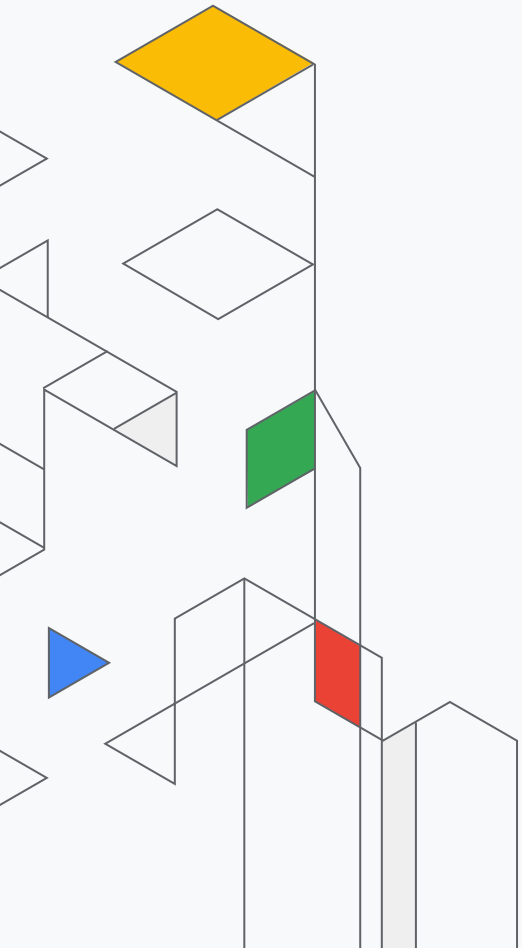


Practical Use of AI, Cyber Security, and Financial Services

David Stone

Office of the CISO, Google Cloud

MANDIANT | Google Cloud

Let’s talk about security, compliance, and trust.

David Stone

Director, Financial Services
Office of the CISO
Google Cloud

Google Cloud’s Office of the Chief Information Security Officer (CISO)

Former:

- CISO @ Wholesale & Enterprise Payments, SVP
- Director of Product Security Architecture @ Lenovo
- CISO @ PCI Level 1 Merchant, Community Bank
- National Security Agency @ US Dept. of Defense
- Advisory Board Member @ EC-Council Certified Chief Information Security Officer
- Masters of Information Security & Privacy, CISSP, C|CISO
- Speaker @ FS-ISAC, Intel Security Conference, Cloud Security Alliance (CSA) and others

