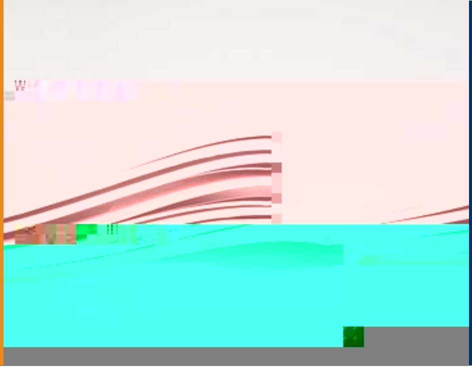
INFORMATICA®
The Data Integration Company™

Collective Intelligence

The Cyber Threat Deterrent

WHITE PAPER



While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. Informatica does not accept responsibility for any kind of loss resulting from the use of information contained in this document. The information contained in this document is subject to change without notice.

The incorporation of the product attributes discussed in these materials into any release or upgrade of any Informatica software product—as well as the timing of any such release or upgrade—is at the sole discretion of Informatica.

This edition published March 2010

Table of Contents

The Asymmetric Cyber-Warfare Threat

Information technology and cyber infrastructure in the United States have evolved into a critical source of national strength. As a result, the nation now has a significant reliance on this infrastructure for finance and transportation, and for military/civilian government operations. As such, these systems represent an inviting and easy target for both state and nonstate adversaries. These adversaries recognize that they cannot match the military and technology might of the United States. Therefore, through asymmetric cyber warfare tactics, they seek to attack, destabilize and exploit the nation's cyber weaknesses and vulnerabilities.

Cyber warfare is any means of penetrating, infiltrating, manipulating, controlling or destroying software controlled systems or data in order to compel and influence an adversary's will. With its low barrier to entry, cyber warfare has proven to be an effective, clandestine and powerful asymmetric tool that attracts both state and nonstate actors, including terrorist organizations and even "hacktivists" that use cyber attack techniques to advance their political and social agendas. Asymmetric cyber warfare is not typically prosecuted through direct and audacious attacks. Instead, more subtle, deliberate and calculated modes of attack tend to be employed. Cyber attackers are patient, favoring slow and well-planned reconnaissance and gradual attack escalation.

The intent of those engaging in cyber warfare against the United States is clear. Recently, General James Cartwright, Vice Chairman of the Joint Chiefs of Staff, stated that 37,000 breaches of government and private systems were reported in FY 2007. Moreover, nearly 13,000 direct assaults on federal agencies and 80,000 attempted computer network attacks on Defense Department (DoD) systems were reported in the same period.

> "The dynamic, asymmetric, and still evolving nature of cyber attacks makes all aspects of cyber defense—including detection, analysis, investigation, prosecution, retaliation, and more—critical questions for national security planners to answer."
>
> Kenneth Geers
> U.S. representative (NCIS), Cooperative Cyber
> Defense, Center of Excellence

Current Solution & Approach – Defending The Perimeter

The line that separates and differentiates simple network hacking from a well-coordinated cyber warfare attack directed by state or nonstate actors against government systems is subtle and often difficult to detect. Only by analyzing the attack intensity, organization, type, intention, and perpetrator location can one fully understand cyber warfare threats and attacks. Current, conventional security practices and doctrine do not typically employ traditional intelligence practices (e.g., sources and methods) when analyzing cyber attacks and the perpetrators behind them.

Until recently, the U.S. government has not been sufficiently engaged in applying traditional intelligence sources and methods to analyze, report and share (cross-agency) cyber warfare indications and warnings. Instead, the federal government, including the military, the Intelligence Community, and the Department of Homeland Security, has directed most of its efforts towards improving its defensive posture to deny and prevent cyber attacks. Tactics and techniques to defend have been largely directed towards advancements in network- and packet-level intrusion detection, prevention and inspection technologies; and while increasingly effective in deterring some well-known and identified attacks, defensive technology alone is no panacea. This type of technology and improved defensive posture helps; however, they are by no means the complete solution to the cyber threat.

