WSO2CON 2024

How to Run a Security Program

Ayoma Wijethunga
Director - Security & Compliance
WSO2

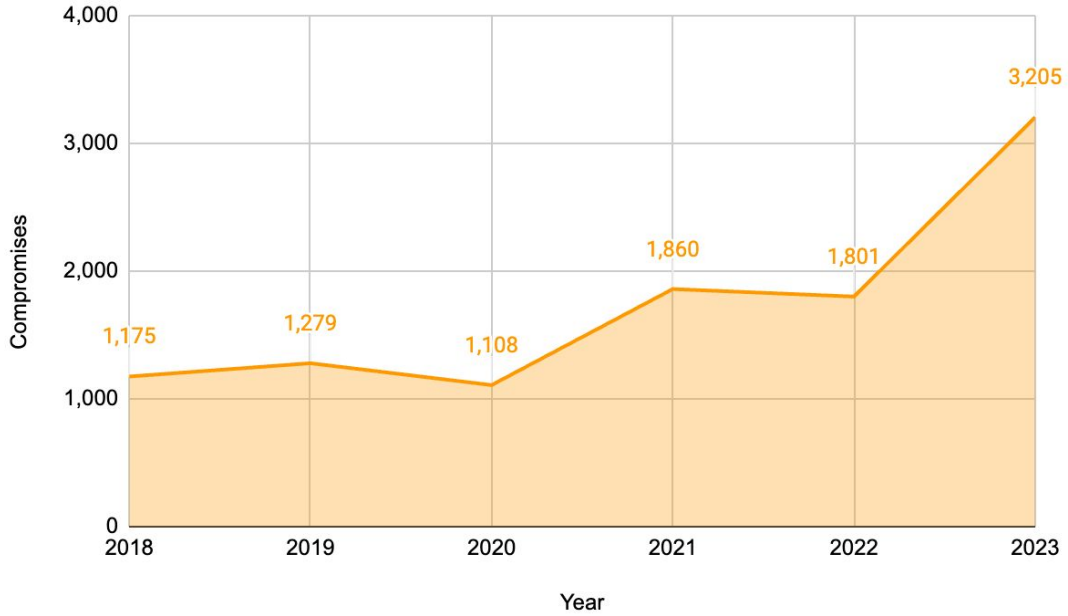
“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it”

- Stephane Nappo -

$ 4.45M

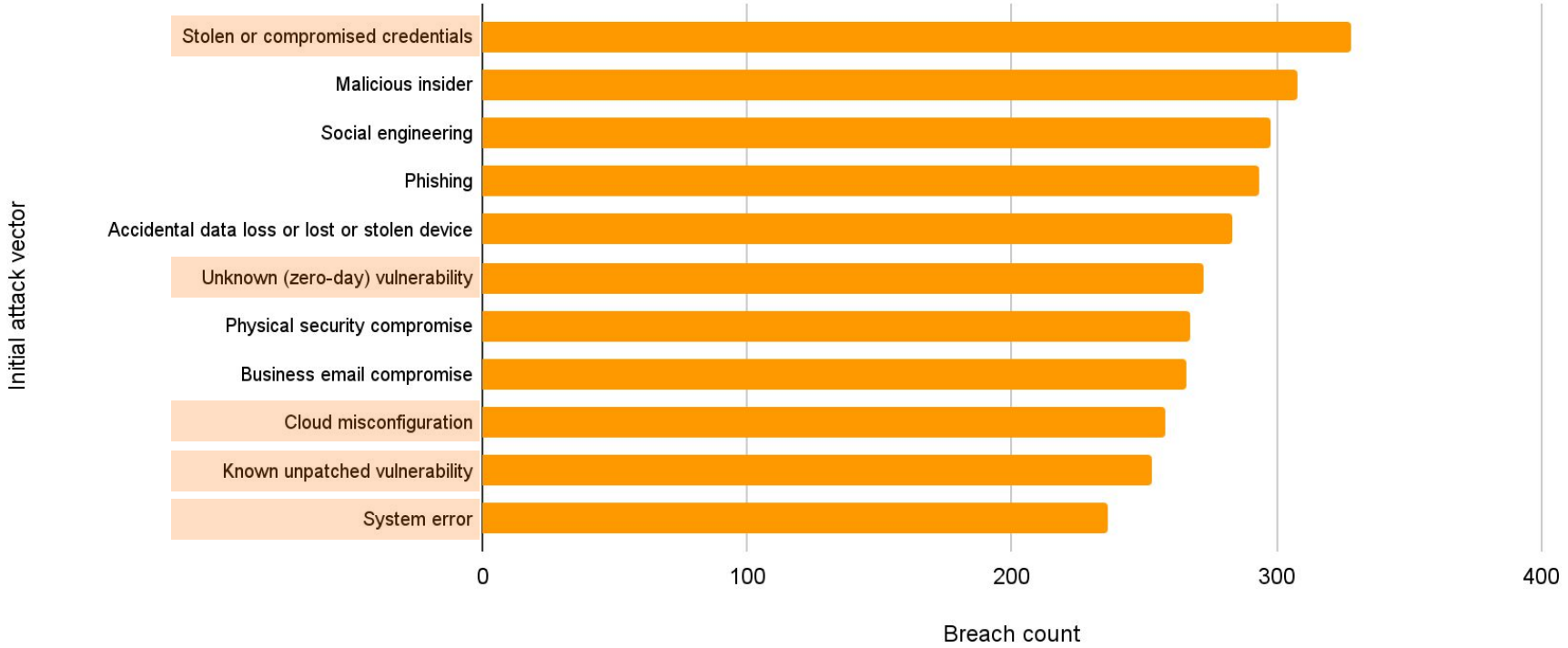
Average cost of a data breach reached an all-time high in 2023

