UNISYS | Securing Your Tomorrow™

LogRhythm
The Security Intelligence Company

Designing an Adaptive Security Architecture with Unisys Stealth and LogRhythm®

by
Salvatore Sinno
Chief Security Architect - Unisys

Franco Negri
Sales Engineer, System Integrators - LogRhythm

Seth Goldhammer
Senior Director of Product Management - LogRhythm

White Paper

Table of Contents

Introduction

The historical approach to network security was one built on strong perimeter defences and a well understood concept of resource and infrastructure allocation. Today's reality is completely different, so it requires a change in the way we think about security and the supporting business process models.

The challenges faced by today's information and network security professionals include amorphous perimeters and constantly evolving security postures; the emergence of the Internet of Things (IoT) and the Internet of Everything (IoE); the transition from IPv4 to IPv6 and the sudden proliferation of readily addressable end points and its direct impact on IoT and IoE; the normalisation of Bring Your Own Device (BYOD), the spread of wide-ranging heterogeneous network devices, cloud services and infrastructure.

Another emerging and critical threat is the broader use of previously unknown, powerful exploitation tools that were, until recently, limited to adversarial Nation-State actors and Intelligence Agencies. Also, underground social media and anonymized monetary transactions provides an ecosystem for sharing tools, information, and receiving instant monetization of stolen data. Different individuals or groups with different motivations are able to cooperate and share information and stolen data in ways never seen previously.

As a result, security architectures have become complex and security controls have been delivered in non-integrated silos, which increases costs and decreases effectiveness. Across all of the recent attacks there is one common thread: the attacker has penetrated the traditional perimeter defences. This shows that the traditional security approach is failing. The fluidity of today's threat landscape, the disappearance of clear network boundaries and the increased number of connections inside and outside the enterprise all increase the likelihood and speed of an attack. The reality today is that attackers get in, move around, and then start doing damage, all the while, going "undetected" for long periods of time.

> **"My message for companies that think they haven't been attacked is: you're not looking hard enough."**
>
> James Snook
> Deputy Director of the Office for Cyber Security and Information Assurance (OCSIA) within the Cabinet Office

A security breach is not a matter of if, but a matter of when. It is imperative that organisations shift their security mindset from 'incident response' to 'continuous response', where systems are assumed to be compromised and require continuous monitoring and remediation.

This can be achieved by developing an Adaptive Security Architecture (ASA), which aims to contain active threats and to neutralise potential attack vectors. Gartner[1] defines an ASA along four security capabilities:

- **Preventive capability:** this is the set of policies, products and processes that prevent a successful attack
- **Detective capabilities:** these are the controls designed to identify attacks that have evaded the preventive measures and reduce the threat amplification
- **Retrospective capabilities:** these provide a way to shrink the attack surface, slow the rate of the attack and reduce remediation time
- **Predictive capabilities:** these capabilities enable the organisation to predict attacks, analyse security trends and move from a reactive to a proactive security posture

This paper introduces concepts associated with adaptive security and shows how Unisys Stealth and LogRhythm (LR) provide a unified platform to enhance system survivability and reduce the impact of potential threats.

Adaptive Security Architecture

Modern organisations can be considered as complex adaptive systems. In his seminal work Adaptation in Natural and Artificial Systems, Holland defines complex adaptive system as

"A dynamic network of multiple dispersed and decentralised agents that constantly interact and learn from one another".[2]

[1] Designing an Adaptive Security Architecture for Protection From Advanced Attacks, 28 January 2016 ID:G00259490

[2] *Adaptation in Natural and Artificial System,* J, H. Holland, *The MIT Press, ISBN 0-262-58111-6, 1995*

Threats today are both known and unknown, anticipated and unanticipated, internal and external. In effect, the threat environment is now everywhere and nowhere. The perimeter, and the traditional security paradigm, is dead.

Modern enterprises need flexible new methods for reliably establishing trust, detecting attacks and recovering from security incidents.

