Security
Please wear your name badge at all times during the meeting.
Please do not leave your personal belongings unattended in the meeting rooms.
Argyle Executive Forum will not be responsible for items left in the rooms.

Mobile Devices
Please do not allow any mobile device to disrupt the meeting while in session.
All devices should be on silent mode.

Conversation
Please use areas outside of the ballroom to converse when the meeting is in session.

Smoking
Please note that smoking is not permitted in the meeting venue.

The content of this program and the attendee list remain the sole property of Argyle Executive Forum and may not be rented, sold, or given to any outside party or used to market or promote any other meeting. Any such unauthorized distribution represents theft of property for which Argyle Executive Forum will pursue any and all appropriate legal remedies.

Speaker Materials are available upon request, pending availability.
WE ANALYZED 219 MOBILE DEVICES FROM A COMPANY AT THIS CONFERENCE

Here is a sampling of the threats that we found:

**Found on 3 devices**

- **Type:** Trojan
- **Family:** NotCompatible
- **Risk:** Can provide backdoor proxy access to an organization's network

**Found on 1 device**

- **Type:** Spyware
- **Family:** IZP
- **Risk:** Can steal a device's browsing history

**Found on 1 device**

- **Type:** Root Enabler
- **Family:** TowelRoot
- **Risk:** Can root a device and compromise its security features

Want to get your own mobile risk assessment? Visit lookout.com/Argyle

No deployments or appliances needed.
Will YOU be ready when RANSOMWARE hits your organization?

Your Ransomware Risk

www.trendmicro.com/ransomware-assessment

Take the Ransomware Readiness Assessment to find out.
Get Cloud Right

- Accelerate compliant software delivery
- Automate infrastructure deployment with policy enforcement
- Continuously protect against misconfigurations and drift

Cloud Infrastructure Governance with Fugue

Cloud is becoming mission critical to your business, yet headlines of data loss, brand damage and regulatory fines have become increasingly common.

Fugue is a cloud infrastructure governance system that accelerates compliant software delivery, automates infrastructure deployment with policy enforcement, and continuously protects against misconfigurations and drift.

Fugue works throughout the application lifecycle, eliminating misconfigurations and compliance violations. Customer results... mitigated risk of downtime and data loss, accelerated deployment of compliant systems and ongoing protection with continuous policy enforcement.

Learn more at www.fugue.co
Higher education and research is, in practice and by necessity, an open and collaborative society driven by the need to share information without hindrance. The daily business practices have the potential to expose protected personal or healthcare information, protected and unpublished research, patentable discoveries and inventions, and large volumes of financial information. Communicating the practices and policies may easily result in promoting fear, uncertainty and doubt, also known as FUD, to motivate users and data owners toward the “right” behaviors. The University of Wisconsin-Madison’s Office of Cybersecurity chooses to move in the direction of partnership as they inform and involve the community of over 22,000 faculty, researchers and staff along with 43,000 students; without FUD as the centerpiece.

In his key note address, Bob Turner provides insight into the issues of communication and community engagement the University of Wisconsin-Madison has travelled with a glimpse of the trail ahead.

Bob Turner
Chief Information Security Officer (CISO)
UW-Madison
9:25am – 9:45am

THOUGHT LEADERSHIP SPOTLIGHT FEATURING LOOKOUT:

“Why Phishing is Both Different and More Problematic on Mobile”

Lookout

The traditional corporate perimeter is evaporating as the enterprise continues its fundamental shift to a mobile-enabled workplace. Now, all endpoints, but particularly mobile devices, are outside the firewall and freely accessing not just enterprise apps and SaaS, but also personal services like social media and email. In this new world, attackers take advantage of the blending of personal and enterprise accounts and the vulnerability of devices outside the firewall to gain access to corporate data and credentials via new vectors for phishing attacks, including SMS and messaging platforms like WhatsApp, Facebook Messenger, etc.

Santosh Krishnan
Chief Product Officer
Lookout

9:45am – 10:10am

Networking Break
10:10am – 10:55am

PANEL DISCUSSION:

“Security Innovation: Unifying Proactive & Reactive”

Session topics include, but are not limited to:

- What are some insider threats that are top of mind for you at your organization?
- How do you pinpoint top weaknesses that increase risk within the company?
- Discuss the importance of implementing both a proactive & reactive strategy within your organization?
- How do you drive innovation while mitigating risk, ensuring continuous compliance & maintaining security?
- How do you leverage tools like the cloud to promote efficiency while maintaining a secure digital environment?
- What are primary threats to the business in the cloud, and what practices & controls are necessary for compliance?
- What’s the best method to plan and prevent insider threats and cyberattacks?
- How do you balance demands that are potential threats to corporate data within your organization?

Moderator:
Bob Turner
Chief Information Security Officer (CISO)
UW-Madison

Panelists:
Arun Desouza
CISO and Privacy Officer
Nexteer Automotive

Sean Nealon
Senior Director, Cyber & Information Security
GGP

Zulzani Noordin
Director of Network Security
A Leading Healthcare Provider

Josh Stella
CEO
Fugue
10:55am – 11:15am

THOUGHT LEADERSHIP SPOTLIGHT FEATURING TRENDMICRO

Milan Urban
Regional Account Manager
Trend Micro

*This session will be off the record.