(15.3% increase from 2020)



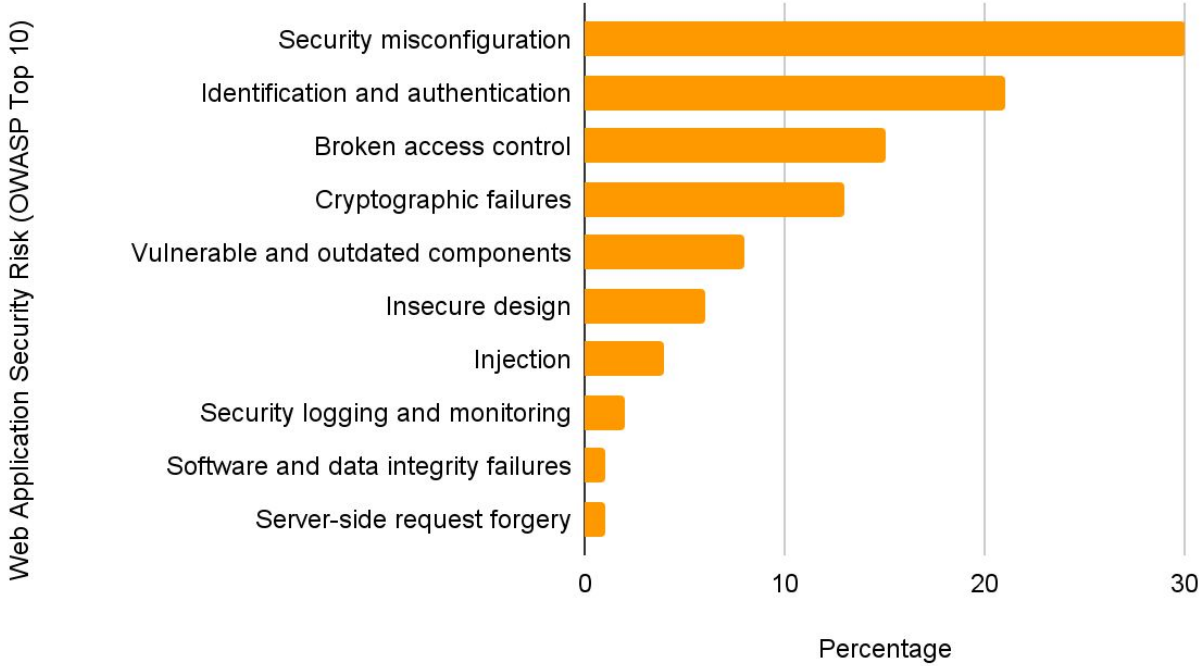
Source: IBM Security - Cost of a Data Breach Report 2023

Bridging the Gap: The Need for Structured Defense



Source: IBM Security - Cost of a Data Breach Report 2023

Bridging the Gap: The Need for Structured Defense

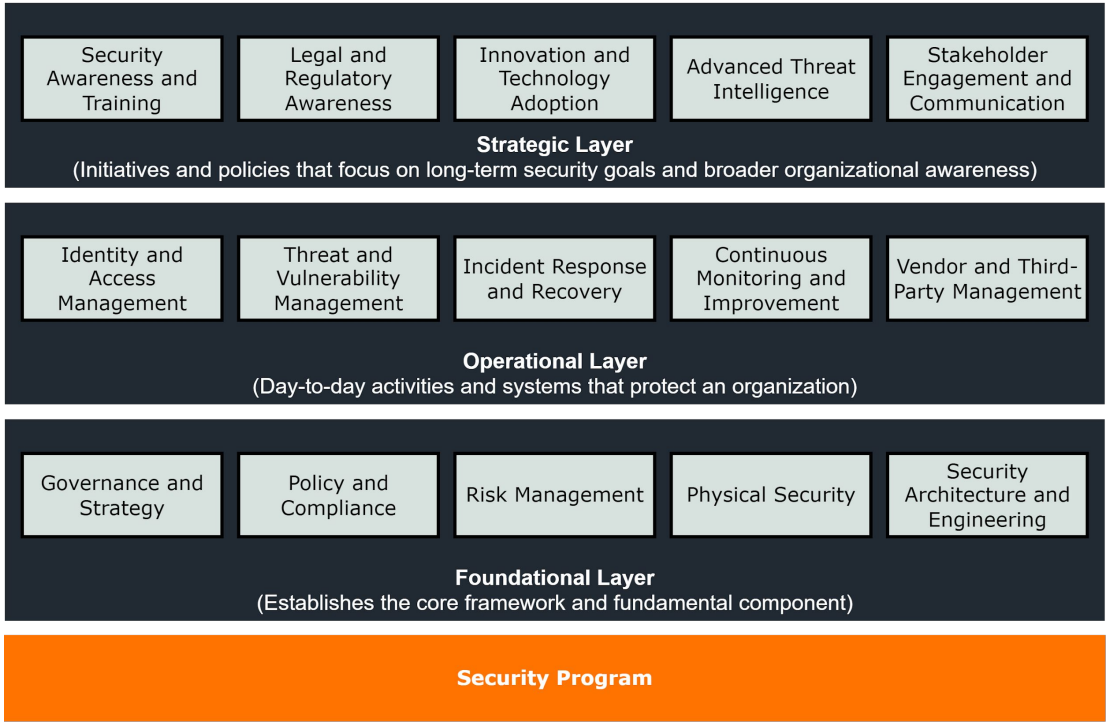


Source: IBM Security - X-Force Threat Intelligence Index 2024

Blueprint for Structured Defense: Security Program

> Comprehensive set of **policies**, **procedures**, and **measures** designed to **protect** an organization's **information, assets, and technology** from **cyber threats and vulnerabilities**

