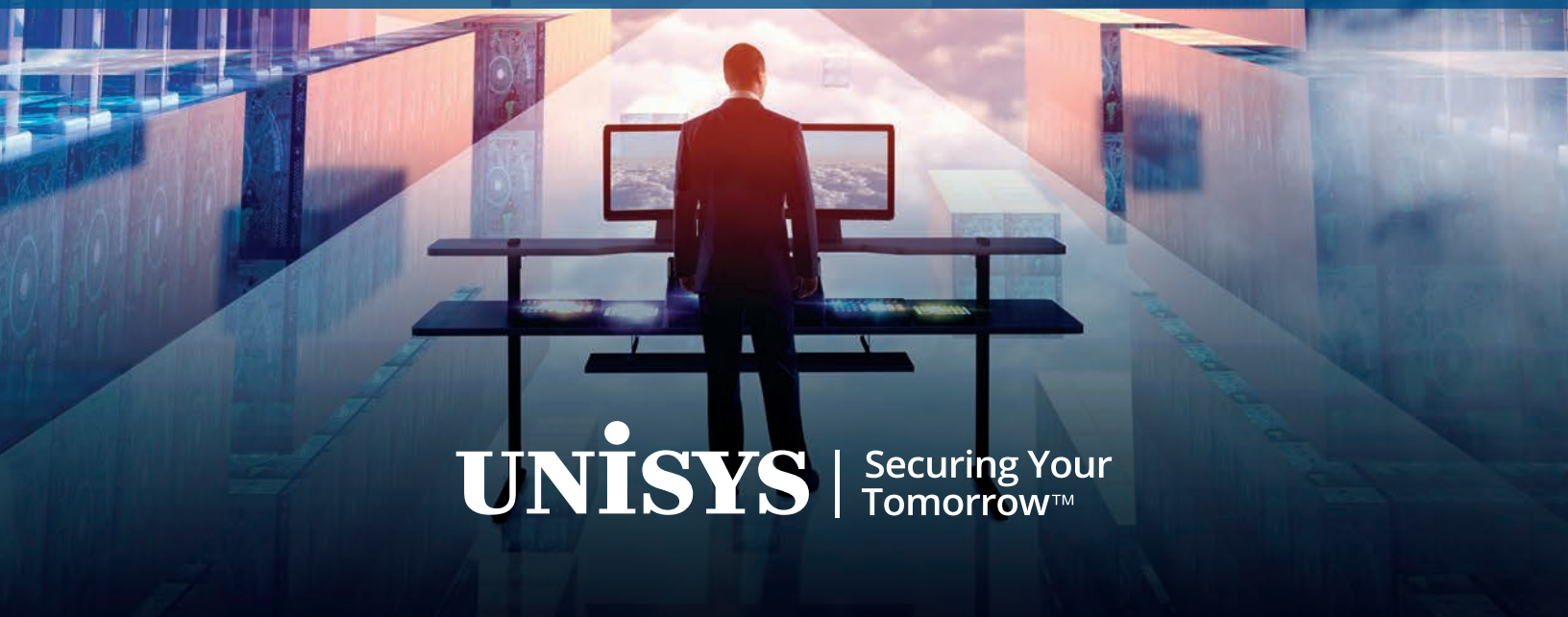
SECURING THE ENTERPRISE

A WHITE PAPER BY UNISYS



UNISYS | Securing Your Tomorrow™

TOO MUCH DATA, TOO LITTLE TIME, TOO FEW RESOURCES

The Enterprise Under Attack

Today's enterprise security landscape is overwhelming. The number of attacks, sophisticated methods, growing community of actors, and open market for malicious code are daunting. The attacks are global and systematic; they infiltrate systems and erode profits. The number of connected devices from Industrial Control Systems (ICS), the Internet of Things (IoT), and Operational Technology (OT) all contribute to expanding enterprise vulnerabilities.

Many companies struggle to identify, vet, and transform reactive information into proactive intelligence in time to meet their specific security needs and secure their critical corporate assets. Because the amount of information is immense and internal resources are always too few, enterprises tend to look back at malicious events that may have taken place days or even weeks previously. Predicting and preventing attacks is an unrealized dream, often because companies:

- Lack understanding of the rapidly-changing network of bad actors across the security landscape
- Feel overwhelmed by the volume of options and the often confusing solutions available in the market
- Are unable to transition from a reactive information-driven model to a proactive actionable-intelligence model
- Don't understand the actual business risk and costs associated with protection
- Lack qualified staff to adequately transform information into intelligence to secure the enterprise
- Have a false sense of security with their current state

The cybersecurity workforce shortage is estimated to hit 1.8 million by 2022 – a 20% increase since 2015.

