SPEAKER: ROB STRICKLAND

Security Audits – Friend or Foe?

M37VENTURES

EXECUTIVE LEADERSHIP TEAM

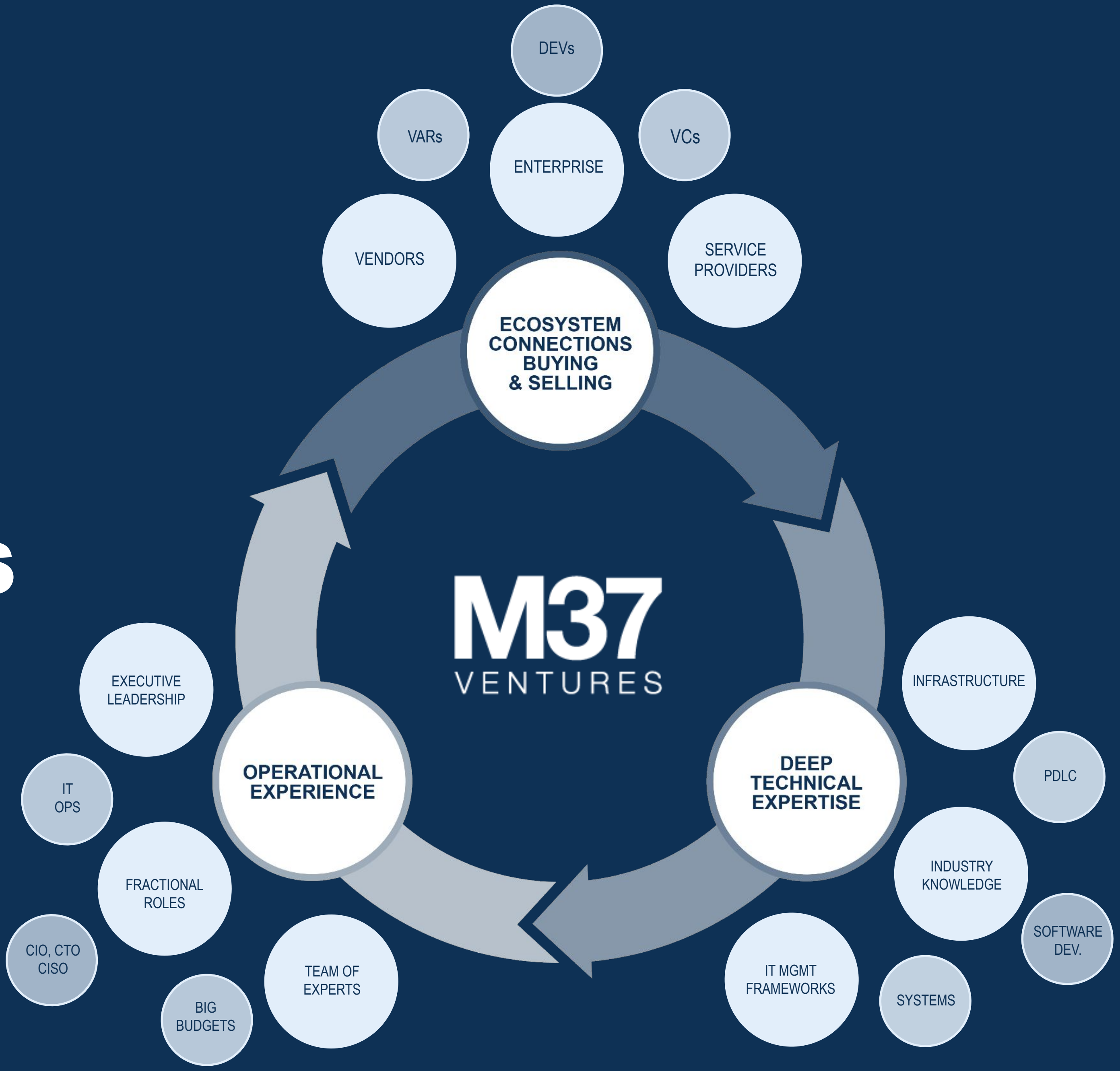
ROBERT “ROB” STRICKLAND

CEO, IT Leadership and Strategy, Advisory

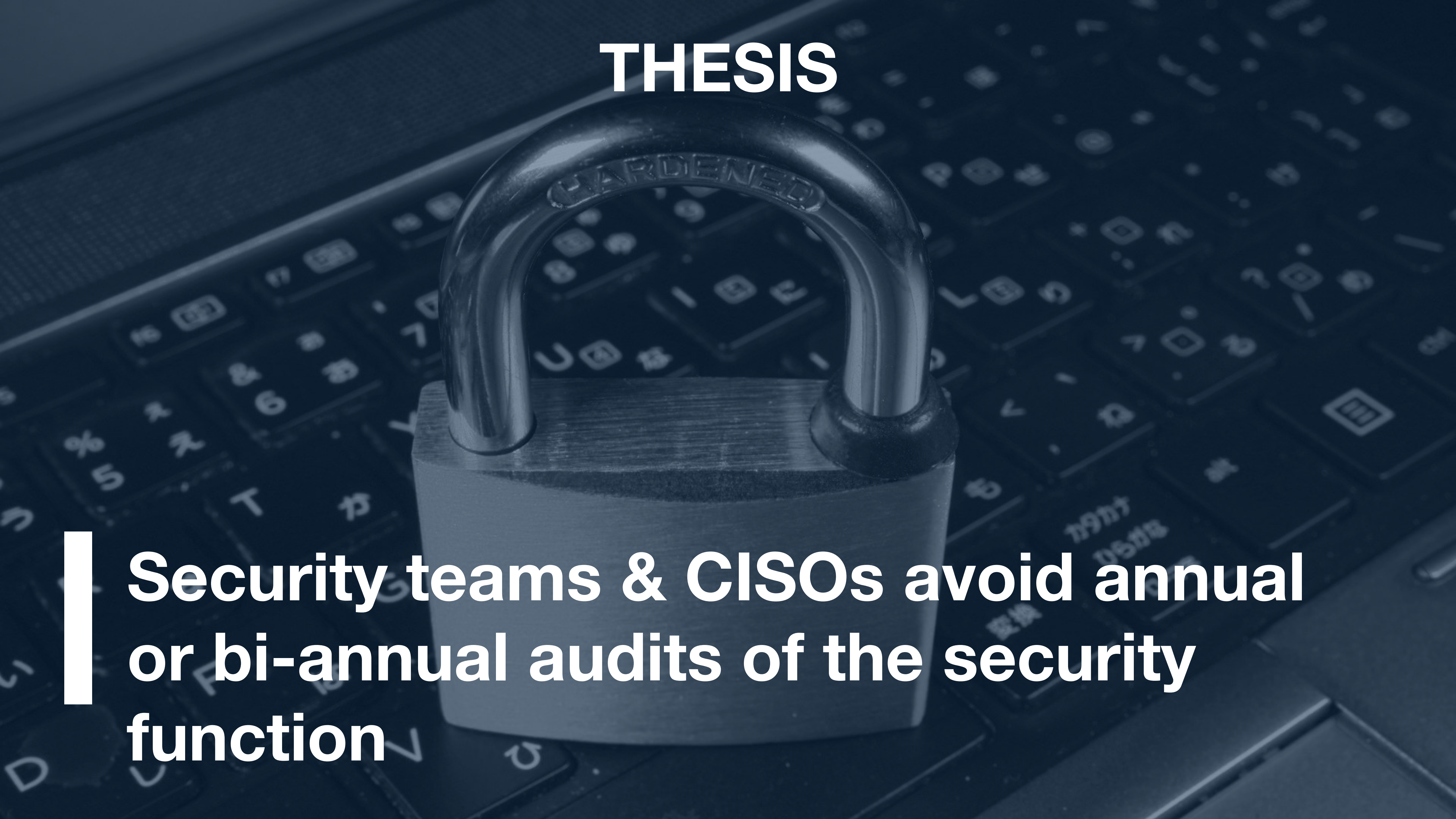
KYLE STRICKLAND

President, Biz Dev, Startups, and Marketing

