



LCSG

LITCHFIELD CYBER SECURITY GROUP

— DISCOVER. EXPLOIT. DEMONSTRATE. —

BUG BOUNTY TRIAGE SERVICES

DISCOVER. EXPLOIT. DEMONSTRATE.

Specialist vulnerability triage for organizations facing rapidly increasing bug bounty and vulnerability disclosure report volumes.

MORE REPORTS. MORE NOISE. THE SAME NEED FOR HUMAN JUDGEMENT.

LCSG combines AI-assisted processing with experienced vulnerability researchers to validate reports, identify real impact, reduce noise and move actionable vulnerabilities to remediation faster.

THE TRIAGE PROBLEM

AI Has Changed the Economics of Vulnerability Reporting

AI is increasing the speed and scale at which security research can be performed and reports can be produced. The result is not simply more noise: programs are receiving more genuine vulnerabilities as well as more speculative, duplicate and poorly validated submissions. Human validation has become the bottleneck.

76% YoY

HackerOne reported 46,947 submissions in March 2026 - an all-time high and a 76% year-over-year increase.

~25% VALID

HackerOne reported that roughly 25% of submissions remained valid and exploitable despite the volume surge.

334% QUEUE GROWTH

Bugcrowd reported its triage queue grew by more than 334% over a three-week period, driven heavily by low-quality submissions.

60-80% INVALID

HackerOne states that 60-80% of vulnerability submissions handled by its triage service are invalid.

Supporting evidence: HackerOne, April/May 2026; Bugcrowd, March/April 2026. Source URLs are listed on the final references page.

DISCOVERY IS SCALING FASTER THAN HUMAN VALIDATION.

Triage by Vulnerability Researchers

LCSG triage is designed to be more than administrative report processing. Submissions are evaluated by people who understand how vulnerabilities are discovered, exploited, chained and communicated - because difficult reports require technical judgement, not just workflow management.

REPORT INTAKE & CLASSIFICATION Normalize incoming reports, confirm affected assets and vulnerability class, and route submissions according to program requirements.	TECHNICAL VALIDATION Reproduce reported behavior, test preconditions and determine whether the vulnerability and claimed impact are genuine.
DUPLICATE & VARIANT ANALYSIS Identify true duplicates while distinguishing variants that expose different root causes, assets or materially different attack paths.	SEVERITY & IMPACT Assess exploitability, preconditions, privilege requirements, affected data or functionality and appropriate severity.
RESEARCHER COMMUNICATION Request missing evidence, clarify reproduction steps, challenge unsupported claims and maintain constructive technical dialogue.	ENGINEERING HANDOFF Convert validated researcher submissions into concise, technically useful findings that remediation teams can act on.

Use AI on Both Sides of the Submission Pipeline

LCSG does not treat AI as the enemy. AI can improve legitimate vulnerability research and it can dramatically improve triage. The problem is not AI usage; the problem is accepting unvalidated output as fact.

AI CAN ACCELERATE

- Initial report classification
- Scope and asset correlation
- Similarity and duplicate analysis
- Extraction of reproduction steps
- Technical context and research
- Queue prioritization

HUMANS MUST DECIDE

- Whether the issue is genuinely reproducible
- Whether claimed impact is realistic
- Whether a variant is materially different
- Whether vulnerabilities can be chained
- Whether severity reflects real exposure
- What additional testing is warranted

AI HELPS US PROCESS THE VOLUME. EXPERIENCE FINDS THE SIGNAL.

This human-in-the-loop model is consistent with the direction taken by major bug bounty platforms: AI performs repeatable analysis and recommendation, while experienced analysts retain responsibility for final validation decisions.

Built From the Researcher's Side of the Table

LCSG's triage capability draws on founder Mark Litchfield's more than 25 years of offensive security and vulnerability research experience, together with extensive first-hand participation in bug bounty and vulnerability disclosure programs.

WHY RESEARCHER EXPERIENCE MATTERS

Experienced vulnerability researchers recognize the difference between a weak report and a weak vulnerability. An unconventional finding may be poorly explained yet technically significant; a polished submission may still be speculative. Effective triage requires the ability to investigate the underlying security behavior rather than judging only the presentation.

FROM SUBMISSION TO IMPACT

The same skills used to discover vulnerabilities - curiosity, reproduction, attack-path reasoning, exploitation knowledge and skepticism - are the skills required to validate difficult submissions accurately.

TRIAGE SHOULD NOT JUST FILTER REPORTS. IT SHOULD RECOGNIZE SECURITY SIGNAL.

From Incoming Report to Actionable Finding

01 INTAKE

Confirm program scope, asset, report completeness and obvious duplicate or previously known conditions.

