2017 Chief Information Security Officer (CISO) Leadership Forum

TUESDAY, JUNE 20, 2017 | SAN FRANCISCO

argyle.
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.
WORKLOAD SECURITY & COMPLIANCE @ DEVOPS SPEED

- INTEGRATE WITH CHEF, PUPPET, JENKINS...
- DEPLOY ON AWS EC2, AZURE, OPENSTACK, ...
- FORTUNE 100 PROVEN
Varonis Protects the
World’s Most Sensitive Information
From the Inside Out

- Lockdown exposed sensitive data
- Restrict accounts with excess permissions
- Analyze accounts with suspicious activity
- Alert on privilege escalation
- Detect CryptoLocker and other malware
- Find unneeded accounts and groups

Protect  Sync  Search  Migrate
YOUR DATA

Varonis
1250 Broadway, 29th Floor, New York, NY, USA 10001
varonis.com  877 292 8767
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
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.
2017 Chief Information Security Officer (CISO) Leadership Forum (San Francisco)

TUESDAY, JUNE 20, 2017 | 8:15AM – 5:15PM

8:15am – 9:15am
Breakfast

9:15am – 9:20am
Argyle Executive Forum Opening Remarks

9:20am – 9:25am
SESSION INTRODUCTION FEATURING IVANTI

Darren Dorsey
Regional Sales Manager
Ivanti

9:25am – 10:00am
KEYNOTE PRESENTATION FEATURING KAISER PERMANENTE:
“Practical Transformation of the Modern Security Leader”

Michelle Nix
Vice President, Technology Risk and Compliance
Kaiser Permanente

A pragmatic approach to transformational, inspirational leadership is required to drive impact for your stakeholders while engaging your people. A balanced and transformative set of elements tied to people, process and technology will be required to succeed. This discussion will provide new approaches you can put to use every day as you pave the path for the strategic realization of a better tomorrow.

Are you ready to transform?
THOUGHT LEADERSHIP SPOTLIGHT FEATURING CLOUDPASSAGE:
“Dissecting the Security Impact of Agile I.T.”

Today’s enterprise business leaders demand speed and flexibility in technology delivery. Application development has been decentralized in most enterprises, now scattered across dozens or more independent technology teams. Adoption of cloud infrastructure, agile application development, containerization, devops, on-demand technology delivery, and other agility-oriented technologies enable this trend. While a plus for business units, security and compliance functions are often disrupted dramatically by never before seen levels of distribution, speed, and autonomy in application development and delivery. In this session, Carson Sweet (Founder & CTO of CloudPassage) will discuss trends, challenges, and strategic foundations for evolving security to harmonize with this now-unstoppable evolution in I.T. delivery.

Carson Sweet
Co-founder and Chief Technology Officer
CloudPassage

10:25am – 10:50am
Networking Break

10:50am – 10:55am
SESSION INTRODUCTION FEATURING LOOKOUT

Chris Tow
Enterprise Sales Engineer
Lookout
10:55am – 11:45am

PANEL DISCUSSION:
“Proactively Securing the Business Today for a Better Tomorrow”

Session topics include, but are not limited to:

- Engaging with the business to ensure that information security is effectively integrated
  - Achieving buy in
- Transformation of the CISO in relation to cyber threats and your business
  - Business wants to move so quickly and cyber threats are emerging at the same speed. How do you balance the two?
- Balancing demands of strategic planning and implementation of programs/projects to move the enterprise forward with day-to-day operational pressures
- Taking a top down and bottom up approach to information security
- Impacts of regulation/GDRP and how businesses think about information security
- New skill sets are necessary to ensure the security of your organization not only in 2017 but also in 2020
- Pinpointing top weaknesses that increase risk within organizations

Moderator:
Stephen Alford
Chief Technology Officer
Worldwide Environmental Products

Panelists:
Auston Davis
Chief Information Security Officer
Stanford Children’s Health

