



NINTH ANNUAL LEADERSHIP EVENT

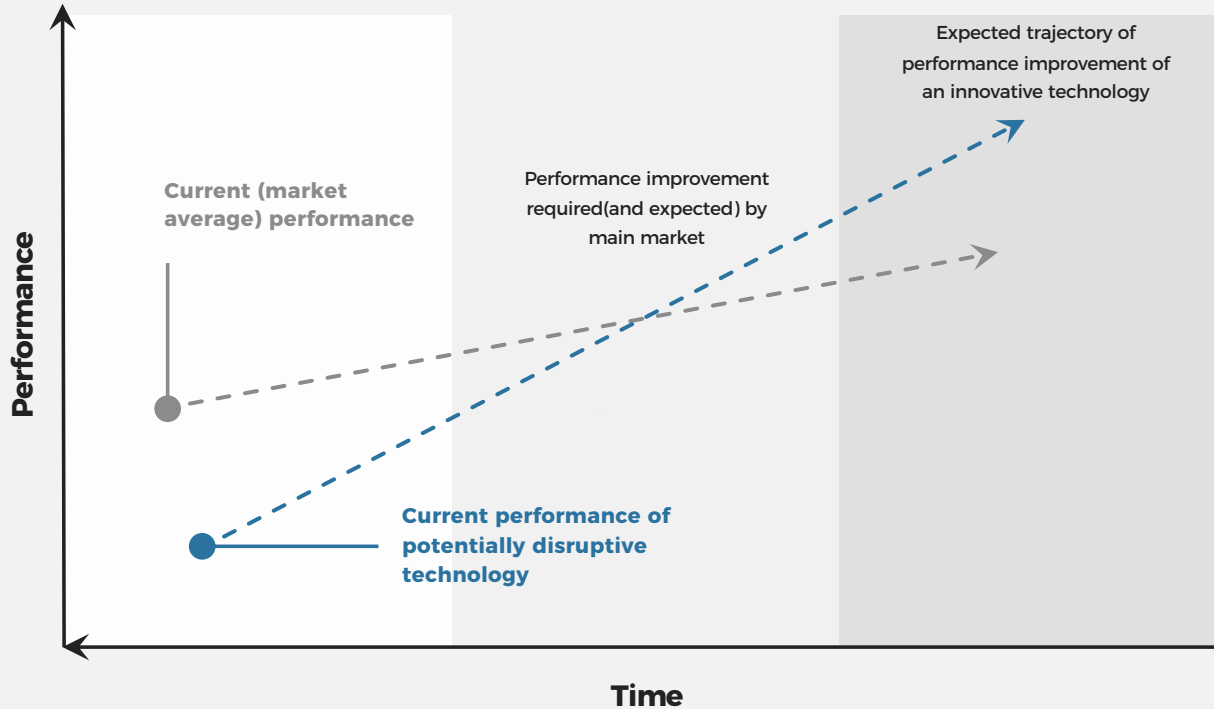
CYBER SECURITY

Security solutions through collaboration.™ **SUMMIT**

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | [#cybersummitmn](https://twitter.com/cybersummitmn)

Defining Innovation



A **cyber innovation** is the implementation of process, technology or new idea for solving a problem which disrupts the existing pattern to create value, reduce risk or dramatically improves on a legacy approach

Cyber Innovation

Cyber Risk Reduction

Where are our **greatest risk exposures** to cyber compromise?
Are their capabilities available which dramatically reduce risk?

PROTECT and **DEFEND** the network from immediate cyber attacks by enhancing the strength and effectiveness of controls

Operational Excellence

Are we spending **time** on activities which can be automated? Are our current technologies an effective use of limited **dollars**?

DESIGN and **BUILD** efficient and effective processes to utilize our time on value-add activities

Cloud and Emerging Tech Cyber

Readiness Are we ready for IT's adoption of **public cloud, emerging technologies and transformation**? Do we have the **knowledge and the skills** for what's next?

THOUGHT LEADERSHIP and **READINESS** for rapidly transforming IT footprint and digital transformation

Energize and Train the Cyber Workforce

Are our people **challenged**, are they learning **new skills**, and are they **rewarded** for taking on new challenges and solving problems?

RETAIN and **DEVELOP** the cyber workforce with new experience, autonomy and empowerment to innovate

Non-Technical Innovation



Alternative Work

Remote, part-time and flexible work arrangements to attract and retain key talent



Public-Private

Information sharing, exercises, and shared resources between trusted partners in industry and government



Job Rotation

Enabling career mobility of existing cyber and IT talent through job shadowing and cross-training



Stakeholder Feedback

Actively seeking input by users, clients and business partners on key security priorities – not just “saying no”.