By contrast, during the Cold War period, the U.S. Intelligence Community tirelessly analyzed Soviet military and technology capabilities. The Community did everything in its power to understand the enemy's capabilities and to manage and mitigate the threat. This included innovative application of technology as well as deep, creative, and persistent analysis of the enemy's intent, organization, command and control structure, and even social affiliations. That same level of intelligence analysis, rigor, and creativity is required today to combat and defeat the current cyber threat.

What's Required – A Cyber "Combat Air Patrol" Equivalent

Today's imperative to address this asymmetric cyber threat demands the creation of new cyber security doctrine. This doctrine must emphasize a multi-INT approach to identify, classify, analyze and anticipate the threat in order to outmaneuver, defend, respond, and even counterattack. In many ways, important concepts in this new doctrine will resemble a strategic cyber "combat air patrol," in which persistent, multi-INT analysis and operations are applied in order to understand the danger before it "comes over the horizon." This doctrine must define an integrated and holistic approach—one in which defensive and offensive cyber operations are integrated and collaborative —in order to mitigate current and future cyber threats.

The United States government must also develop a capability to respond to and retaliate against cyber attacks where the government determines not only the identity of the attackers, but also their intentions, associations, capabilities, and how or if they fit into the larger operational picture. Paul Kurtz, former Presidential advisor to Bill Clinton and George W. Bush, underscored this point: "We must begin by addressing the question of attribution," Kurtz said. The ability to collect, share and analyze data in order to tailor responses to a threat is "the beginning of a deterrence policy." Similar to the findings after the 2001 terrorist attacks, successful prevention will be determined by our ability to not only "connect the dots," but to also ensure that corporate America, public institutions, and the Intelligence Community can effectively share information to disrupt potentially catastrophic cyber attacks.

A cyber and counter-cyber warfare doctrine must account for the collection, analysis, correlation, and sharing of all sources of traditional intelligence (HUMINT, SIGINT, GEOINT, OSINT, FININT) with the traditional cyber (network- and packet-level) data derived from lower-level security tools. Many server-, network-, and packet-level tools are currently being used to provide lower-level network event-oriented alerts. These tools include SIMs (Security Information Managers), intrusion detection systems (IDS), intrusion prevention systems (IPS), application firewalls, deep-packet inspection (DPI) firewalls, and even home-grown tools. In most cases, these applications are designed for and used by highly technical network security experts. However, these tools provide only a small piece of the intelligence picture required to combat the cyber threat. Defensive technology alone is not sufficient, and the data and analysis derived from defensive operations must be used in conjunction with other multi-INT sources in an integrated and holistic cyber intelligence strategy.

> "An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by hi-tech means. This would disrupt and destroy the US economy."
>
> China's People's Liberation Daily
> February, 1996

Cyber Security Policy

At a minimum, the following components, characteristics, and capabilities must be prescribed within the nation's comprehensive cyber security policy:

- Event-driven, collective intelligence architectures that facilitate cyber event detection and multi-INT correlation to discover meaningful data dependencies and relationships ("connect the dots"), and time-sensitive indications and warnings (I&W) that facilitate enterprise-wide response
- Persistent, automated, and analyst-defined cyber intelligence, surveillance, and reconnaissance (ISR) operations across the multi-INT spectrum (including open source intelligence)
- Cross-agency multi-INT sharing – collection, analysis, alerting and response
- Cross-domain multi-INT operations – collection, analysis, alerting and response
- Automated, system-level inter- and intra-agency tipping and cueing for cyber consequence management and counter-cyber operations

Open Source And The Multi-INT Analyst

As part of this comprehensive cyber security policy, the value and importance of persistent open source monitoring and analysis are worth a more detailed examination. Many intelligence analysts agree that much of the information that the world wants and needs to know is found in the open source. This is especially true in cyber and counter-cyber intelligence operations. The very same tools, protocols, and applications that have become the target of cyber warfare are the technologies that cyber warfare perpetrators will use to communicate, collaborate, deceive and attack. Open source blogs, e-mail, wikis, web sites, and even Twitter communications provide rich intelligence sources that must be correlated with other data available to the multi-INT cyber analyst.

