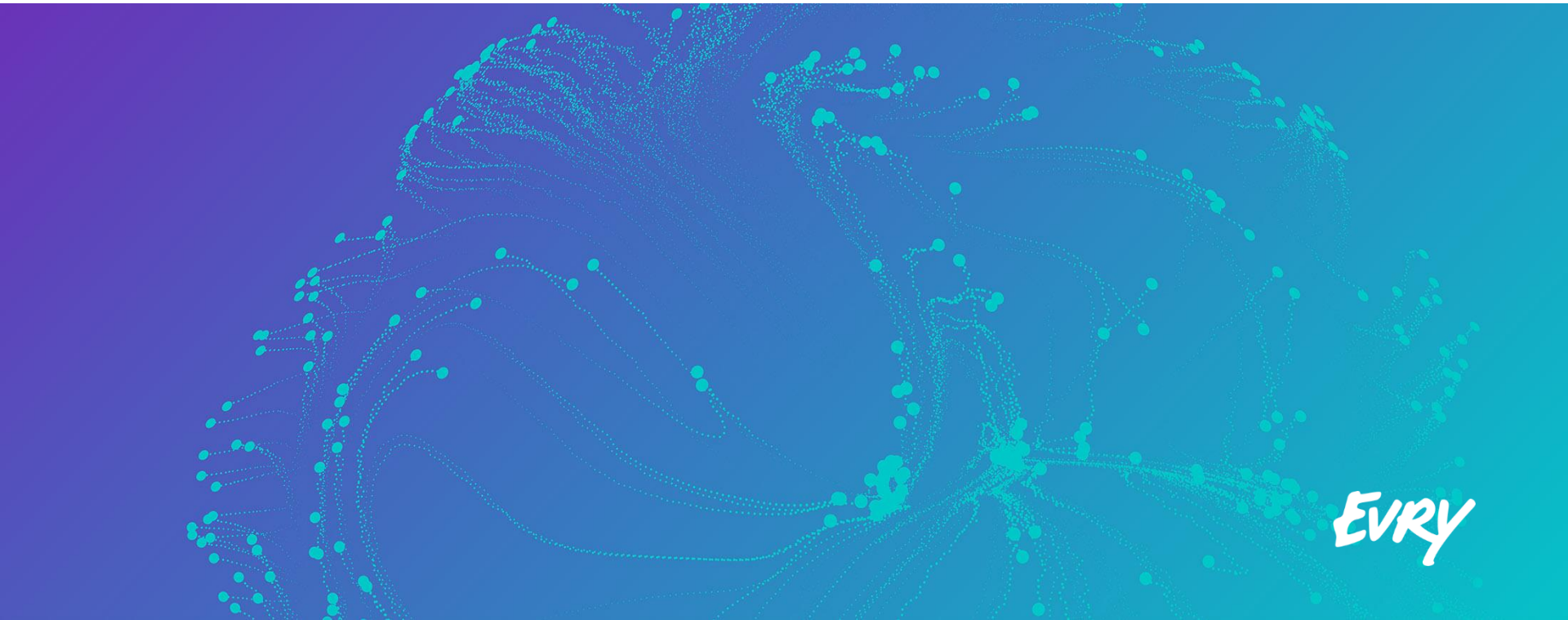


Segmentation

Source: https://www.securitymetrics.com/static/resources/orange/new-penetration-testing-requirements-explained.pdf