11:15am – 11:35am

Networking Break

11:35am – 12:10pm

KEYNOTE PRESENTATION FEATURING MOTOROLA MOBILITY

Richard Rushing
Chief Information Security Officer
Motorola Mobility

12:10pm – 1:10pm

Lunch
1:10pm – 1:55pm

PANEL DISCUSSION:


Session topics will include but are not limited to:

- Describe your career journey and your personal experience in your previous and current role in the industry.
- In your experience, how have you seen women break down barriers in regards to challenges in your department and organization?
- How do you define InfoSec excellence?
- If we understood and valued more of the right skills needed in today’s environment, would that naturally translate to more women in InfoSec?
- How are you partnering with HR and other departments in efforts to bring in more women into InfoSec?
- What advice do you have for the audience to increase the number of women working and holding management positions in InfoSec

Moderator:
Sarah Reeser
CEO
Analytical Intel, LLC

Panelists:
Cherisse Estes
Assistant Vice President, Information Technology Product Management
Fifth Third Bank

Susan Nuccio
SVP, Global Manager
Information Security Compliance
JLL

Nazia Raoof
Managing Director - Transformational Strategist / Technology Business Partner
CIBC US

Arlene Yetnikoff
Director of Information Security
DePaul University
1:55pm – 2:15pm
Networking Break

2:15pm – 2:20pm
SESSION INTRODUCTION FEATURING IVANTI

Ray Shum
Enterprise Account Manager
Ivanti

2:20pm – 2:55pm
KEYNOTE SESSION FEATURING NORTHERN TRUST:
“Know, Control, Enable”

Ed Giles offers that through a change in perspective and approach, information security professionals can provide a smoother more secure path to enable business innovation and profitability.

Ed Giles
Senior Vice President, Security Technology Operations & Architecture
Northern Trust
KEYNOTE SESSION FEATURING KELLOGG’S:
“Cybersecurity Practice Overview”

Kellogg’s

New technologies driving the digital transformation and intensifying the new risks have emerged to the business. Despite how sophisticated information security has become, the fundamental of Cyber Security Framework to integrate the People, Process, and Technology is the key to successfully protect the organization from the cyber threats and risks.

Raghbir Sandhu
Sr. Security Architect
Kellogg’s

3:30pm – 3:35pm
Argyle Closing Remarks

3:35pm – 4:35pm
Closing Reception

*Please note, the agenda is subject to change.

The information, views, and opinions expressed by speakers and other participants at our conferences are those of the individual and do not necessarily reflect the views and opinions of Argyle Executive Forum.

Argyle Executive Forum, its directors and officers, do not guarantee that any information provided by a speaker or other participant is accurate or complete and Argyle Executive Forum does not endorse any opinions that may be presented.
Achieve IT Service Excellence with Ivanti Service Manager

IS YOUR HELP DESK PLATFORM READY FOR TOMORROW’S CHALLENGES?

With Ivanti Service Manager, you improve your service team’s efficiency and effectiveness for today’s workload and prepare for tomorrow’s requirements. You gain enterprise-class capabilities coupled with drag-and-drop workflow automation and cloud-based or on-premise deployment to provide effective, world-class service delivery and increase customer satisfaction.

Contact us today at 1.800.982.2130  |  Or visit www.ivanti.com
Hackers Never Take a Break. Neither Do We.

eSentire Managed Detection and Response™ protects against cyber-attacks that traditional security technologies can miss.

We detect, analyze, interpret, classify, isolate and report on suspicious and malicious activity on your endpoints and network.

Our high-touch, turn-key service is designed to ensure your organization assumes the minimal amount of risk possible.

We reduce the time to respond and recover so your organization can return to a known state of good without disruption to your business.
Thought Leadership Spotlight & App Partners

Lookout

Lookout is a cybersecurity company that predicts and stops mobile attacks before harm is done to an individual or an enterprise. Lookout’s cloud-based technology is fueled by a global network of more than 100 million sensors and tens of thousands of apps that are added daily. With this dataset of virtually all the mobile code in the world and the predictive machine intelligence to analyze and make sense of the data, Lookout can identify connections that would otherwise go unseen and stop cybercriminals from attacking mobile devices. The world’s leading mobile network operators, including AT&T, Deutsche Telekom, EE, KDDI, Orange, Sprint, T-Mobile and Telstra, have selected Lookout as its preferred mobile security solution. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com.

Trend Micro

Trend Micro, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. Trend Micro solutions provide layered content security for mobile devices, endpoints, gateways, servers and the cloud. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks. All solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™.
Panel Partner

Fugue

Fugue is a cloud infrastructure governance system for security, operations, and development teams seeking to deploy and operate cloud applications securely and efficiently while simplifying compliance. Fugue is about going fast, seeing everything, and getting enterprise cloud right, right from the start.