Source: Global Information Security Workforce Study

Unisys' Cyber Security Intelligence Platform

How are you to deal with the compounding factors of too much data, too little time, and too few resources? Unisys' Cyber Security Intelligence platform provides leading-edge machine learning and predictive technology to proactively protect businesses from bad actors and malicious events.

Unisys doesn't replace your security information and event management (SIEM) tool or your firewall. Instead, we focus on enhancing your ability to see the unseen, and on drastically reducing the number of false positives. This methodology enables your resources to zero in on real threats in real time, rather than digging through logs to see what happened yesterday. While post-mortem forensics are important, it is much more effective to predict and prevent attacks from happening in the first place.

Unisys Cyber Security Intelligence platform incorporates:

Machine Learning

Machine learning offers unrivaled capabilities to respond in real time to the ever-changing security landscape:

- Review and assess billions of records of known threats and attack signatures in real time
- Generate proactive alerts and actionable insights
- Correlate all threat intelligence sources to create a complete context for known threat and risk data
- Match vulnerability data to known risk profiles specific to a given network and industry
- Predict threats before they become damaging events
- Deliver 360-degree protection for all related threats

Behavioral Analytics

Rules-based security systems have two problems. First, it is impossible to write a rule for a behavior that is not known. Second, it is impossible to write a rule for every potential anomaly. Unisys eliminates these vulnerabilities by monitoring behavior at a user level and providing insight through our unique behavioral analytics. Our models create a behavioral baseline and determine what is normal and abnormal. Anomaly detection algorithms then note even the smallest changes from the baseline behavior analysis (see Figure 1, Anomalous Behavior). In response, the model scores that behavior and the likelihood that it is actually malicious in nature.

