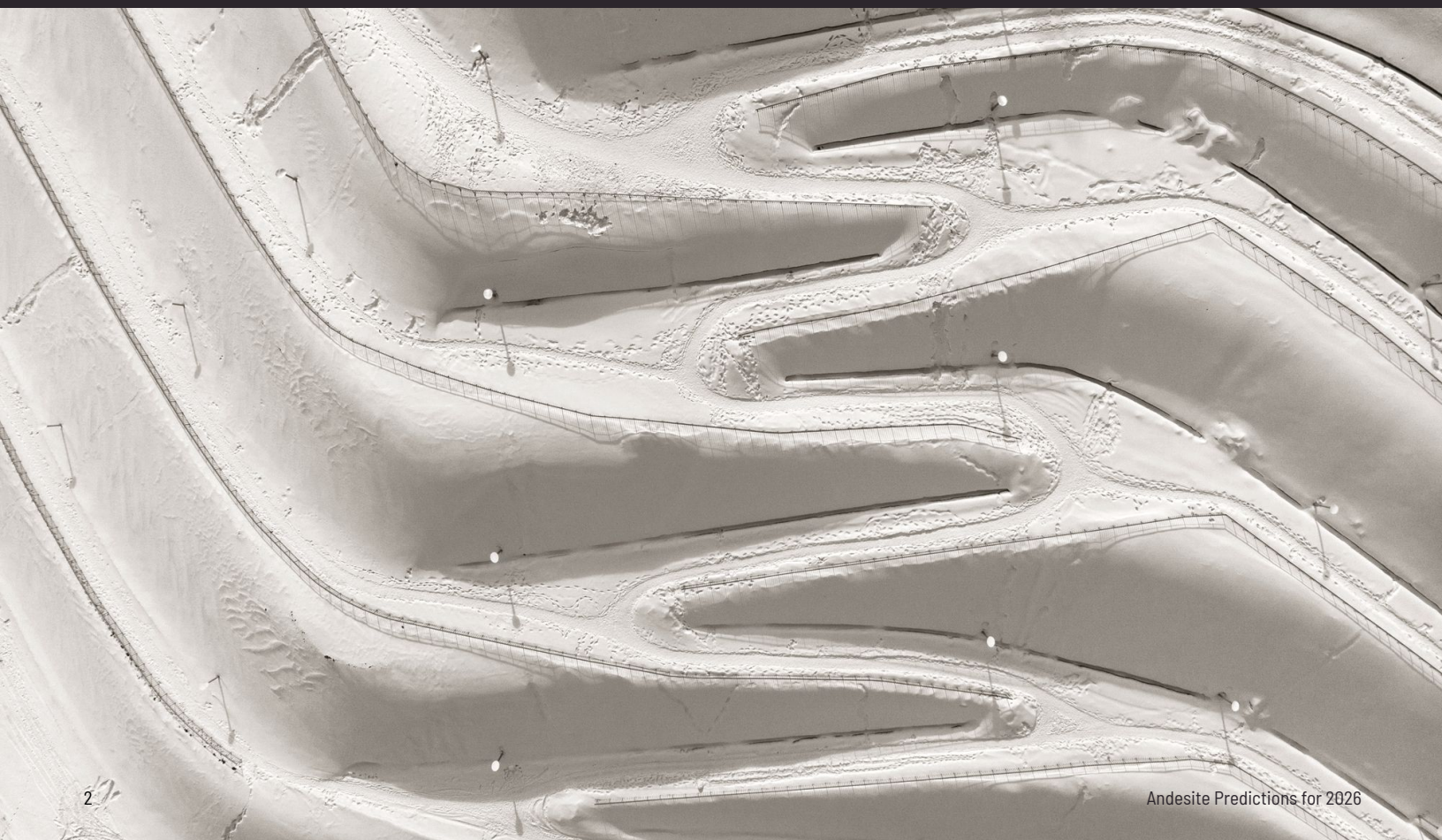
Andesite Predictions for 2026

What's Next for AI-powered Cybersecurity

ANDESITE

With AI entering the enterprise ecosystem, change is coming faster than ever before.

At Andesite, we are dedicated to arming cybersecurity teams with actionable insights that put humans at the helm enabling them to assess risk, make critical decisions, and build a sustainable advantage based on prevention rather than reaction. We gathered predictions for 2026 from Andesite leaders and advisors to help understand where security technology for the enterprise market is going.