Academic

Direct academic engagement on curriculum, internships and scholarships.

v2.5

Application Security

[illegible]

Mobile Security

Messaging Security

[illegible]

Abstract:

Security Consulting

Blockchain

Hacking | Amazon BT COVID Deloitte DEERN GROUP edge

AWS AWS AWS leidos nccgroup

BLACK PANTHER Chain CRAXEL edge

VULNER guardtime IDEE Manifold

remme ShoCard vchain xag

OPTIV pwc STOD FRIDBERG STG/A

aud & Transaction Security

IdeaTrust

[illegible]

<http://www.oxfordjournals.org/>

ACALVIO



GuardiCore

Attivo
NETWORKS
illusive

Deception
Counter
Craft
PACKET
VIPER

CyberTrap
SMOKESCREEN

Cymmetria
TRAPX
SECURITY

Cyber Technologies Innovation

Forward-leaning organizations engaging with startups, incubators, venture capital firms and consortiums



Investment

Direct and indirect investment to generate return on investment

Many large organization now have a direct stake in cyber innovation through direct investment, incubators and indirect investments through fiduciaries, creating opportunities for entrepreneurs and companies to partner closely on cyber solution development.



Adoption

Cyber program uplift through development, acquisition of breakthrough technologies

Early adopters of breakthrough technologies and solutions have the opportunity to leapfrog to new levels of control effectiveness to available through legacy technologies, scale quickly to meet demand and growth targets and quickly counter rapidly emerging cyber threats.

Cyber Innovation Success Factors

It's not just about new technologies



Leadership

Commitment and participation in innovative initiatives, including rewarding innovation with incentives



Testing and Proofs of Concept (POC)

Limited scope and duration testing under realistic conditions to evaluate solution effectiveness



Process and Program Design

Establishing basis processes and principles which guide innovation towards agreed upon objectives



Organizational Change

Training, resources and operating procedures for staff whose work and tools may be re-engineered



Technology and Vendor Selection

Partnership with VCs, incubators, and directly with innovative companies to solve problems



Operational Excellence

Established, objective measures of success, performance, maturity or risk reduction

Cyber Innovation Organization Models



Product-Centric

Business, IT and Security teams formed for a single purpose/mission

Business and IT transformations in many organizations are product-centric, breaking down silos to create teams of cross-functional professionals focused on one primary product or platform



Innovation Lab

In-house team of security staff whose sole focus is cyber innovation

Dedicated team, budget and technology resources to incubate and develop innovative solutions; Often move rapidly towards new solution evaluation, but may lack buy-in broadly outside the team



Organic

Growing the security team's existing focus to adopt innovative practices

Enhancing security team's processes and technologies with innovation techniques, POCs or testing as an extension or modernization of the team's existing format

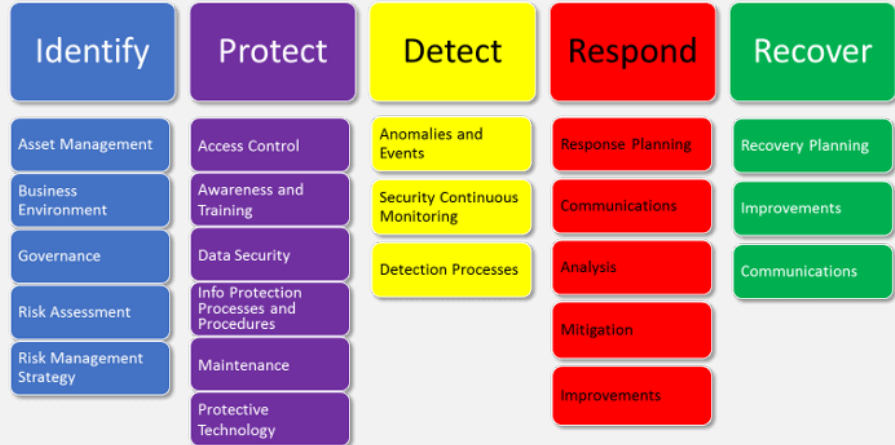
Innovation Foundations



Divide and Conquer

Establish high level categories to use which breakdown "cyber" into more actionable, meaningful groupings to focus and simplify