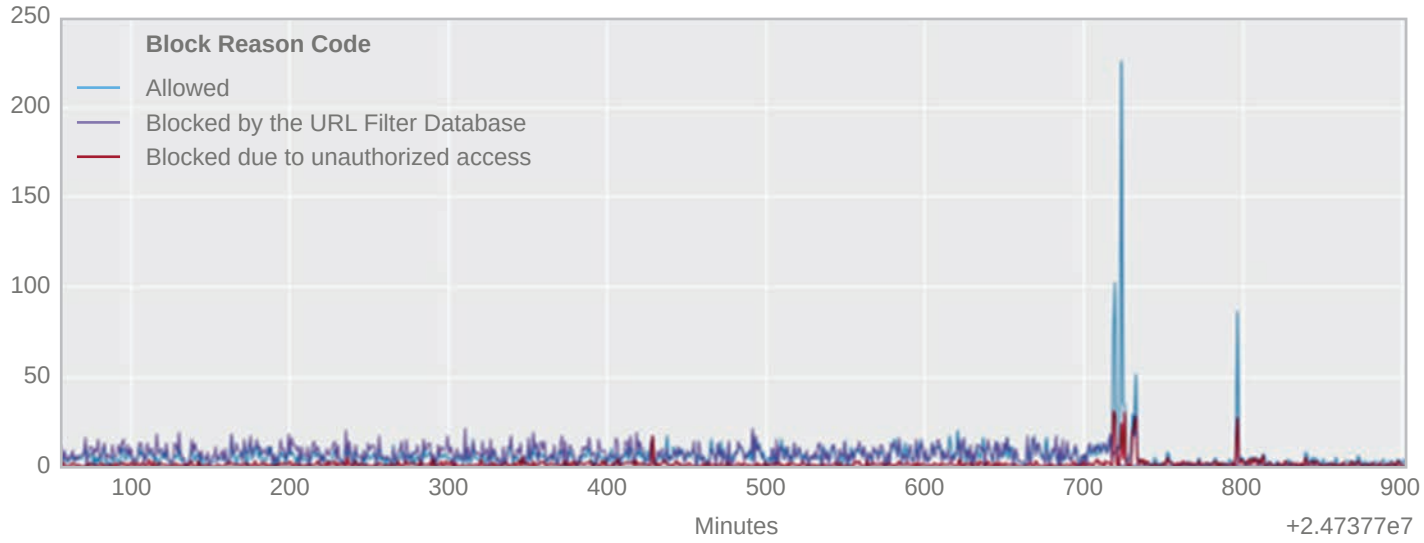


Figure 1: Anomalous Behavior

Threat Intelligence Engine

Unisys utilizes billions of known threats to constantly train our threat intelligence engine to identify unknown threats. Our anomaly models score all network events, no matter how slightly they fall outside the norm as malicious (see Figure 2, Event Scoring). Because of this deep learning process, the intelligence of the engine continues to grow, and events that could never be detected with traditional systems are immediately identified, generating actionable alerts in real time. This gives you the opportunity to stop attacks or infiltrations before damage or exfiltration can be attempted. As attack vectors and strategies change, the model also changes, recognizing these differences and adapting to identify new threats as they evolve.

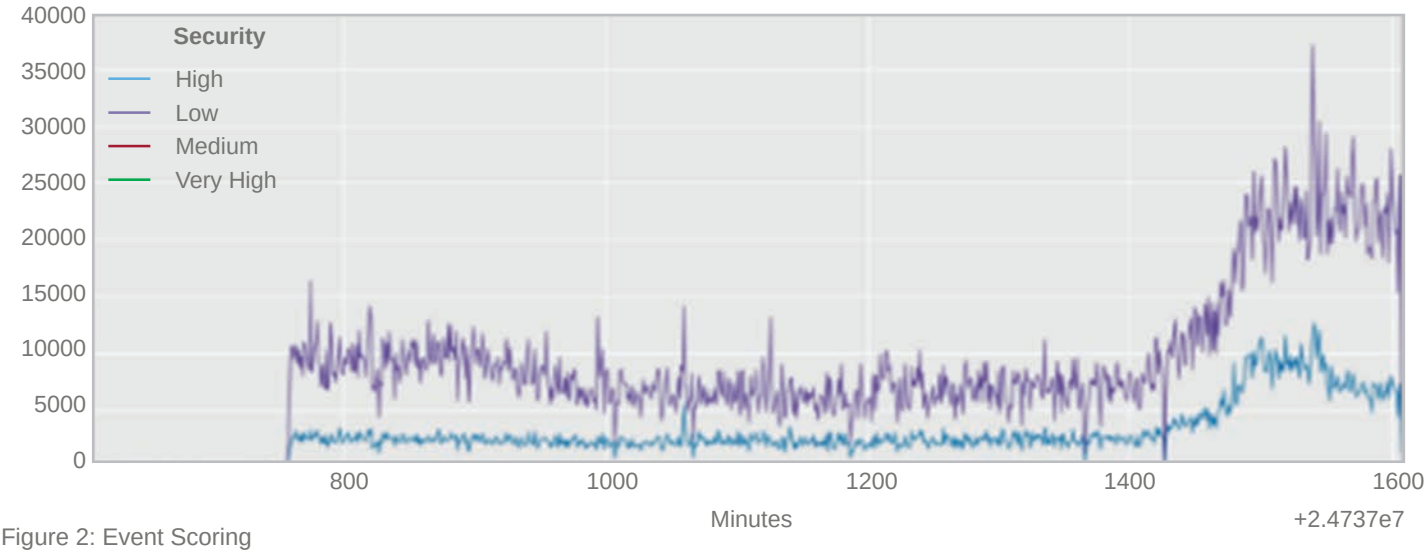


Figure 2: Event Scoring

Securing Success at a Global Energy Company

A Fortune 100 energy-sector company was confronted with multiple security challenges, including a complex global network of IT and OT devices and numerous industry and governmental regulatory requirements. The company wanted to gain greater insight and control over their risk and threat landscape.

After conducting a full security audit of the company's network, Unisys recommended evaluating network security through the use of advanced data analytics. After ingesting and normalizing all the log data from firewalls, switches, and other network devices, including Active Directory Services (ADS) data, Unisys was able to identify a significant amount of malicious behavior and attempts at exfiltration of data. As a result, Unisys recommended several action steps, including:

Establishing a Dynamic Alert System

Working closely with the energy company's management and the Unisys Security Operations Center (SOC), a dynamic alert system was created to provide actionable data for suspicious behaviors. This empowered the company to identify potential events much earlier than would have been possible under normal circumstances.