Consider the comments referenced by the National Intelligence Council in its publication, Global Trends 2015: A Dialogue About the Future With Nongovernment Experts. "Most adversaries will recognize the information advantage and military superiority of the United States in 2015. Rather than acquiesce to any potential U.S. military domination, they will try to circumvent or minimize U.S. strengths and exploit perceived weaknesses. IT-driven globalization will significantly increase interaction among terrorists, narco traffickers, weapons proliferators, and organized criminals, who in a networked world will have greater access to information, to technology, to finance, to sophisticated deception-and-denial techniques and to each other. Such asymmetric approaches—whether undertaken by state or nonstate actors—will become the dominant characteristic of most threats to the U.S. homeland." It is imperative that innovation in multi-INT cyber operations drive this new process of collection, analysis, sharing, alerting, and response.

COLLECT, SHARE, & ANALYZE

The ability to collect, share, and analyze data in order to tailor responses to a threat is "the beginning of a deterrence policy."

Paul Kurtz

Cyber Security Expert and Presidential Advisor

The Cyber Threat Deterrent: Collective Intelligence

Informatica provides the cyber intelligence analyst with an event-driven, collective intelligence solution that leverages the multi-INT (e.g., multiple sources of intelligence) resources of the Intelligence Community in order to monitor and understand cyber threats at a tactical, enterprise, and even strategic level. By combining and correlating data collected by the tools and techniques used by traditional network security analysts, the cyber analyst can leverage SIGINT, GEOINT, HUMINT, and other relevant data sources. This capability enables the cyber analyst to develop the same intelligence operational picture that characterizes conventional intelligence disciplines, such as counter-terrorism/insurgency and weapons proliferation.

With Informatica's solution, non-technical cyber intelligence analysts can write rules that correlate events and alerts, in real time, across network threat tools, traditional intelligence sources, and watch lists of suspected targets. Geospatial processing and integration with traditional intelligence tools such as GIS applications and Analyst's Notebook can also be leveraged as part of the overall collective intelligence effort by complementing the rule and response creation process. Based on these user-defined rules, the Informatica solution enables automated correlation and analysis, event enrichment, automated responses, tipping and cueing, cross-agency and cross-domain threat alerting, and automatic dissemination of reports to other agencies.

Persistent Real-Time Cyber Analysis

The Informatica cyber solution provides cyber intelligence analysts and investigators with a multi-INT, cross-domain, user-defined collective intelligence platform that correlates enterprise intelligence sources to reveal hidden threats and opportunities in time-sensitive environments. The result is a reduction in the time gap between collection and analysis or action via the delivery of real-time intelligence to users anywhere in the organization. Informatica's self-service rules-based system provides a simple and powerful user interface that facilitates collaborative processes while enabling analysts to monitor events of interest and alert or respond when conditions associated with those events are met. The expression language used for creating rules is natural and simple, and it allows for analysts to use their own vocabulary, through watch lists and analytics, to characterize their personal conditions of interest. Moreover, the system itself enables analysts to create expressions that involve temporal and geospatial intersections, dramatically simplifying the process of adding time and space dimensions to cyber analysis.

THE GROWING THREAT

- 37,000 breaches of government and private systems
- 13,000 direct assaults on federal agencies
- 80,000 attempted computer network attacks on Defense Department (DoD) systems

Data for FY 2007 as reported by
General James Cartwright,
Vice Chairman of the Joint Chiefs of Staff

Components, Characteristics, & Capabilities

The Informatica event-driven collective intelligence solution addresses the five minimally-required components, characteristics, and capabilities that must be prescribed within the new comprehensive cyber security policy as follows:

1. **Event-driven, collective intelligence architectures**
   Persistently monitor, detect, correlate, alert, and respond to cyber events (changes in relevant and significant operational data sources) and conditions of interest across all sources of available intelligence; move beyond situational awareness to situational dominance—connect the dots and respond to the big picture in real time.