Security Incidents

CHAPTER IV



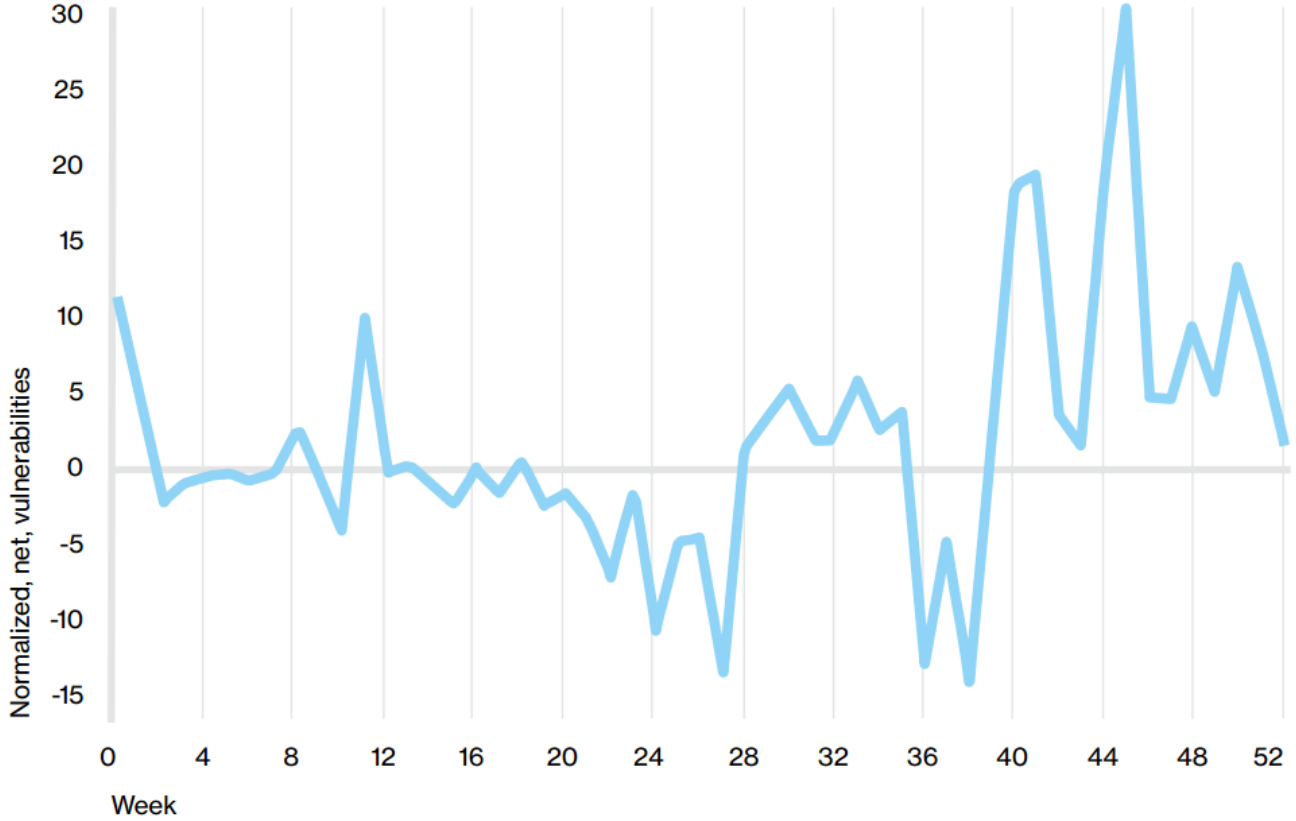
2016 Data Breach Investigations Report

2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

