

Illuminating the Future of Cybersecurity

Illumen is pioneering the future of cybersecurity with innovative AI-driven solutions that empower organizations to easily assess their compliance posture against industry accepted security frameworks.



Samuel Bradley & Joshua Paulson



Illumen Overview: Pioneering AI-driven Security & Compliance

Cutting-Edge Technology

Illumen leverages the power of artificial intelligence and machine learning to deliver unparalleled cyber security assessment results.

Comprehensive Approach

Illumen's solutions address the full spectrum of cybersecurity challenges, from governance and risk management to compliance and cyber security.

Trusted Expertise

Illumen's team of cybersecurity experts bring deep industry knowledge and a passion for safeguarding organizations in the digital era.



Agenda (1 of 2):

1

Cybersecurity Landscape

Delving into the cyber security domains, and evolving threats and challenges organizations face in the digital age.

2

Governance, Risk, and Compliance

Exploring a holistic approach to managing security, risk, and compliance requirements.

3

Security Frameworks

Navigating the complex landscape of security standards and best practices, and why they matter





Agenda (2 of 2):

4

Artificial Intelligence

How does AI impact security: the good, the bad, and the ugly.

5

Interactive Activity

Let's get your hands on an AI use-case we are using in the field today.

6

Wrap-up

Recap and Q&A.



The Team



Samuel Bradley

Chief Executive Officer &
Co-Founder, with over 17 years
of experience in enterprise
security solutions.

Experience



Alma Mater



Contact



Joshua Paulson

Chief Technology Officer &
Co-Founder, leveraging AI and
machine learning to enhance
cyber security assessments.

Experience



Alma Mater



Contact



Cybersecurity Breakdown:



1 Architecture Security

2 Application Security

3 Network Security

4 Security Operations

5 Corporate Security

6 Physical Security

Cybersecurity Breakdown:



1 Architecture Security

Immutable infrastructure, cloud security, server hardening, golden images, vulnerability mgmt., infra-as-code, encryption, backup & restore

2 Application Security

Secure coding (OWASP), continuous integration / continuous deployment (CI/CD), code scanning (SAST/DAST), QA, staging, change control, access mgmt., PAM

3 Network Security

Segmentation, VPNs, load balancers, port scanning, certificate mgmt., encryption, vuln mgmt, pentests, access mgmt.

4 Security Operations

SIEM, incident response, threat intelligence monitoring

5 Corporate Security

Endpoint protection, email security, phishing, incident response, awareness

6 Physical Security

Badging, video surveillance, datacenter & cage security, physical pentests



Governance, Risk, and Compliance: A Holistic Approach



Security

Implementing robust security controls to protect against evolving threats.



Compliance

Ensuring adherence to industry regulations and standards.