Jay Gonzales
Chief Information Security Officer
Samsung Semiconductors

Jim Graham
Manager of Engineering, West
Varonis

Steve Zalewski
Chief Security Architect
Levi Strauss & Company
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:45pm – 12:10pm</td>
<td>Networking Break</td>
</tr>
</tbody>
</table>
| 12:10pm – 12:45pm | **KEYNOTE PRESENTATION FEATURING JOHN MUIR HEALTH:**
|               | “A Risk-Based Approach to Information Security”                       |
|               | Join Tom in discussing ways to implement a risk-based approach to developing information security program roadmap. Topics include risk assessment, identification of risks, threats and threat actors, identification of potential initiatives, and ideas for developing budget & staffing models. |
|               | Thomas August                                                        |
|               | Chief Information Security Officer                                    |
|               | John Muir Health                                                     |
|               | *Please note: this session is off the record.*                       |
| 12:45pm – 1:45pm | Lunch                                                                |
1:45pm – 2:35pm

PANEL DISCUSSION:
“Securing and Closing the Gap on IT Talent”

Session topics include, but are not limited:

• Laying the groundwork for IT & HR to collaborate in your business
  • Best practices and lessons learned for establishing this collaborative relationship
  • Partnering with different functions outside of IT to develop the skills of existing teams
• Addressing training and development challenges for these new skills
• Creating organizational changes around employee engagement to create long-term development of talent and align business objectives
• Efforts impacting retention rate
• Hiring differently with regards to the millennial generation
  • Organizations adapting to better accommodate millennials in terms of the tools that they expect

Moderator:
Eric Svetcov
Chief Security Officer & Chief Privacy Officer
MedeAnalytics

Panelists:
Kwame Fields
Vice President, Information Security Risk Management
E*TRADE Financial Corporation

Jackson Muhirwe
Acting City Chief Information Security Officer
City & County of San Francisco

Keith Tresh
Commander
California Cyber Security Integration Center, California Governor’s Office of Emergency Services

*Please note: this session is off the record.

2:35pm – 2:55pm

Networking Break
2:55pm – 3:30pm

KEYNOTE PRESENTATION FEATURING CBS INTERACTIVE

Floyd Fernandes
Vice President & Chief Information Security Officer
CBS Interactive

*Please note: this session is off the record.

3:35pm – 4:10pm

KEYNOTE PRESENTATION FEATURING STANFORD UNIVERSITY:
“Cybersecurity: How Can We Win The War?”

We’re losing the cybersecurity battle, and the trajectory indicates increasing challenges ahead. Michael highlights the latest trends in information security, presents an unvarnished perspective on what’s working and what isn’t, and explains what needs to happen in order for us to win the war.

Michael Duff oversees the Stanford community’s efforts to protect its computing and information assets and to comply with pertinent laws, regulations and policies. He has a distinguished reputation for producing innovative solutions while balancing entrepreneurial spirit and evoking prudence for corporate risk management.

Michael Duff
Assistant Vice President and Chief Information Security Officer
Stanford University

4:10pm – 4:15pm

Argyle Executive Forum Closing Remarks
4:15pm – 5:15pm

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.
It’s When, Not If.

Compromised credentials? Systems hacked? Data breached? In today’s IT environment, it’s a question of when, not if. LogRhythm’s Security Intelligence Platform unifies SIEM, log management, file integrity monitoring, network forensics & host forensics to help you detect and respond to breaches and the most sophisticated cyber threats – faster and with greater accuracy than ever.

Call 1-866-384-0713 to learn more or schedule a demo. Or visit www.LogRhythm.com
Agari - stops targeted phishing attacks by identifying the **TRUE SENDER** of emails

Agari is trusted by leading Fortune 1000 companies to protect their organizations from advanced email phishing attacks.

Agari's proprietary analytics engine and email telemetry network provides unparalleled visibility into more than 10 billion email messages per day across 3 billion mailboxes.

Secure your email ecosystem with Agari - contact us to find out how:
info@agari.com • 650.627.7667
Axiad IDS Trusted Identity Solutions

HOLISTIC NO-SILO APPROACH ENABLES SECURE DIGITAL TRANSACTIONS THROUGHOUT THE ENTERPRISE.