2. **Persistent, automated, and analyst-defined cyber ISR across the Multi-INT spectrum**
   Expose multi-INT event data properties directly to cyber analysts for rule and response management based on changing conditions of interest; adapt to dynamic circumstances by changing analysis and decision-making logic accordingly—adjust analysis automation on the fly.

3. **Cross-agency multi-INT sharing**
   Extend collective cyber intelligence, persistently and automatically, to all relevant agencies through events, rules, and response sharing; preserve and extend collective knowledge.

4. **Cross-domain multi-INT operations**
   Concurrently tap into rich data sources at all levels of classification and facilitate the automatic movement of this information across multiple security domains.

5. **Automated, system-level inter- and intra-agency tipping and cueing**
   Improve delivery of key information to knowledge workers with e-mail, real-time alerts, GIS applications, portals, dashboards, chat, and machine-to-machine responses; maximize the precision of decisions, responses, and actions.

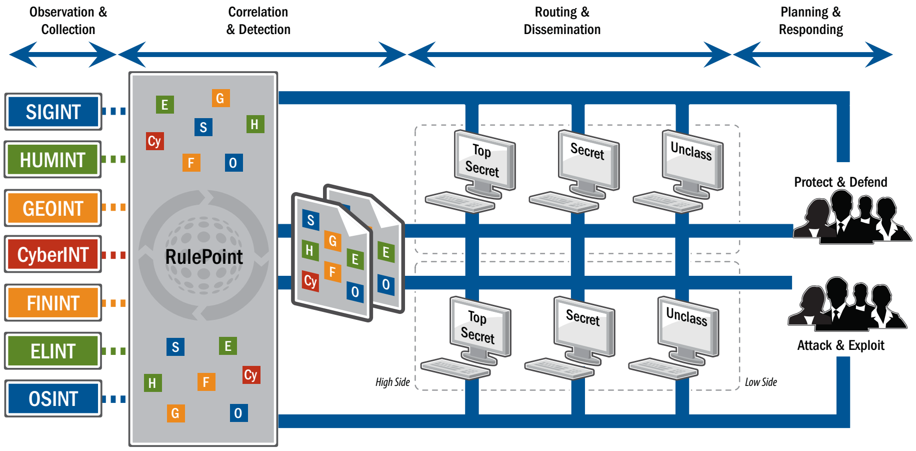


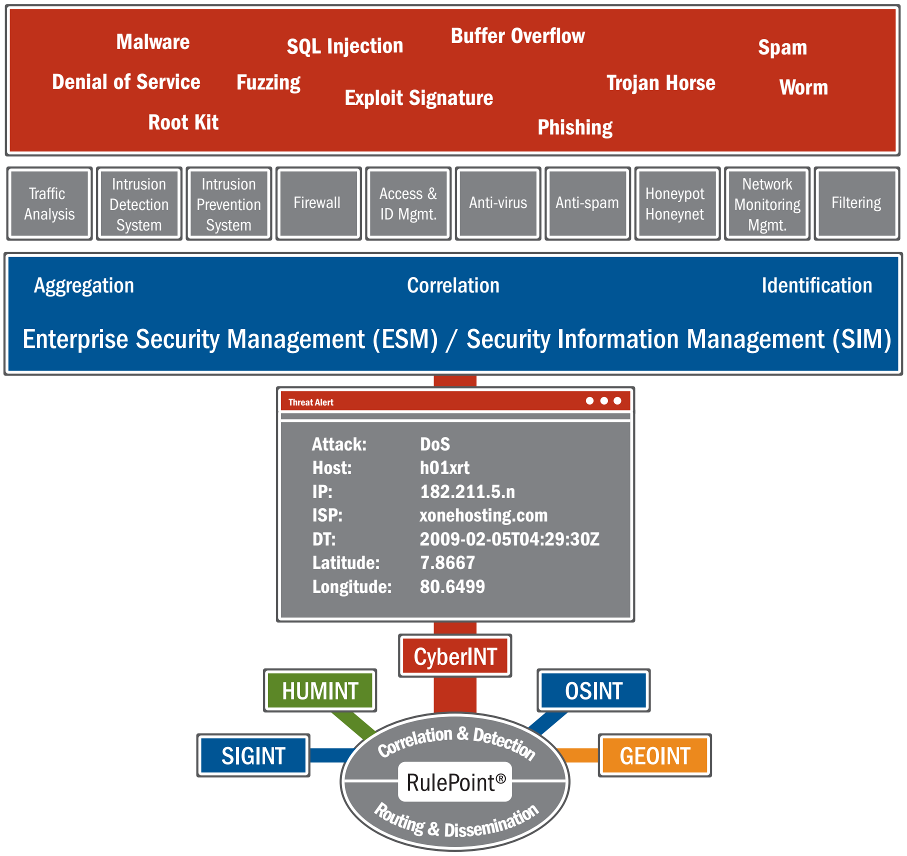
Figure 1 – RulePoint, Informatica's enterprise-class, user-driven CEP software product, ingests all observed and collected intelligence, performs correlation and detection of threat information, and then routes and disseminates packaged intelligence to various security networks.

Implementing The Informatica Solution

