Uleska Platform Product Factsheet

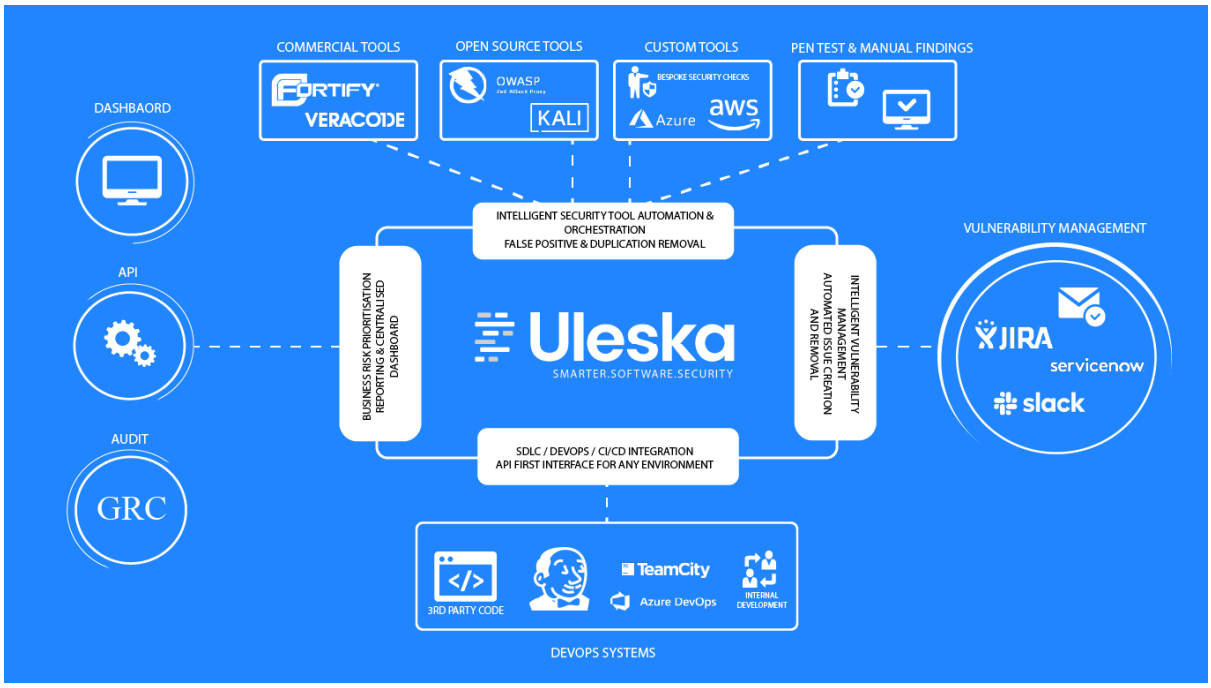
The Uleska Platform provides automated and centralized software security testing, interconnecting security with agile & DevOps systems, whilst uniquely translating technical issues into cyber business risk, all without the need for more personnel.

Stakeholders including management, auditors, and software teams can easily manage security challenges without upskilling or slowing feature releases.

Uleska Platform Overview

The Uleska Platform allows you to easily connect security tooling and assurance into your existing software development lifecycle. Whether you have teams running Azure DevOps and needed to connect SonarQube SAST testing, or CI/CD teams using Jenkins and requiring numerous Kali Linux testing against nightly builds, the Uleska Platform allows you to easily and quickly get the security testing you need done.

That's why the Uleska Platform gives you security testing that's as agile as you are.



For deployment options, please refer to the Uleska Platform Deployment Guide, for extensive options on SaaS, on-premise deployments, and much more.

Uleska Platform Feature List

As the world becomes more connected than before, businesses rely heavily on applications to succeed. To meet business expectations, developers face tight deadlines and ambitious feature, functionality requirements. Software vulnerabilities are a serious problem introduced by mistake, through poor software security practices, or intentionally by internal threat actors.

