



REVA
UNIVERSITY

NAAC
GRADE A⁺
ACCREDITED UNIVERSITY

HACKURITY -2026

powered by - 

Problem Statements

TRACK -A | AI+SECURITY CROSSOVER

Problem Statement -1

GUARDING THE AGENT

RunTime Defence for MCP-Connected AI-Tools



Problem

Model Context Protocol has become the standard way AI agents call external tools, and the ecosystem's security hasn't kept pace: a 2025 survey of 2,614 MCP implementations found roughly 82% used file operations vulnerable to path traversal and over 40% carried command-injection flaws, part of a wave of more than 30 CVEs filed against MCP infrastructure in a single 60-day window in early 2026. Separate 2026 audits found a large share of public MCP servers still run with no authentication at all, with one scan finding 40% still requiring none as of mid-2026. Build a runtime guard that validates MCP tool calls and responses before an agent acts on them.



What we Expect

A working solution that meaningfully improves the security of MCP-connected AI tools, shown handling a realistic scenario. What it covers and how it is built is up to the team; be ready to explain your reasoning and its limits.



Stretch Tier

Teams that go well beyond the basics — in depth, robustness or real-world readiness — will stand out. How you choose to do that is up to you.

A working defense layer against the exact vulnerability classes currently being exploited in production MCP deployments — not a theoretical exercise, since public CVEs already confirm these flaws are live.



Applicable Industries

SaaS/enterprise /Enterprise Software / Fintech - Banking / Internal Developer Tooling /

TRACK -A | AI+SECURITY CROSSOVER

Problem Statement -2

TRUST BUT VERIFY

Continuous Authorization for Autonomous Agent Workflows



Problem

Most organizations deploying AI agents authenticate once and let the agent act with standing privilege after that — a 2026 survey of 900+ practitioners found only about 22% of teams treat agents as independent, identity-bearing entities, while nearly half still rely on shared API keys for agent-to-agent authentication. The consequences are already showing up: 88% of surveyed organizations confirmed or suspected an AI-agent security incident in the past year, and separately, 89.5% of organizations reported at least one GenAI-related security breach in the prior 12 months. Build a policy engine that re-evaluates authorization on every sensitive action an agent takes.



What we Expect

A working solution that gives organizations better control over what autonomous agents are allowed to do, shown holding up in a realistic scenario. Scope, approach and tooling are left to the team.



Stretch Tier

Teams that push further than the obvious solution, and can back it up with evidence, will stand out. Choose where to go deeper.

Directly answers the identity/authorization gap that two independent 2026 industry surveys identify as the core driver of agentic-AI incidents today. Hackurity_2026_Problem_Statemen...



Applicable Industries

Enterprises deploying autonomous or multi-agent workflows, fintech and banking (agents that move money or touch customer data), SaaS vendors shipping agent features, and any organization giving agents access to internal systems.

TRACK-B | IoT in CYBERSECURITY

Problem Statement -3

BREACH AT THE EDGE

Default-Credential & Firmware Exposure Scanner

Note: Participants must bring their own IoT components, if required for their project.



Problem

Consumer and small-business IoT devices remain the easiest way into a network: roughly a third of devices ship with default credentials and a meaningful share carry permanent firmware backdoors, and botnets built almost entirely from this exposure — like BadBox 2.0 — have compromised more than 10 million devices through supply-chain and firmware weaknesses, while credential- and firmware-exploiting botnets like Aisuru have grown large enough to reach over 20 Tbps of DDoS capacity. Build a scanner that fingerprints devices on a network, flags default credentials, outdated firmware, and known CVEs, and produces a remediation report a non-security owner can act on.



What we Expect

A working solution that helps a non-expert owner understand and reduce the risk from their connected devices. Choose your own scope and approach, and show it working on something realistic.



Stretch Tier

Teams that make their solution more accurate, more useful to a non-expert, or closer to something people would really run will stand out. A lightweight, deployable tool that a small business or home network owner could actually run — directly addressing the single most common IoT entry vector attackers use today, rather than a theoretical exercise.



Applicable Industries

Small and medium businesses and home-office networks, retail and hospitality (cameras, POS peripherals, smart devices), managed service providers, and building or facilities operators with mixed IoT fleets.

TRACK-B | IoT in CYBERSECURITY

Problem Statement -4

GUARDING CRITICAL INFRASTRUCTURE

Industrial IoT (OT) Intrusion Detection

Note: Participants must bring their own IoT components, if required for their project.



Problem

Industrial IoT is now a live target, not a hypothetical one: industrial IoT attacks have risen 75% over two years per Verizon's Data Breach Investigations Report, the energy sector alone saw a 459% jump in IoT-targeted attacks in 2025, and ICS vulnerability disclosures nearly doubled year over year, from 1,690 to 2,451. Build a passive intrusion-detection system tuned to industrial protocols (Modbus, DNP3, etc.) that flags anomalous commands or process behavior without touching production traffic.



What we Expect

A working solution that improves visibility into suspicious activity in an industrial environment without getting in the way of operations. Define your own scope, show it in action, and be ready to discuss its limitations.



Stretch Tier

Teams that tackle the harder, more realistic version of the problem, and can show how well it performs, will stand out. A demonstrably safe, non-intrusive detection layer for exactly the sector experiencing the sharpest growth in IoT-driven attacks — directly deployable value for energy, water, or manufacturing operators, not just a lab exercise.



Applicable Industries

Energy and utilities (power grid, water treatment), manufacturing and heavy industry, oil and gas, and any critical-infrastructure operator running SCADA/ICS environments.