EVRY

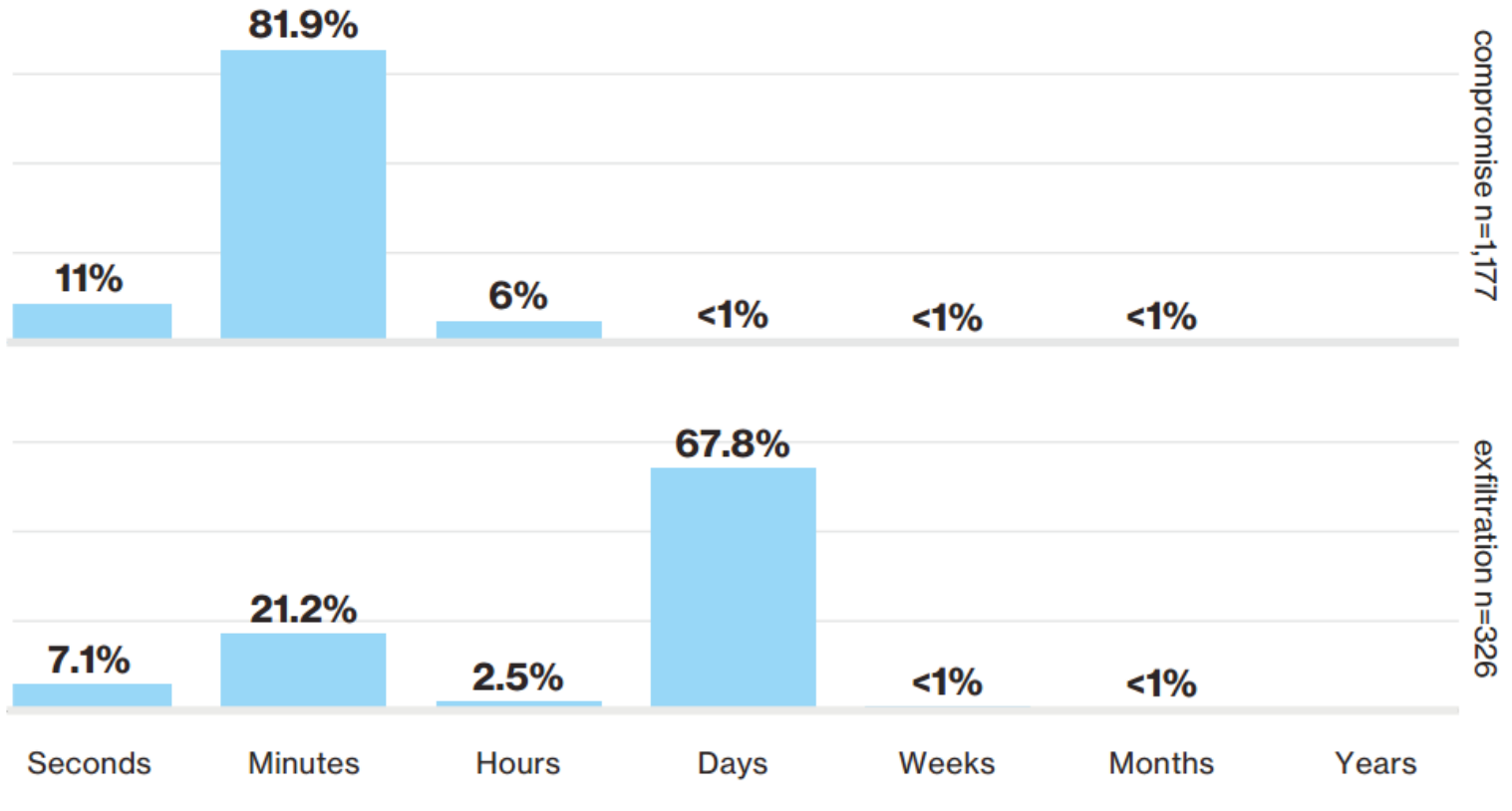


Delta of Number of Vulnerabilities Opened Each Week and Number Closed

Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

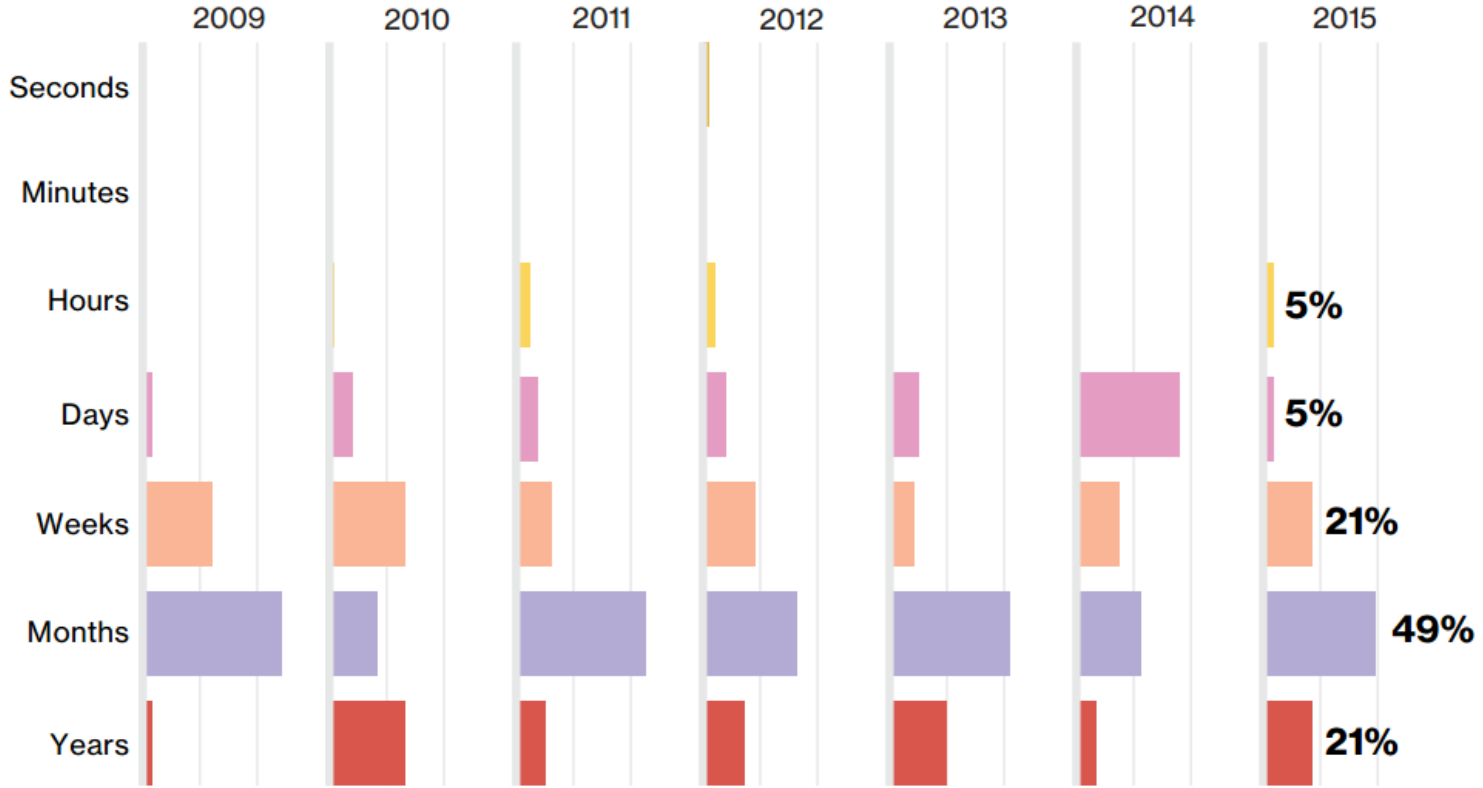
EVRY

Time to Compromise and Exfiltration