One of the best methods to avoid negative impact is to develop code with quality and security in mind from the early phases of development.

Automation & Orchestration	The Uleska platform contains an ever-growing list of security testing tools, including the leading commercial and open source tools used by penetration testers around the world. This list can then be extended with 'custom' tools, created by security teams or the industry, to test important aspects of security programs not achievable by off-the-shelf security tooling. For each security tool the Uleska Platform automates and orchestrates the tool execution and reporting, including: • Automatically invoking selected tools for every invocation of a testing cycle. • Intelligently incorporating application configuration as needed for each security tool invocation. • In the case of dynamic security tooling, running 'spidering' to learn new interfaces, ensuring they are tested on subsequent test runs. • Findings from every tool are aggregated back to the Uleska Platform and stored against the test run. • Findings from all tooling and combined and displayed on one place for the test run. Results are visible, editable, and easily extracted. The advantage of scanning with multiple tools is greater security coverage and a more comprehensive understanding of your software vulnerabilities. Note that invocation of some tools may require invocation outside of the Uleska Platform, depending on the tool and features in question. When invocation is required outside of Uleska Platform, Uleska provides plugins and scripts for popular CI/CD systems, see below for more details.
Application Configuration	Save time configuring access to application once, which is then automatically used to invoke multiple tools.
Intelligent False Positive Removal	The Uleska Platform allows false positive findings to be flagged and removed from reported issues in the test run. Subsequent test runs will remember the issue is a false positive and continue to remove it from future test runs, meaning UI pages and reports will continue to ignore these false positives. False positive issues can still be viewed in the Uleska Platform UI, and the API, for future reference. False positive issues can be categorized back into actual issues at any time.
Duplicate Issue Handling	When multiple security tools return the same finding, these duplicate issues can easily be consolidated into on finding, making it easier to handle. Any number of same findings can be consolidated into duplicate findings, which are remembered in future test runs, saving time when handling security reports.
Security Issue Tracking	New security issues discovered by the Uleska Platform suite of testing tools are automatically recorded for every test run. As new issues are found, teams and stakeholders can be updated via the Uleska Platform UI, API, reports, and through configured issue tracking systems such as Jira or Slack. As these issues are subsequently fixed, the Uleska Platform recognizes this through subsequent test runs, and flags those issues as fixed, again through the Uleska Platform UI, API, reports, and in updates to tracking systems such as Jira and Slack.

CI/CD and DevOps Integration	The Uleska Platform features an API First design allowing any CI/CD and DevOps tooling to authenticate with and invoke the Uleska Platform for security testing. A list of currently support CI/CD platforms is listed below: • Jenkins • Bamboo • Azure DevOps • TeamCity • GitLab CI If your current CI/CD tooling is not listed, contact Uleska for an integration.
Tool Coverage	The Uleska Platform comes with an array of security tooling as listed below. This list is continually being updated as Uleska develop new integrations, contact Uleska for the latest list, or to ask about tooling you wish to integrate. Dynamic Testing (DAST) • OWASP Zap • Fortify DAST • SQLMap • Burp Suite • Nikto2 • Sslyze • OWASP ZapProxy • Veracode DAST • Xsser • w3af Static (Code) Analysis (SAST) • SonarCube • Veracode SAST • Fortify SAST Software Composition Analysis (SCA) • Veracode SCA • OWASP Dependency Checker Cloud Security • Amazon Insepctor Container Security • Clair Network Security Testing • Nmap