TRACK -C | WEB3 / BLOCKCHAIN SECURITY

Problem Statement - 5

CONTRACT UNDER THE MICROSCOPE

Smart Contract Vulnerability Scanner



Problem

Access control failures and reentrancy remain the costliest smart-contract vulnerability classes on record: OWASP's 2026 Smart Contract Top 10 attributes \$953.2 million in 2025 losses to access-control vulnerabilities alone, with reentrancy adding another \$35.7 million and logic errors \$63.8 million — a category that traces back to the 2016 DAO hack and remains a top recurring exploit nearly a decade later. Build a scanner that catches these bug classes before deployment.



What we Expect

A working solution that helps developers spot security problems in smart contracts before they ship. Decide what to cover and how, and show convincingly that it works.



Stretch Tier

Teams that push further than the obvious solution, and can back it up with evidence, will stand out. Choose where to go deeper. Targets the two vulnerability categories responsible for the largest documented on-chain losses in OWASP's current ranking — directly usable by any small team shipping a contract without a full audit budget.



Applicable Industries

DeFi protocols and exchanges, Web3 startups and NFT platforms, blockchain auditing/security firms, and any fintech exploring tokenization or on-chain settlement.

TRACK -C | WEB₃ / BLOCKCHAIN SECURITY

Problem Statement - 6

CHAIN OF CUSTODY

Tamper-Evident Logging for Critical Systems



Problem

Attackers routinely tamper with logs after a breach to cover their tracks — in the SITA data breach, attackers modified and deleted log files to hide data exfiltration, and the SolarWinds supply-chain attack involved tampering with syslog data specifically to evade detection. Centralized logs can be edited by anyone who gains admin access — exactly when the log matters most. Build a tamper-evident logging system that makes any retroactive edit provably detectable



What we Expect

A working solution that makes it harder for anyone to quietly alter or hide records of what happened on a system. Approach and scope are open; show that it holds up and be honest about its tradeoffs.



Stretch Tier

Teams that anticipate how a determined attacker would respond, and show their solution still holds up, will stand out.

Builds a control against a documented, recurring post-compromise technique — not a hypothetical one — seen in incidents ranging from nation-state supply-chain attacks to ransomware cover-ups.



Applicable Industries

Banking and fintech (regulated audit trails), security operations and incident-response teams, critical-infrastructure and SaaS operators, and blockchain auditing/security firms.



TRACK-D | Digital Inclusion & Public Access Problem Statement - 7

ACCESSIBLE BY DEFAULT

Automated Barrier Scanner for Public Digital Services



Problem

Roughly 1.3 billion people, 16% of the world's population, live with a disability that affects how they use the internet, yet an annual scan of the web's top million homepages found that the overwhelming majority still fail basic WCAG checks, averaging around 50 detectable accessibility errors per homepage — with low color contrast, missing image alt text, and unlabeled form fields among the most common faults. In the US, only about a quarter of adults with disabilities have high-speed home internet, and accessibility-related digital lawsuits topped 5,000 filings in a single recent year, showing the gap is both a usability problem and a legal-exposure problem for any organization running public-facing services. Build a scanner that audits a website or app for accessibility barriers and turns findings into a prioritized, plain-language fix list a non-specialist team can act on.



What we Expect

A working solution that helps teams find and fix accessibility barriers in digital services. Pick your own scope and approach, and show a real improvement for real users.



Stretch Tier

Teams that go beyond reporting problems to actually helping fix them, and test with real-world examples, will stand out. A practical tool that gives any team — not just those with a dedicated accessibility budget — a way to find and fix the barriers that keep roughly 1 in 6 people worldwide from fully using their digital services.



Applicable Industries

Government and public-sector digital services, banking and insurance (regulated customer-facing portals), healthcare patient portals, e-commerce, and education platforms.

TRACK-C | Digital Inclusion & Public Access Problem Statement - 8

EASY PAY – – SAFE PAY

Guided Assistant for Older Adults
Digital Payments & Essential Apps



Problem

As payments, banking, and public services move online, older adults are increasingly at risk of fraud and digital exclusion. In India, 1,03,488 senior citizens reported financial cyber fraud in 2025, losing ₹4,005.12 crore. Only about two in five people aged 60+ can use the internet, and just 8% know how to complain about cybercrime. Build a guided assistant that helps older adults complete essential digital tasks, such as making a UPI payment, in plain language while flagging scam patterns before money moves.



What we Expect

A working solution that helps older adults complete everyday digital tasks more safely and with more confidence. Choose your own task, scope and approach; success is judged by how well it would serve a real person.



Stretch Tier

Teams that make the experience work for more people, in more situations, and test it with real users will stand out.

A tool that helps a person with low digital confidence finish everyday tasks and stops the scam before the money moves — judged by whether a real older adult can complete the task, not by feature count.



Applicable Industries

Banks, fintech, and UPI/payment apps (and bodies such as NPCI and RBI that shape their safeguards), government and public-sector digital services, telecom providers, healthcare portals, and senior-care and community organizations.

Hackurity_2026_Problem_Statemen...



NOTE - Talent knows no track.

Participation in any HACKURITY 2026 problem statement can lead to hiring opportunities.

Choosing the IBM-sponsored Track's only is not a requirement for hiring eligibility.

Participants across all tracks will be evaluated based on their skills, problem-solving ability, technical depth, innovation, and overall performance.

for any queries

contact : hackurity@revacyberclub.tech