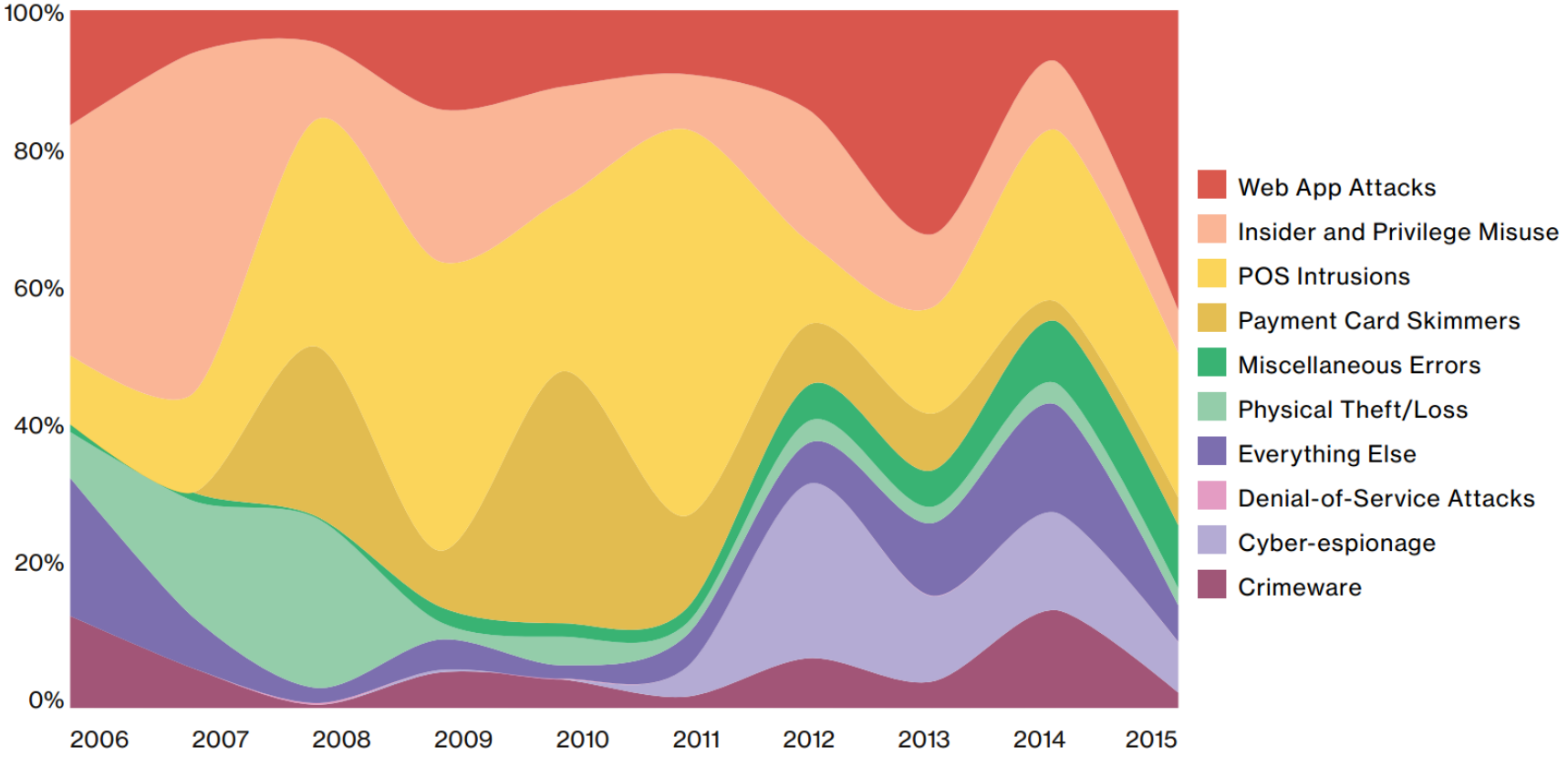
Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Discovery Timeline Within Insider and Privilege Misuse Over Time