This new approach to information security architecture has to try to mimic a complex adaptive system that can adjust to constantly emerging and changing security threats. This is the essence of Adaptive Security Architecture, to serve as the enterprise security immune system.

The Adaptive Security Architecture is the enterprise security immune system

Adaptive Security Architecture (ASA) is based on solutions that use adaptive and dynamic operational styles to maintain the integrity of data, systems and their survivability.

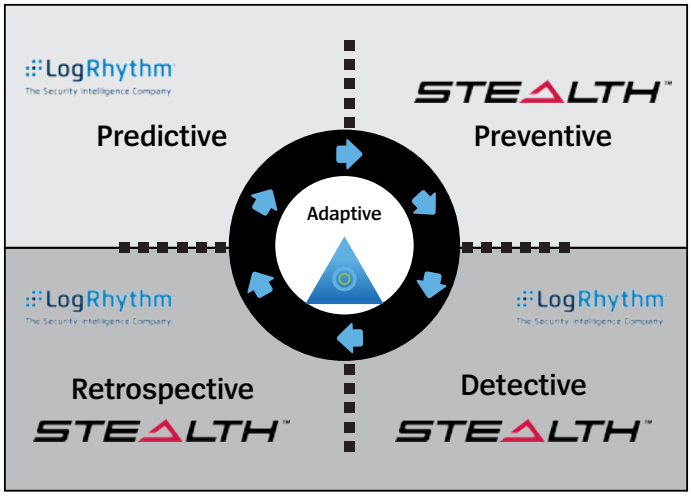
To extend the parallel between biological ecosystems and enterprise IT infrastructures, ASA follows the Darwinian concept of 'adapt or die'. Successful IT infrastructures must adapt or they will eventually fall to predator attacks, viral infections or the inability to adjust to environmental changes.[3] ASA behaves similarly to how an organism defends against a localised disease outbreak or even a pandemic.

Using an adaptive approach, ASA is an autonomic system that effectively mimics both an organic immune system and a large-scale natural ecosystem. To this end, the key objective of an Adaptive Security Architecture (ASA) is to be able to detect, contain and respond to cyber threats before they cause damage by:

- Continuously monitoring the "entire IT stack"
- Shifting from "incident response" to "continuous response"
- Moving to a "unified" or "integrated" detection, response, prediction & protection capability
- Preventing "successful attacks"
- Reducing the surface and velocity of attacks
- Reducing the Mean-Time-To-Detect Threats (MTTD) and the Mean-Time-To-Respond to Threats (MTTR)
- Implementing a continuous response-enabled operations (SOC)

Moreover, the ASA has to provide the ability to take remedial actions such as:

- The quarantine of resources for forensic purposes so that the ecosystem can learn from the breach
- The provisioning of other resources to replace affected systems, enabling service continuity
- The application of corrective measures as needed



Source: Gartner (February 2014)

Preventive capabilities protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional. These include controls and processes such as security policies, security awareness programs, access control procedures and the well-known approaches based on 'signature-based' anti-malware (such as host and network intrusion prevention systems, and network and perimeter security).

Detective capabilities provide visibility into malicious activity, breaches and attacks. These controls include logging of events and the associated monitoring and alerting that facilitate effective IT management. These include typical security information and event management (SIEM) technologies, but the ASA requires continuous and pervasive monitoring to perform analytics and identify anomalies.