CISO Challenges in an Ever Shifting Landscape

Balancing Innovation and Security

Closing Talent & Skills Gap

Resiliency

Multi Cloud / Multi SaaS / On-Prem

Integrating Security into DevOps

Security Policy / Configuration / Operations

Digital Complexity & Configuration Errors

Digital Sovereignty

Compliance & Regulation

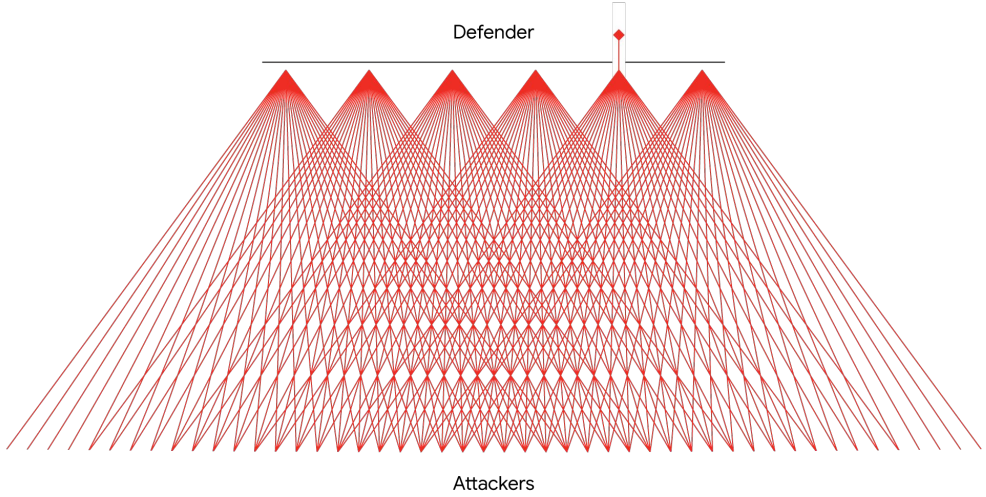
Evolving Threats

Ensuring Board & CxO Support

...etc

Underscored by the Defender's Dilemma

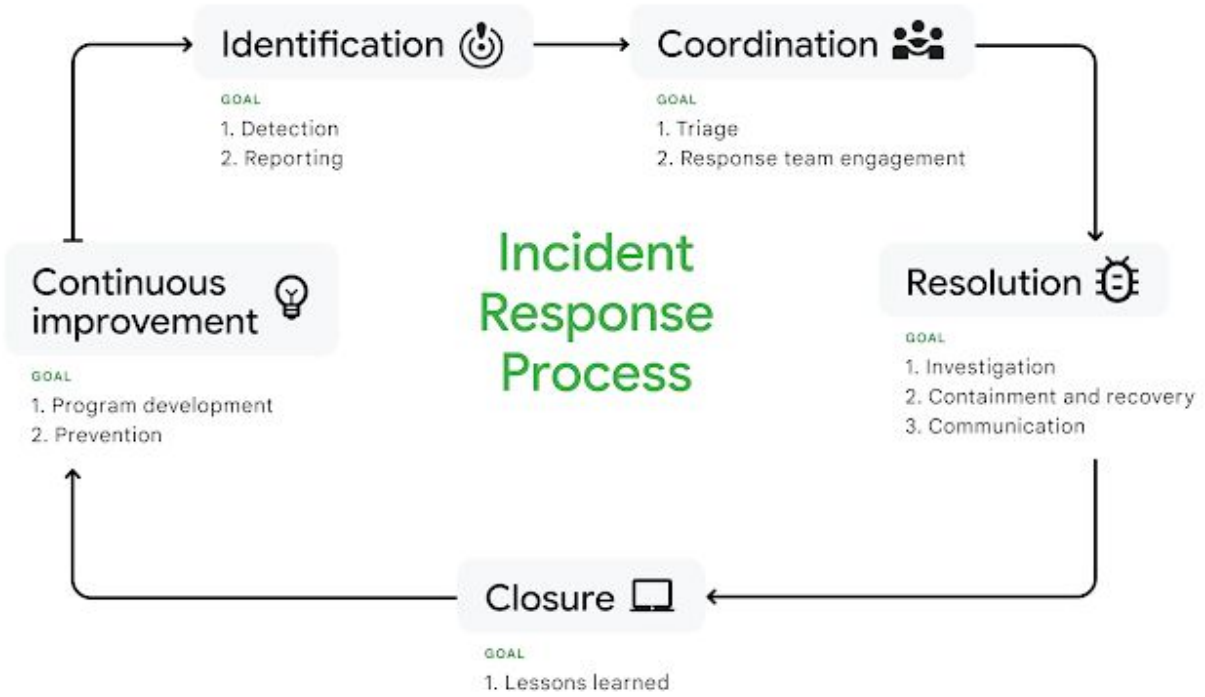
We believe AI affords the best opportunity to upend the Defender's Dilemma, and tilt the scales of cyberspace to give defenders a decisive advantage over attackers.



