Team Overview

ZeroDay Response Team

Henry Ng, s5423376, (Project Manager & Team Leader)

Minhaj Ahmed, s5419774, (Security Architect)

Ansaf Althaf, s5405482, (Security Engineer)

Sherina Lu, s2717884, (Security Analyst)

ZERODAY

RESPONSE TEAM

Presentation Overview

ZeroDay Response Tackles Phishing with ServiceNow

Table of Contents

- Project Presentation
- Project Introduction
- Motivation
- Objectives & Outcomes
- Critical Issues
- Innovative Solution Proposals
- Tools Used
- Methodology
- V-Model
- Risk & Sustainment Plan
- Project Impact
- Prototype Demo in ServiceNow
- Q&A

Project Introduction & Motivation

Purpose – ⬇️ successful email phishing attacks by at least 50%

Motivation – ⬆️ staff morale and confidence in detecting phishing emails

How to do that? Technical solutions (ServiceNow), Microsoft Authenticator, incident response management, role-based access controls (RBAC), KnowBe4

Non-technical solutions – 24/7 support team answering Q&A tailored for each staff member's knowledge and understanding

We understand the difficulties you're encountering, and we're here to support you with solutions that make a meaningful difference 🤝🙂🔧

Objectives & Outcomes

Strengthened Cybersecurity Posture: Strengthen the organisation's cybersecurity by reducing email phishing vulnerability by **50%** by end-2025 and **90%** by end-2026, alongside a 30% reduction in related costs.

Incident Reporting: Maintain a detailed record of phishing incidents in ServiceNow, with a rolling **30-day** dashboard for real-time monitoring.

Streamlined Incident Management: Implement a customised incident management workflow in ServiceNow to ensure response times **under 30 minutes** and prompt service restoration.

Upgraded Security Infrastructure: Upgrade security infrastructure through integration of MFA and RBAC within existing systems, targeting **100%** resolution of integration issues by project completion.

On-going Training Program: Establish a *quarterly* staff training program with phishing simulations and refresher courses to mitigate cyber threats.

What is email phishing? 📧 🎣

Email phishing: A cyberattack in which individuals are deceived into disclosing login credentials or sensitive information via fraudulent emails and malicious links, often leading to password breaches and data theft.

Critical issues

Phishing email attacks

Staffs receive fake emails impersonating company executives and HR leading to financial loss through fraudulent fund transfers