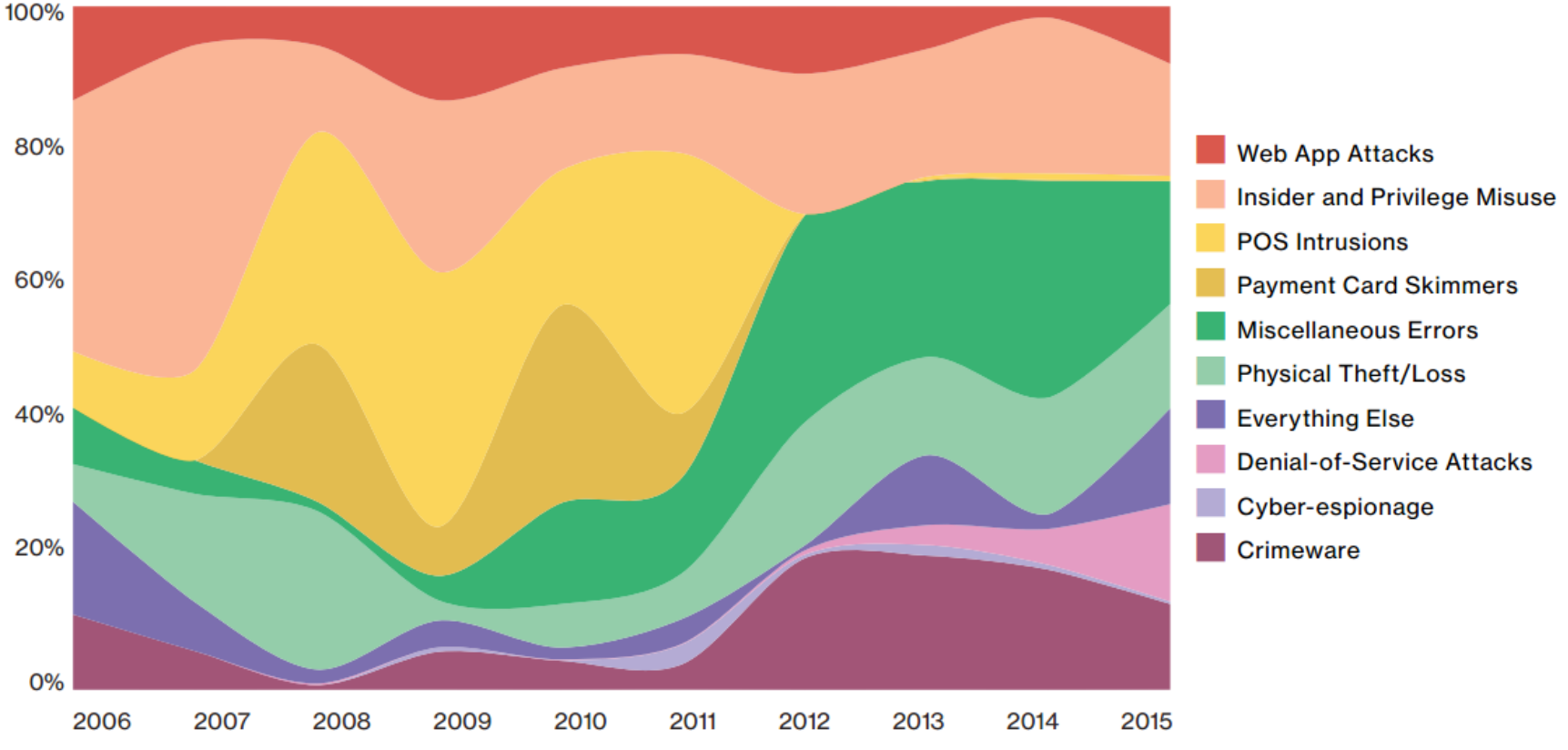
Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Frequency of Incident Classification Patterns Over Time Across Confirmed Data Breaches