Examples of How AI Capabilities Can Help Defenders with Cybersecurity Tasks

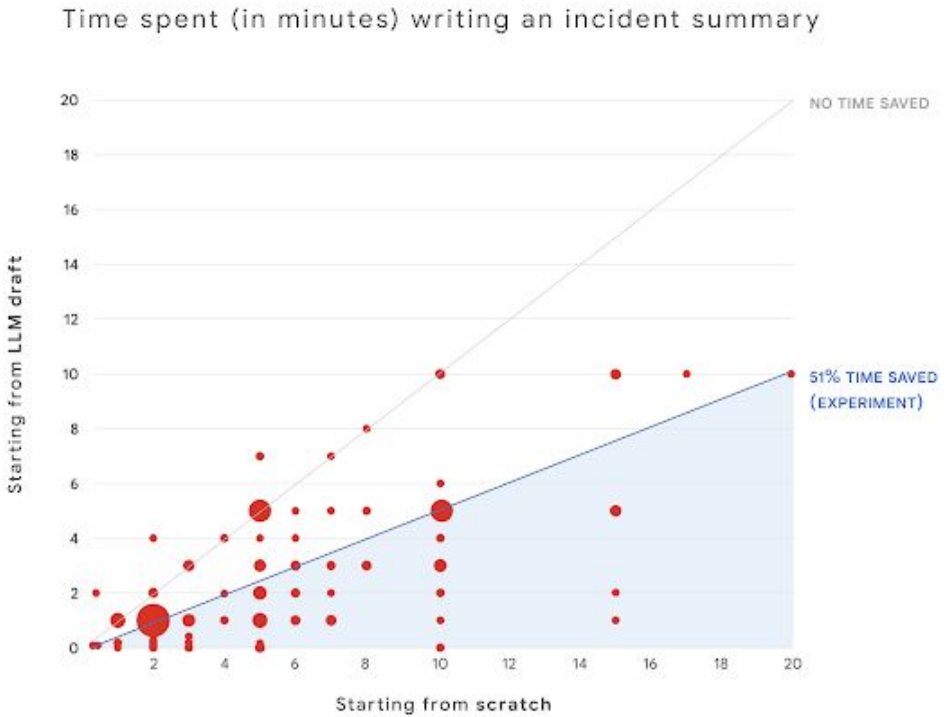
Complex Data, Intuitively Accessible	Critical Insights, Readily Surfaced	Specialized Syntax, Instantly Translated	Abstract Away Complexity, Securely
• Concisely explain behavior of suspicious scripts • Summarize relevant and actionable threat intelligence & reports • Summarize case investigations • Summarize vulnerability reports	• Classify malware • Categorize and prioritize threats • Detect unusual and malicious events • Run attack path simulations • Monitor performance of controls and assess early risk of failures	• Generate queries from natural language • Create detection rules • Generate security orchestration, automation and response playbooks • Generate identity and access management rules and policies	• Identify security vulnerabilities in code • Generate safe code • Create configuration fixes • Deploy fixes to production rapidly • Monitor development environments for compliance

Incident Response at Google (Example)



Incident Response at Google (Results)

51% time saved, per incident summary drafted by an LLM, versus a human



Top concerns around AI

Google Cloud customers are often concerned about the following risk themes:

- Security
- Privacy
- Rapidly evolving legal & regulatory requirements
- Governance and compliance
- Bias
- Transparency and accountability
- Appropriate awareness
- Environmental impact

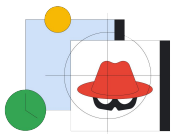
How Google Cloud addresses these concerns:

- Security and Privacy by design, default and in deployment
- Contractual commitments
- AI Governance and compliance with existing regulations, such as GDPR / privacy compliance
- Responsible AI
- Regulator and industry engagement
- Education and Thought-Leadership
- ESG Commitments

Google's Secure AI Framework (SAIF)

AI is advancing rapidly, and it's important that
effective risk management strategies evolve along with it