NIST Cyber Security Framework



Innovation Foundations

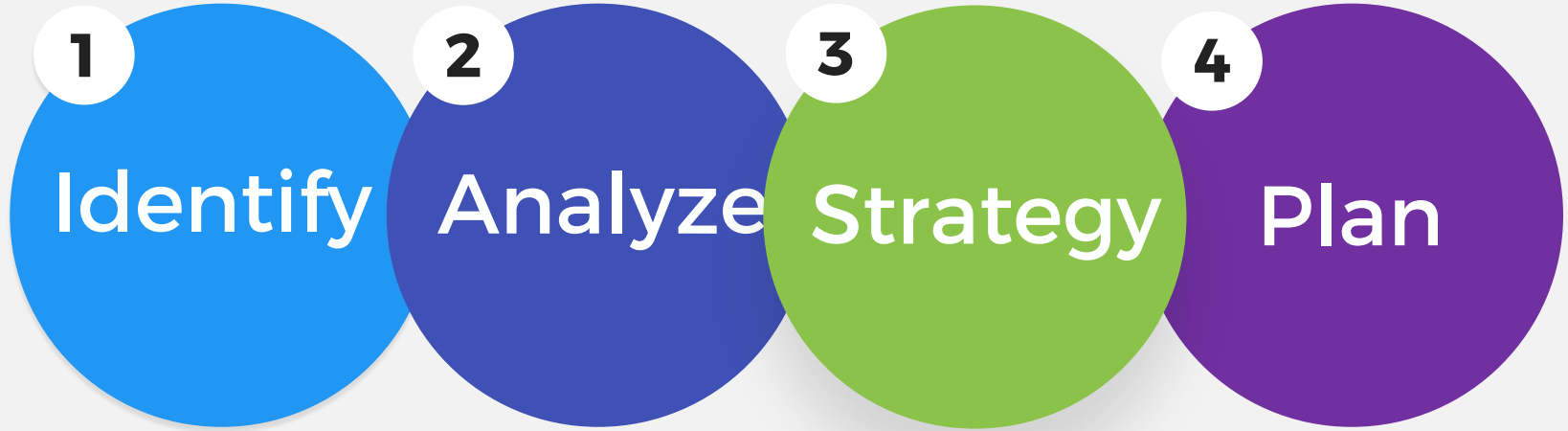


Divide and Conquer

Direct and indirect investment to generate return on investment

- Network and Infrastructure
- Application Security
- Access and Identity
- End User/Training
- Risk and Compliance
- Security Operations
- Threat and Vulnerability Mgmt
- Data Security
- Privacy, Risk and Compliance
- Business Continuity and Disaster Recovery
- Cloud Security
- Mobile Security

Cyber Innovation Process



Cyber Innovation Process

Establish Monthly Innovation Cycle



Innovation is a Process

Establish the routines by which the organization will invest in its continued progress and improvement

[illegible]

1

Identify

Identify the Innovators and Disruptors

Cyber Innovation Tourism

Security leaders traveling to innovation hubs, often in partnership with other security leaders and organizations