William MacMillan

Chief Product Officer, Andesite

William previously served as Senior Vice President for Information Security at Salesforce. Prior to transitioning to the private sector, he was the CISO at the Central Intelligence Agency, where he led a sweeping transformation of the agency's cybersecurity strategy and organization. He was actively involved in the development of the Cybersecurity Operations Center (CSOC).

Prediction 1

Enterprise cybersecurity teams will begin widely implementing AI SOC solutions.

After studying the AI SOC landscape in 2024 and getting hands-on with various products and homegrown tools in 2025, enterprise cybersecurity teams will begin widely implementing AI SOC solutions in 2026. SOC transformations that embrace scalable, human-at-the-helm workflows will win the day. It will be increasingly clear that thinking in terms of agents replacing humans is overly simplistic and serves only to hide risk from decisionmakers.

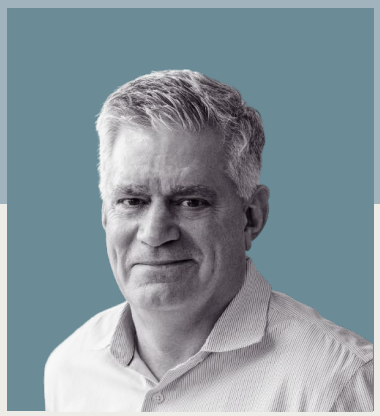
Prediction 2

Investigation timelines for SOC teams that embrace AI SOC tech will accelerate dramatically, shifting the focus from investigation speed to investigation *quality*.

Prediction 3

SecOps teams in government and heavily regulated private sector industries will rethink erstwhile outsourcing strategies.

This will result in the steady pull of detection, investigation, and response workflows back in-house throughout 2026.



Greg Rattray

Chief Strategy and Risk Officer, Andesite

Greg started his security career in the armed forces, serving as the Commander of the Operations Group of the Air Force Information Warfare Center and Director for Cybersecurity at the National Security Council of the White House. In the private sector, he served as Chief Internet Security Advisor for the Internet Corporation for Assigned Names and Numbers (ICANN) and as Global CISO at JPMorgan Chase.

Prediction 1

Geopolitically-driven cyber threats will continue to rise.

This will create the probability of deep attacks against financial systems as part of escalating nation-state competition and conflict.

Prediction 2

Rapidly escalating fraud threats will grow in scale, sophistication, and variety.

These serious defense challenges will cause greater friction for users and contribute to decreasing trust in financial transactions and institutions.

Prediction 3

Cyber defense teams at all levels will look to AI to increase speed of response and enhance the ability to meet the growing scale of attacks.

AI will also play a role in effective governance of technology, controls, and spending. However, organizations will face challenges in speed of deployment and comprehensiveness relative to AI and model risk management concerns.

Alex Thaman

Chief Technology Officer, Andesite

Prior to Andesite, Alex was an engineering leader at Microsoft, Unity Software, and Scale AI. As Chief Architect and Manager for Computer Vision at Unity he developed and led an engineering team charged with simplifying the creation of synthetic data to train and test computer vision models. At Microsoft he worked in compiler technologies before transitioning to AI, helping to develop Xbox Kinect, Hololens, and Microsoft's speech platform.

Prediction 1

The cost/value equation will finally tip in favor of value.

It's projected that OpenAI alone in 2024 spent about $2.25 to make every $1 and most AI companies or business lines are not profitable[1,2]. However, AI is quickly making its way into the value chain. Correctly used coding agents with a human in the loop are resulting in markedly faster code velocity.

Companies that have shifted labor towards AI budgets are seeing results and the technology is sticking. The next step is cost reduction, and it's already in the works. While we won't see companies raking in billions in profit in 2026, we will see buyers open their pocketbooks as the metrics show ROI that's worth paying for.

Prediction 2

This is the year we'll see the first major attack vector through an AI system.

Security research designed to discover vulnerabilities has already demonstrated exploitation of AI products, especially coding agents[3]. Since LLMs and other models lack access to data sources, they are rarely the direct source of vulnerabilities, but AI is being integrated into increasingly complex systems that can dynamically access data and execute actions. As this combined architecture integrates identity and access, exploitable mistakes are being made, which means the attacks are coming.

Prediction 3

AI systems will not be trusted to operate with autonomy in most cases.