Expand strong security foundations to the AI ecosystem



Extend detection and response to bring AI into an organization's threat universe

Automate defenses to keep pace with existing and new threats

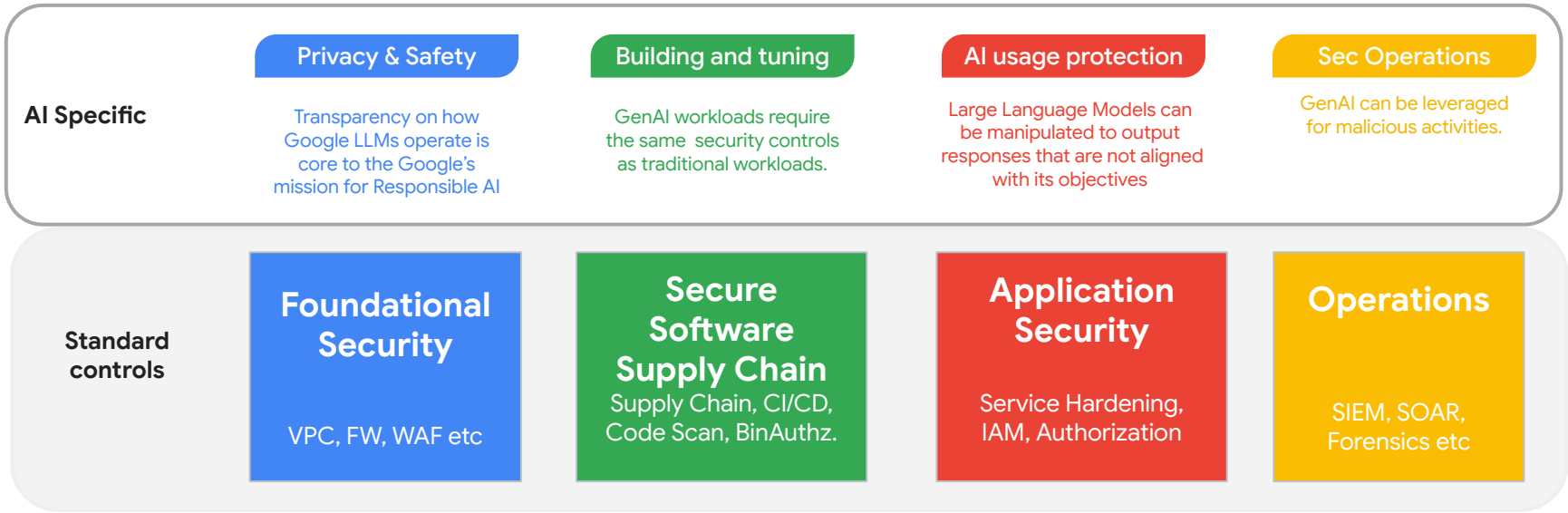
Harmonize platform level controls to ensure consistent security across the organization

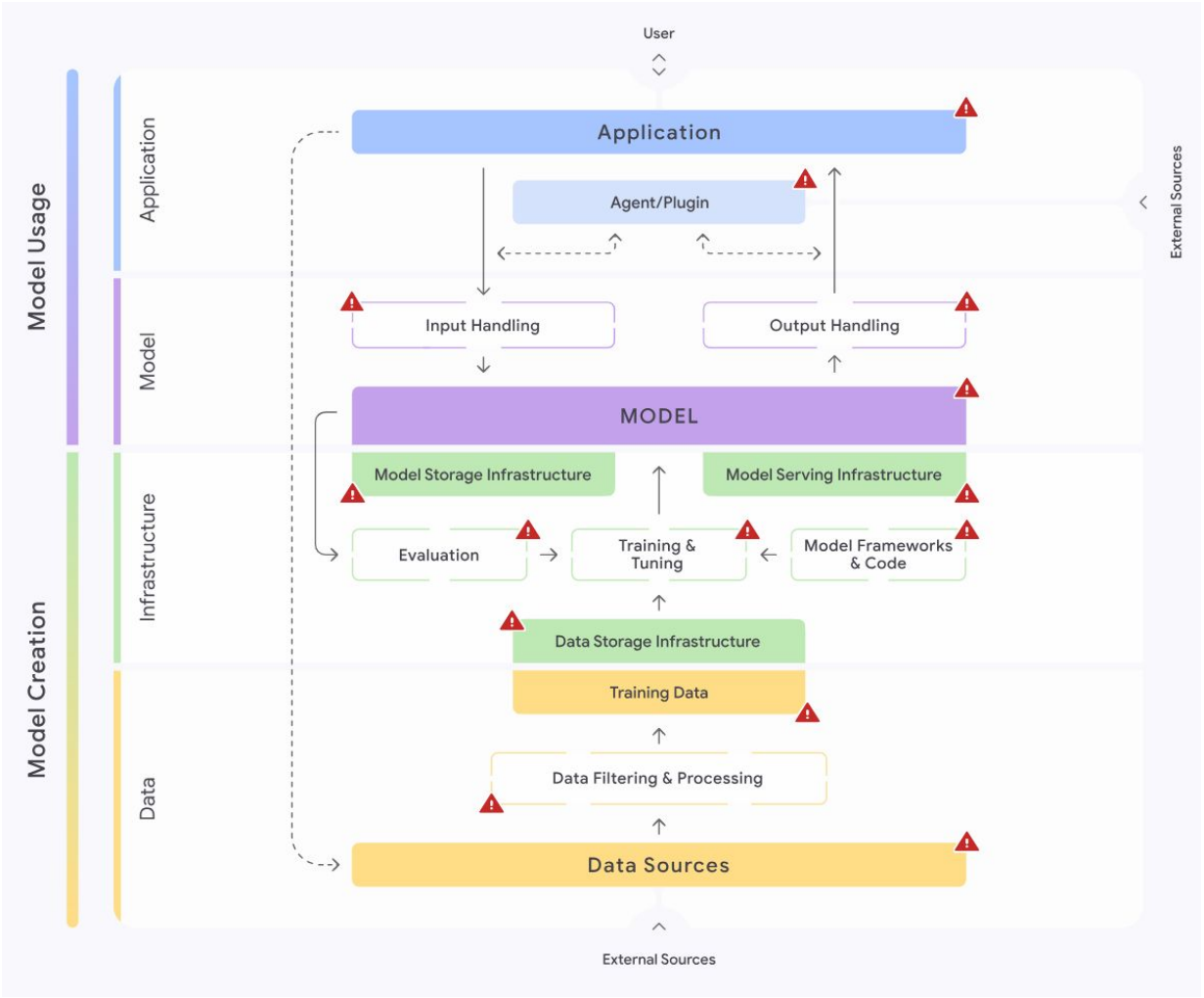
Adapt controls to adjust mitigations and create faster feedback loops for AI deployment