- Protection Against Threats -
- Compliance with Regulations -
- Business Continuity -
- Reputation and Trust -

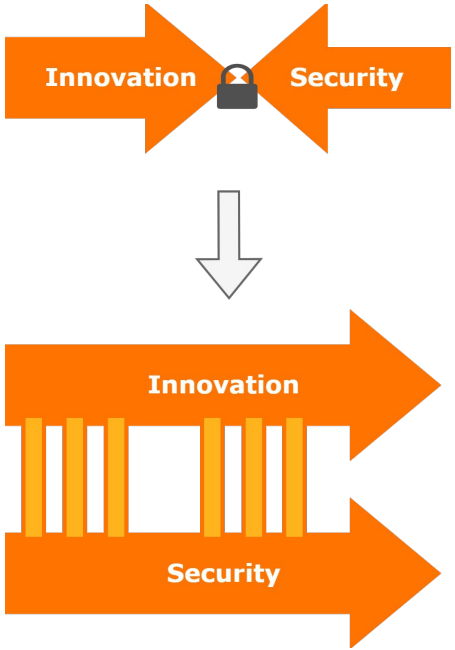


Foundation Layer

The core framework and fundamental component

Governance and Strategy

- Today’s digital innovations are tomorrow’s cyber risks
- While innovation drives business forward, it also expands the threat landscape
- The challenge for security program is to **safeguard critical assets without hindering innovation**
- It's not just about protecting assets but **enabling the business to achieve its goals securely**
  - Balancing Business Strategies, Risk and Innovation
  - Trust as a Competitive Advantage



Policies and Procedures

- **Backbone of any robust security program.** Defining how an organization protects its information assets and meets regulatory obligations.
- Compliance posture is dynamic and should be proactive.
  - Regulatory requirements
  - Business strategy and innovation
- Compliance should be ongoing
  - Internal and external audits
  - Automation and continuous monitoring

Harmonize Security Measures with Policy Development

Don't wait for perfect policies to start implementing security

Architecting for Security

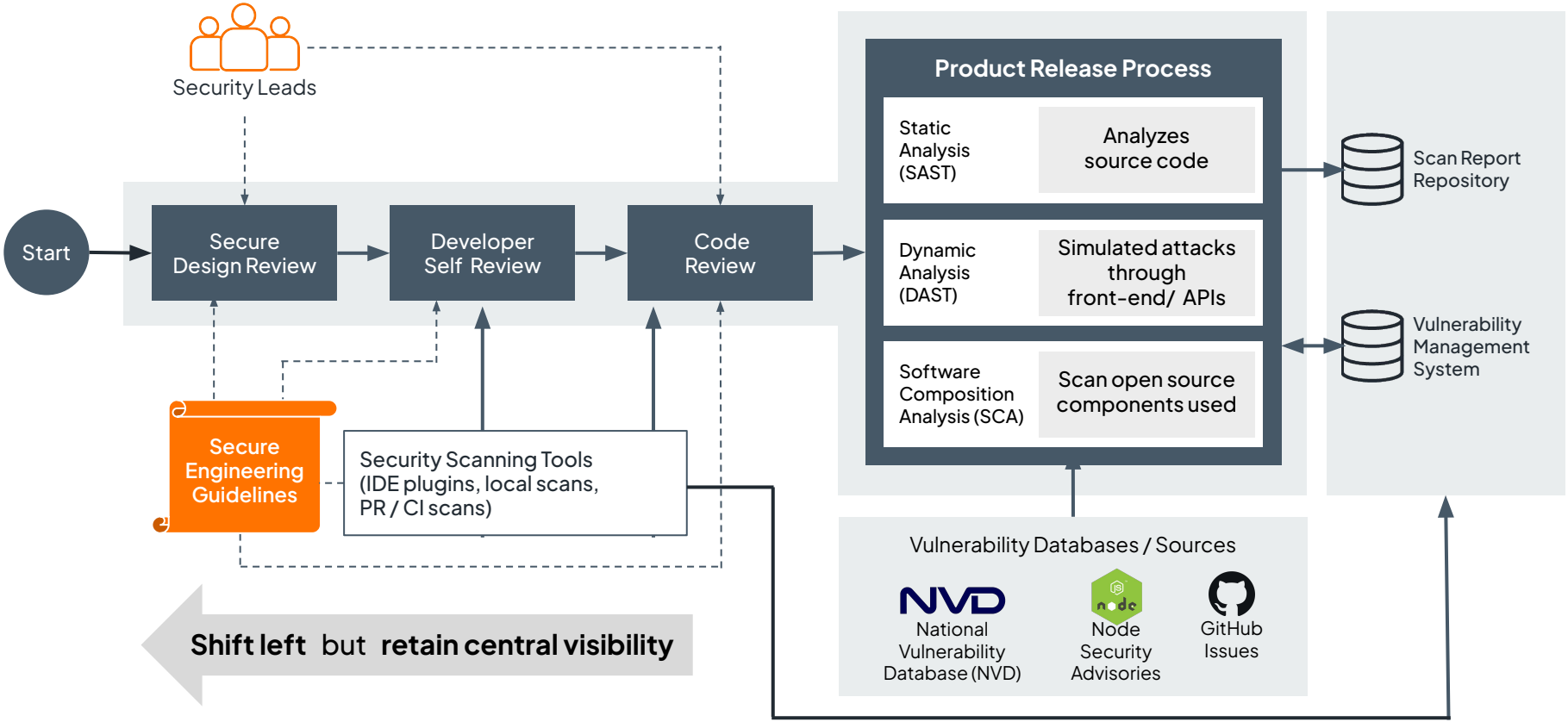
Robust security begins with a solid architectural foundation.

Security is not an afterthought but a fundamental component.