[3] *Design and Adaptive Security Architecture,* J. Weise, *Sun Blue Print, Part. No. 820-6825-10, 2008*

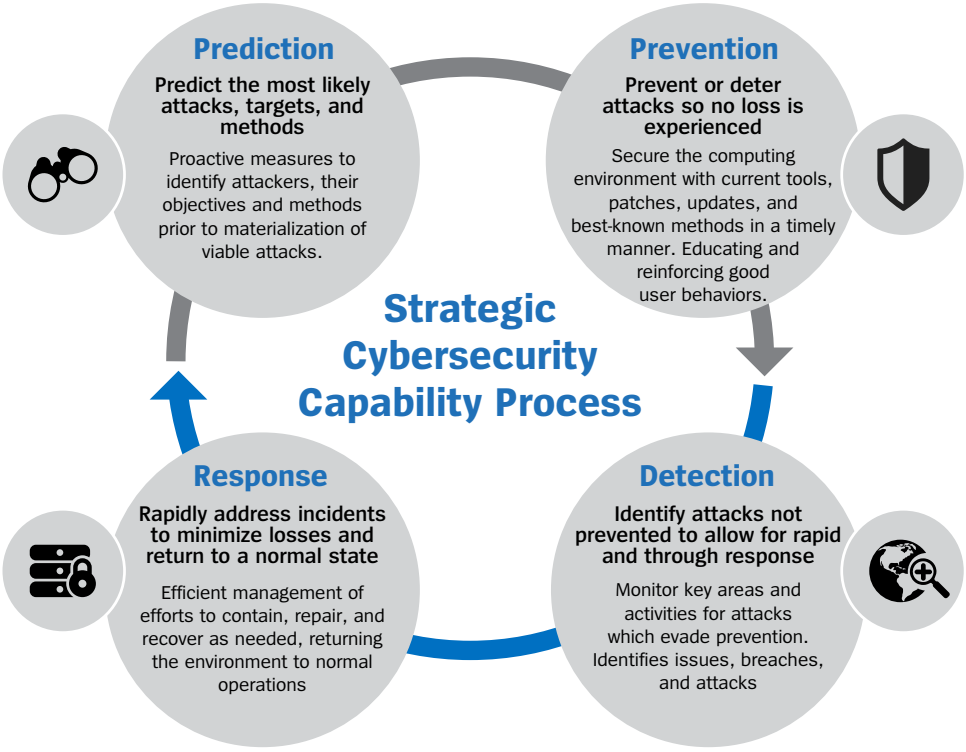
A good way to test the detective control is to use the Lockheed Martin Cyber Kill Chain framework, which can be used to detect cyber threats and includes surveillance (e.g. scanning), weaponisation and delivery (e.g. malware), exploitation (e.g., vulnerability), command and control (e.g. compromised administrator accounts), and exfiltration of data (e.g. intellectual property [IP]).[4]

It is imperative for a threat detection system to take a "holistic" approach, providing visibility across all endpoints, networks and user behaviors. It important to monitor across all of these vectors in real-time to avoid blind spots and to also increase "true positives". The alternative approach of deploying security point products, "miss" advanced attacks whose behaviors transcend individual attack surfaces and their detection capabilities.

A threat detection capability should also incorporate the use of machine-based analytics in order to automate the threat detection process and also to find patterns and behaviors previously "undetectable" by humans. Given the necessary volume of data and the associated concerns of "alarm fatigue", emanating from many point solutions generating "non-qualified" false alarms, machine-based analytics also play the vital role of reducing false positives.

Response/Retrospective capabilities provide the process, procedures and technology necessary to take appropriate action in response to a variety of cybersecurity events. These include forensic investigations, network changes, remediation changes and automated response capabilities. While this has been addressed in non-integrated silos through different processes, procedures and technologies, continuous response requires an intelligent, automated response platform that enables the "unified" orchestration of these capabilities. To this end, all information security processes, personnel and technology should be cohesively integrated, controlled and managed.

Predictive capabilities provide security intelligence from the monitoring of internal and external events to identify attackers, their objectives and methods prior to the materialization of attacks. This should be based on the internal generation of threat data based on recognized activities including the use of watched lists, watched hosts, or use of internal honeypots. Additionally, the ability to recognize threats in the early stages of kill chain activity in order to anticipate and predict attacks before they progress to later stages. This predictive capability needs to also integrate "external" events and threat intelligence to provide a warning of imminent threats to the environment.