Contextualize AI system risks in surrounding business processes

Securing the AI application

Build on the solid secure foundation

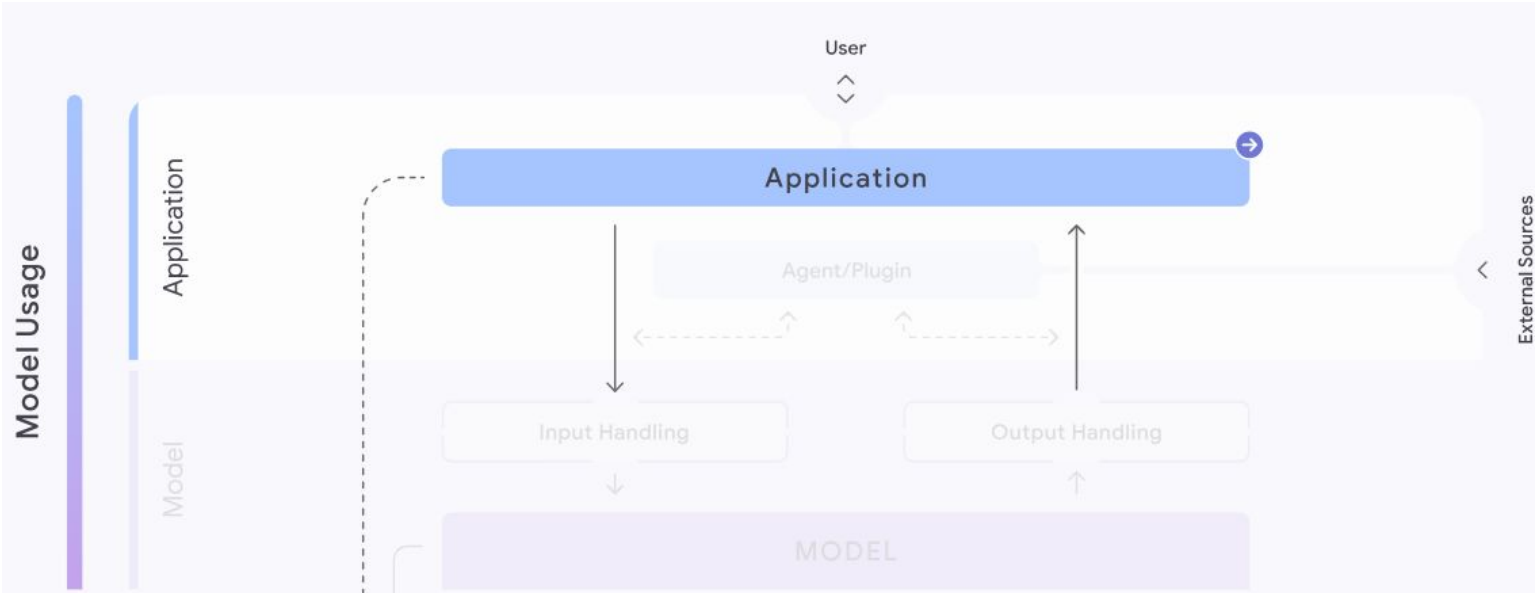




The components where security practitioners, systems, or users can recognize or encounter risks that have been introduced.