Security should be integrated into every aspect of an organization's operations from the beginning, **not added on as an extra measure later**.

- **Least Privilege**: Access only to what they need to perform their jobs.
- **Defense in Depth**: Use multiple safeguards to protect. If one layer fails, another steps up immediately to thwart an attack.
- **Secure Defaults**: Systems and software should be shipped with the most secure configuration as the standard setting. Security shouldn't dependent on user customization
- **Fail-Safe Defaults**: In the case of a system failure or anomaly, default settings should minimize risks by reverting to a secure state.
- **Privacy by Default**: Privacy settings should be set at maximum by default, and personal data should only be collected and processed when absolutely necessary, protecting user data from the outset.

Secure Engineering – Products



https://security.docs.wso2.com/en/latest/security-processes/secure-software-development-process/

Secure Engineering – Clouds

CI/CD Pipeline
Mandatory Quality and Security Checks

Software Composition Analysis (SCA)

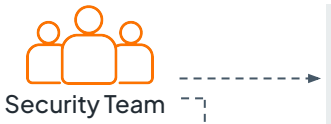
- Third Party Dependency Vulnerabilities
- License Violations
- Container Scanning

Linting and Static Security Analysis

- Quality Checks
- Static Application Security Testing (SAST)

Infrastructure as Code (IaC) Scanning

- Misconfigurations
- Compliance issues
- Vulnerabilities



Penetration Testing
and Periodic Dynamic Scans

Monitor Cloud Security Posture
and Compliance

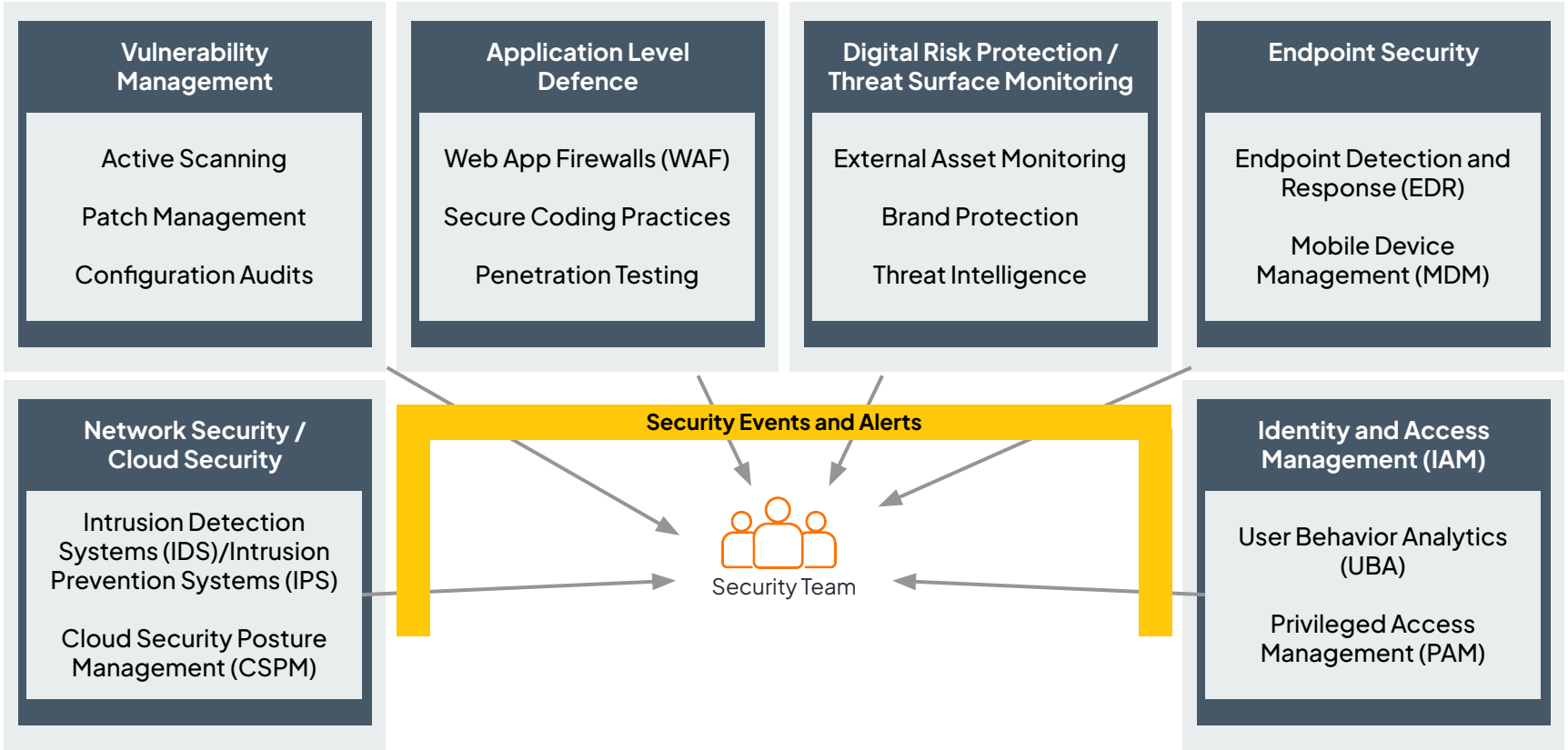
Monitor Security Events
and Security Incident Response

https://security.docs.wso2.com/en/latest/security-processes/cloud-security-process/