[4] Lockheed Martin, *Cyber Kill Chain*, *www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/tradecraft/cyber-kill-chain.html*

This framework can be used to classify existing and potential security investment to ensure that there is a balanced approach to security investments.

How Unisys Stealth and LogRhythm deliver an Adaptive Security Architecture

Together, Stealth and LogRhythm provide an integrated solution which enables an “Adaptive Software Defined Security” as described in the diagram below:

Stealth protects high-value assets by defining and dynamically deploying micro-segmentation security polices to permit, restrict or completely block communication among these assets. Stealth deploys this software defined network segments in response to varying threat conditions identified by LogRhythm and provides the fine-grained control over configuration and enforcement of policies. Stealth technology also renders these high-value assets invisible to threat actors via its cloaking technology.

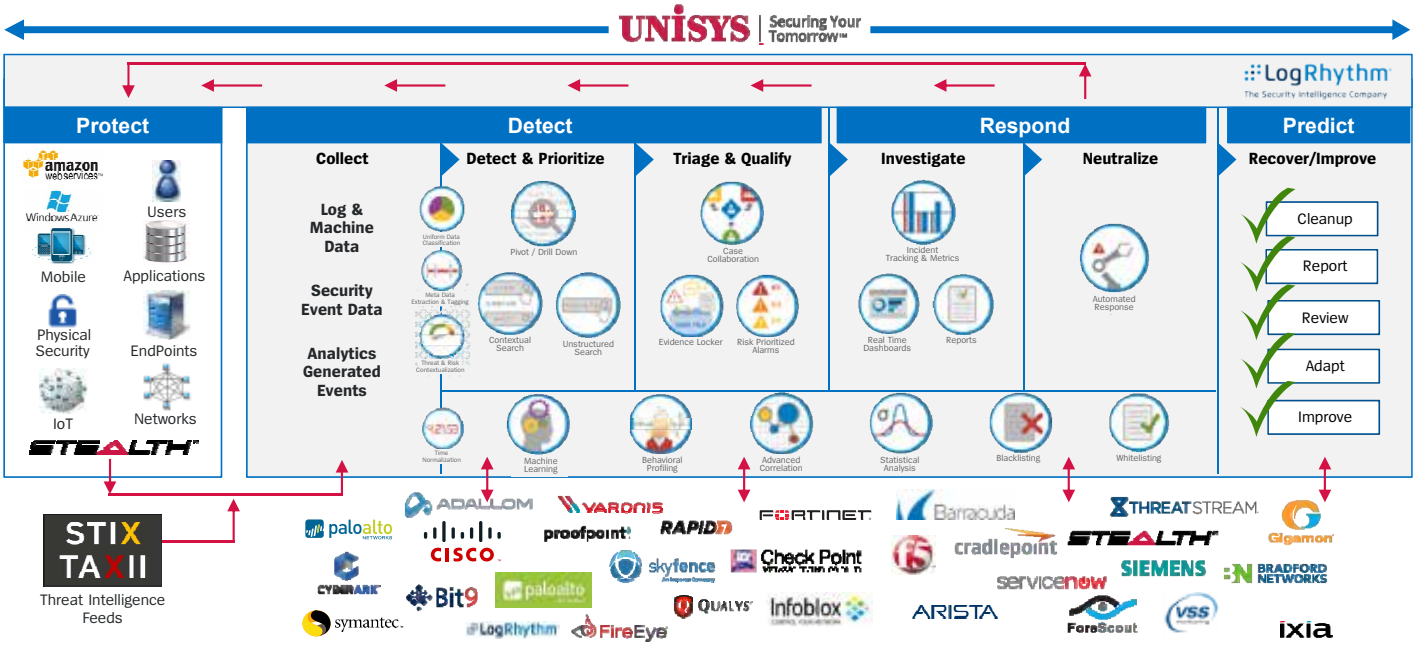
LogRhythm enables a “unified” threat detection and response capability leveraging its advanced security analytics and machine intelligence. It provides a holistic monitoring capability, continuously monitoring endpoints, networks and user behaviours, enabling cohesive end-to-end security visibility.

