Trellix Xpand

Living Security Now

ARIA Resort & Casino | Las Vegas
September 27-29, 2022

Breakout Sessions

28-29 September, 2022

Trellix Xpand

Discovery themes

This year's discovery themes are arranged across five key areas of modern security.

All keynotes and breakout sessions of Xpand LIVE will dig deep, both strategically, and technically into these categories.

Earn (ISC)[2] Continuing Professional Education (CPE) credits for each hour spent in training or breakouts at Xpand Live.

SecOps Revolution

Threats have evolved, but security hasn't - until now. Learn how XDR will be a key driver for the Security Operations Center (SOC) of the future.

Key use cases, practical guidance, what to expect from XDR – and how it makes your SOC more efficient, empowers your security practitioners and analysts, and automates and drives your end-to-end detection and response workflows.

Unifying Endpoint

Future-proof your defenses and build resilience with unified endpoint protection.

Accelerate detection and response with the context, visibility, and capabilities to uncover, investigate, and act on threats with increased speed and accuracy. Proactively protect every endpoint, prevent ransomware and other advanced threats, and find how to easily scale and manage all your endpoints.

Securing the Ecosystem

Get an in-depth look at the most comprehensive set of security controls and control points in the industry – all designed to provide you with earlier, better protection across all phases of the attack chain.

Network, Email, Data and Cloud Security – learn deployment and operational best practices and use-cases.

Activating Intelligence

Learn the depth and breadth of our visibility, research, and thought leadership in the threat intelligence space.

Whether it's the bad actors we track, specific takedowns of cyber criminals, discovered vulnerabilities – we will share how research and innovations make it from the lab and into our products.

#SoulfulWork

The cybersecurity industry is seeking 2.72 million professionals, and that number is only continuing to grow. For decades, we have relied on the same tactics to close the talent gap.

We need to rethink who we view as talent and work together as an industry to solve this talent shortage. Collectively, we can make a difference. Hear from customers on their challenges and successes in the human element of cybersecurity.

REGISTER NOW

Trellix Xpand

SecOps Revolution

Best practices of today's SOC

Riana Smallberger, Director, Advanced Cyber Threats, Trellix

Mark Boltz-Robinson, Manager, Advanced Cyber Threats, Trellix

Why is a Cyber Security Operation Center so important?

A SOC exists with the core mission to monitor a wide range of possible threats against an organization. During this session we will discuss some of the best practices, procedures, and processes to modernize a SOC. We will also cover the importance of incorporating Threat Intelligence as a requirement to be successful.

Making Security Staff Effective in the Cloud with XDR

Martin Holste, Chief Technology Officer, Cloud, Trellix

What information do security staff have to do their job? When they get an alert, do they understand what is affected, who is involved, a timeline of what happened, and what normal behavior looks like? It's hard enough for SOC operators to get quality alerts, it's even harder for them to know what to do with them, and impossible to make thousands of good decisions every day without being armed with the insights they need.

Learn how Trellix Helix is the truly open managed XDR platform that incorporates over a hundred vital integrations to collect raw event telemetry from things like cloud infrastructure, directories, security products, and source code repositories and forges it into meaningful models and timelines. This session will detail how Helix Cloud Connect makes integrating data sources quick and easy, and shows the power of what can be done when defenders are armed with answers. It will dive into the different types of data Helix can collect, how they are used in detection and response, and advanced hunting use cases.

Enterprise ePO, DXL and TIE infrastructure designs

Steen Pedersen, Principal Architect, CISSP, Trellix

This session will take a look at enterprise designs for ePO infrastructures with Data Exchange Layer (DXL) and Threat Intelligence Exchange (TIE).

Several real-world examples of infrastructure architectures will be showcased, as will how a current ePO, DXL and TIE infrastructure can transform to include cloud servers located in AWS, AZURE and more, to create a hybrid ePO architecture.

REGISTER NOW

SecOps Revolution

Invasion of the Information Stealers

Taylor Mullins, Sales Engineer, Trellix

Information stealers have become one of the most utilized, damaging, and simplest to acquire variants of malware observed today. The effects of a successful information stealer attack can lead to access of company accounts, deployment of ransomware, and widespread data exfiltration.

In this presentation, we will unveil how threat intelligence and utilizing an open XDR framework can help a security team proactively apply countermeasures to prevent, detect an ongoing activity, and monitor the aftermath of a successful attack across their security solutions.

How XDR is a game changer for SecOps

Deepak Seth, Director, XDR Platform Services, Trellix

In the current threat environment, SOC teams continuously face the pressure of detecting an intrusion as quickly as possible before it becomes a major security incident. With so many point products in use in a typical organization, it is often very time consuming and challenging for the SOC team to search through the noise to find important alerts that may indicate the presence of a threat in the environment.