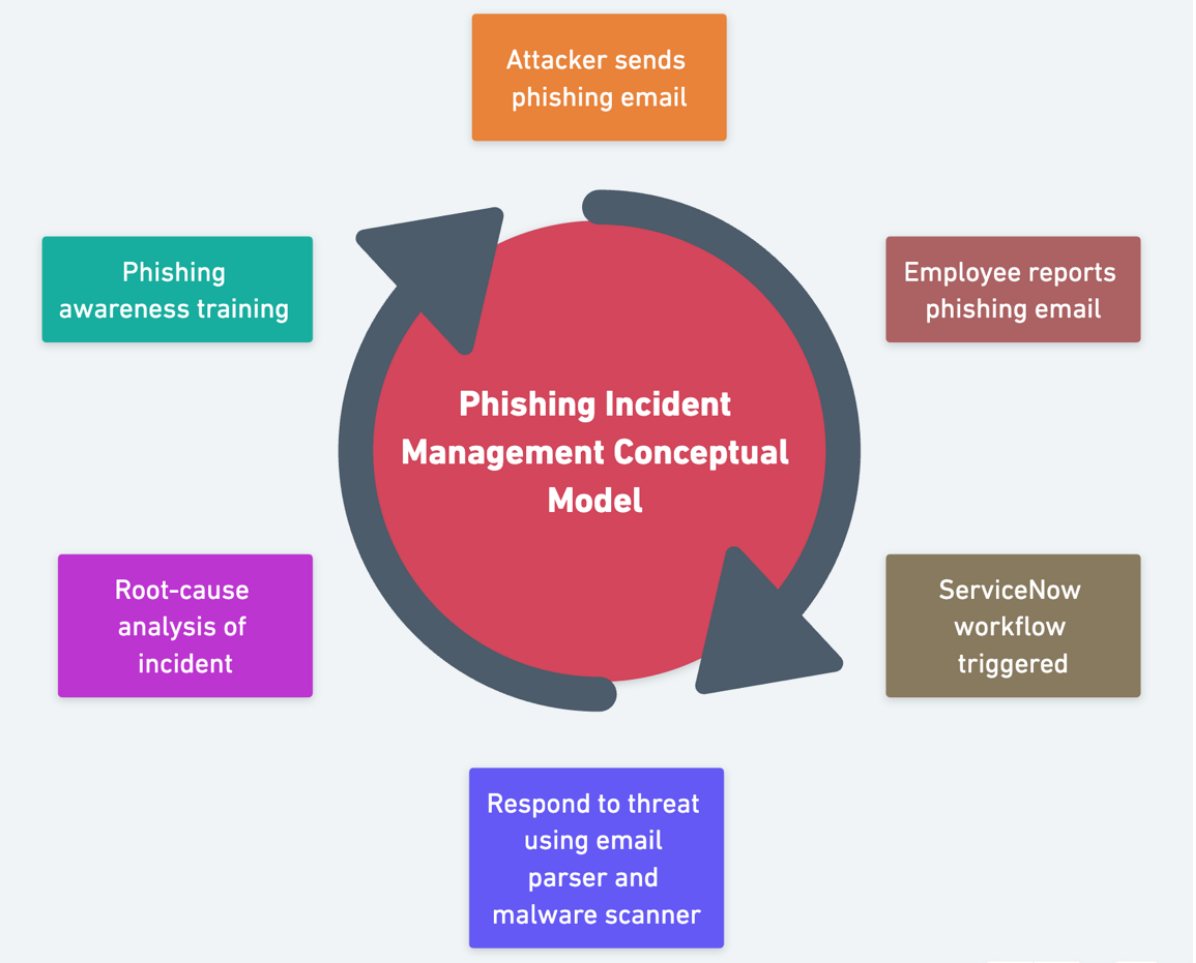
Password Compromises

Weak employee passwords have increased the success rate of phishing attacks, exposing internal systems to unauthorised access and data breaches

