Incident Response

Overcoming the Main Challenges

Presenter Introduction

- Angelo Violetti, 5+ years of experience in Digital Forensics & Incident Response
- Senior DFIR Analyst @ Swisscom CSIRT
- Threat Intelligence Analyst and Contributor @ The DFIR Report
- BSc in Computer Engineering and MSc in Cyber Security
- AWS & Azure Incident Response Certifications, Certified Forensic Analyst (GCFA) and Red Team Operator
- Speaker at Defcon 32 Blue Team Village, SANS Ransomware Summit, etc.

Section 1

Why Incident Response Matters

Section 2

Key Challenges in Incident Response

Section 3

Real-World Case Study

Section 4

Strategies for Effective Incident Response

Why Incident Response Matters

Data breaches and incident statistics

$4.88 million (USD)

Global average cost of a data breach in 2024

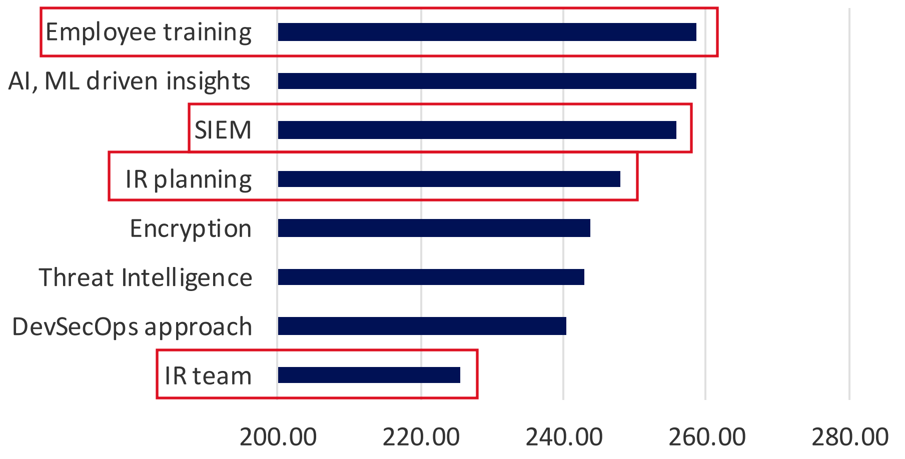
+10% ↗

Increase of the global average cost of a data breach in 2024 over 2023

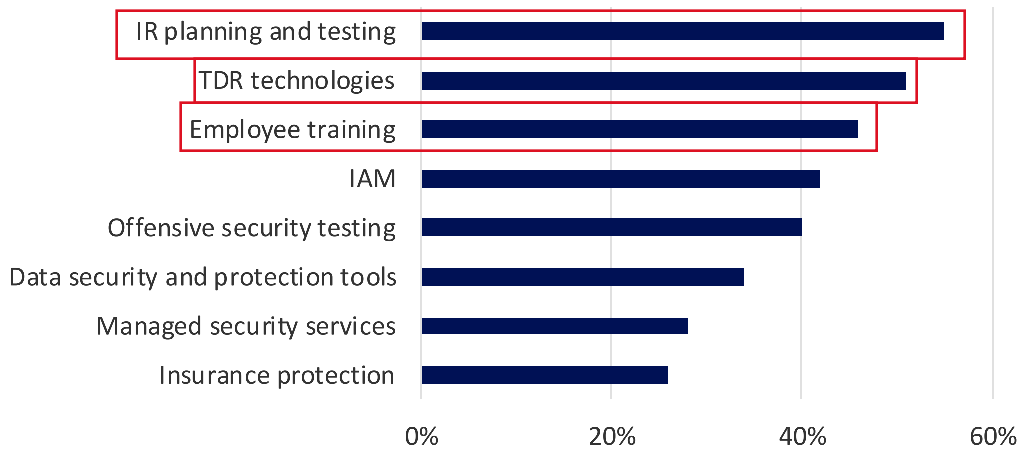
62,954 cyber incidents reported

Switzerland NCSC reported incidents in 2024 (an increase compared to the 49k in 2023)

Main factors that reduced the average breach cost (cost difference from USD 4.88M breach average)



Most common investment types among those increasing security investments after a data breach



Sources: IBM - Cost of a Data Breach Report 2024, Switzerland NCSC – Semi-Annual Report 2024/II

Key Challenges in Incident Response

Insufficient Asset Management

Inadequate Log Visibility and Collection

Absence of Appropriate Incident Response Technologies

Shortage of Cyber Security Personnel

Absence of Incident and Crisis Management Processes

Regulatory and Compliance

Difficulty in Implementing Remediation Measures

Real-World Case Study - Ransomware

Attack chain

Initial Access

Initial access broker gains access into the infrastructure via **publicly exposed vulnerability** and sells the access to a ransomware affiliate