EXPERIENCE FROM MANY SIDES

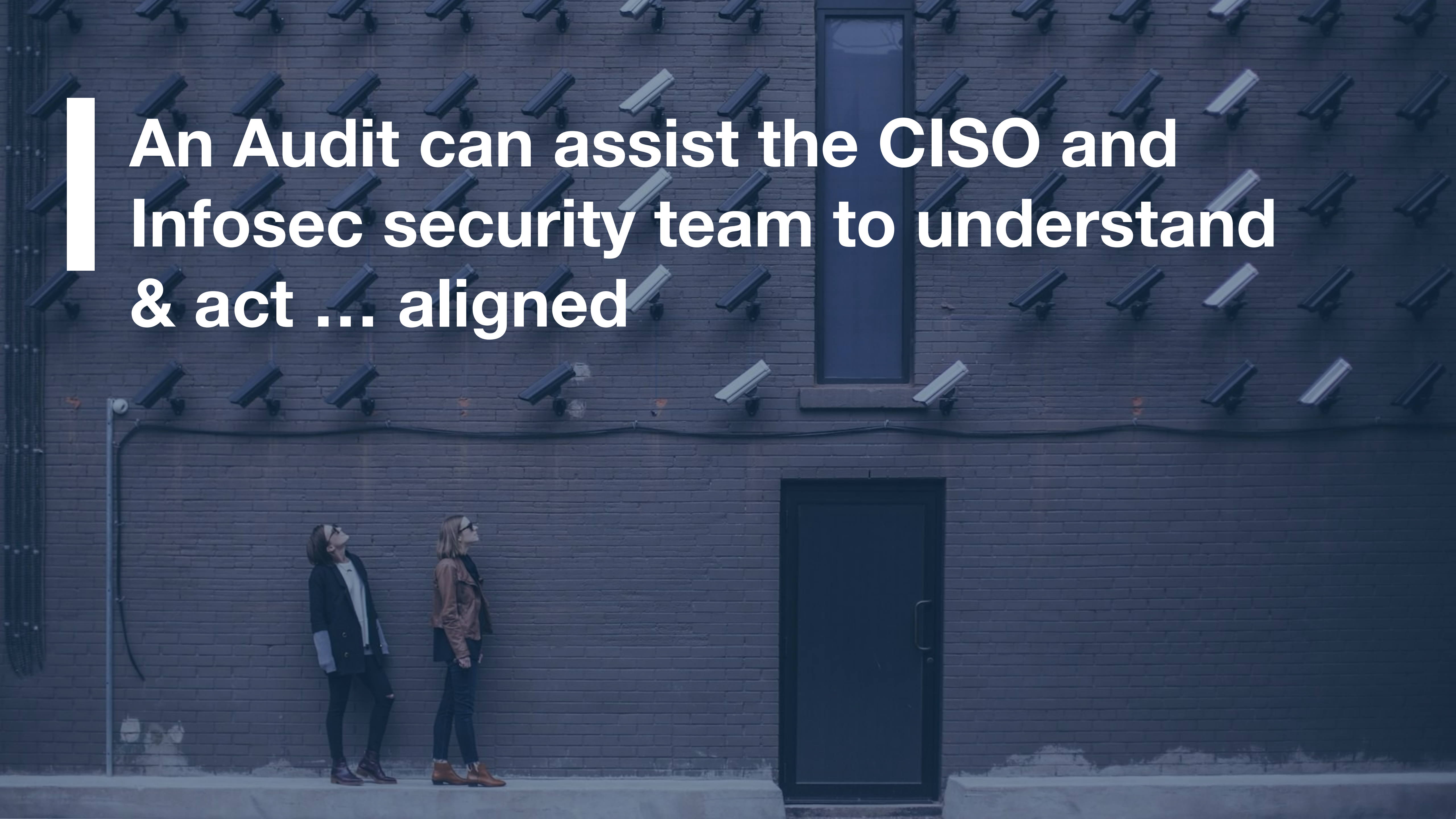


THESIS



Security teams & CISOs avoid annual or bi-annual audits of the security function

An Audit can assist the CISO and Infosec security team to understand & act … aligned



5 Pillars of Technology Management

PEOPLE

PROCESS

STRATEGY

TECHNOLOGY

GOVERNANCE

5 Pillars of Technology Management

**PEOPL
E**

- Feedback on talent & assignments to workstreams
- Organizational structure
- Where to supplement the workforce/process (e.g. Guidepoint)
- Alignment across the company and BU heads
- Continue to improve the Culture of Security
- Dashboards & reporting via SOC (e.g. expel)