1

Identify

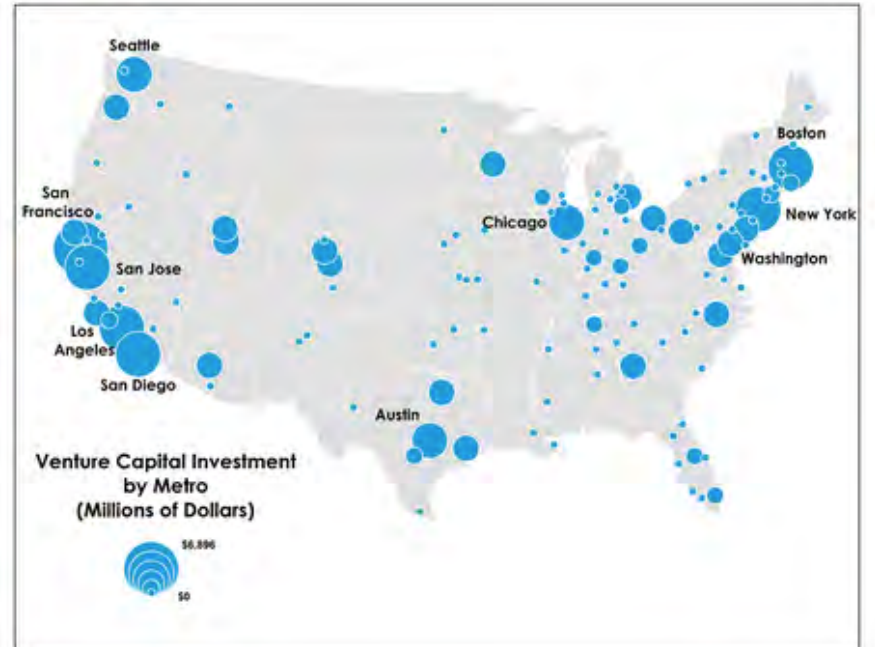
Identify the Innovators and Disruptors

Venture Capital Firms

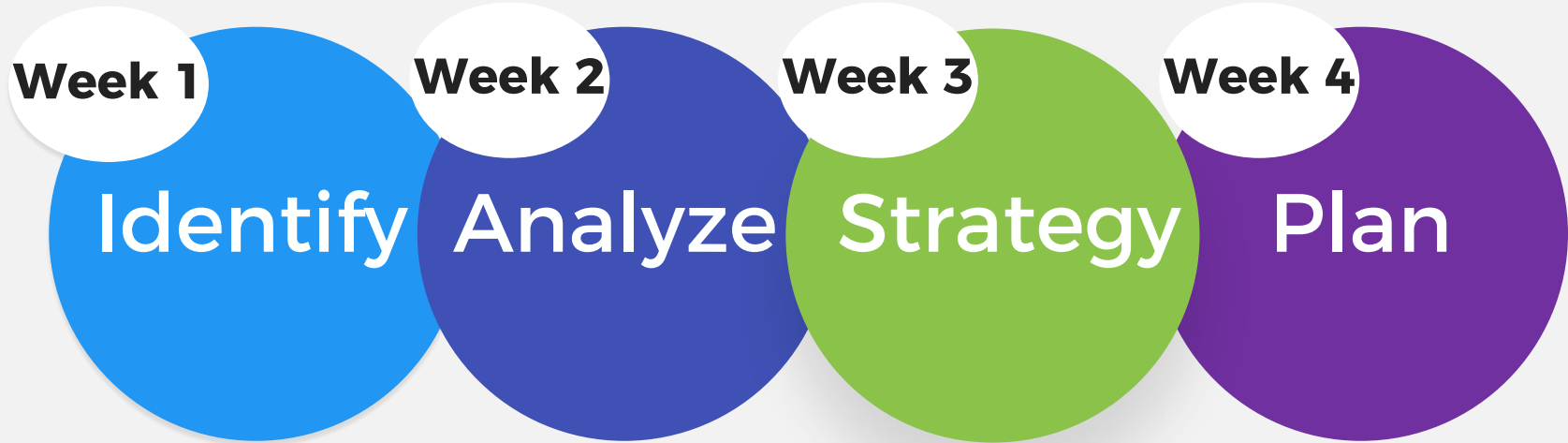
Security teams engaging directly with Venture Capital firms to review full portfolio of cyber investments

