Elevate Security

PRODUCT BRIEF

Elevate Control

Automate SecOps Controls and Response to High-Risk Users

Analysis finds that 8% of the workforce contribute to 80% of an organization's security incidents. For Security Operations (SecOps), the computing behaviors of these high-risk users place considerable burdens on teams already overwhelmed defending against external threats. It's time to flip this script!

Your Problem:

Defending against external cyber threats is difficult enough without your own workforce contributing to the assault. Poor computing behaviors by high-risk users end up consuming valuable time and staffing resources desperately needed to fight real threats.

Actions spent responding to user-driven incidents are cycles not being spent where it counts most—identifying bad actor attempts at account take over, lateral movement, and compliance violations.

Our Solution:

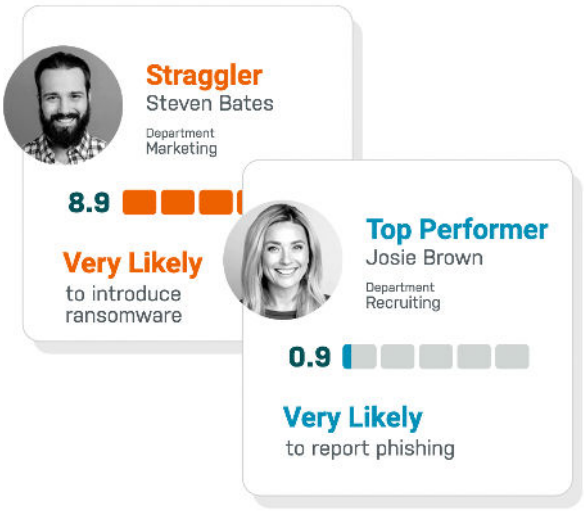
By injecting workforce risk data into SecOps systems and workflows, security and operational teams gain visibility into the activities of high-risk users to better detect and respond to security incidents caused by them, and isolate damage before it can spread.

Further, workforce risk data can be used to inform SecOps policies and controls that work to improve your overall security posture by automating analysis and response to workforce behaviors and patterns contributing to threat exposure.

Reduce Workforce Risk Burdens on Your Security Operations Teams and Automate Safeguards and Responses to High-Risk Users

How Elevate Control Works

Elevate Control injects workforce risk intelligence into your security operations tooling and processes to accelerate incident triage and response, enable better help desk decision making, and automate controls for your riskiest individuals. By making contextual user risk data available to Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and help desk tools, you'll have insights that drive faster incident response times, reduce damage from incidents, and an overall improved security posture.



Deepen Security Intelligence

Ingest high-risk user data into your SIEM for better analysis of behaviors, patterns, and detection of potential threats-in-motion.

Automate Controls

Apply high-risk user data to SOAR workflows and playbooks to trigger automated responses for events generated from this user group.

Speed Incident Triage and Response

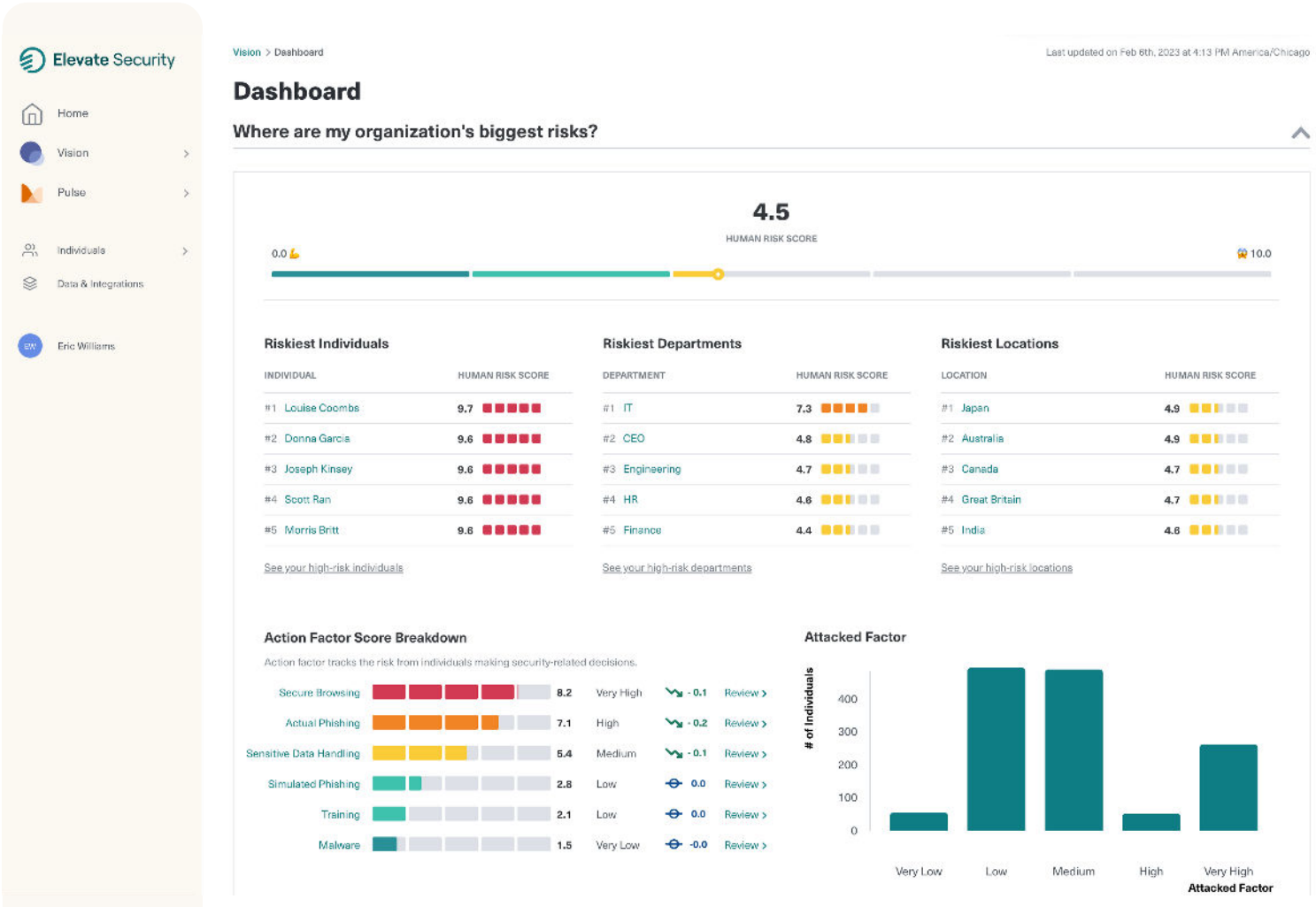
Leverage high-risk user data in your SOC to better triage and prioritize incidents, and quickly identify the scope of blast radius on other people and systems.

Enable Better Decision Making

Providing Help Desk analysts with user risk data enables more intelligent decision making to user requests, and greater protection of sensitive resources.

Gain Control and Visibility of Your Riskiest Users

By operationalizing data about those individuals who make up 80% of your incidents into your Security Operations systems, policies and workflows, you'll improve your security posture and make more efficient use of limited resources. Finally, you'll have a means to flip the tables on workforce cybersecurity risk to better safeguard your business and your people.



Measure individual cyber risk across the workforce and deliver the right feedback, to the right person, at the right time, to drive measurable behavioral change and stronger defense across the organization.

Book a Demo

Elevate Security