If you were under cyber attack would you ever know?

EY and Los Alamos National Laboratory introduce a shift in cybersecurity strategy and bring behavioral analytics inside the network

The better the question. The better the answer. The better the world works.

EY

Building a better working world

Asking behavioral questions inside the network

Constantly under cyber attack

In today's cyber threat environment, attackers' approaches to targeting victims have significantly matured. Breaches are inevitable where threat actors are highly sophisticated, strategic and agile, and when their targets are growing in complexity and size. Traditional defense mechanisms — perimeter controls and end-point antivirus protection — cannot keep pace with these increasingly innovative and sophisticated adversaries.

Because it is no longer a matter of "if" but a question of "when," an intelligent, complementary approach is necessary to quickly identify intruders and contain their impact.
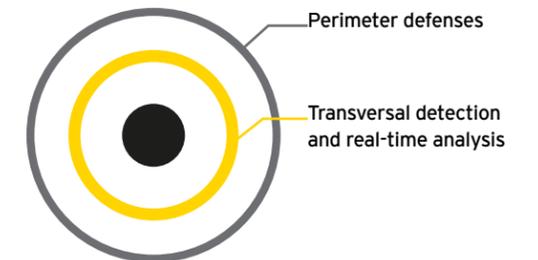
Los Alamos National Laboratory and EY — bringing innovative approaches to cybersecurity

The collection and storage of digital information have empowered businesses to create new markets and deliver services more effectively to their customers. As data volume and sources continue to grow, threat actors are increasing their activities, and defense efforts have become largely ineffective in keeping pace. Organizations now have greater areas of exposure and increased vulnerability due to mobile technology, third-party risk and malicious insiders.

The US Government, however, has long confronted this issue. Having been under attack for decades, by many of the same criminal organizations and nation-state actors that are now attacking industry with such zeal, Government security researchers have developed innovative approaches to protecting networks and the national security data that they contain. Industry is now seeing transition efforts on the part of the Government to bring that experience and technology to bear in the protection of private sector data.

After a competitive selection process, EY is proud to announce that we have been chosen by Los Alamos National Laboratory to bring to market the technologies developed by it to protect its most sensitive US networks. This relationship will leverage the power of that prestigious research institution and EY's deep business knowledge and security experience to bring these innovative services to clients.

A shift in strategy — behavioral analytics inside the network

Recent breaches and elevated concerns over insider threats have demonstrated that perimeter security is not a complete solution to today's cyber threats. Continuously monitoring all assets within the firewall is necessary for situational awareness and rapid response to active attacks. However, because hackers continue to innovate and insiders already have access, signature-based methods that recognize patterns already seen are insufficient. Zero-day behavioral analytics promise to change the game in network security by asking, "Is this activity expected, or is it deviating significantly?" Statistical models have proven to be effective at quantifying the significance of deviations from modeled behavior.

In an organization made up of complex, changing relationships and dependencies, identifying this irregular activity can feel like looking for the proverbial needle in a haystack. It requires the following:

- Advanced tools that can sift through unprecedented amounts of data
- Continuous, automated learning of dynamic network patterns
- Statistical models that capture relevant behavioral attributes
- Extracting actionable intelligence to threats
- Minimizing false positives when billions of events are observed

About EY

As one of the largest professional services organizations in the world, EY firms have implemented enterprise-wide technology, strategy and design programs for some of the most complex IT infrastructures in the world, including those of Fortune 100® companies.

Our knowledge of clients' businesses and industries has enabled us to help companies better understand their day-to-day transactions and behaviors, and identify the true risk that cyber-related events pose to their organization. Additionally, EY brings extensive experience in cyberforensics and cyberincident response. This means that the cybersecurity strategies we develop are aligned to the specific business needs and threats our clients face.

In a survey of information consulting firms and services, Forrester ranked EY as the leader in cybersecurity strategy, which includes new service offerings, future directions, R&D investment and information security business value.

About Los Alamos National Laboratory

Los Alamos scientists have extraordinary access to the most advanced technology and they consider the hardest security problems. Applied mathematics, machine-learning experts, and statisticians collaborate with front line security operations personnel to provide relevant, cutting-edge solutions.

Los Alamos is focused on national security threats to the nation's cyber infrastructure. They develop innovative technologies for detection, response, and predictive vulnerability analysis.

As a capability leader in information security and networking science, Los Alamos is dedicated to predicting and solving critical problems in the cyber domain using novel yet practical solutions. Information security and networking science is a growth area of the Laboratory, and diverse customers are leveraging excellence via the Laboratory's cybersecurity capabilities.

Collaboration with the Los Alamos National Laboratory

Today, Los Alamos National Laboratory continues to focus its resources on making significant achievements in national security issues such as cybersecurity. It is now beginning to share the technologies that have been designed and used to protect some of the most sensitive national security information with the broader private sector. Included among these is a behavioral analysis tool to find threat actors – PathScan®.

EY's collaboration with Los Alamos allows for this tool to be used by organizations in the private sector. EY's knowledge of its clients' IT environments and market forces has honed Pathscan® for private sector and industry-specific needs.