- Speed Dating
- CISO Advisory Boards
- Security Events

Direct feedback on portfolio is a tremendous value to VCs

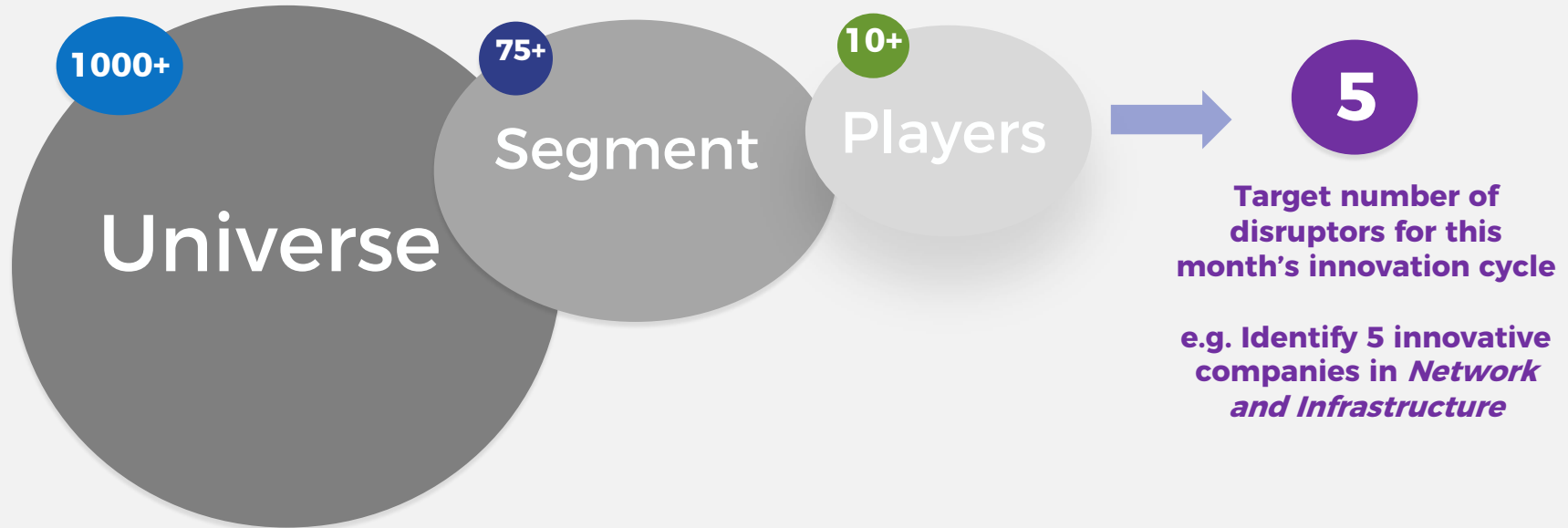


Cyber Innovation Process - Monthly





Identify the Innovators



Cyber Innovation Process

2

Analyze

Establish Monthly Innovation Cycle

Hold an **Innovation Day** each month

Invite to present to your **security** team and **relevant stakeholders** (e.g. App Dev, Network, LoB)

- Threat update (inside or outside analyst)
- Industry expert (Gartner, VC firm)
- Current Technology and Service Providers
- Target 5 disruptive companies

Invite each to provide a **30-60 minute overview**; which highlights their processes, technologies, and how they solve problems or view the cyber world

Cyber Innovation Process

3

Strategy

Strategize Internally

Do we have a new understanding of the **threat** or problem?

Do we have a new understanding of **solutions**?

Does our direction need to **change**?

Are we prepared with **resources, skills and dollars**?

Cyber Innovation Process

4

Plan

Set in motion a plan for innovation

Which **products** and **services** will we renew and continue?

What is the **next action** towards these objectives and on what timelines?

Who are the **key stakeholders** who need to be engaged?

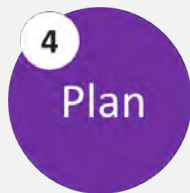
Which **innovators** and **startups** will we engage with?



Cyber Innovation Process

Legacy Security Investment Plan

Network Security		Q1			Q2			Q3			Q4		
		January	February	March	April	May	June	July	August	September	October	November	December
Network Access Control (NAC)	Technology A	Renew											
	Technology B							Lifecycle Upgrade Project					
Intrusion Detection/Prevention	Technology C				New Implementation								
Firewall Policy Management	Technology D	Sprint 1			Sprint 2			Sprint 3			Sprint 4		
DNS Security	Technology E							Renew					



Cyber Innovation Process

Security Investment Plan with Organic Innovation

Network Security		Q1			Q2			Q3			Q4		
		January	February	March	April	May	June	July	August	September	October	November	December
Network Access Control (NAC)	Technology A	Renew											
	Technology X			Innovation POC				Lifecycle Upgrade Project					
Intrusion Detection/Prevention	Technology C			New Implementation									
Firewall Policy Management	Technology D	Sprint 1			Sprint 2			Sprint 3			Sprint 4		
Firewall Change Automation	Technology Y								Innovation POC				
DNS Security	Technology E							Renew					
Network Behavioral Analytics	Technology Z			Date Pending - New Talent Hire									

Working with Startup Companies

Awesome

1 Shaping Product Roadmap

Influence the product's features or bug fixes with speed and customization for your environment

2 Executive-Level Engagement

Direct relationship with Founders, CEO, CTO and key leadership

3 Breakthrough Capabilities

New solutions for new threats and major advancements in control quality and effectiveness

Less Than Awesome

1 Due Diligence Challenges

Some have difficulty passing vendor due diligence processes

2 Corporate support

Depth of engineering and support teams is limited

3 Durable Business Presence

New startups entail risk that their business will be acquired or go out of business

Proofs of Concept

Best Practice Ideas for Innovative POCs

1

Requirements

Set objective measures

- **Architectural Fit**
- **Operational Readiness**
- **Functional Outcomes**

2

POC Plan

Timelines

Are the stakeholders involved ready and able to commit the time and effort for a meaningful POC?