LogRhythm also incorporates a Threat LifeCycle Management (TLM) and orchestration capability that helps to reduce the Mean-Time-To-Detect (MTTD) and Mean-Time-to-Respond (MTTR) to threats.

Integration between Stealth and LogRhythm provides a mechanism to identify early-warnings of impending threats and the ability to automatically implement remediation via SmartResponses™ In conjunction with Stealth.

By combining the strengths of both LogRhythm’s Unified Security Intelligence Platform to detect and remediate threats across the stack and Stealth’s ability to dynamically micro-segment and cloak the environment, Unisys delivers “now” on the promise of Gartner’s futuristic “Adaptive Security Architecture”.

Stealth and LogRhythm solutions working in concert, provide a security capability which enables continuous monitoring, threat detection/remediation and multiple layers of defence while altering its defensive posture relative to the level of risk – “Adaptive Software-Defined Security”.



In the following sections we will discuss how Stealth and LogRhythm work together to address all of the elements of the "Adaptive Security Architecture" including Preventive, Detective, Response and Preventative capabilities.

Preventive Capability

Stealth is a software-based micro-segmentation platform that implements a 'zero-trust' security model. Forrester Research is widely credited with coming up with the concept of the zero-trust model, in which rules and policies can be assigned to workloads, Virtual Machines (VMs) or network connections. This means that only necessary actions and connections are enabled in a workload or an application, while everything is blocked.

The solution quickly discovers physical and virtual endpoints and qualifies them on your network so you understand how they are communicating with each other. It uses both discovery agents and industry-standard packet capture (pcap) files to uncover high-risk and high-value traffic and the critical endpoints that you need to secure. The discovered data is presented on an easy-to-use, drag-and-drop visual interface or 'canvas'.

After it discovers and visualises your environment, Stealth proposes security policies – via a visual model on the canvas – for targets ranging from large groups of endpoints all the way down to individual traffic flows. Stealth modelling intelligently groups similar endpoints for the application of security policies, enabling businesses to rapidly develop finely-tuned micro-segmentation policies.

Stealth also provides multiple model views so organisations can select the best starting point for their environment and customise the proposed model as needed. It enables organisations to automate the deployment of micro-segmentation policies to the endpoints in their infrastructure, while also supporting customisation of the level of enforcement.

One of benefits to this approach is the ability to establish security policies for each workload rather than the network hardware, meeting these three main requirements:

- Security remains consistent in an environment that is subjected to continuous change
- Security becomes available everywhere: in the cloud, in the traditional Datacentre, on the BYOD, on mobile devices
- Security becomes extensible and adapts to changes

In addition to Stealth's state-of-the-art ability to protect and prevent security breaches, LogRhythm provides additional capabilities in this category enabling a "layered security" or "defence-in-depth" ability. By integrating with industry-leading Anti-Malware, Host and Network Intrusion Prevention Systems and Network Perimeter Security Systems, LogRhythm helps to leverage existing security investments while incorporating these systems into an overall end-to-end security ecosystem. Logs from these systems are analysed and correlated along with other endpoints, networks and user behaviours to provide a real-time end-to-end understanding of an enterprises' security posture. LogRhythm then applies its advanced security analytics and machine intelligence to detect threats and anomalous behaviours and to remediate threats with its patent SmartResponse™ technology. While detecting and responding to threats in the environment, LogRhythm can also relay this threat and risk information to Stealth in order to adapt its defences accordingly.

Detective Capability

Stealth integration with LogRhythm combines security policy controls with deep, enriched application-layer visibility. LogRhythm provides integrations to over 750 security information sources and integration with hundreds of leading security systems and devices. These sources can be categorized into five areas including Security Events, Log Data, Flow Data, Environmental Context and External Threat Intelligence Feeds. This data is then normalized into a unique metadata taxonomy which simplifies and abstracts data into a "common language" applicable across the entire heterogeneous ecosystem.