Model Reverse Engineering -

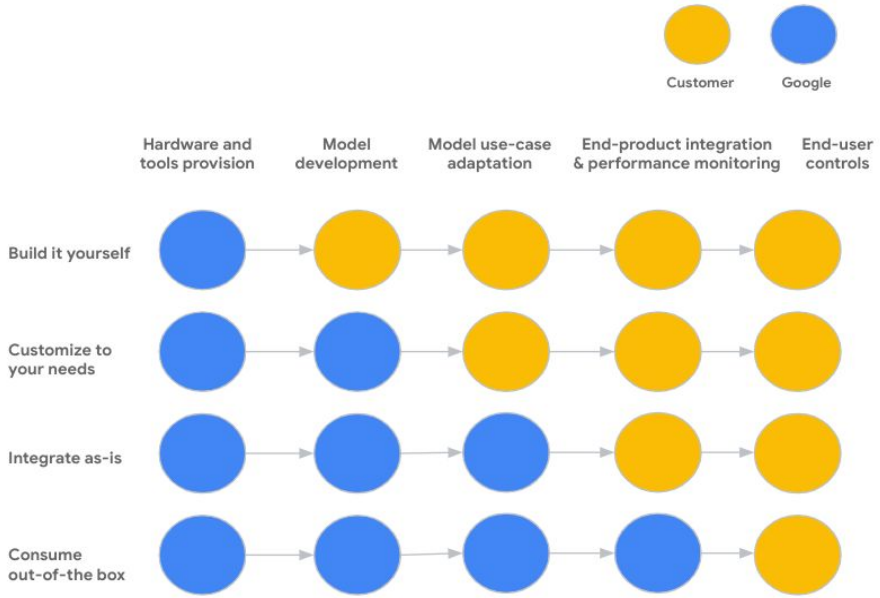
Mitigate this risk with rate limiting within the application API or using other protective measures at the application level to prevent excessive model access.



Tailored AI risk governance approach

Risk profiles are often complex. Importantly, the specific risks and mitigations vary depending on how customers choose to procure and use AI:

1. **Build it yourself:** developing own AI applications, leveraging AI platforms such as Vertex AI
2. **Customize to your needs:** adapting and tuning model and services developed by a third party (such as Google Cloud) with proprietary data
3. **Integrate as-is:** simply use pre-trained models and services without any further adaptation
4. **Consume out-of-the-box:** no development effort needed; consume powerful applications with fully integrated AI capabilities