XDR can enable a SOC team to detect, respond to and remediate threats across all attack channels. These include Email, Endpoint, Network and Cloud - without the inefficiencies of switching between multiple point solutions, and with the ability to work with relevant data that's actionable.

We want to help the SecOps team ultimately achieve a stress-free life. This session will highlight different phases of a malware attack, the challenges SecOps face in these phases and how Trellix XDR can help in each of these phases.

Automated responses - out of the box!

Simon Tiku, Snr Director, Engineering, Trellix

We want to make life simpler for security analysts. This session will share templated security playbooks, task flows and scripts that can be easily tailored to your organization's needs.

Built by Trellix security experts, this template library takes the work out of developing things from scratch for common use cases. For example, a task flow that covers common functionality and processing related to specific plugins, which can then be inserted into a multi plugin playbook.

REGISTER NOW

Unifying Endpoint

Advanced Forensics

Ryan Fisher, Senior Engineer, Trellix
Fred House, Director, Engineering, Trellix

The Endpoint Security Research and Custom Engineering (RACE) team has been operating since 2015 with the mission of building rapid-response endpoint capabilities in support of Mandiant Incident Response engagements. The team has built over 50 forensic capabilities that enable advanced endpoint forensic investigations at scale. These forensic capabilities have been used on thousands of IR engagements, including some of the most high profile breaches around the world.

The RACE team's recently released Extended Forensics module, gives customers, partners, and other IR firms access to this advanced forensic tool set.

In this session, the RACE team will dive into the advanced forensics capabilities, describing why they are relevant to forensics, how to run them, and how to analyze the results. We will cover common investigative workflows such as frequency analysis (stacking), indicator searching (sweeping), YARA hunting, live response, and timelining across the enterprise.

Endpoint Efficacy and Coverage Reporting

Chris Ubando, Senior Principal Architect, Trellix
Charles Wiggins, Principal Architect

How do we prove to the business the value of any cyber security investment?

Attend this session and learn ways to build reporting within ePO that can be used to present to the business to the value the Trellix solutions are providing across the environment.

We will show how to report on the coverage of protection features that help protect against common malware attacks like Ransomware. We will also discuss how to use ePO with Active Directory and SCCM to provide clear reporting on the coverage of the Trellix solutions on systems within the environment - and highlight systems that are potentially at risk of being targeted by malware that are unprotected.

Leveraging EDR Integrations into SOC Processes to Build a Better Defense

Matt Smith, Snr Manager, Professional Services, Trellix

Adding another SecOps tool into the day-to-day mix of tools and techniques used during investigation and triaging threats creates a common concern for the SOC. How can that tool be incorporated into existing processes so that it does not duplicate functions provided by an assortment of free and commercial tools? Is the full value of the new data collected used to pre-emptively block attacks before they need to be triaged?

Trellix EDR offers several features natively - and externally through via API integration - which can provide the SOC the ability to consolidate their tools and techniques used during investigation and triage. It also enables direct integration with the defense layer to save the business both on time and costs when tackling threats.

Learn how Trellix EDR is being used by Trellix Professional Services consultants to enable SOCs to collect information needed during DFIR processes, as well as provide the ability to react to threat activity using a combination of Trellix EDR, DXL, ePO and other tools found in many SOC toolkits.

REGISTER NOW

Trellix Xpand

Unifying Endpoint

Trellix Endpoint Security for Breach Investigations

Vinoo Thomas, Principal Product Manager, Trellix

Learn how Trellix Endpoint Security can handle investigating 1000's of endpoints in a security breach. Get an inside look into how breaches are discovered and how one compromised endpoint can turn a company upside down.

We will demonstrate how Endpoint Security unleashes world class forensics - from detection to containment. From detecting data theft, credential harvesting, compromised assets, actioning alerts, new features and much, much more!

Trellix Unified Endpoint: An Architectural Overview

John Teddy, Engineering, Trellix

This session will preview the architecture of the upcoming Trellix Unified Endpoint – bringing together the best capabilities of FireEye and McAfee technologies into an endpoint framework with a common agent serving protection, detection, and forensics.

We will cover the design goals, the elements that comprise the platform, the phases of implementation, with some minor deep dives into event handling, orchestration, and reputations.

REGISTER NOW

Securing the Ecosystem

Accelerating transformation with Detection-as-a-Service

Arthur Cesar Oreana, Account Manager, Trellix

In a Digital Transformation journey, meeting the demands of business areas quickly is essential for survival in a competitive and connected world. With businesses needing to launch products quickly - security cannot be an impediment. Security can be a facilitator and a great ally to business agility.