LogRhythm further applies advanced security analytics including machine learning, pattern detection, statistical baselining and trending to this data in order to automatically detect anomalous activity across the ecosystem while reducing false positives. This unique combination of machine intelligence enables the early detection of advanced threats and patterns

that are otherwise “undetectable” by operators. These advanced security analytics then generate actionable “risk-prioritized-alarms”.

Stealth administrators can leverage these “risk-prioritized-alarms“ with its associated evidence and forensic data to further refine its defences against advanced threats. A thorough investigation of attacks, helps operators to rapidly understand the various phases of an attack. Operators can also leverage these forensics to prevent against “like-kind” future cyber-attacks.

LogRhythm also provides a “unified” threat detection and response workflow enabling operators with a full Threat Lifecycle Management (TLM) and Orchestration capability. TLM includes customizable interfaces/dashboards, Incident Management, Case Management, Investigation and Forensic capabilities. All of these functions are “unified” into one singular platform, enabling operators to “quickly” detect advanced attacks early in the kill chain, before a damage occurs, without having to context switch to other external systems. Although it’s possible to provide these capabilities by integrating many “individually purposed” security products, a unified solution, incorporating all or most or the required functionality, generally provides the most efficient workflows and the best results.

LogRhythm’s implementation of advanced security analytics and unified Threat Lifecycle Management capabilities work together to dramatically reduce the “effective time” it takes to detect and respond to an attack, ”Mean-Time-to-Detect (MTTD) and the “Mean-Time-To-Respond” (MTTR).

Following are other examples of LogRhythm-enabled capabilities that contribute to early threat detection and an overall lower operational MTTD/MTTR:

- Unified Contextualized/Unstructured Search capability; enables faster searches with relevant event context
  - Unstructured Search; search raw data from any source, keyword search across full text including structured metadata
  - Structured Searches; applied to normalized metadata across the entire ecosystem
  - Clustering; distributed searches across multiple nodes for faster search speeds & larger data sets
- Logical Event Taxonomy; provides the proper event context via “clearly worded” metadata for improved search accuracy and rapid event assimilation
- Proper Event Context; geolocation (country/city: origin & impacted), Classification (security, audit or operational), Hostname (origin or impacted), Network (origin or impacted), etc.
- Unique integration with Stealth platform to enforce security policies enabling superior “protection” of high-value assets, communications and workloads

Threat Response and Retrospective Capability

Stealth enables the quick deployment of software defined network segments. Through the definition and deployment of micro-segmentation security policies, it is possible to restrict or completely block communication between sensitive assets and those that have been compromised.

LogRhythm’s machine intelligence and SmartResponse™ technologies enables the Stealth platform to quarantine, quarantine with approval, or remove workloads from network segments based on the early detection and identification of threats and high-risk abnormal behaviours.

To provide the best possible Threat Response, Stealth and LogRhythm work in “unison” to provide an adaptive and “layered security” or “defence-in-depth” capability. Stealth provides unparalleled defences by micro-segmenting the environment, rendering high-value assets invisible to bad actors while LogRhythm provides additional layers of defences via its advanced threat detection and remediation via its SmartResponse™ capability. The following describes the combined approaches to enable these effective “Threat Response” capabilities:

Stealth reduces threat risk exposure, enables Adaptive Security:

- Reducing the threat amplification –micro-segmentation contains the threats inside a specific network segmentation. Even if a system is compromised inside a specific community of interest, nothing can be sent outside the segment. In essence, Stealth contains the unauthorized attempt to access sensitive information inside a specific microsegment;

