G DATA Study2Protect Award 2025

Infos & Teilnahmebedingungen

Start frei zur zweiten Runde des G DATA Study2Protect Award für Bachelor- und Master-Abschlussarbeiten in den Bereichen Cybersecurity, Cybercrime, Cyberdefense und Cyberresilienz.

Die G DATA CyberDefense AG bietet mit diesem Wettbewerb interessierten Nachwuchstalenten eine Plattform, ihre Beiträge für eine sichere digitale Zukunft vorzustellen. Gefragt sind frische Ideen, die durch wissenschaftliche Exzellenz und praktische Relevanz überzeugen, um die stetig steigenden Herausforderungen der Cybersicherheit erfolgreich anzugehen. Die eingereichten Arbeiten werden von einer Fachjury aus unabhängigen ehrenamtlichen Gutachtern aus Wissenschaft, Wirtschaft sowie von Behörden und Verbänden bewertet.

Beim Festakt zum Finale am 5.11.2025 auf dem G DATA Campus in Bochum wird es dann spannend. Urheberinnen und Urheber der fünf besten Einreichungen präsentieren live vor Jury und Publikum ihre Arbeiten. Die Jury zieht sich danach zur Beratung zurück und gibt anschließend die Gewinnerin oder den Gewinner bekannt. Der G DATA Study2Protect Award ist mit 1.000 Euro Preisgeld dotiert.

Für erfolgreiche Einreichungen lesen Sie bitte aufmerksam die angehängten Teilnahmebedingungen, füllen Sie die Teilnahmeerklärung vollständig aus und vergessen Sie nicht zu unterschreiben.

Wir sind bereits jetzt gespannt auf neue Ideen und freuen uns über rege Teilnahme.

Einreichen einer Arbeit

Überprüfen Sie vor Einreichen einer Abschlussarbeit zum Study2Protect-Award, ob der Absolvent oder die Absolventin die unten aufgeführten Teilnahmebedingungen erfüllt. Bestätigen Sie das abschließend mit Ihrer Unterschrift und senden Sie das vollständig ausgefüllte Formular zusammen mit der Arbeit
(bevorzugt als PDF) und eventuellen weiteren Begleitinformationen an **award@gdata.de**

Informationen zum Absolventen, zur Absolventin

Kontaktdaten

Name:	
Adresse:	
E-Mail:	
Telefon:	

Einordnung des Absolventen/der Absolventin (Verdienste im Studium, Potentiale etc.):

Informationen zur Abschlussarbeit

Titel und ggf. Untertitel der Arbeit:

Welches Themengebiet wird behandelt (s. angehängte Liste der aufgeführten Themengebiete)?

Art des akademischen Abschlusses:
(Bachelor, Master oder ähnlich)

Abgabedatum der eingereichten Arbeit:

Note:

Begründung: Warum ist diese Arbeit preiswürdig?
(Umfangreichere Erläuterungen gern in separat angehängten Empfehlungsschreiben):

Einordnung der Arbeit: Publikationen, Konferenzen, Auszeichnungen etc.

Informationen zum Einreichenden

Kontaktdaten

Name:	
Institut:	
Adresse:	
E-Mail:	
Telefon:	
Rolle bei der Arbeit (Prüfer, Betreuer, Reviewer etc.)	

Bestätigung

Ich habe die Teilnahmebedingungen gelesen und bestätige das mit meiner Unterschrift.

Teilnahmebedingungen

- Verfassende von Abschlussarbeiten eines Studiums an einer deutschsprachigen Universität, Hochschule oder vergleichbaren Bildungseinrichtungen in Deutschland, Österreich oder der Schweiz.
- Als Abschlussarbeit gelten Bachelor- und Masterarbeiten oder vergleichbare akademische Abschlüsse (im Zweifelsfall gern nachfragen).
- Ausgeschlossen sind Dissertationen.
- Teilnahmeberechtigt am Study2Project Award 2025 sind Arbeiten ab dem 1.10.2023.
- Die Abschlussarbeit kann in deutsch oder englisch verfasst sein.
- Das Thema der Abschlussarbeit sollte das weite Feld von Cybersicherheit, Cybercrime, CyberDefense oder Cyberresilienz abdecken (s. unten stehende Liste).
  Vorschläge für eine Erweiterung der Liste sind willkommen.