Fugue accelerates application delivery with policy-driven cloud infrastructure automation that continuously protects against policy violations and misconfiguration exposures. Your team can build on best practices and enterprise policies with policy-as-code validation and enforcement at every stage of the infrastructure lifecycle—including design, provisioning, and ongoing operations. Fugue mitigates the risk of data loss and downtime that can result from infrastructure misconfigurations, configuration drift, and human error.

Fugue can be used for new cloud infrastructure deployments or existing infrastructure that currently lacks sufficient compliance and security controls. Fugue works with today’s cloud workloads, toolchains, and workflows. Learn more at www.Fugue.co.

Session Introduction Partner

Ivanti

Ivanti is IT evolved. By integrating and automating critical IT tasks, Ivanti is modernizing IT and helping IT organizations successfully navigate digital workplace transformation. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

Breakout Session Partner

eSentire®

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $3 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.esentire.com and follow @eSentire.
Senior Supporter Partners

Lastline is revolutionizing the way companies improve network breach protection with technology that detects malware- and browser-based attacks and malicious network activity before suffering a costly data breach. And we enable you to do this with fewer resources and at lower cost than existing malware detection tools.

In 2011, Drs. Engin Kirda, Christopher Kruegel, and Giovanni Vigna, three of the world’s most influential academic researchers in cybersecurity, founded Lastline. The company’s vision is informed by the founders’ world-renowned research on malware analysis and evasion techniques, academically-rooted rigor, innovative approaches to network breach protection, and a passion to improve enterprise cybersecurity.

Lastline’s unmatched level of visibility, accuracy and effectiveness, and our focus on IT managers’ ever-increasing pressure to secure company networks and assets, has resulted in the company providing specific, actionable, context-rich threat intelligence and decreased data loss to many of the largest and most successful companies around the world.

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint’s open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint’s customers are among the world’s largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.

Sonatype

More than 10 million software developers rely on Sonatype to innovate faster while mitigating security risks inherent in open source. Sonatype’s Nexus platform combines in-depth component intelligence with real-time remediation guidance to automate and scale open source governance across every stage of the modern DevOps pipeline.
Senior Supporter Partners

Tufin

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,000 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries. Find out more at www.tufin.com.

AREA 1

Area 1 Security stops targeted phishing, the #1 cyber attack vector to organizations large and small. Area 1 Horizon™, the industry’s first and only preemptive cybersecurity solution, identifies and stops phishing attacks before they can cause damage. By focusing on the early stages of developing attacks, beyond the enterprise edge, Area 1 Horizon is able to preemptively intercept, disrupt, and disable attacks from 5 to 363 days before it is actually launched.
Identity is power.


With The Power of Identity.™

SailPoint’s open identity platform gives you the security and confidence you need.

SailPoint
sailpoint.com
3 in 10 organizations suspected or verified breaches stemming from vulnerabilities in open source components — a 55% increase since 2017*

We live in an application economy where innovation is king, speed is critical, and open source usage is massive and growing. While open source provides speed and efficiency – it also creates some risk as developers unknowingly use vulnerable components within their applications.

In a DevOps world, manual open source governance policies are guaranteed to fail. That is why more than 120,000 organizations have turned to Sonatype to shift security practices left and empower developers to innovate faster while mitigating security risks inherent in open source components. Sonatype’s Nexus platform combines in-depth component intelligence with real-time remediation guidance to automate and scale open source governance across every stage of the modern DevOps pipeline.

To learn more, call Matt Flechet at (312)543-1231 or visit sonatype.com/2018survey.

*2018 DevSecOps Community Survey
Area 1 Horizon is a cloud-based service that stops phishing attacks across all traffic vectors—email, web, or network.

PROACTIVE DISCOVERY

With globally distributed sensors, massive scale web-crawling, and comprehensive pre-attack analytics, Area 1 Horizon identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle.

DECISIVE ACTIONS

Using cloud-based email and web security platforms, automated infrastructure connectors, and comprehensive APIs, Area 1 Horizon takes preemptive action against phishing attacks across all traffic. These actions are transparent, flexible and can occur either at the customer’s network edge or in the cloud.

For the first time, organizations can get ahead of phishing attacks instead of dealing with the consequences of a breach after the fact.

Phishing is the most common cause of financial and data breaches today, and these attacks come from all directions—email, web, and network.

All it takes is one click, one message, or one network callback for a targeted attack to be successful. Existing solutions continue to miss these extremely low volume, socially engineered, and highly damaging phishing campaigns.
• Argyle is proud and protective of our high standards in ensuring the value of all content presented at our events.

• Strict guidelines are in place to ensure that all content presented is balanced and vendor neutral.

• All topics that are covered at our member events are thought leadership-focused and in line with the expectations of our members.

• Argyle seeks to prevent overt sales pitches or unbalanced vendor references.

• Argyle provides all speakers with content presentation guidelines at the behest of our executive membership.

We ask that all speakers, members and sponsors respect Argyle’s content neutrality guidelines. We thank you for your continued support for this policy as a way of protecting the high content standards and trust that Argyle has established with its members.

If you are interested in recommending a speaker for a future forum, please email:

speakers@argyleforum.com