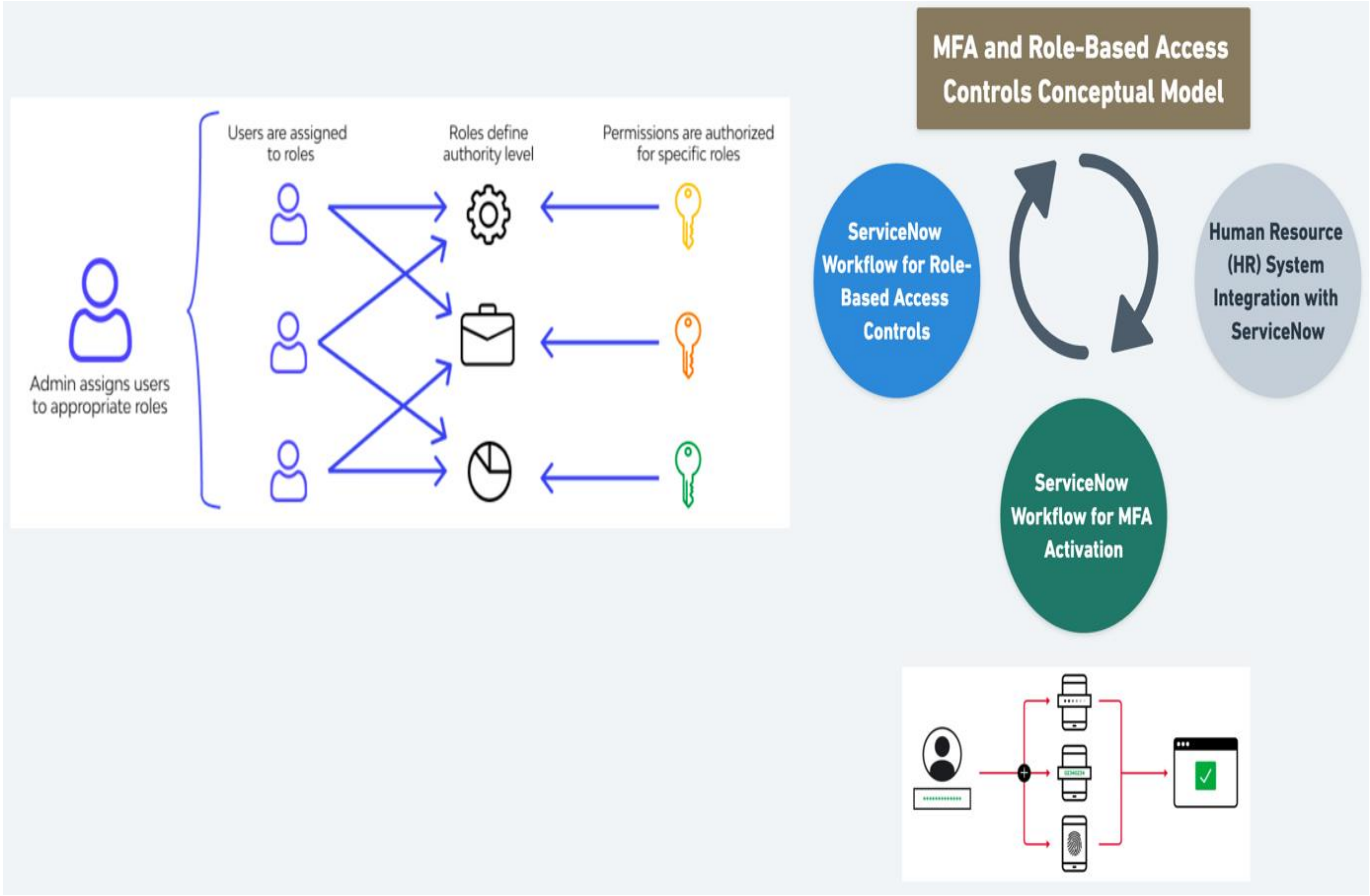
Documentation and Awareness 📘

Incidents have not been documented or used to update training materials, reducing the effectiveness of employee training

Innovative Solution Proposals #1



Innovative Solution Proposals #2



Tools Used

Software	Description
ServiceNow	A cloud-based ITSM platform that automates incident response and workflows. It will track phishing and MFA-related issues by integrating with the company's CRM, ERP, and IoT systems.
Microsoft Authenticator	An MFA application, in sync with Azure Active Directory (AD) to access accounts securely. It improves login security by requiring users to validate their identity through push notifications, OTP codes, or biometric verification.
Zapier	An automation tool that connects to ServiceNow to parse emails and send structured data, enabling faster phishing incident response.
VirusTotal	An open-source threat intelligence tool that scans emails for malicious files, URLs, and IPs using antivirus engines and behaviour analysis, providing malware detection and threat classification

Methodology

Waterfall is a sequential project methodology where each phase planning, development, testing, and deployment follows a fixed order with little overlap.

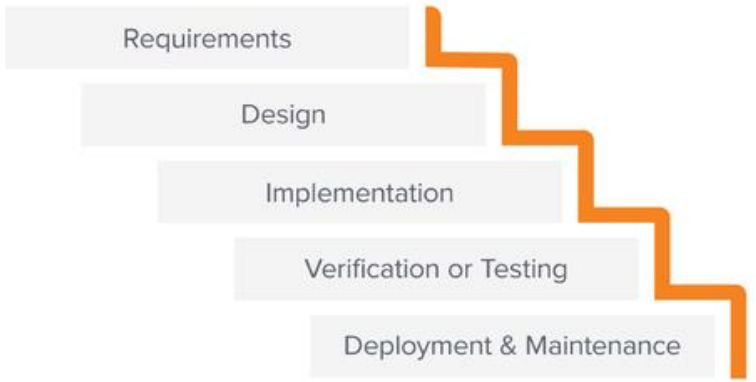
Why did we choose it?

Fixed Requirements 📋 : The project scope, including MFA and phishing workflows, was well-defined from the start.

Clear Phase Structure 📊 : Tasks were designed to follow a strict order. Design first, implementation next, then testing.

Milestone-Based Progress 🎯 : Communication and reviews with stakeholders were scheduled only at key milestones, aligning well with the Waterfall model.

End-to-End Testing 🧪 : Testing and issue resolution were planned as a separate phase, which fits Waterfall's structure.