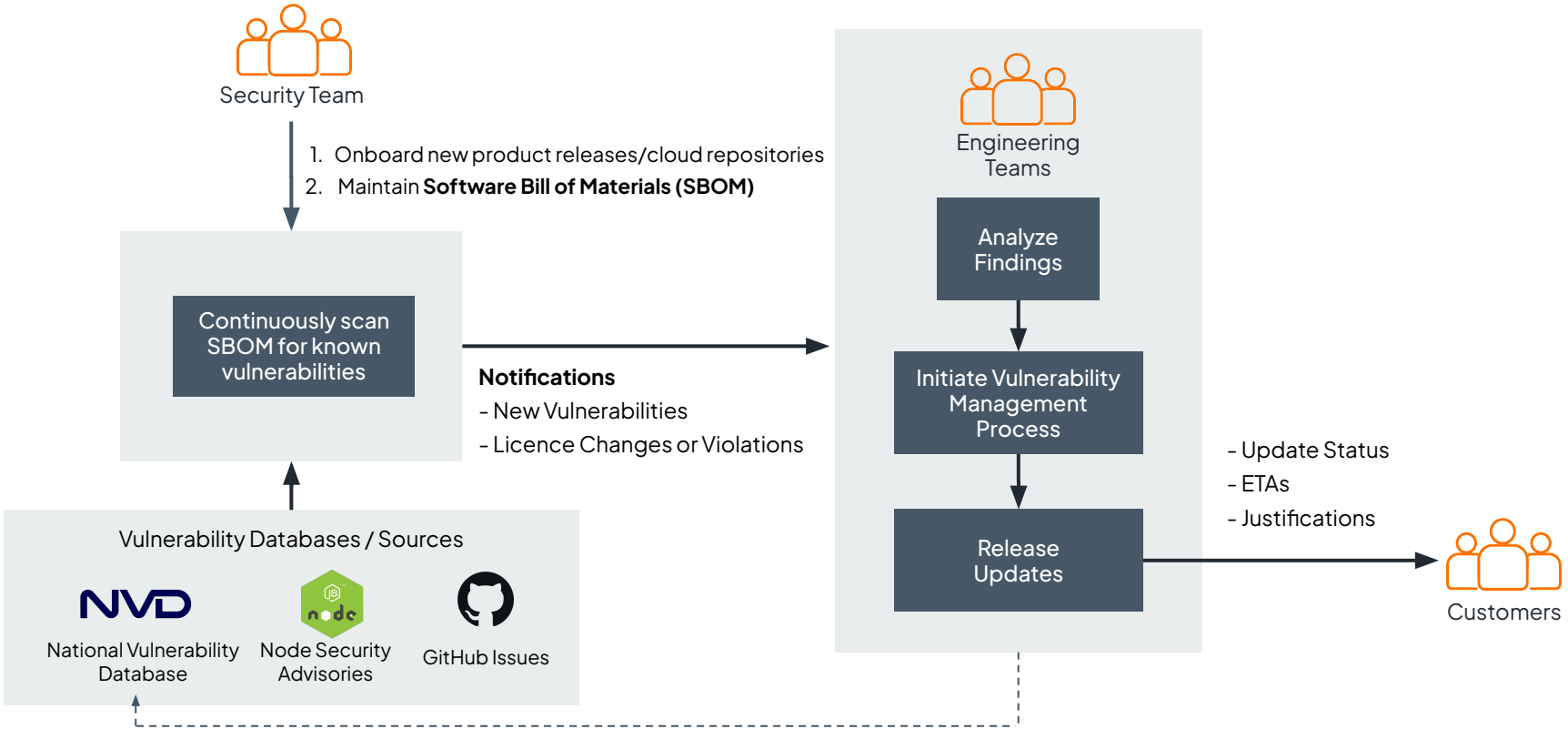
Operational Layer

Day-to-day activities and systems that protect an organization

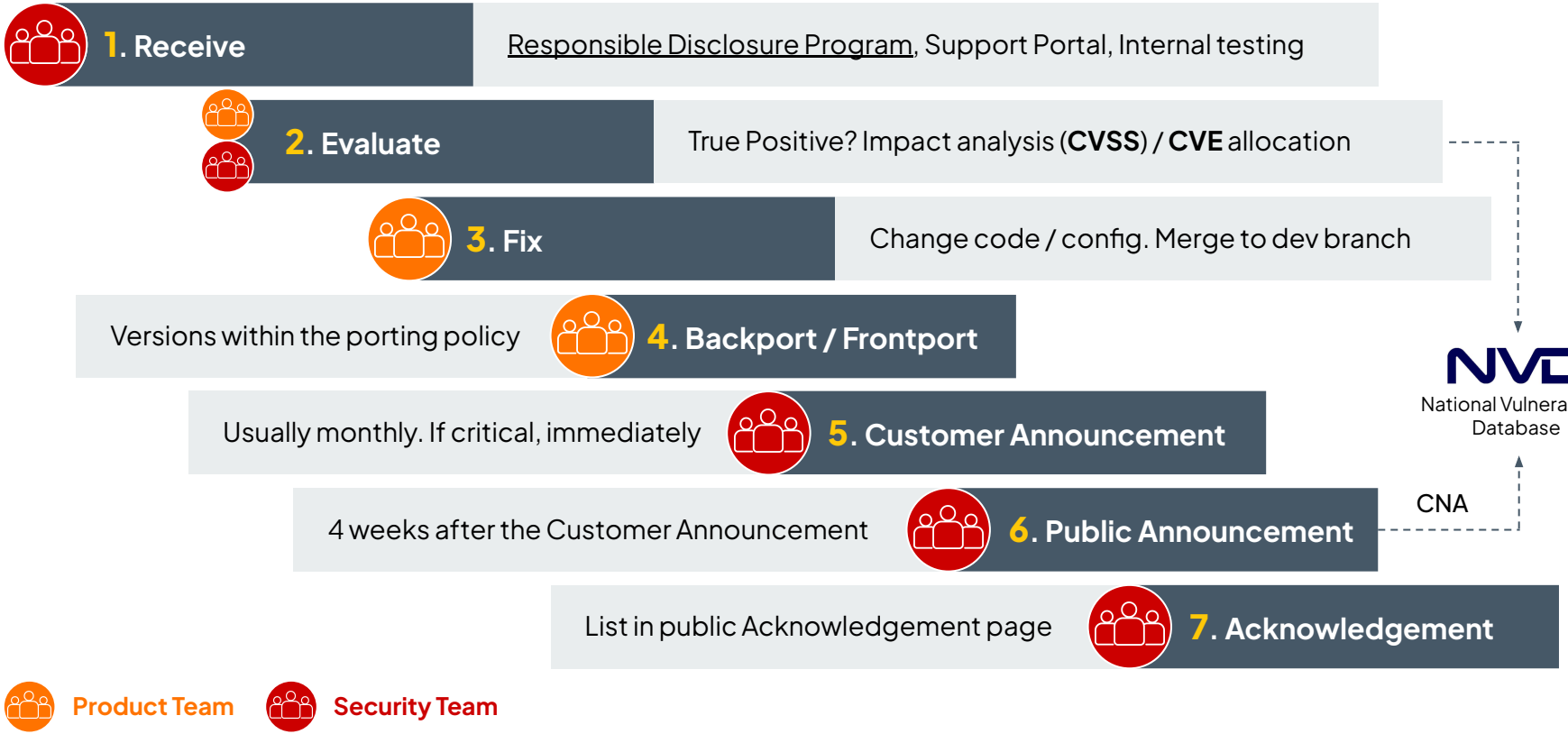
Continuous Scanning of Infrastructure and Digital Threats



