A vulnerability is a weakness in a system that can be exploited by a threat actor. A weakness can be anything from a programming mistake, to a lack of security due to oversight or process errors. Usually, a threat actor’s intent is to work their way up through privilege boundaries until they have administration rights and can access more valuable information.

However, a vulnerability is not necessarily a risk. In risk management, a risk = chance x impact. That means contextual data is needed to assess to what degree action should be taken. With threat actors increasingly using automated techniques to quickly determine their target’s weak spots, it’s imperative you stay in control of your attack surface and are constantly aware of the possible entry points.

A vulnerability most often occur through programming mistakes. Usually, it is because of improper input validation, and it’s impossible to test for every single possible input.

Additionally, a logic flaw is not so much a software error, but a design mistakes. For instance, when team-specific data is supposed to be separated, but can still be accessed by someone outside the team.

When a vulnerability is exploited, it poses the risk of threat actors gaining access to your systems, where they can obtain data, abuse resources, and install malware / ransomware.

**COMMON TYPES OF VULNERABILITIES**
- SQL injection
- Buffer overflows
- Remote code execution
- Privilege escalation
- Encryption faults
- Cross-site scripting

**OUR ATTACK SURFACE MANAGEMENT PLATFORM WILL HELP YOU TO**
- **PREVENT INCIDENTS**: Continuous insights from an outside-in perspective help identify vulnerabilities and assess risks.
- **IMPROVE PRODUCTIVITY**: Automated risk detection and risk scoring for improved prioritisation actions.
- **IMPROVE SECURITY**: Contextual asset information and proposed mitigation actions help to delegate security fixes.
- **STRENGTHEN RESILIENCE**: Risk assessment data provides input for further vulnerability management processes.

**WHY YOU NEED VULNERABILITY & RISK ASSESSMENT**
AUTOMATED, OUTSIDE-IN, AND CONTINUOUSLY

The Vulnerability & Risk Assessment is at the basis of to the Attack Surface Management platform. After the Asset Detection & Inventory, the platform automatically scans each asset for any risks, resulting in a risk score and detailed overview of possible mitigation actions.
THE ATTACK SURFACE MANAGEMENT SOLUTION TO VULNERABILITY & RISK ASSESSMENT

The Cybersprint Attack Surface Management platform helps you by passively identifying the vulnerabilities in your attack surface. Automatic risk assessment provides the contextual data to determine the risk level, evidence, and proposed mitigation actions.

When you understand the exact location, cause, and severity of your vulnerabilities, you have the input needed to direct other vulnerability management processes more precisely, such as for pentesting or sharpening the security governance.

**ASM PLATFORM SOLUTIONS**

**IDENTIFY**
- Detect and assess assets related to the brand
- Scan individual assets for vulnerabilities (CVE) and misconfiguration

**ASSESS**
- Receive a risk rating for each asset
- Create vulnerability-based dashboard insights
- Identify the potential business impact

**MANAGE**
- Receive remediation advice and track status changes over time
- Automatic notifications for new vulnerabilities
- Integrate with CMDBs and vulnerability scanners

**REPORT**
- Export vulnerability and risk information to support:
  - Governance and vulnerability management
  - Audits and compliance

**OUR ATTACK SURFACE MANAGEMENT PLATFORM WILL**

**ASSESS EACH IDENTIFIED ASSET FOR THE EXISTENCE OF VULNERABILITIES**

**DETERMINE THE RISK LEVEL BASED ON CONTEXTUAL INFORMATION**

**PROVIDE INPUT FOR OTHER VULNERABILITY MANAGEMENT PROCESSES**