V-Model (Verification and Validation)

- ✅ Early bug detection
- ⚙️ Confident integrations with external IT systems
- 📈 Scalable, testable, and reliable automation

One of our 🔑 objectives:

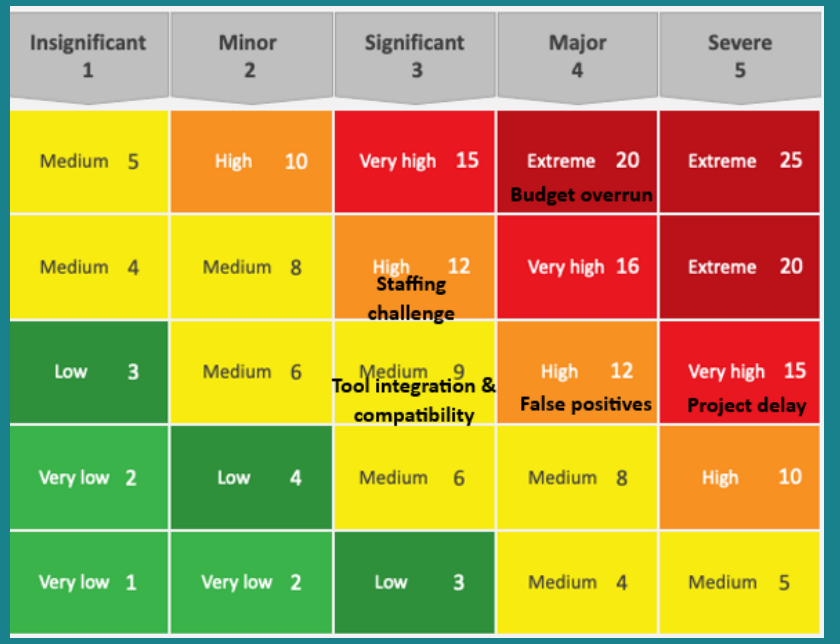
Aim for integration bugs **100% FREE** by the end of project.

What will we do? Schedule 2️⃣ rounds of system integration testing

- 📨 **Phishing Reported** → Test: Incident is created
- 🔍 **Domain Check** → Test: Flag as malicious if blacklisted
- 🔗 **IT System Integration** → Test: AD account is disabled
- 📬 **Notify Users** → Test: Email sent with resolution update

Risk & Sustainment Plan

Risk Title	Description	Priority	Actions / Timelines
Budget Overrun ⚠️💵	Project exceeds allocated budget	❗❗❗	1 Create a 10% contingency buffer. 2 Track actual vs. budget monthly.
Project Delays 🕒⏳	Delay in key phases	❗❗❗	1 Set milestone dates. 2 Hold fortnightly progress meeting. 3 Use project dashboard for real-time tracking. 4 Escalate unresolved blockers within 48 hours.



Risk	Likelihood	Consequence	Risk Level
Budget Overrun	5	4	20 🚨
Staffing Challenges	4	3	12
Tool Integration Compatibility	3	3	9
False Positives	3	4	12
Project Delays	5	3	15 🚨

Ongoing Monitoring & Maintenance:

🔄 **Automation** – 24/7 Monitoring & Incident Management on ServiceNow

🧠 **Targeted Training** – Quarterly stimulation test & awareness refresher training

📊 **Continuous Evaluation** – Performance Dashboards & Scheduled Maintenance

Project Impact

COSTS 💰 💰 💰

- **Average cost of a phishing attack** exceeds **USD$4 million**.
- The total budget is projected at approximately USD$2.3 million per year.
- Organisations could **save up to USD$1.9 million** if they have implemented IR plannings and employee training.

	2025	2026
Planning cost		
	$169,500	$38,500
Staff cost		
	$1,157,500	$1,205,375
Software cost		
	$888,338	$883,588
Hardware cost		
	$66,600	$2,000
Total cost	**$2,281,938**	**$2,129,463**

BENEFITS 🌟 🌟 🌟

- 💻 A structured and automated phishing detection and response system is implemented and centrally integrated with ServiceNow.
- 🚀 24/7 team has set up to provide on-going IT support and training.
- 💪 Enhance network security with MFA & RBAC.
- 🎯 Achieve the 5 project GOALS.

Prototype Demonstration in ServiceNow

16

Q&A

Thank you

ZeroDay Response Team

- Henry Ng, s5423376, (Project Manager and Team Leader)
- Minhaj Ahmed, s5419774, (Security Architect)
- Ansaf Althaf, s5405482, (Security Engineer)
- Sherina Lu, s2717884, (Security Analyst)