Continuous Monitoring of Third Party Dependency Vulnerabilities



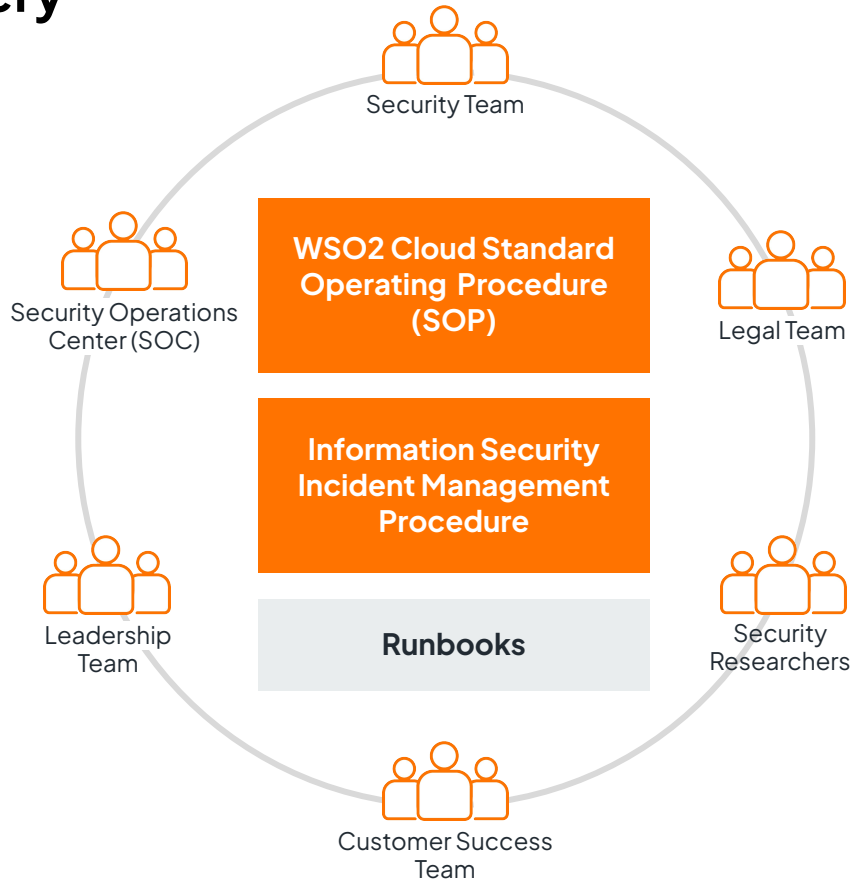
Vulnerability Management Process



https://security.docs.wso2.com/en/latest/security-processes/vulnerability-management-process/