- Validate the identity before issuing a credential through identity proofing and screening
- Securely manage the trusted credential over time: issue, store, revoke, update or suspend
- Enable the infrastructure to use the trusted credentials issued
- Leverage strong authentication to authenticate and make secure access decisions
The Global Storage Network

Plug in.

ClearSky delivers:

Economics and scalability of the cloud

+ Performance, reliability and security of on-prem storage

ClearSky

clearskydata.com/boston
Easy 2FA + Healthy Devices + Secure SSO =
Security They’ll Want to Use.

Secure your cloud & BYOD environment with best-in-class two-factor authentication, plus detailed access policies, a secure single sign-on experience, support for cloud and on premises applications, and phishing vulnerability assessments.

Europe, Middle East & Asia +44 8003 585 309
North America 866.760.4247
WE PROTECT YOU FROM THREATS THAT OTHER TECHNOLOGIES MISS

24x7 Human Monitoring, Hunting, Investigation and Remediation

End-to-end, Fully Managed Service

Embedded Incident Response
*Thought Leadership Spotlight Partner*

**CloudPassage**

CloudPassage® Halo® is the world’s leading agile security platform that provides instant visibility and continuous protection for servers in any combination of data centers, private clouds and public clouds. The Halo platform is delivered as a service, so it deploys in minutes and scales on-demand. Halo uses minimal system resources; so layered security can be deployed where it counts, right at every workload – servers, instances and containers. Leading enterprises like Citrix, Salesforce.com and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility. Headquartered in San Francisco, CA, CloudPassage is backed by Benchmark Capital, Lightspeed Venture Partners, Meritech Capital Partners, Tenaya Capital, Shasta Ventures, Musea Ventures and other leading investors.

*Panel Partner*

**Varonis**

Varonis is the foremost innovator and provider of access, governance, and retention solutions for human-generated data, the fastest-growing and most sensitive class of digital information. Based on patented technology and a highly accurate analytics engine, Varonis solutions give organizations total visibility and control over their data, ensuring that only the right users have access to the right data at all times from all devices, all use is monitored, and abuse is flagged. Varonis makes digital collaboration secure, effortless and efficient so that people can create and share content easily, and organizations can extract more value from their content while being confident that it is protected and managed efficiently. Voted one of the “Fast 50 Reader Favorites” on FastCompany.com, and winner of the SC Magazine Innovation, Product or Service of the Year, and Best Network Security Awards, Varonis has more than 2,000 customers worldwide and is headquartered in New York, with regional offices in Europe and Asia.

*Session Introduction Partners*

**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.
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.

LogRhythm, the leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company’s patented and award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.
Identify, Analyze and Prevent email threats from targeting your customers

Agari builds new, internet scale, data driven security solutions that eliminate email as a channel for cyberattacks and enable businesses and consumers to interact safely. The Agari cloud-based SaaS solution aggregates data from 2.5 billion mailboxes hosted by the email receivers including Gmail and Yahoo! to help global brands, including JPMorgan Chase, Facebook, Aetna, and UPS, eliminate email threats, protect customers and their personal data, and proactively guard brand reputation. Today, Agari analyzes over 7 billion messages per day, identifies over 2 million malicious URLs per month, and blocks over 200 million malicious emails per month.

Agari enables CISOs to protect consumer data and partner with CMOs to build a foundation of customer trust and loyalty to fuel digital transformation and revenue growth. Agari provides global brands with the experience, tools and analytics they need to eliminate email threats, protect customers and their private data, and pro-actively guard brand reputation.

Founded by the thought leaders behind Cisco’s IronPort solutions, Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is headquartered in Silicon Valley. Learn more at http://www.agari.com
Axiad IDS, recently named Top 25 Cybersecurity Provider 2017 by CIO Applications magazine, is a Trusted Identity solutions provider for enterprise, government and financial organizations. The dramatic increase in cybersecurity threats have made this clear: Organizations require strong identities they can trust to conduct business, while customers, employees, and citizens need a less frustrating method to authenticate their identity. Our mission is to help customers issue, manage, and use Trusted Identities for people, systems, and devices to prevent unauthorized access and IT breaches.