Attend this session to learn how one of the largest Brazilian digital banks managed to address the risks of analyzing all files received from external sources, quickly and easily, positively impacting the customer experience.

Data Security : The Trellix Roadmap

Product Management, Trellix

Data Protection is a top priority for today's organizations. In addition to adhering to constantly changing regulatory requirements, there are continuous concerns over external and internal threats. Any breach can have an impact beyond just the cost of clean-up. Fines can add up, and the loss of trust can take a very long time to overcome.

In this session, we will discuss the Trellix Data Security portfolio. We will show the challenges faced by administrators today and illustrate how Trellix Data Protection products help customers classify, monitor, and protect their most sensitive data. We will also highlight recent features that have been added to the products and give a forward-looking view of plans that are in progress for this suite of products.

Email Security: The Trellix Roadmap

Product Management, Trellix

Email continues to be the top attack vector. It is imperative that customers continue to evaluate their Email security solutions to ensure that they are capable of detecting the latest threats. Many customers must also protect a wide range of Email systems including on-premise and Cloud deployments.

In this session we will discuss the Trellix Email Security portfolio of products that provide protection to on-premise and cloud based deployments. We will discuss the deployment challenges customers face today and highlight how Trellix provides the industry's most comprehensive set of detection engines to keep users safe.

REGISTER NOW

Trellix Xpand

Securing the Ecosystem

Network Security: The Trellix Roadmap

Product Management, Trellix

With network infrastructure now located on-premise, as well as in private, hybrid and multi-cloud environments - managing and securing them has become increasingly complex.

In this session, we'll discuss the opportunities and challenges our customers face across a growing variety of use cases, how customers can integrate Trellix detection directly into their custom application, and how they can leverage the Trellix Network Security portfolio to address infrastructure security wherever they need it.

Achieve a True Zero Trust Architecture with Trellix and Okta

Martin Holste, Chief Technology Officer, Cloud, Trellix

Trellix and Okta have a strong partnership, demonstrated by the popular Helix XDR integration - and advanced anomaly detection for Okta.

Learn how organizations are taking advantage of the ability to analyze identity audit events to find anomalies and correlate those anomalies with a wide range of information, such as application behavior and user roles. This allows the matching of suspicious logins with post-login actions in the context of the person's role. Response actions can then be taken to limit any potential damage from a compromised identity. This extended detection and response (XDR) forms the basis for a Zero Trust Architecture (ZTA).

But what about ZTA for on-prem? Businesses are operating hybrid environments and manage many endpoints in addition to SaaS and cloud infrastructure. Preview a universal Trellix ePO connector for Helix XDR that will ensure that on-prem solutions are fully cloud-aware. This link between Trellix ePO on-prem and Helix XDR in the cloud lets defenders unlock complete Zero Trust.

The Cyber EO 14028's Effect on Software Development

Kent Landfield, Chief Standards and Technology Policy Strategist, Trellix

The US 2021 Executive Order 14028 is changing the way the U.S. Federal government is viewing the software it purchases and deploys. The EO will alter the way the software industry creates and delivers software and services.

From the definition of critical software, to requiring software bill of materials (SBOMs), to documenting secure software development lifecycle practices, and more, the Cyber EO is impacting the way software producers view the way they do business.

This lively panel includes those involved in delivering on the requirements of 14028, from NIST and CISA, and a former Federal CISO who will discuss the EO's intended impacts and the effect it is having both in and out of government.

REGISTER NOW

Trellix Xpand

Activating Intelligence

PhishVision : Caught On Camera

Manoj Ramasamy, Research Scientist, Trellix

URL Phishing is one of the most well-known threats in the wild where attackers try to deceive the users by fake websites of various brands.

Learn how a new state-of-the-art machine learning model is used to interpret and understand URL screenshots - to predict if a brand is being spoofed. PhishVision uses deep learning techniques, including the implementation of a deep convolutional neural network, to determine whether a webpage screenshot associated with a URL is part of a phishing attack.

Discover how PhishVision learns and adapts through the retraining of its convolutional neural network at periodic time intervals, with new datasets retrieved by an automated dataset collector – improving the detection of zero-days cyber-attacks.

Catch Me If You Can: Living Off the Land Binaries, and The Adversaries Who Abuse Them

Tim Hux, Security Researcher, Trellix
Alfred Alvarado, Security Researcher, Trellix

The Trellix Threat Intelligence Group collects, correlates, and analyzes attack techniques deployed by threat actors, and their use of malicious and non-malicious tools.