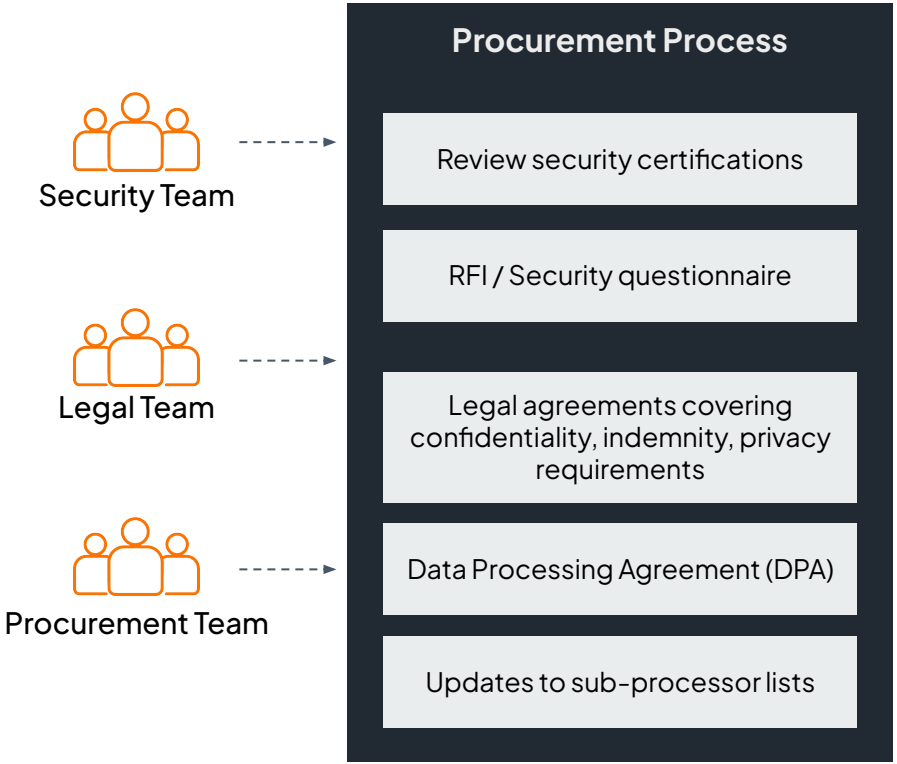
Incident Response and Recovery

Speed at which an organization can respond to an incident often determines the severity of its impact



Extending Security: Managing Third-Party Risks

Third-party ties bring significant security risks, potentially becoming your weakest link in the face of a breach, regardless of your security program's strength



Strategic Layer

Initiatives that focus on long-term security goals and broader organizational awareness

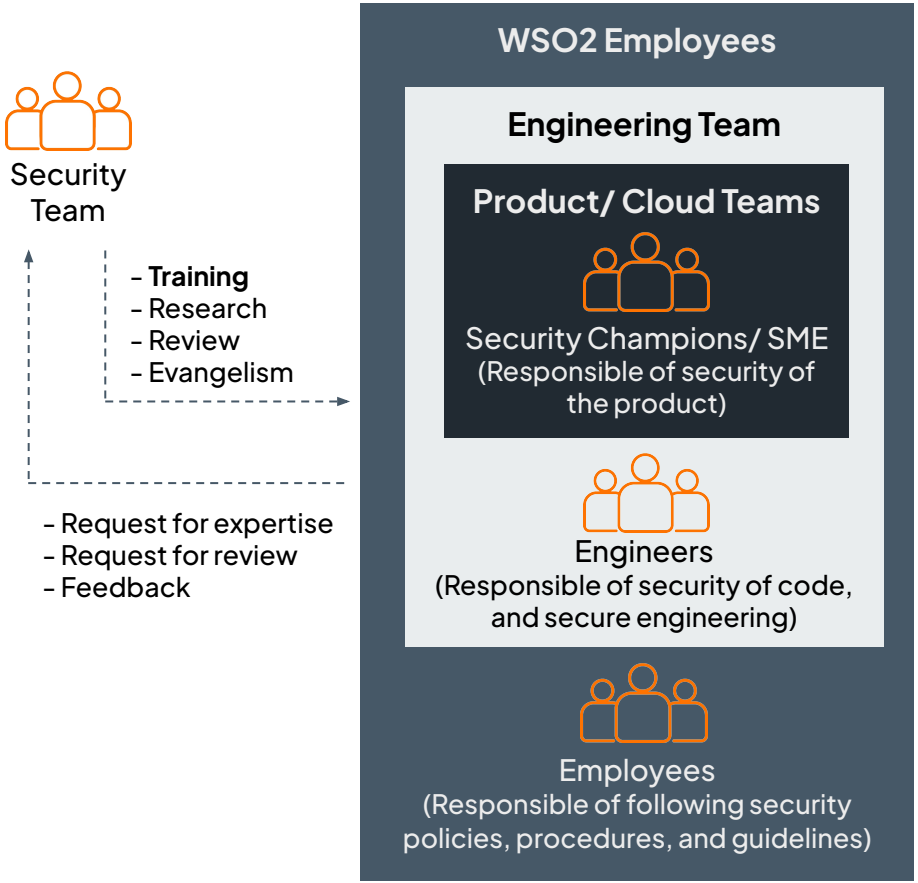
Security Awareness

A security-aware workforce complements technical defenses, enhancing overall security posture and reducing the risk of breaches.

Simulate, assess awareness, and continuously improve.

Building a Security Culture

Security awareness isn't just about knowledge; it's about **creating a culture where security is everyone's responsibility**.



Community and Collaboration

Opportunity to tap into the global security community, benefiting from the vast experience of researchers.

Work together with the security community to improve security together.

Community and Collaboration – WSO2.com/security

Security and Compliance

At WSO2, we prioritize the security and resilience of our products and services. We adhere to industry best practices and maintain a transparent security program to continuously improve our offerings.

Report a Vulnerability

Read Security Docs

Security Attestations

ISO/IEC 27001:2013

WSO2 is certified to the globally recognized ISO/IEC 27001:2013 standard for Information Security. This standard specifies how to implement, monitor, maintain, and continually improve an Information Security Management System (ISMS) to ensure that your data is shielded from unauthorized access, maintaining its integrity and availability.

System & Organization Controls (SOC)

WSO2 has successfully obtained the SOC 2® Type 2 Report for its Public and Private Cloud services. The SSAE18 SOC 2® Type 2 examination provides you with a detailed assessment of our system controls. Focusing on the key aspects of security, confidentiality, and availability of customer data, this report assures you that your information is protected at all times.

Security Programs

Vulnerability Management Process

Examine how we manage vulnerabilities related to our products and services.

Learn More→

Secure Engineering Guidelines

Discover security best practices followed by our engineering team for WSO2 products and services.

Learn More→

Responsible Disclosure Program

Discover how we reward contributors who responsibly disclose vulnerabilities and contribute to our products and services through our Hall of Fame.

Learn More→

WSO2 Product Security

Secure Software Development Process

Learn how we prioritize security throughout the Software Development Life Cycle.

Learn More→

WSO2 Cloud Security

We secure all WSO2 cloud deployments by following industry-standard processes.