Core to Axiad IDS’ offering is the Axiad ID Cloud which allows organizations to quickly, easily and cost-effectively implement strong, high assurance MFA solutions — addressing potential breaches before they happen. Beyond designing, implementing and managing the solution, Axiad IDS also handles reporting necessary for an organization to show proof of compliance with security mandates and policies. By removing the complexity, Axiad ID Cloud enables organizations to conduct business without compromise through a future-proof secure solution.

The company’s approach starts with what customers need from a business and security perspective: Axiad IDS then builds solutions that address these needs. Customers get a single supplier providing a single solution without sacrificing security. We integrate advanced and non-intrusive technologies that simplify and ensure a better user experience. Axiad IDS’s portfolio of technology partners enables solutions from a rich product range.

Partners include:

- **Wallix**: Privileged Access Management solutions that monitor and control authenticated privileged users with a simple, elegant architecture that deploys easily and quickly across all sensitive devices and applications providing privileged access management to complement Axiad’s identity management.
- **Micro Focus**: A single framework for all your authentication needs allowing organizations to control authentication via easily configured policies in a single console, which is important when a user, or group of users, either change roles or exit the organization.

ClearSky Data’s global storage network simplifies the entire data lifecycle and delivers enterprise storage as a fully managed service. IT is now liberated from the treadmill of managing primary, backup and disaster recovery storage infrastructure, and empowered to access all data as if it were local, with on-demand scaling and agility. ClearSky delivers data where it’s needed, enterprise-ready and fully optimized to eliminate the cost and data center footprint of traditional storage solutions. Learn more at clearskydata.com.
Senior Supporter Partners

Duo Security is a cloud-based Trusted Access provider protecting thousands of the world’s largest and fastest-growing companies and organizations, including Dresser-Rand Group, Etsy, Facebook, K-Swiss, Paramount Pictures, Random House, SuddenLink, Toyota, Twitter, Yelp, Zillow and more. Duo’s innovative and easy-to-use technology can be quickly deployed to protect users, data and applications from breaches, credential theft and account takeover. The Ann Arbor, Michigan-based company also has offices in San Mateo, California; Austin, Texas and London. Duo is backed by Benchmark, Google Ventures, Radar Partners, Redpoint Ventures and True Ventures. Try it for free at https://duo.com.

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.

Morphick provides security Managed Detection and Response (MDR) services to organizations globally. Morphick’s proven approach combines attack detection, threat hunting, incident response, and tailored threat intelligence to deliver morphing defensive postures. The Morphick service provides multiple types of network security monitoring, full packet capture, and agentless endpoint threat-hunting capabilities. All events are aggregated on the Morphick Defense Platform and are monitored, validated, and remediated by US-based dedicated security analysts in the Morphick Threat Intelligence Center. Organizations can also leverage Morphick’s NSA CIRA-Accredited Incident Response services for breach response support. Morphick provides threat intelligence for deep intelligence gathering and analysis, and other incident response services such as malware reverse engineering and customer signature development.
Despite all efforts, it’s difficult to put security details into business context fast enough to determine what impact they have on business continuity, personal data, intellectual property, and reputational damage. Until now.

RSA delivers transformational business-driven security solutions helping over 30,000 customers comprehensively and rapidly link security incidents with business context to respond effectively and protect what matters most. With award-winning solutions for rapid detection and response, identity and access assurance, consumer fraud protection, and business risk management, RSA customers can thrive in an uncertain, high-risk world.

RSA solutions hold leadership positions in four Gartner Magic Quadrants and protect over 50 million identities and over a billion consumers worldwide. With over 700 dedicated security practitioners and a global ecosystem of over 400 partners, RSA delivers unified capabilities in the essential areas of an effective, business-driven security strategy.