EY and Los Alamos have worked together to test this tool in "live fire" environments to make it applicable to a business's priorities and risk appetite. EY and Los Alamos, through a collaborative research and development agreement, will continue to innovate for the nation's most demanding security needs.
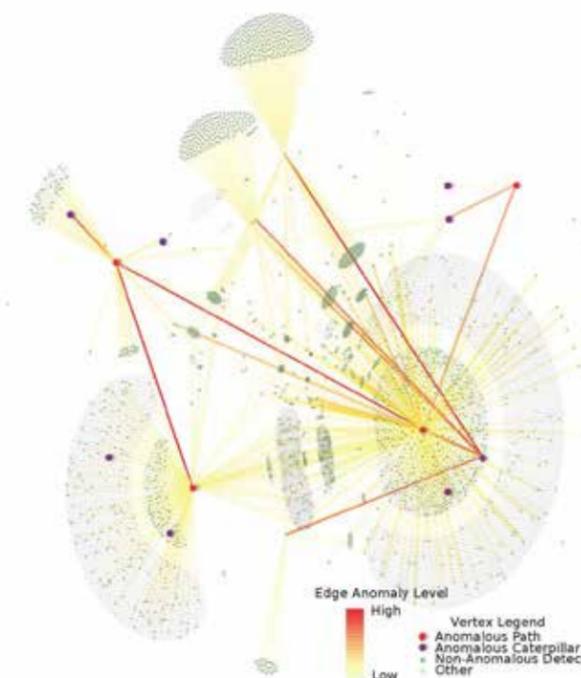
PathScan®

PathScan is a network anomaly detection tool that seeks to identify traversal through the network by an adversary. Unlike traditional security tools that look for malware or network signatures, PathScan searches for deviations from normal patterns of communication that are indicative of an intruder's presence. By creating a deep behavioral model of your network, it can expose intruders and insiders causing local anomalies during their activity. PathScan's three-step approach:

1. Builds statistical models to characterize the normal flows of traffic between each pair of communicating computers

2. Actively enumerates multi-hop paths of communication

3. Passively monitors each path and tests whether the flows observed are expected in the context of the statistical models or whether they are unlikely and, therefore, indicators of a possible adversary moving through the network

The tool's modeling capabilities are as dynamic as your network, continuously updating parameters in step with the non-stationary use of the network, thus reducing alerts due to unusual but non-threatening behavior. PathScan can work with an organization's legacy information security framework and does not require significant infrastructure development or vast stores of data to operate. Its network collection is passive, limiting impact to operations.

Source: Call for Commercialization and/or CRADA Partners for PathScan, Los Alamos National Laboratory (LANL), http://www.lanl.gov/

Mitigating cybersecurity threats is no longer about deterring and detecting something that "looks" like a threat. It is now about being able to identify and anticipate something that "acts" like a threat.

PathScan received support from the Transition to Practice program, an initiative of the Department of Homeland Security Science and Technology Directorate that helps to advance and raise the visibility of promising technologies that are developed in the national laboratories and deemed ready for transition to the commercial marketplace.
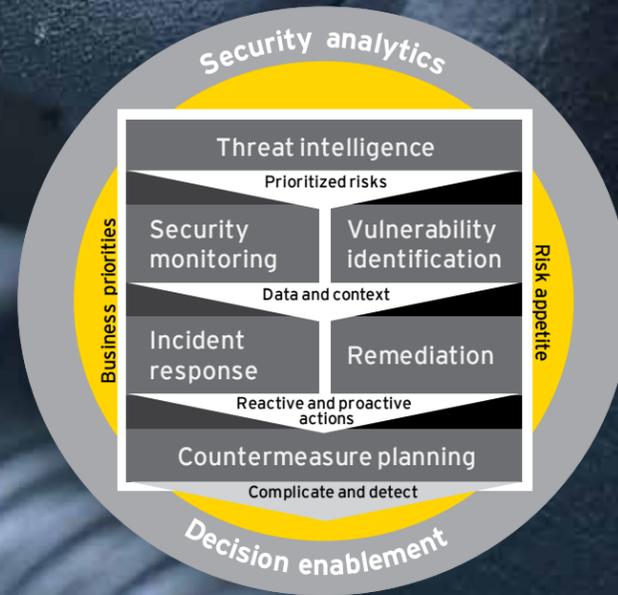
Securing your organization

Through the practical business application of PathScan, EY can help deliver robust:

▸ **Assessments** – point-in-time perspectives of an organization's cybersecurity environment and topography

▸ **Transformations** – cybersecurity program improvements through integration with your legacy security tools

▸ **Managed services and subscription services** – a full suite of services to help clients establish and manage an effective security operations center

This tool can also enhance the following programs:

▸ **Threat intelligence** – manageable action plans to anticipate threats and create actionable intelligence to rapidly detect and respond to incidents and remediate areas of exposure

▸ **Security monitoring** – monitoring threat indicators and detecting attacks before critical services are disrupted or high-value sensitive assets are compromised

▸ **Incident response** – investigations to determine cause and scope of security incidents, coordinate containment and recovery and support forensic analysis

▸ **Countermeasure planning** – methodologies to mitigate identified risks, inclusive of threat intelligence, business priorities and risk tolerance

The EY cyber threat management framework

Security analytics

Threat intelligence

Prioritized risks

Business priorities

Security monitoring

Vulnerability identification

Risk appetite

Data and context

Incident response

Remediation

Reactive and proactive actions

Countermeasure planning

Complicate and detect

Decision enablement

Through collaboration with Los Alamos National Laboratory, EY is committed to making your organization more secure and building a better working world.

Contacts

Stan Brown
Ernst & Young LLP
+1 513 612 1836
stan.brown@ey.com

Chip Tsantes
Ernst & Young LLP
+1 703 618 6816
chip.tsantes@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace
Nearly 43,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,900 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

About Los Alamos National Laboratory (www.lanl.gov)

Los Alamos National Laboratory, a multidisciplinary research institution engaged in strategic science on behalf of national security, is operated by Los Alamos National Security, LLC, a team composed of Bechtel National, the University of California, BWX Technologies, Inc., and URS for the Department of Energy's National Nuclear Security Administration.

Los Alamos enhances national security by ensuring the safety and reliability of the U.S. nuclear stockpile, developing technologies to reduce threats from weapons of mass destruction and solving problems related to energy, environment, infrastructure, health and global security concerns.

ey.com