Learn More→

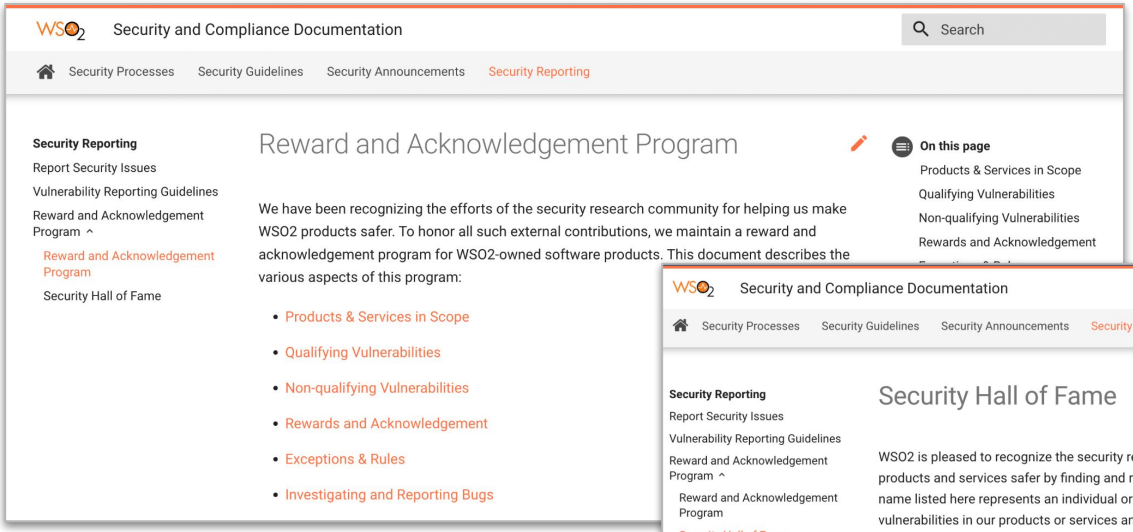
FAQs

How is data managed in WSO2 Private and Public Clouds?

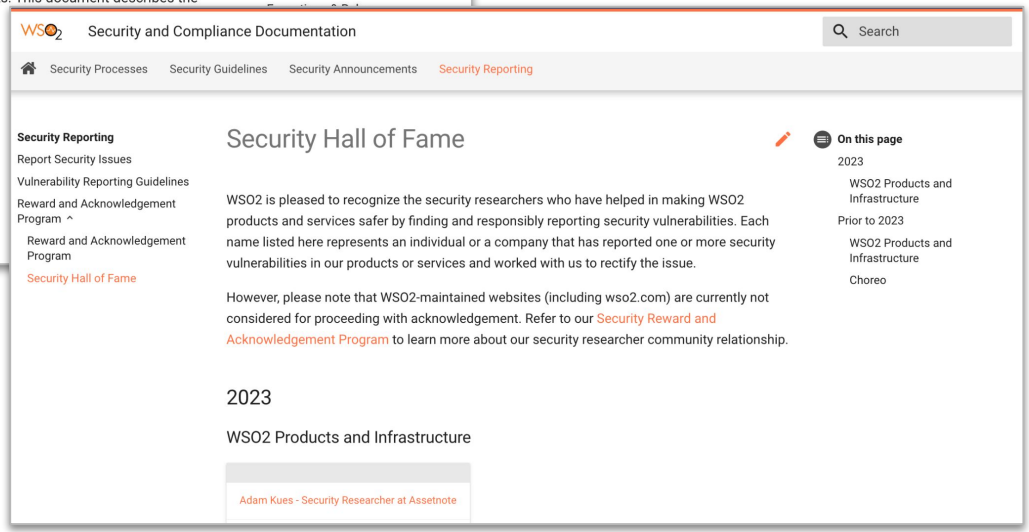
What is the WSO2 Subprocessor list?

How do we secure WSO2 Private and Public Clouds?

Reward and Acknowledgement Program



Established clear guidelines and standards for collaboration, ensuring that all parties are protected and the work is conducted responsibly.



Incentivize ethical hackers to safely find and report security flaws, turning potential threats into protective insights.

https://security.docs.wso2.com/en/latest/security-reporting/reward-and-acknowledgement-program/

Utilizing Advanced Technologies

- Automation streamlines security protocols, reducing manual workload and human error. AI enhances threat detection with predictive analytics and real-time response.
- Use DevSecOps to integrate security at every phase of software development, ensuring that every release is secure by design.
- Gathers data on new and emerging threats to anticipate and prepare for potential attacks, keeping the organization one step ahead.

People

Cybersecurity is a vast and ever-evolving field. No one can master every aspect.

Balance Specialization with a Solid Foundation.

Align individual interests and the needs of the organization.

- Application Security
- Infrastructure Security
- Cloud Security
- Security Compliance
- Legal & Regulatory Compliance
- Security Operations

The Evolution of Security at WSO2

2013

Security Mailing List

First email sent to dedicated mailing list for security (security@wso2.com). "Threat Model for StratosLive WSO2 ESB" by Prabath Siriwardena

2015

Inception of Platform Security Team

Inception of the Platform Security Team overlooking security of WSO2 products. Objective was to improve security scanning, reduce vulnerabilities, and start a formal security program.

2020

Security & Compliance Team

Scope of the team was expanded to overlooking every security and security compliance aspect within WSO2, including products, infrastructure, and clouds.

2021

ISO 27001:2013 Certification

WSO2 was certified to the globally recognized ISO/IEC 27001:2013 standard for Information Security.

2024

SOC2 Certification

WSO2 successfully obtained the SOC 2® Type 2 Report for its Public and Private Cloud services.

FUTURE

ISO/IEC 27001:2022

Question Time!

Thank You!