02 ANALYZE

Review evidence, reproduction steps, vulnerability class, preconditions and the researcher's claimed impact.

03 REPRODUCE

Independently validate the behavior where authorized and technically possible; request additional evidence where necessary.

04 ASSESS

Determine exploitability, severity, business impact, duplicate/variant status and whether further attack-path testing is warranted.

05 COMMUNICATE

Provide clear technical feedback to the researcher and coordinate questions requiring program-owner context.

06 ESCALATE & HAND OFF

Surface urgent findings quickly and provide internal teams with a concise validated report suitable for remediation.

Triage Without Replacing Your Program

LCSG can operate as the specialist technical triage layer while the organization retains its existing bug bounty platform, VDP, researcher community and internal remediation workflow.

MANAGED TRIAGE Ongoing first-line and technical triage for organizations operating their own bug bounty or vulnerability disclosure process.	OVERFLOW CAPACITY Additional triage capacity during submission spikes, program launches, scope expansions or AI-driven volume surges.
SPECIALIST ESCALATION Deep technical review of difficult, disputed, novel or high-impact reports that require experienced vulnerability research judgement.	PRIVATE / INVITE-ONLY PROGRAMS Triage support for controlled researcher programs where quality, discretion and direct technical communication are priorities.
PLATFORM-AGNOSTIC Operate alongside an existing platform or customer-managed intake process rather than requiring migration to a new bounty ecosystem.	PROGRAM INTELLIGENCE Identify recurring vulnerability classes, systemic weaknesses, duplicate trends, researcher patterns and areas where scope or guidance should be improved.

OUTCOMES

Reduce Noise Without Losing the Finding That Matters

The goal is not simply to close reports faster. It is to increase the quality and consistency of the decisions made at the point where external research meets the internal security organization.

FASTER SIGNAL Critical and high-impact vulnerabilities reach the right internal teams without waiting behind large volumes of low-value submissions.	LOWER INTERNAL BURDEN Security and engineering teams spend less time reproducing, classifying and debating reports before remediation can begin.
CONSISTENT DECISIONS Structured validation and severity assessment improve consistency across researchers, vulnerability classes and program history.	BETTER RESEARCHER EXPERIENCE Clear, technically credible responses reduce unnecessary friction and help retain high-quality researchers.
LESS AI NOISE AI-assisted and templated submissions are evaluated on technical evidence rather than presentation quality or AI usage alone.	MORE PROGRAM INTELLIGENCE Triage data becomes a source of insight into recurring weaknesses, emerging attack patterns and areas needing deeper testing.

MORE REPORTS DO NOT HAVE TO MEAN MORE DISTRACTION.

SUPPORTING EVIDENCE

The Submission Surge Is Already Here

HackerOne - April 15, 2026. HackerOne reported 46,947 vulnerability submissions in March 2026, a 76% year-over-year increase. It stated that roughly 25% remained valid and exploitable, while high and critical findings represented 32% of validated findings.

<https://www.hackerone.com/blog/continuous-threat-exposure-management-remediation-crisis>

Bugcrowd - March/April 2026. Bugcrowd reported that its triage queue increased by more than 334% over a three-week period, with many submissions characterized by thin evidence, templated write-ups and insufficient validation.

<https://www.bugcrowd.com/blog/bugcrowd-policy-changes-to-address-ai-slop-submissions/>

HackerOne Hai Triage. HackerOne states that 60-80% of vulnerability submissions are invalid and describes a triage workflow in which AI handles intake, classification and duplicate/noise reduction while human analysts reproduce and validate findings.

<https://www.hackerone.com/platform/triage>

HackerOne Agentic Validation - May 2026. HackerOne explicitly describes AI validation as decision support rather than autonomous adjudication: recommendations are reviewed by humans, who retain responsibility for final outcomes.

<https://docs.hackerone.com/en/articles/13603896-agentic-validation>

THE MARKET DIRECTION IS CLEAR.

AI is being used both to discover vulnerabilities and to scale the triage process. The differentiator remains expert validation: determining what is real, what matters and what should happen next.



DISCOVER. EXPLOIT. DEMONSTRATE.

Specialist bug bounty and vulnerability disclosure triage combining AI-assisted scale with experienced human vulnerability research.

BUG BOUNTY TRIAGE | PENETRATION TESTING | RED TEAM OPERATIONS
VULNERABILITY RESEARCH | M&A; CYBER DUE DILIGENCE |
GOVERNMENT CYBER CAPABILITIES

LCSG.US

LITCHFIELD CYBER SECURITY GROUP