This presentation will detail the most common tools used by threat actors, their associated MITRE techniques, and the countermeasures which can be used to assist organizations defend their network.

Living off the Land (LotL) attacks are increasing, and often going unnoticed during the initial infection phase, due to the method's use of common non-malicious tools and Windows binaries. You will learn how threat actors may gain initial access via spear-phishing, access brokers or unpatched vulnerabilities, and then use common tools and Windows binaries to allow reconnaissance and persistence phases to remain undetected while additional payloads are retrieved, exfiltration is automated, and the final payload is prepared.

US Government Cyber Security and Privacy Policies: What to expect in 2023

Panel hosted by Kent Landfield, Director, Trellix Public Policy

This panel session will provide a perspective on what public policies to expect from both the White House and Congress in 2023.

Government policies define the contours of the cyber security market. New legislative initiatives will focus on protecting critical infrastructures and government agencies, with a focus on EDR, XDR and Zero Trust solutions. Congress will once again take up national, privacy legislation. These initiatives impact both government and private sector users of cyber security solutions.

Panelists will include former, senior US government officials, a former White House official and federal Chief Information Security Officer, a representative of the Center for Strategic and International Studies, and Tom Gann, Chief Public Policy Officer of Trellix.

REGISTER NOW

Trellix Xpand

Activating Intelligence

Cyber Tools Shaping Foreign Policy? A False Chinese APT Responds to Nancy Pelosi's Visit to Taiwan

Ann An, Security Researcher, Trellix

Trellix endpoint detections reveal cybersecurity and geopolitical activities well before the media begins reporting them.

On July 29, 2022, Trellix telemetry data showed a spike in detections in Taiwan, with over 32,000 detections hitting the self-governed island in one day - well over a typical day range of 9,000 to 17,000 detections. This spike occurred five days before Nancy Pelosi's visit to Taiwan on August 3, 2022. Telemetry data also showed that a significant portion of detections were directed at Taiwan's government entities between July 29 and August 6, 2022.

On August 3, 2022, the day after Pelosi' visit, one Chinese hacker collective that calls themselves "APT27" announced a special cyber operation against Taiwan's government services, infrastructure, and commercial organizations.

Trellix analysts will explain these DDoS operations and scrutinize the true identify of APT27 and subsequent activities throughout this Xpand session.

The Minority Threat Landscape Report

Christiaan Beek, Snr Principal Engineer, Trellix

In this session we will take you on a trip through parts of the current threat landscape and our predictions for its future. Our research will highlight where we know adversaries are operating now – and our informed position on where they will go next.

We will unveil how Trellix analyzes threats and anticipates them. Learn how we innovate, and adapt, to counter unexpected threats.

Using Critical Threat Intelligence Strategically

Panel hosted by Patrick Flynn, Head of Advanced Programs Group, Trellix

The overarching threat facing cyber organizations today is a highly skilled asymmetric enemy, well-funded and resolute in their task and purpose. While you never know exactly how they will come at you, come they will. It's no different than fighting a kinetic foe in that, before you fight, you must choose your ground and study your enemy's tendencies.

Much focus has been placed on tools and updating technology, but often we are pushed back on our heels and in a defensive posture.

This panel features senior US government representatives debating that while technology strategy is important, we must embrace and create a thorough Cyber Threat Intelligence (CTI) doctrine which must take many forms.

REGISTER NOW

#SoulfulWork

From Books to Beating Bad Guys

Mike Kizerian, Principal Technical Instructor, Trellix

We have long lamented the growing need for soulful cyber security roles to be filled as we struggle to find the experienced hires to fill them.

Ten years ago, Mike was a Team Lead in Kuwait as a contractor for the Army. Although asked for his open requisitions to be filled with candidates that were experienced cyber security professionals, he was constantly given candidates with no security background. But, it did not deter him. Through a careful program of on-the-job training, each of the hires easily filled their cyber security roles. They have gone on to have extremely successful cyber security careers.

Come and learn how the desktop support tech, the developer, the server admin, and anyone with a desire to learn can find rewarding, #soulfulwork in cybersecurity.

Panel Session : Cyber Security – the soulful profession

Hosted by Michael Alicea, Chief Human Resources Officer, Trellix

There's a place for people who want to protect others. Who want to contribute to the greater good of society. Who want to keep businesses, essential infrastructure, and vital information safe. That place? Cybersecurity.

If you're looking for a career that provides you with the opportunity to do meaningful, soulful work that enriches people's lives—you've found it. Michael Alicea will host a thought provoking panel designed to inspire us to help others blaze their own trail in cybersecurity.

REGISTER NOW

Trellix Xpand