Privilege Escalation

Affiliate **compromises** an **administrator account** which provides elevated privileges

Lateral Movement

Affiliate leverages the compromised account to **access multiple systems**

Data Exfiltration

Affiliate **exfiltrates sensitive** and **confidential data** from the victim infrastructure

Impact

Affiliate **deploys** the **ransomware** enterprise widely

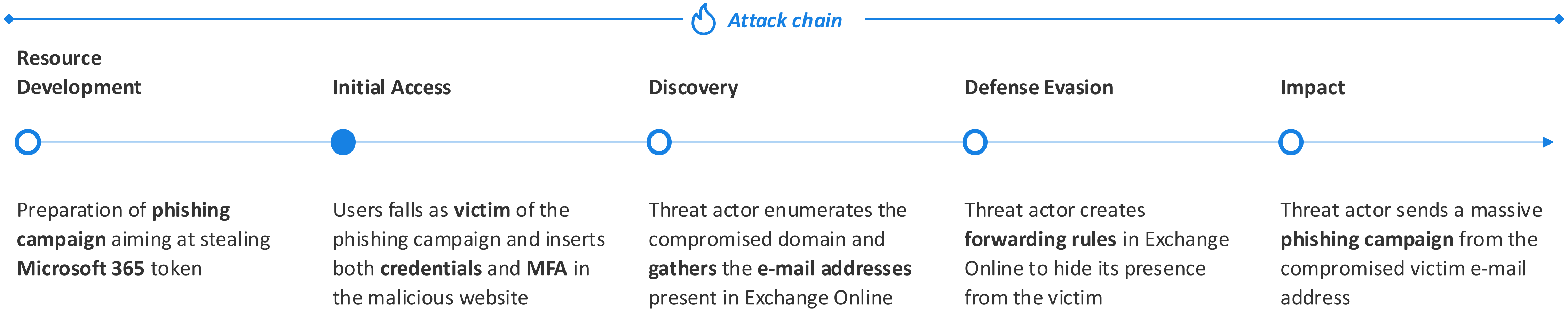
Common Issues Identified

Missing enough logs to identify and analyse the activities performed by the threat actors

Absence of **technologies** to automatically **detect** and **block** the attack

Unavailability of **Crisis** and **Incident management processes**

Real-World Case Study – M365 Identity Theft



Attack chain

Resource Development

Preparation of **phishing campaign** aiming at stealing **Microsoft 365** token

Initial Access

Users falls as **victim** of the phishing campaign and inserts both **credentials** and **MFA** in the malicious website

Discovery

Threat actor enumerates the compromised domain and **gathers** the **e-mail addresses** present in Exchange Online

Defense Evasion

Threat actor creates **forwarding rules** in Exchange Online to hide its presence from the victim

Impact

Threat actor sends a massive **phishing campaign** from the compromised victim e-mail address

Common Issues Identified

Absence of a centralized **log collection** technology and enough retention

Missing proper **prevention policies** to block the attack

Lack of **monitoring** of **alerts** generated by Microsoft native detections

Strategies for Effective Incident Response

Enhance Asset Knowledge: Implement an authoritative Configuration Management Database (CMDB) or asset inventory tool that automatically discovers and tags all hardware, software, virtual machines, cloud workloads and data repositories.

Improve Log Visibility and Collection: Deploy a centralized log-aggregation platform (SIEM) that ingests logs from firewalls, endpoints, servers, applications and cloud services.

Acquire and Integrate Proper Response Technologies: Build a technology stack that includes technologies to properly respond to a cyber security incident, like: EDR/XDR, network IDS/IPS, etc.

Incident Response Personnel or Retainer: Invest in ongoing professional development (e.g., certifications, tabletop exercises, etc.) to build internal expertise. Supplement staff with external partners or managed-service providers to fill gaps and provide capacity during major incidents.

Establish Robust Internal Crisis-Management Processes: Document a formal Incident Response Plan and related playbooks, including clear escalation criteria, RACI roles, and communication templates. Exercise the process regularly through tabletop scenarios and full-scale simulations, then refine playbooks based on lessons learned.

Embed Compliance in IR: Maintain up-to-date documentation (e.g., risk assessments, DPIAs, evidence logs) to demonstrate “adequate measures” and to streamline any audits or investigations.

Streamline Deployment of Remediation Measures: Adopt a change-management framework that allows rapid, risk-controlled deployment of patches, configuration changes or network controls—even in crisis situations.

Contact information

Swisscom (Schweiz) AG
B2B-ITL-PSY-TDR-CYD
Angelo Violetti
Förrlibuckstrasse 60/62, 8005 Zürich

+41-79-664 29 75
Angelo.Violetti@swisscom.com