Extensible Security Tooling	The Uleska Platform is uniquely extensible to allow further security tooling and test script to be integrated into test runs. Take test tools not already integrated into the platform or create your own scripts and easily repeat their test execution by adding them to the default tools. Custom tools can be written in any language, using any means necessary to conduct a security check of your software. They can inspect code, dynamically test a running system, probe networks, handle containers or anything else you wish to run or script. There's no limit to the number and size of custom tooling you can integrate with the Uleska Platform. All custom tooling will be: • Invoked automatically by the Uleska Platform during test runs. • Will have access to the existing application configuration available to all security tools (including spider output). • Will report issues back to the Uleska Platform in the same way as existing integrations. • Can have their security issues handled in the same way as any other issue, including false positive removal, and duplicate handling. • Will result in reports being updated, or issue management systems such as Jira or Slack receiving updates.
CVSS Tagging	The Uleska Platform assigns CVSS scores to every issue. Common Vulnerability Scoring System is an open framework for communicating the characteristics and severity of software vulnerabilities, from 1-10, with high, medium and low ratings. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
ASVS Tagging	The Uleska Platform uses the OWASP Application Security Verification Standard (ASVS) as a way to categorize every security issue found. With over 280 different categories for issues, this provides a basis for testing application technical security controls and also provides developers with a list of requirements for secure development. OWASP ASVS categories can then be mapped to other common security standards, such as ISO 27001, NIST, and others.

Security Issue Advisories	One of the time-consuming aspects of finding security vulnerabilities is the time it takes for receiving software teams to understand the issue, identify the solution that is correct for the system or company, and implement the change. Different security tools can describe security issues, and subsequent remediations, in various ways, with varying degrees of readability and communication. Also, many companies have their own technical solutions, trainings, or teams to contact, depending on the type of vulnerability. When this communication fails, security teams are often inundated with requests for clarification, or questions on what solutions to apply. Thus, skilled software teams have to spend much of their time communicating the same information to different teams, instead of concentrating on security work. Therefore, the Uleska Platform allows security teams to set Security Advisories, which map to categories of vulnerabilities (e.g. SQL injections, access control issues, etc) and overwrite the remediation suggested by the security tooling. This allows security teams a single, centralised place to set their advisories, for example, their own take on proper remediation advice for a type of issue, which internally developed wrapper library to use, which e-learning module to take, which OWASP page to read, or other. Security Advisories are then supplied instead of the tool recommendation, for all subsequent issues returned to the Uleska Platform, and returned to development teams through the UI, API extractions, and PDF reports. This allows security teams to save time and effort communicating the most relevant fix to all application teams, regions, and business units, from one centralised place.
Auditable System of Record	In todays modern software security programs, stakeholders and regulators require evidence that testing was run, findings processed, and fixes applied. The Uleska Platform implicitly provides such audit material, tracking issues raised and fixed between test runs, proving that testing was executed against code and dynamic systems, and providing a measure of the success with which issues were removed.
Automated Reporting	The Uleska Platform automatically generates test run reports in multiple formats, including: • Uleska Platform UI displaying issues and allowing editing of issue descriptions or impact analysis. • Editable and configurable PDF reports, including in your own brand colours (when you take your own instance of the Uleska platform). • Easy to use API to plug technical issue and risk/impact metric into your own systems or portals. • CSV outputs.
Recording of Manual Security Test Findings	When manual penetration testing is conducted, you will wish to have the issues discovered in that activity to be recorded, measured, risk calculated, and reported in the same fashion as automated security issues. The Uleska Platform provides a UI and API to integrate manually discovered issues with the rest of the issues in the Uleska Platform, combined with automated findings. This means that manually discovered issues will be included in the stats for that application, including overall risk analysis. Changes to risk calculations will affect manual issues just the same as automatically discovered issues. Manual and automatically discovered issues are reported in the same way through the UI, and in PDF reports.