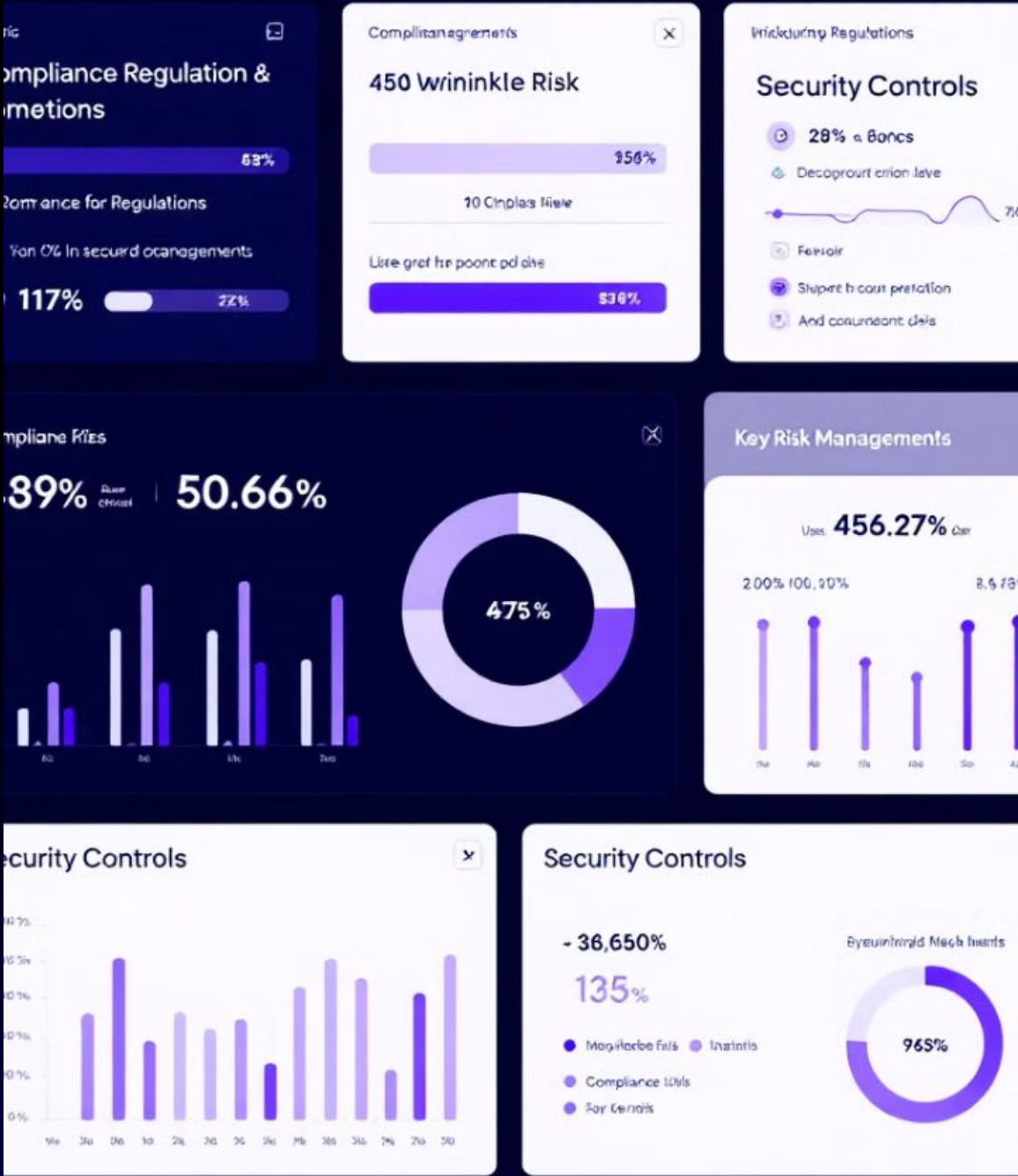
Risk Management

Identifying, assessing, and mitigating potential risks to the organization.



Governance

Establishing and enforcing policies and procedures to manage security and risk.





Governance, Risk, and Compliance Breakdown:

<div>1</div> <div>Governance</div> <div>Policies, standards, procedures, steering committees, board meetings</div>	<div>2</div> <div>Risk Management</div> <div>Rollup of risks, top of the jigsaw puzzle, prioritization</div>	<div>3</div> <div>Compliance</div> <div>Proving security, establishing trust</div>	<div>4</div> <div>Business Continuity</div> <div>Resilience, availability, recoverability</div>
<div>5</div> <div>Vendor Risk</div> <div>Supplier risk, due diligence, security reviews</div>	<div>6</div> <div>Legal & Privacy</div> <div>Contract mgmt., consent, cookie mgmt, data sensitivity, data protection</div>	<div>7</div> <div>Internal Audit</div> <div>Internal review of policies, controls and processes</div>	<div>8</div> <div>Information Security</div> <div>All the aforementioned security domains</div>



Security Frameworks: Why They Matter

1

SOC 2

Table steaks for companies to prove baseline security capabilities to their buyers (AICPA), often a non-negotiable

2

ISO 27001

An international standard for information security management systems (ISMS), widely accepted globally.

3

ISO 42001

Brand new security framework to use artificial intelligence safely and securely, for users and developers.





Security Frameworks: 00s of them





AI-powered Security: The Good, The Bad, The Ugly

The Good

AI vastly improve organizations' ability to identify and respond to vulnerabilities and threats quickly and succinctly. AI can also make managing numerous security compliance frameworks much easier.

The Bad

On the flip side, AI greatly enhances the ability of threat actors to exploit vulnerabilities quickly. Zero days are likely to become even more common.

The Ugly

No one really knows just how far AI will go, and what the implications will be for securing organizations and maintaining trust and transparency across our markets.



Activity: Assess Your Organization with AI

Engage in an interactive session to explore practical steps your organization can take to enhance its cybersecurity posture. Each team will assess one of the following four fake companies: **LuminoGen**, **MediVault**, **AeroSync**, and **TerraBloom**, against the NIST 800-53 r5 framework for control gaps and improvements.



LuminoGen

Specializes in developing and deploying smart grid solutions for renewable energy.



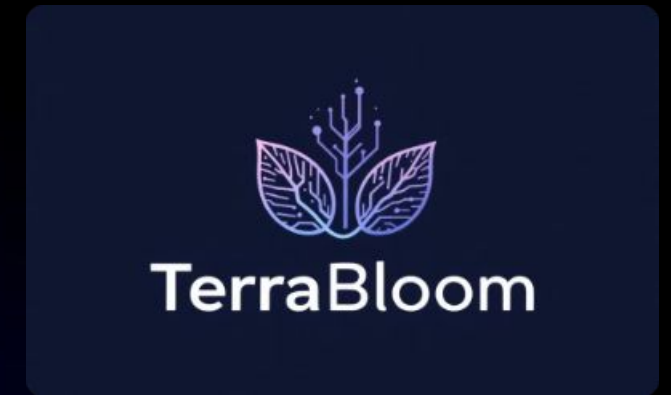
MediVault

Specializes in secure data storage, analytics, and digital solutions for healthcare providers.



AeroSync

Designs and develops mission-critical software and avionics systems for the aerospace industry.



TerraBloom

Develops advanced environmental monitoring systems and smart agriculture solutions.



Imagine the Possibilities



Intake large unstructured data for large multinational companies.



Assess multiple complex, industry-leading security frameworks simultaneously.



Automatically identify gaps in security against these frameworks.



Generate detailed remediation activities, and plot on a roadmap, in seconds.



AI-Powered Security Assessment Agents



Framework Mapping

AI agents link security controls to standards and regulations.



Gap Analysis

Agents identify gaps and vulnerabilities in security.



Remediation Planning

Agents suggest solutions to fix security issues.



Continuous Optimization

Agents monitor and adapt to new threats.

Illumen's AI-powered security assessment solution deploys a team of specialized "agents" to comprehensively review an organization's security posture against industry-leading frameworks. Each agent brings unique expertise, working together to deliver precise, actionable insights.

By leveraging the collective intelligence of specialized AI agents, Illumen delivers a robust, data-driven security assessment that empowers organizations to strengthen their security posture and achieve compliance with confidence.



Real Life Example

[Link](#)



Closing Thoughts and Q&A

Illumen is committed to empowering organizations with the latest AI-driven security solutions and expert guidance to stay ahead of evolving cyber threats, streamlining traditional security assessments, and disrupting the traditional (and expensive) compliance assessment process used today