Teilnahmevoraussetzungen

- Die Absolventen verpflichten sich, ihre Abschlussarbeit im Finale am 5.11.2025 persönlich vor Ort auf dem G DATA Campus zu präsentieren, sofern sie von der Jury ausgewählt wurden.
- Der Vortrag im Finale sollte auf deutsch gehalten werden, das gilt auch für verwendete Sheets.
- Die Kontaktdaten und die eingereichten Materialien von Absolventen und Einreichern werden im Award-Team geteilt, um einen reibungslosen Ablauf des Wettbewerbs zu gewährleisten.
- Einreicher und Absolvent*innen sind damit einverstanden, dass Autoren, Titel und eventuell auch Abstracts oder Kurzfassungen der Finalisten unter anderem auf der Webseite des Awards, in Social Media Postings oder in E-Mails veröffentlicht werden.
- Die Abschlussarbeiten werden an Jury-Mitglieder weitergegeben. Diese sind zur Geheimhaltung angehalten. Eine Garantie für die Vertraulichkeit kann jedoch nicht gegeben werden.
- Das Finale auf dem G DATA Campus wird vor, während und nach der Veranstaltung mit Foto- und Videoaufnahmen begleitet.
- Einreicher und Absolvent*innen stimmen der Verwertung von Bildern auf Webseiten, in Social Media und anderen Materialien zur Award-Bewerbung zu.
- Die Übernahme von Reisekosten oder Aufwandsentschädigungen ist nicht vorgesehen.

Arbeit einreichen

- Das Einreichen von Arbeiten erfolgt durch Betreuer, Gutachter oder Prüfer von Abschlussarbeiten. Sie wählen die beste Arbeit für die Einreichung beim Study2Protect Award aus. Pro Person darf nur eine Arbeit eingereicht werden.
- Die Abschlussarbeit selbst soll im PDF-Format ohne aktive Inhalte dieser Teilnahme-E-Mail angehängt werden. Andere Formate nach Rücksprache.
- Betreuer und Absolvent*innen stimmen sich ab.
- Die Kontaktdaten des Einreichenden und der Absolvent*in ermöglichen dem Award Team Rückfragen und sollen einen möglichst reibungslosen Ablauf gewährleisten.

Bewerbungsunterlagen

Formloses Anschreiben per E-Mail an award@gdata.de mit folgenden Anhängen:

- Dieses unterschriebene Formular inklusive Informationen und Teilnahmebedingungen
- Die Abschlussarbeit als PDF
- Weitere Informationen zur Einreichung

Termine

1. September 2025: Einsendeschluss für Einreichungen

5. November 2025: Finale des Study2Protect Award auf dem G DATA Campus in Bochum

Liste möglicher Themen

- Malware Descriptions
- Malware Analysis
- Malware Detection, Evasion
- Malware Protection
- Malware Response und Defense
- Endpunktsicherheit, ergänzend zu Malware (inkl. Systemsicherheit)
- Cybercrime Activities
- Cybercrime Economy
- Threat Modelling
- Attack Scenarios, TTPs
- CyberDefense Strategies
- APT & Targeted Attacks
- Social Engineering Attacks & Protection
- Scams, Phishing & Anti Phishing
- Awareness & Education
- Secure Behavior
- Security Culture
- Usable Endpoint Security
- CyberDefense Management
- Incident Handling
- CTI, Data Exchange Standards
- Improving Security & Resilience with AI
- Network Security
- Security Metrics
- Visualization
- Cyber Resilience
- Mobile Malware
- Website Security
- Cloud Computing Security
- SecOps und DevSecOpps
- and more, we are open for proposals