Successful implementation of Informatica's cyber solution begins with identifying and ingesting all relevant operational cyber data. It is across these rich data sources that conditions of interest are defined and applied for persistentently monitoring events. These data sources might include enterprise databases; real-time, streaming sensor feeds; correlated or un-correlated network- and packet-level security data (alerts, reports, intercepts, anomaly detections, signature profiles, forensic input, etc.); unstructured or semi-structured intelligence reports; geo-tagged documents; social link analysis tools; open source data feeds (RSS, Twitter, blogs, etc.); and targeting systems.

Bridging The Gap Between Cyber Data And Traditional Intelligence

Current IT tools and techniques focused on identifying and suppressing cyber threats, such as Intrusion Detection Systems, Firewalls, and Network Monitors, coupled with integrated Enterprise Security Management (ESM) and Security Information Management (SIM) platforms, serve to detect frontal assaults on the cyber infrastructure. However, identifying coordinated and pre-meditated attacks on our cyber infrastructure must proactively combine cyber threat data with traditional intelligence sources. To accomplish this, RulePoint receives cyber threat data from these specialized third-party tools and automatically correlates that data with all other sources of intelligence—bridging the gap to build an actionable operational picture of threats directed at our national security and the homeland—more efficiently and in less time.



Attack: DoS
Host: h01xrt
IP: 182.211.5.n
ISP: xonehosting.com
DT: 2009-02-05T04:29:30Z
Latitude: 7.8667
Longitude: 80.6499