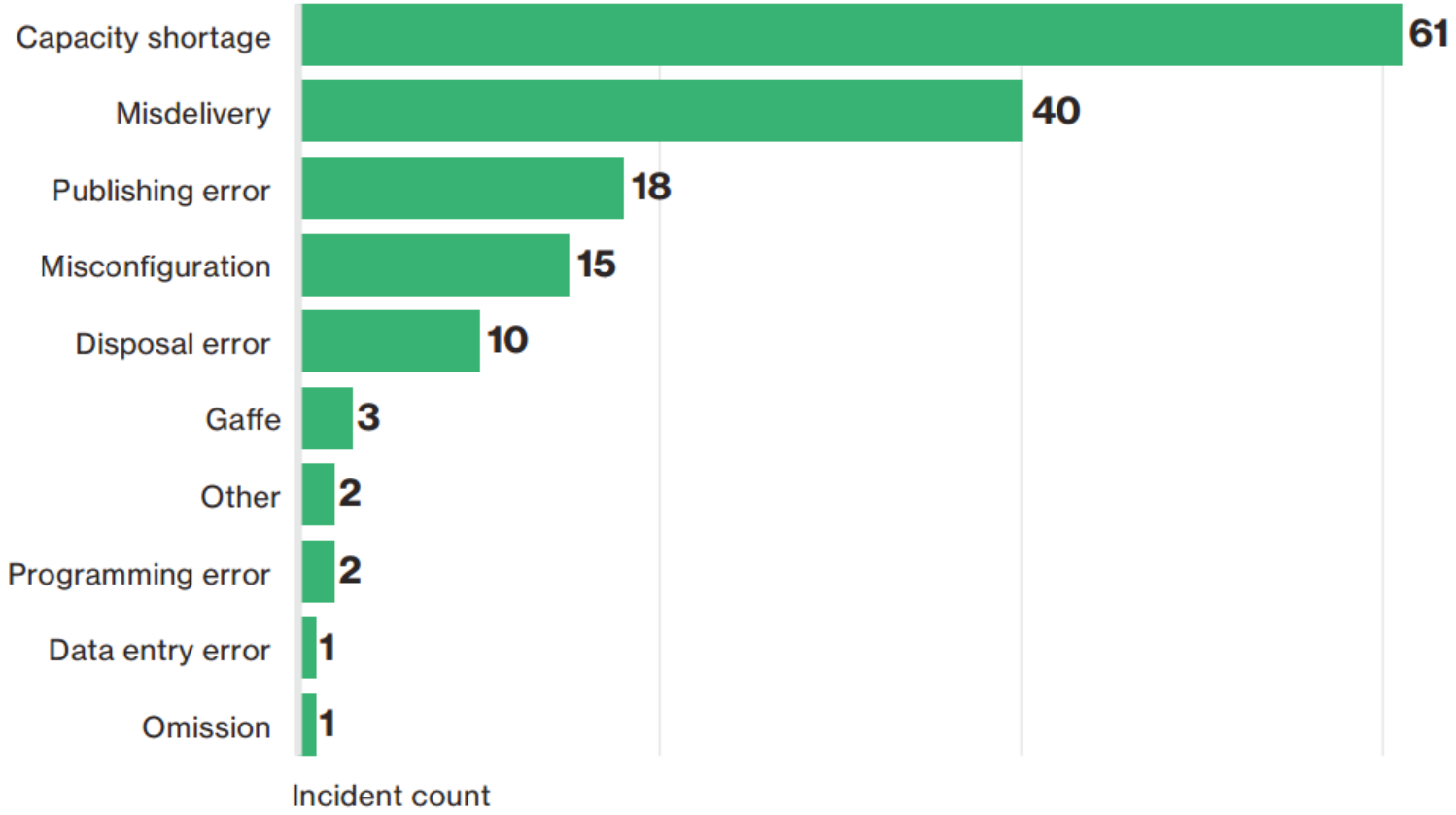
Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Frequency of Incident Classification Patterns Over Time Across Security Incidents