Blocking External Threats

In the security audit, Unisys identified multiple endpoints attempting to connect with malware botnet control centers. Although much of the traffic was blocked, there was still considerable traffic getting through (represented in blue in Figure 3). By leveraging machine learning and real-time intelligence feeds, the endpoints were successfully blocked from associating with these known malicious threats.

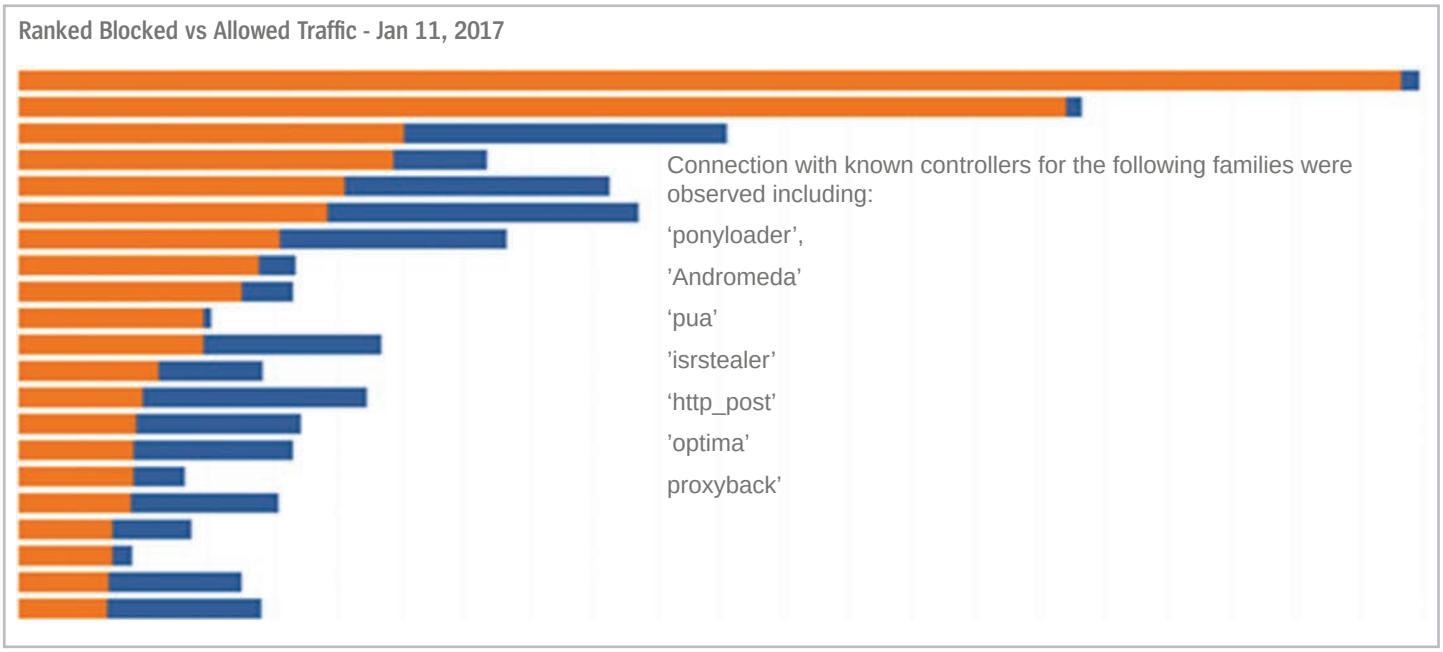


Figure 3: Observed External IP Traffic

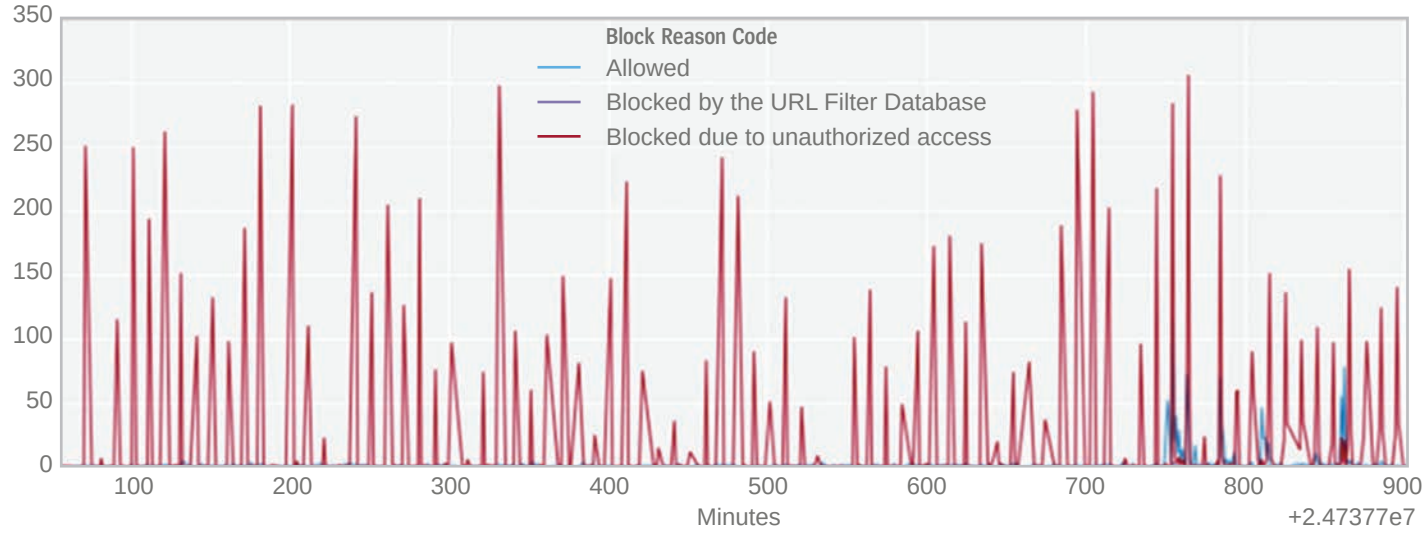


Figure 4: Blocked Traffic

Employing Behavioral Analytics

Unisys' ability to observe peculiar user- and machine-level behavior in very short time intervals enabled the swift identification of bad behavior, as illustrated by the red spikes of blocked activity in Figure 4. Knowing the type of behavior along with the frequency of the behavior provided a signature that could be easily scored as a high-risk malicious event.

Eliminating Internal Threats

Unisys was able to identify exfiltration of sensitive data from internal users to personal shared cloud resources (which was against company policy). These events, whether maliciously perpetrated or done out of ignorance, were promptly stopped. Administrators were able to approach the end users directly to discuss the breach in company policy, armed with the specific proof by time of day, amount of data, and external location of where the data was sent.

Protecting Network Assets

The energy company needed to comply with a new compliance requirement within their industry to have a real-time inventory of critical assets on their network. They had been using multiple traditional inventory methods to identify and inventory a full list of IT and OT infrastructure assets, but with little success. Unisys' analysis provided a full inventory of valuable assets and their risks based on known connectivity to other devices. Plus, Unisys supplied the appropriate level of protection for each asset based on firewall rules, thereby helping the company meet their compliance requirement goals. This capability alone saved the energy company millions of dollars in potential fines, as well as complications with the federal government.