In the same way self-driving cars were hyped long before they were reality (approximately 10 years), AI autonomy is still just a promise. We are only three years out from the release of ChatGPT, which gave a step-function improvement in capabilities, but I suspect we are a few years out before we can remove the human from the loop in most AI-enabled systems and products. For the foreseeable future, the industry will focus on increasing the effectiveness of humans rather than automating everything.

1. https://www.nytimes.com/2024/09/27/technology/openai-chatgpt-investors-funding.html
2. http://hbr.org/2025/11/ai-companies-dont-have-a-profitable-business-model-does-that-matter
3. https://www.darkreading.com/application-security/-lies-in-the-loop-attack-ai-coding-agents

Merritt Baer

Andesite Advisor - Chief Strategy Officer, Enkrypt.AI

In addition to being the CISO at Enkrypt.AI, Merritt advises companies and leaders in the security space. She previously served as a Deputy CISO at Amazon Web Services for more than five years, where she helped secure AWS infrastructure at scale. She also worked in security in all three branches of the U.S. government.

Prediction 1

The approach to red teaming will fundamentally change.

Instead of quarterly pentesting that assesses a point in time, it now has to be continuous and sensitive to every configuration change.

If you're taking a traditional data loss prevention approach, it will be like sand slipping through your fingers. AI has to be an integral part of the process.

Prediction 2

This will be a year of immense change.

The nature of data is continually evolving. What security agents are assigned to work on has to shift to ensure they don't go off the rails. And when it comes to reporting to the board, we're in a whole new world.

It's no longer just about what your security teams are doing with AI. The impact of AI will reach well beyond the SOC, making it an essential part of every report from every part of your organization.

Prediction 3

In 2026 we will increasingly question whether data is the primary thing that must be protected.

Keeping your core business processes from being disrupted is moving front-and-center in the cybersecurity purview. Likewise, as data takes different forms because models are non-deterministic, it's not just about protecting the data at the namespace level. When everything is unstructured, it's the meaning of the data that must be protected. And contextualization will be increasingly important for validation and approvals. More than just "Do I let this person in?", permission may be granted based on dynamic attributes contingent upon behaviors.
The days of a simple yes/no are behind us.

Kris Merritt

Andesite Advisor - Founder & President, Vector8, Inc.

Before founding his own cybersecurity consulting and advisory firm, Kris led security efforts for more than two decades within the U.S. government, corporate America, and Silicon Valley. This included running the U.S. Air Force Cyber Security Operations Center, bringing a new model of security operations to General Electric, and helping to create the industry's first cyber threat hunting service at CrowdStrike.

Prediction 1

This is the year of metrics as new AI for security solutions must prove their value.

SOCs with weak metrics programs will feel the pressure for introspection to understand how much human time is saved, as well as how much capacity and margin they have. SOC and SOC-adjacent practitioners will be concerned about being replaced (unlikely anytime soon), leading them to up their game and generate positive metrics, making it more difficult for AI solutions to break in.

Prediction 2

Security labor has to scale.

Availability of security analysis, vulnerability discovery and management, intelligence analysis, DFIR, remediation strategists, and other insight generators must grow faster than we can train. Expect AI solutions to enter the space of equipping dynamic human work rather than replacing repetitive work.

Prediction 3

Telemetry and workflow will likely converge.

Security tooling today separates data systems (SIEM, data lakes, data orchestrators) from workflow systems (SOAR, ticketing, case management). LLMs have bolstered human ability to reason at scale, but data and federated information is core to this. There's significant opportunity in vertically integrated security stacks for new solutions like the next-next-gen SIEM to emerge in 2026.

About Andesite

The Human-AI SOC empowers cybersecurity teams with the actionable insights they need to make critical decisions, assess threats, and determine risk levels.

Andesite's Human-AI SOC enables cyber defense teams to conduct and automate investigations and enrichment, manage high-volume alerts and process threat intelligence reports in minutes. Our AI technology connects silos and reduces inefficiencies across data sources, tools and platforms in their security ecosystem, helping SOC teams to accelerate time to detect, investigate and respond. Andesite's leaders and founders spent decades protecting our nation and some of the largest enterprises on the planet against sophisticated adversaries. The company embodies their sense of mission and commitment to develop security products that empower those who work protecting others.

Visit us →

Request a demo →

Our trust center →

Follow us on LinkedIn →