Tool Execution Logs	As security tools are automatically invoked, users can track the progress of tool execution, as well as view the technical output of relevant tools. Tool execution is recorded and logged encase any subsequent analysis is required. Note that some commercial tooling may not provide 100% of logs to the Uleska Platform.
PDF Report Branding and Configuration	The Uleska Platform allows you configurable control over the PDF reports that are generated from the lists of security issues for an application. This allows branding within the report and provides extensibility for further sections or analysis needed in the report. Elements of the PDF report that can be configured includes: • Report Title • Title Colour • Headers • Footers • Key-Value pairs within report text • Create overview sections or insert any section text required. • Configure fonts, and images to match your branding.
Intelligent Issue Impact Determination	The Uleska Platform intelligently understands the nature of the issue found and its impact on the software system, to communicate the priority or risk that the issue can pose to you and your business. The Uleska Platform combines three key pieces of information to determine this impact: 1) The technical nature of the vulnerability/issue. This comes from CVSS scores, and pre-programmed technical configurations, to determine risk based on the technical nature of the bug. 2) The application context. Is this app running internal to a network, or public to the internet? Does it process sensitive data, such as financial, personal, IP, or other data that this technical bug could leak or affect? How many users are there for the system, 1 or 1 million? How critical is the system to the business? 3) The organisation. Is the company running this software system a start-up, or an IPO'ed multinational? Is there a share price to affect if a security bug leaks data? Is the company subject to GDPR, PCI DSS, HIPAA, or other regulations? All of this information is combined and handled through industry best practice algorithms to determine the true impact, and therefore priority of each and every issue handled by the Uleska Platform. These risks/impacts are then reported as you require, through a configurable interface, reporting as: • Red/Amber/Green • Very High/High/Medium/Low/Very Low • CVSS • Cyber Value-at-Risk • Generic Security Scores

Risk/Impact Enumeration and Configurability	The Uleska Platform automatically determines the impact ratings for vulnerabilities found. These measures of the impact of an issue can be useful for various stakeholders within an organisation. Reporting mechanism for risk/impact are configurable to fit your needs, and include: • Red/Amber/Green allows you reflect the risk/impact of each issue in a simpler colour coded way. Uleska Platform screens allows you to configure the bands for Red/Amber/Green. • Very High/High/Medium/Low/Very Low allows you to communicate the risk/impact through Very High to Very Low descriptions. Again, Uleska Platform screens allows you to configure the bands. • Common Vulnerability Scoring System, CVSSv3, is an open framework and de-facto standard for security teams, communicating the characteristics and severity of software vulnerabilities, from 0.0-10, with high, medium and low ratings. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. • Cyber Value-at-Risk (VAR) assigns a monetary business risk value to each issue, and is useful for a commercially minded audience, giving you an understanding of the financial risk associated with each vulnerability. • Generic Cyber Security Scores allows you to communicate risk/impact value as a value between 0 and 1000, giving plenty of granularity when discussing and prioritizing issues across many software systems.
Risk/Impact Configurability	The Uleska Platform allows for flexibility in how risk/impact calculations are applied across all applications and teams. Configurability is provided for levels of likelihood, downtime costs, and maximum fines. Upon the change of this risk configuration, the Uleska Platform will use this new risk configuration for all new issues discovered. If you wish to update the risk of existing issues, this can be done at the touch of a button.
Flexible Scope of Reporting	Risk/Impact reporting, as described above, is important to understand in numerous contexts and scopes. It could apply to a single issue as a review is occurring or a developer is looking for the next priority issue to resolve. In other scenarios it may be important to compare the accumulated risk across multiple applications within a team, to understand which one exposes the greatest risk. Furthermore you may wish to compare risk/impacts between teams, suppliers, or across your entire organization. The Uleska Platform provides risk/impact statistics and trends across all of these levels, from the risk/impact of an individual issue, to the accumulated risk of all issues in an application, to the risk of all applications within a team, region, or across the entire organisation.
Security Metrics	The Uleska Platform allows security metrics and risks to be visualised across an entire organisation, informing your security strategy and progress. Number and risks across multiple applications, teams, and regions are reported in the Executive Dashboard, showing: • Weekly measurements of onboarded applications, issue numbers, and aggregated risk/impacts • Trends showing differences from week to week on numbers of issues and overall risk/impacts. • Track top 5 risks categories faced by all applications. • Statistics showing the number of applications, number if vulnerabilities, average vulnerabilities, overall risk, average risk, and trends over the last 5 weeks. This can be viewed per region, or team.