- Shrinking the attack surface –the target of the attack is made smaller by dynamically changing the membership to a specific micro-segment. This means that, in the event of an attack, sensitive assets can be further isolated from the rest of the network, making it difficult for an attacker to identify them. Infected machines are then moved to an isolated micro-segment to enable forensic analysis. The integration with LR allows real-time forensic analysis which can be used to further refine policies for increase protection against threats;
- Decreasing attack velocity – Stealth's dynamic micro network segments introduce new barriers that slow the rate of attack. Assets such as servers, end-points and even entire datacentres are rendered undetectable. Data is also encrypted in motion from the datacentre to the VM in the public cloud, and between VMs in the cloud. Lateral movement is restricted to within the zone only and this decreases the attack velocity.

  LogRhythm delivers continuous threat response and enables Adaptive Security via Stealth technology:

  From a security operational perspective, LogRhythm enables a "continuous response" capability with its "risk-prioritized alarms"(RPAs). RPAs provide an operational framework whereby operators can use these "actionable" alarms to prioritize their activities based on the relative threat and risk to their organization. Additionally, the aforementioned Threat Lifecycle Management (TLM) framework and its associated unified capabilities, enables operators to manage the threat from early detection to remediation, early in the kill chain.

  LogRhythm's SmartResponse™ uniquely enables automated incident responses. It also allows semi-automated, approval-based operation so users can review the situation before countermeasures are executed. LogRhythm reduces the time needed to perform common investigation and mitigation steps, preventing high-risk compromises from escalating. A great SmartResponse™ example is "quarantining" a Stealth User or removing a Stealth User from a Community-of-Interest based on the detection of high-risk behaviours.

Predictive Capability

As today's threat landscape rapidly evolves, it is imperative to have the most current intelligence data available to enable rapid and effective response to todays advanced threats. Advanced threats are dynamic and attack vectors change constantly. LogRhythm enables a "predictive" threat capability by integrating and correlating rich "external threat intelligence" with "internal early threat detection" leveraging its advanced machine intelligence and analytics capabilities. LogRhythm's machine intelligence and predictive analytics capabilities can detect and even anticipate advanced threats early in the kill chain, detecting patterns and behaviors representative of the early stages of advanced threats. It automatically detects never before seen patterns in the environment (automated anomaly detection), which operationally, are eminent indicators of emerging threats.

In addition to early threat detection capabilities, integration to "Threat Intelligence" services enables you to immediately know about external risks that can impact your environment. LogRhythm seamlessly incorporates threat intelligence from STIX/TAXII-compliant providers, commercial and open source feeds, and internal honeypots, all via an integrated "threat intelligence ecosystem". The LogRhythm platform uses this data to reduce false-positives, detect hidden threats, prioritized alarms and even help to warn and predict of impending risks and attacks.

LogRhythm consumes and leverages threat intelligence feeds and integrates and correlates them with its advanced security analytics to expose a myriad of threats and risk including; low reputation IP addresses and URLs, nefarious email addresses, file names and processes to mention a few. You can select which feeds to integrate, including open source feeds and commercial feeds that require their own subscriptions.

LogRhythm's Threat Intelligence capabilities enable you to better understand the global implications of emerging or existing threats, prioritize threat mitigation strategies and maximize internal resources to make more accurate and efficient decisions to support successful incident response.

Conclusion

Stealth and LogRhythm provide an integrated platform enabling an adaptive security architecture that can adjust and respond to existing and new threat conditions. They enable the cohesive orchestration and management of people, processes and technology into a “unified” Threat Lifecycle Management (TLM) framework necessary for the early detection and mitigation of advanced cyber threats. Gartner’s “Adaptive Security Architecture” proposes four “integrated” key capabilities including “preventive”, “detective”, “responsive” and “predictive” capabilities to combat advanced cyber threats. Stealth and LogRhythm deliver on this promise by combining these capabilities in an integrated solution, protecting against not only known cyber threats, but also against new and unknown threats.

For more information visit www.unisys.com

Printed in the United States of America 02/17 17-0057