5 Pillars of Technology Management

- PEOPLE
- PROCESS
- STRATEGY
- TECHNOLOGY
- GOVERNANCE

5 Pillars of Technology Management

PROCESS

- Review of Security Policies
- Review of training programs and effectiveness
- Score carding or tracking specific KPIs for process improvement
- Alignment with industry standards and comparisons to these standards
- Identification of gaps or processes not yet in place
- Efficiency of controls… Processes and Technology
- Validate Play Books

5 Pillars of Technology Management

- PEOPLE
- PROCESS
- STRATEGY
- TECHNOLOGY
- GOVERNANCE

5 Pillars of Technology Management

STRATE GY

- Refinement and validation of the Security Plan of Record (~ 2 year)
- Review of Security posture and alignment to the Company Strategy
- Sign-off and socializing the Threat Risk Register by BU heads
- Best practices against industry leaders – Sectors vary
- Budget strategy – OPEX and CAPEX
- How to align Security with PDLC or service delivery of the Company
- Prepare for disruptive technology evolution
- Align to the goals of the business

5 Pillars of Technology Management

PEOPLE

PROCESS

STRATEGY

TECHNOLO
GY

GOVERNA
NCE

5 Pillars of Technology Management

TECHNOLOGY

- Evaluation of Tools currently in place – what is missing? What works?
- Effectiveness of SOC – Quarterly Reviews – Outside-In Viewpoint
- Identification of newly emerging tools and techniques (e.g. AI)
- Determination of technology use for “Offense” and “Defense”
- Evaluate Technology Stack – standardized, simplified
- Find technology debt and complexity to de-Risk

5 Pillars of Technology Management

PEOPLE

PROCESS

STRATEGY

TECHNOLO
GY

GOVERNA
NCE

5 Pillars of Technology Management

GOVERNANCE

- Security and PMO Alignment – work done and made secure
- Repeatable, scalable, measurable, financeable = valuable
- Not just the CISO’s problem – Security IS EVERYONE’s Responsibility
- KPIs and Dashboards reviewed in Operations Committees
- Of course, Audits – How are we doing? Risk Register review
- Everyone must know what to do in case of an event! Table Tops w/ Executives
- Demonstrate 3rd Party and supply chain security goals

infovista

Case Study: Security Audit by Guidepoint Security

Interim CIO/CPO at Infovista

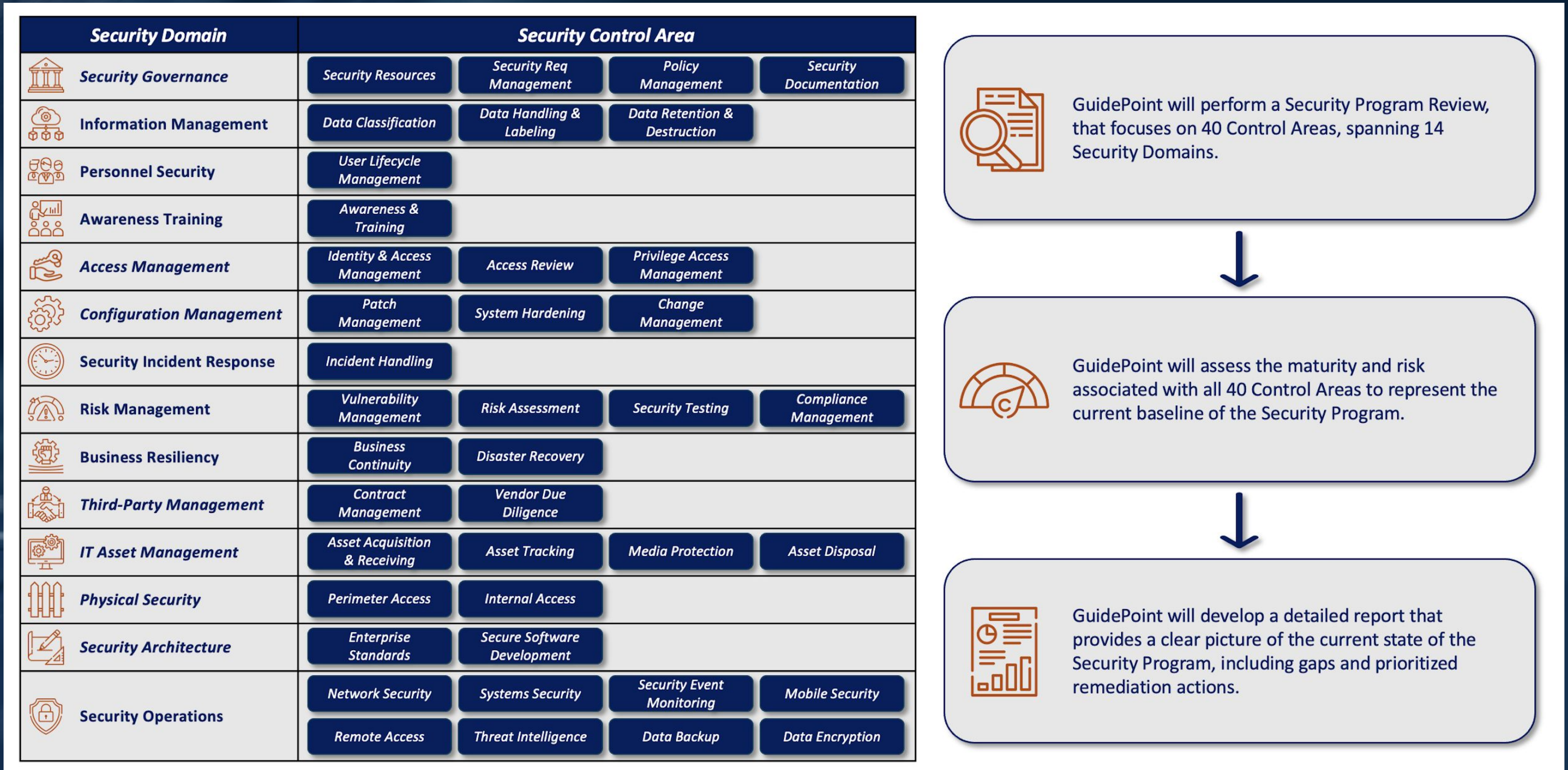
Case Study: Security Audit by Guidepoint Security – 30 Days