Securing Your Tomorrow

Today's security professionals are faced with malicious campaigns by rogue nations, the growing availability of information for free or for sale on the dark web, and attackers who are employing advanced machine learning and predictive algorithms to make their signatures less recognizable through traditional technologies. The only way to combat these threats is through solutions such as Unisys' Cyber Security Intelligence platform, which employs the most sophisticated tools available to secure your tomorrow.

About Unisys

Unisys is a global information technology company that specializes in providing industry-focused solutions integrated with leading-edge security to clients in the government, financial services, and commercial markets. Unisys offerings include security solutions, advanced data analytics, cloud and infrastructure services, application services, and application and server software.

ABOUT THE AUTHOR

Unisys Thought Leader
Mark Loucks

Mark Loucks is a senior data scientist with Unisys and serves as Principal Practice Director for our Cyber Security Intelligence group. He also has responsibility as a member of Unisys Advanced Data Analytics leadership team to promote the advancement of data intelligence and automation to solve some of our client's most difficult problems.

An entrepreneurial and visionary executive with 25 years of experience in digital technology, advertising, marketing, strategy, product development and growth. His leadership, expansive technical knowledge, and market development capabilities have helped organizations experience significant growth. Working across multiple verticals internationally including Retail, Financial Services, Automotive, Technology, Travel, and Telecommunications.

For more information,
visit: www.unisys.com/cyber-analytics

Follow Unisys on Twitter and LinkedIn

© 2017 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

Printed in the United States of America 07/17 17-0408