RSA solution and benefits include:

- **RSA NetWitness Suite** triples the impact of security teams by providing essential visibility to detect advanced threats and deliver the right response in minutes not months.
- **RSA SecurID Suite** enables organizations of all sizes to ensure the right individuals have the right access, from anywhere on any device leveraging risk analytics and context-based awareness.
- **RSA Archer Suite** is the industry’s leading business risk management suite, proven to help customers confidently advance their command of risk and understand what risks are worth taking.
- **RSA Fraud & Risk Intelligence Suite** gives organizations transforming their digital, multi-channel strategy, the ability to both protect consumers against fraud and improve the user experience by reducing transaction friction.
- **RSA Risk & Cyber Security Practice** provides essential consulting, support and incident response expertise so that you can take command of your evolving security posture.

It’s time to thrive in an uncertain, high-risk world. It’s time for Business-Driven Security.

TITUS solutions enable organizations to discover, classify, protect and confidently share information, and meet regulatory compliance requirements by identifying and securing unstructured data. TITUS products enhance data loss prevention by classifying and protecting sensitive information in emails, documents and other file types – on the desktop, on mobile devices, and in the Cloud.
Verisign, a global leader in domain names and internet security, enables internet navigation for many of the world’s most recognized domain names and provides protection for websites and enterprises around the world. Verisign Security Services (VSS) include Distributed Denial of Service (DDoS) Protection and Managed DNS services.

ZixCorp is a leader in email data protection. Trusted by the nation’s most influential institutions in healthcare, finance and government, ZixCorp offers innovative email BYOD security, industry-leading email encryption and a unique email DLP solution. Zix Email Encryption provides easy-to-use secure email to anyone, anywhere. ZixCorp provides the only transparent email encryption for both senders and recipients – enabling the exchange of encrypted email without any extra steps, passwords or additional set-up. Leveraging our leadership and expertise in email encryption, ZixDLP combines our proven policy and content scanning capabilities with an intuitive quarantine interface. By focusing on email, ZixDLP addresses business’s greatest data risk while decreasing cost, reducing the deployment timeline from months to hours and minimizing the impact on your team. Our BYOD security solution ZixOne offers a new and different approach that never allows corporate email to reside on the device. With ZixOne, organizations control access to corporate email without jeopardizing data protection or productivity. If a mobile device is lost or stolen, access is simply disabled. Employees maintain control of their devices and their privacy, and employer liability risks are eliminated. For more information, visit zixcorp.com.
PROVEN APPROACH TO CYBER SECURITY.

MANAGED DETECTION & RESPONSE SERVICES

PROACTIVE THREAT HUNTING SERVICES

NSA CIRA ACCREDITED INCIDENT RESPONSE

LEARN MORE AT MORPHICK.COM
GIVE CYBER THREATS A 1-2-3 PUNCH WITH RSA NETWITNESS® SUITE

3X MORE VISIBILITY WITH LOGS, PACKETS AND ENDPOINT*

3X FASTER INCIDENT RESPONSE TIME

3X THE IMPACT WITH YOUR EXISTING SECURITY TEAM

RSA NetWitness Suite: the heavyweight champion for threat detection and response.

*Based on data vs. comparable products
It’s Time to Transform Your Security Culture

Traditional Business Boundaries Are Gone
The growth and success of your organization necessitate embracing the intensification of data sharing.

Despite Security Technology, Human Error Still Reigns
Despite heavy investments into data security systems, human error still puts your valuable data at risk.

Users Need a New Attitude Toward Information Protection
Promote a culture of security by prompting users to stop, think, and consider the business value of the information they are creating and handling.

Transform Your Security Culture with TITUS
With over a decade of experience helping organizations transform their security culture and protect their data, TITUS understands the critical success factors of navigating the current digital business transformation. Data classification empowers both people and security technology to make better information governance and sharing decisions.
OUR EXPERTISE.
YOUR PROTECTION.

VERISIGN
Security Services

DDoS Protection
DNS Firewall
Managed DNS
Recursive DNS

Verisign.com/SecurityServices
ZixCorp offers the industry's only fully transparent delivery of encrypted email. With transparent email encryption, users send and receive secure email as they would conventional email. No extra steps are required, and workflow is not interrupted.

To learn more visit www.zixcorp.com, or contact us at 866-257-4949.
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.