3

Execute

Implement and Test

In the execution of a POC, the testing activity itself should follow an organization's standard IT, change or testing process

4

Analyze

Transparency

Analyze the results and outcomes of testing and POCs with transparency to internal stakeholders

Proofs of Concept

Criteria for Selection



POC Results

Defensible and objective basis for production selection. Expect to be second-guessed every step of the way – *show your work*

	Criteria	Vendor A				Vendor B			
		Points	Weighting	Total	Must	Points	Weighting	Total	Must
50%	Understanding project goal	10	15%	1.5	1	7	15%	1.05	1
	Price	10	20%	2	1	3	20%	0.6	3
	Vendor impression	3	15%	0.45	2	3	15%	0.45	1
10%	101 Non functional requirement 1	3	5%	0.15	2	3	5%	0.15	3
	102 Non functional requirement 2	7	5%	0.35	1	7	5%	0.35	1
20%	201 Functional requirement 1	7	5%	0.35	1	7	5%	0.35	1
	202 Functional requirement 2	7	5%	0.35	1	7	5%	0.35	1
	203 Functional requirement 3	7	5%	0.35	1	3	5%	0.15	2
	204 Functional requirement 4	7	5%	0.35	1	3	5%	0.15	2
10%	301 Functional requirement 5	10	3%	0.3	1	7	3%	0.21	1
	302 Functional requirement 6	10	7%	0.7	1	7	7%	0.49	1
10%	401 Service provisioning A	3	5%	0.15	2	3	5%	0.15	2
	402 Service provisioning B	7	5%	0.35	1	7	5%	0.35	2
100%	TOTAL:	91	100%	7.35		67	100%	4.8	

Legend Score:

- 10 Fully accomplished
- 7 Mostly accomplished
- 3 Partially accomplished
- 0 Not usable

Legend Killer Criteria:

- 1 All Must Criteria met
- 2 All Killer Criteria met
- 3 Killer Criteria not met



Establish Monthly Innovation Cycle



Security Investment Plan with Organic Innovation



		Vendor A				Vendor B			
		Points	Weighting	Total	Must	Points	Weighting	Total	Must
50%	Understanding project goal	10	15%	1.5	1	7	15%	1.05	1
	Price	10	20%	2	1	3	20%	0.6	1
	Vendor impression	3	15%	0.45	2	3	15%	0.45	1
10%	301 Non functional requirement 1	3	5%	0.15	2	3	5%	0.15	1
	302 Non functional requirement 2	7	5%	0.35	1	7	5%	0.35	1
	301 Functional requirement 1	7	5%	0.35	1	7	5%	0.35	1
20%	302 Functional requirement 2	7	5%	0.35	1	7	5%	0.35	1
	303 Functional requirement 3	7	5%	0.35	1	3	5%	0.15	2
	304 Functional requirement 4	7	5%	0.35	1	3	5%	0.15	2
10%	301 Functional requirement 5	10	3%	0.3	3	7	3%	0.21	1
	302 Functional requirement 6	10	7%	0.7	1	7	7%	0.49	1
	401 Server provisioning A	3	5%	0.15	2	3	5%	0.15	2
10%	402 Server provisioning B	7	5%	0.35	1	7	5%	0.35	2
100%	TOTAL:	91	100%	7.35		67	100%	4.8	

Legend Score:

10 Fully accomplished
7 Mostly accomplished
3 Partially accomplished
0 Not usable

Legend Killer Criteria:

2 All Must Criteria met
2 All Killer Criteria met
Killer Criteria not met

Cyber innovation is a deliberate process an organization undertakes to accelerate by inviting new ideas and challenging itself to raise the bar



Karl Mattson

karlmattson00@gmail.com

(612) 404-0550

Karl Mattson is an independent security consultant, President of the Los Angeles Cyber Lab and Senior Fellow at the University of Minnesota's Technological Leadership Institute.

Karl served for four years as the CISO for City National Bank in Los Angeles. He previously was Senior Vice President for IT Risk at PNC Bank and held leadership roles at Target, Unisys and eight years of Active Duty military service in the US Army as an intelligence analyst and Non-commissioned Officer.

Karl holds a bachelor's degree in Business Administration from St. Mary's University, an MBA from Auburn University, and an M.S. in Computer Information Systems from Boston University. Karl holds CISSP, CRISC and CISM certifications.