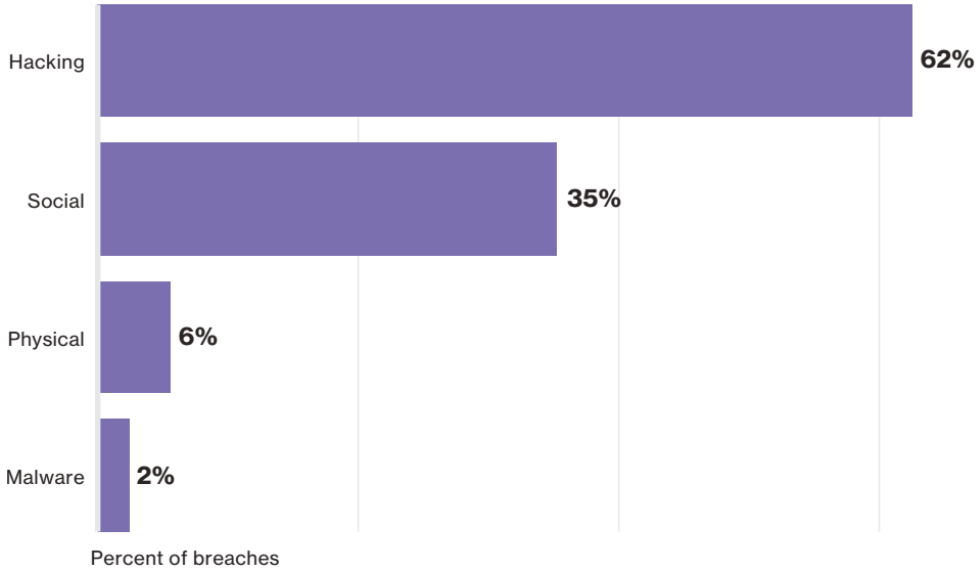
Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

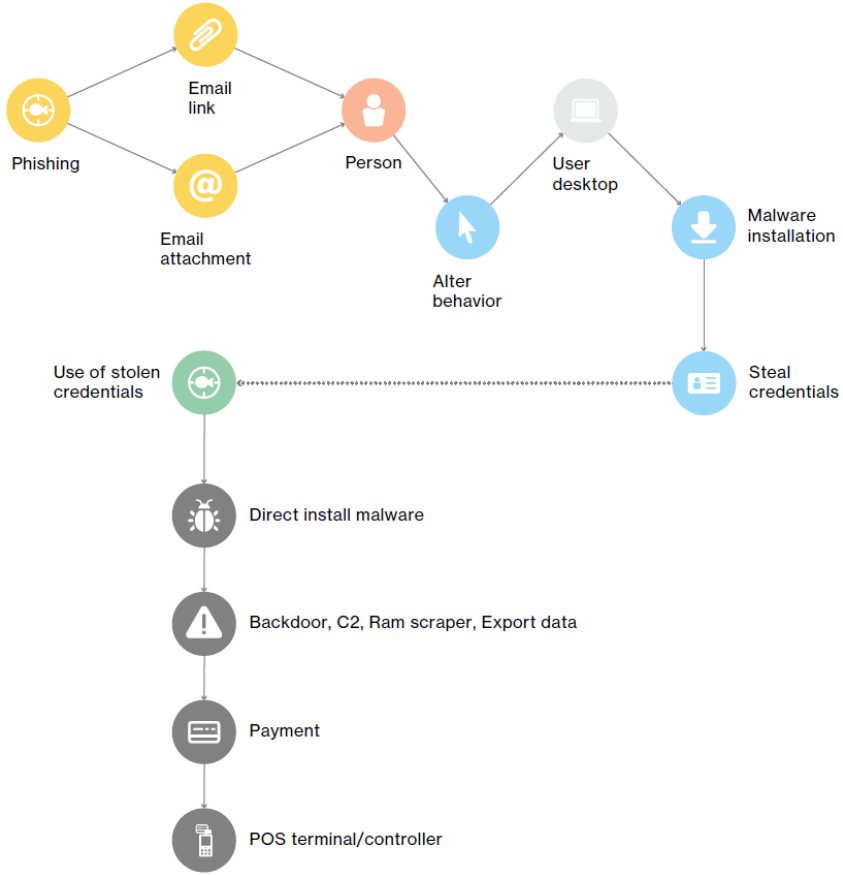
Top 10 Threat Action Varieties Within Miscellaneous Errors, Excluding Public



Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Summary





Threat Actions Within Everything Else Breaches

Source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf


EVRY
Digital
+\dvantage