- Review expel’s SOC and escalation tree – notifications, awareness, escalations - Dashboard
- Review of Help Desk and correlations between tickets and potential issues
- Review of all Tools and Processes/Procedures
- Full review of recent PenTest and remediation execution
- Interviews across the company – Security Team, Legal, BUs
- Review all access levels, permissions, logging and reporting
- Socialized Risk Register to Executive team and BU heads

Case Study: Security Audit by Guidepoint Security – 30 Days

- Initial push-back from Security Team – but became fully engaged & enlightened
- Very valuable feedback and identification of strengths/weaknesses
- Identification of tool gaps and opportunities
- Established a Dashboard to further track Security Function and its outcomes/measurements
- Validation of process controls and procedural frameworks
- Full report available to the management team (transparency-ownership)
- Further validation of the Security 2-year Strategy
- Quarterly Reviews with expel/SOC & Guidepoint for security operations

Sample Security Audit Best Practices – Guidepoint Security



Security Domain	Security Control Area			
Security Governance	Security Resources	Security Req Management	Policy Management	Security Documentation
Information Management	Data Classification	Data Handling & Labeling	Data Retention & Destruction	
Personnel Security	User Lifecycle Management			
Awareness Training	Awareness & Training			
Access Management	Identity & Access Management	Access Review	Privilege Access Management	
Configuration Management	Patch Management	System Hardening	Change Management	
Security Incident Response	Incident Handling			
Risk Management	Vulnerability Management	Risk Assessment	Security Testing	Compliance Management
Business Resiliency	Business Continuity	Disaster Recovery		
Third-Party Management	Contract Management	Vendor Due Diligence		
IT Asset Management	Asset Acquisition & Receiving	Asset Tracking	Media Protection	Asset Disposal
Physical Security	Perimeter Access	Internal Access		
Security Architecture	Enterprise Standards	Secure Software Development		
Security Operations	Network Security	Systems Security	Security Event Monitoring	Mobile Security
	Remote Access	Threat Intelligence	Data Backup	Data Encryption

GuidePoint will perform a Security Program Review, that focuses on 40 Control Areas, spanning 14 Security Domains.

↓

GuidePoint will assess the maturity and risk associated with all 40 Control Areas to represent the current baseline of the Security Program.

↓

GuidePoint will develop a detailed report that provides a clear picture of the current state of the Security Program, including gaps and prioritized remediation actions.

Q & A

M37VENTURES

empowering new ventures, growing businesses, and connecting technology leaders

www.m37ventures.com