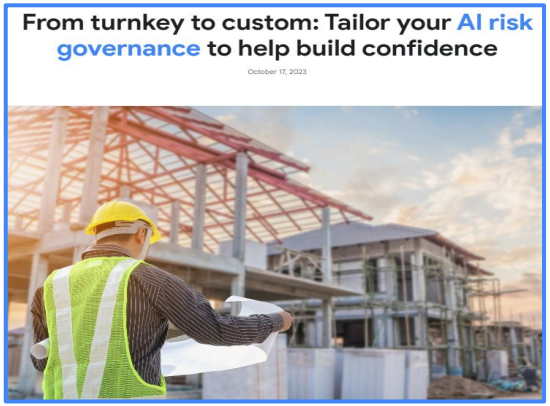
Adversarial Use Of AI

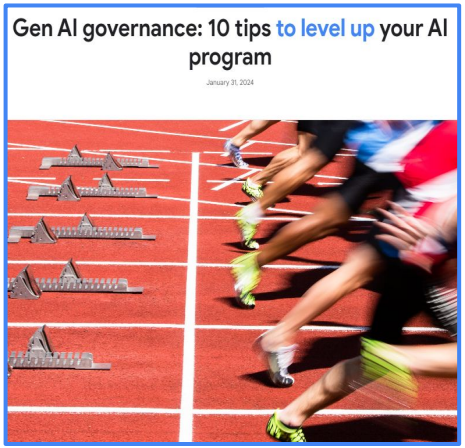
ATTACK LIFECYCLE	TOPICS OF GEMINI USAGE
Reconnaissance	**Recon - Iran** > Recon on experts, international defense organizations, government organizations > Topics related to Iran-Israel proxy conflict **Recon - North Korea** > Research on companies across multiple sectors and geos > Recon on US military and its operations in South Korea > Research free hosting providers **Recon - China** > Research on US military, US-based IT service providers > Understand public database of US intelligence personnel > Research on target network ranges; determine domain names of targets
Weaponization	> Develop webcam recording code in C++ > Convert Chrome infostealer function from Python to Node.js > Rewrite publicly available malware into another language > Add AES encryption functionality to provided code
Delivery	> Better understand advanced phishing techniques > Generating content for targeting a US defense organization > Generating content with cybersecurity and AI themes

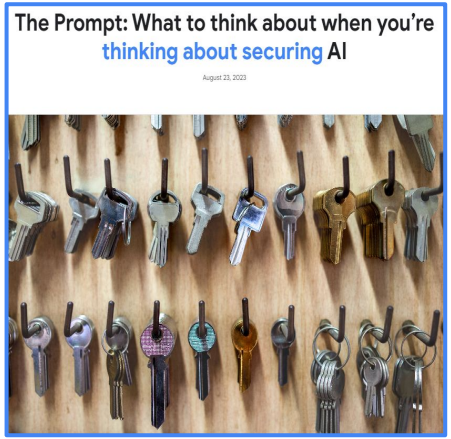
Adversarial Use Of AI (cont.)

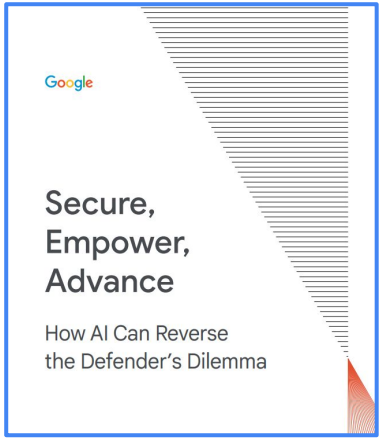
Exploitation	> Reverse engineer endpoint detection and response (EDR) server components for health check and authentication > Access Microsoft Exchange using password hash > Research vulnerabilities in WinRM protocol > Understand publicly reported vulnerabilities, including Internet of Things (IoT) bugs
Installation	> Sign an Outlook Visual Studio Tools for Office (VSTO) plug-in and deploy it silently to all computers > Add a self-signed certificate to Active Directory > Research Mimikatz for Windows 11 > Research Chrome extensions that provide parental controls and monitoring
Command and Control (C2)	> Generate code to remotely access Windows Event Log > Active Directory management commands > JSON Web Token (JWT) security and routing rules in Ruby on Rails > Character encoding issues in smbclient > Command to check IPs of admins on the domain controller
Actions on Objectives	> Automate workflows with Selenium (e.g., logging into compromised account) > Generate a PHP script to extract emails from Gmail into electronic mail file (EML) files > Upload large files to OneDrive > Solution to TLS 1.3 visibility challenges

AI Thought Leadership









Key AI Resources

Google Cloud Controls Posture / Security Guidance:

- Google Cloud's Approach to Trust in Artificial Intelligence
- Generative AI, Privacy, and Google Cloud
- Securing AI: Similar or Different?
- Why Red Teams Play a Central Role in Helping Organizations Secure AI Systems
- Security controls for Vertex AI
- Secure, Empower, Advance: How AI Can Reverse the Defender's Dilemma
- Best Practices for Securely Deploying AI on Google Cloud
- 7 key questions CISOs need to answer to drive secure, effective AI
- Coalfire evaluates Google Cloud AI: "Mature," ready for governance, compliance
- Navigating the EU AI Act: Google Cloud's Proactive Approach
- Google Cloud's commitment to responsible AI is now ISO/IEC certified

Vertex AI:

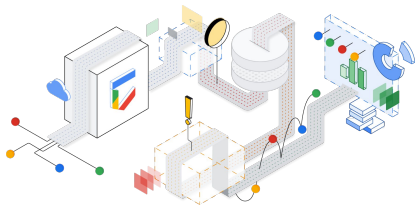
- Overview of Generative AI & corresponding resources
- Certifications

Legal:

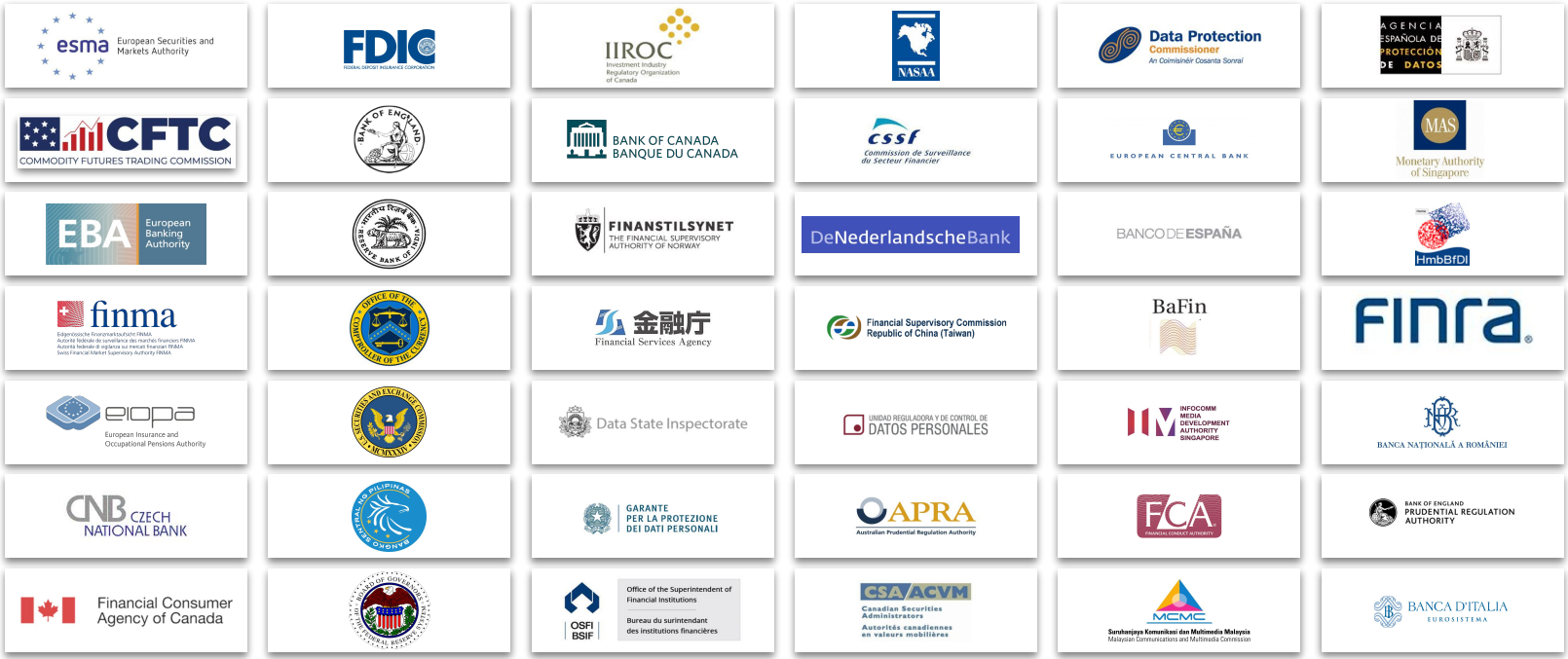
- GCP Terms
- GC Service Terms
- GC Services Summary
- Protecting customers with Generative AI Indemnification (blog)
- Cloud Data Processing Addendum

AI Frameworks:

- Introducing Google's Secure AI Framework
- Secure AI Framework Approach
- SAIF Risk Assessment
- Applying Model Risk Management Guidance to Artificial Intelligence / Machine Learning-based risk models
- Generative AI Risk Management in Financial Institutions



Engagement with Global Regulators



Financial Services + Google Cloud = Shared Fate

Thank you.