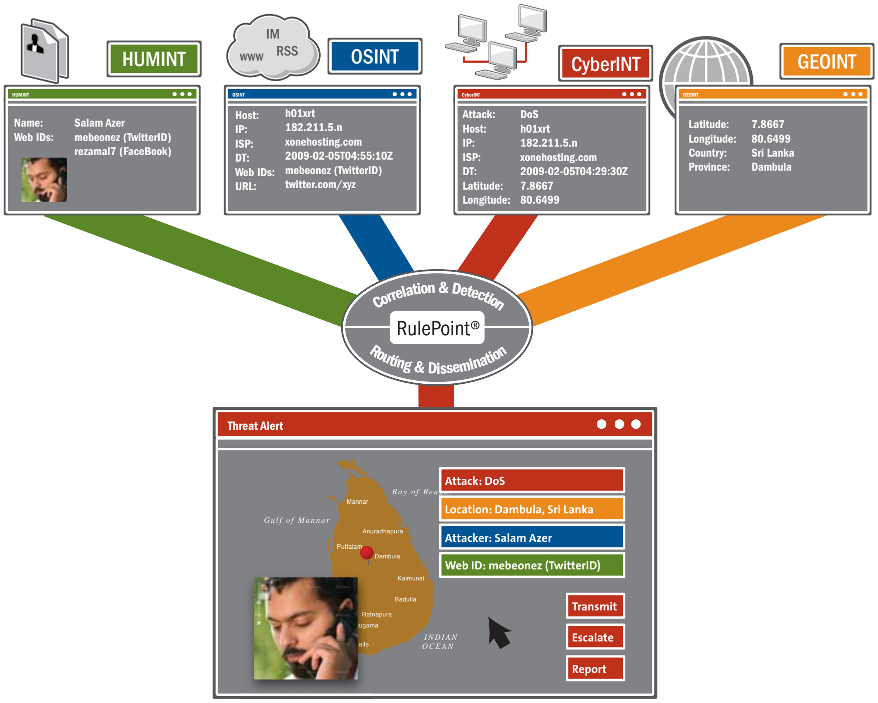
Figure 2 – Bridging the Gap Between Cyber Data and Traditional Intelligence

Event-Driven Collective Intelligence Platform

Informatica RulePoint® is an enterprise-class, user-driven CEP software product that ingests, organizes. and exposes event data such that cyber analysts can build rules to monitor, detect, correlate, and respond when conditions of interest are met. Rules allow users to identify specific events to detect and the responses to execute when detection occurs.

RulePoint also allows the cyber analyst to "mix" in temporal, geospatial, multi-source correlations and analytics when building rules. That is, a relevant cyber rule might be developed to correlate event data from network security event sources, watch lists of targets, and geo-referenced entity databases, as follows:

"Notify me when 2 related cyber threat alerts occur within a 30 minute period and the source IP address of the alert is associated with a person of interest on my watch list, or matches an active case or report within an intelligence database, and the originating Internet services of this connection are determined to be from a potential foreign ISP of interest that is in one of my geographic named areas of interest."



HUMINT

Name: Salam Azer
Web IDs: mebeonez (TwitterID)
rezamal7 (FaceBook)

OSINT

Host: h01xrt
IP: 182.211.5.n
ISP: xonehosting.com
DT: 2009-02-05T04:55:10Z
Web IDs: mebeonez (TwitterID)
URL: twitter.com/xyz

CyberINT

Attack: DoS
Host: h01xrt
IP: 182.211.5.n
ISP: xonehosting.com
DT: 2009-02-05T04:29:30Z
Latitude: 7.8667
Longitude: 80.6499

GEOINT

Latitude: 7.8667
Longitude: 80.6499
Country: Sri Lanka
Province: Dambula

Threat Alert

Attack: DoS
Location: Dambula, Sri Lanka
Attacker: Salam Azer
Web ID: mebeonez (TwitterID)

Figure 3 – Multi-INT Cyber Threat Detection & Response

WHILE SIGNIFICANT CHANGES HAVE HAPPENED IN THE WORLD AND IN TECHNOLOGY, THE FUNDAMENTAL SENTIMENT HAS REMAINED THE SAME:

"Given our present vulnerabilities as a nation, a well planned, coordinated IW attack could have strategic consequences. Such an attack, or the threat of such an attack, could thwart our foreign policy objectives, degrade military performance, result in significant economic loss, and perhaps even undermine the confidence of our citizens in the Government's ability to protect its citizens and interests."

Contextual Responses

The response in these scenarios might simply be a notification to tip the analyst to take the next step in analysis or information sharing. The low-level cyber threat data might include account information from the Internet Service Provider associated with the particular IP address, or it might include historical data associated with previously identified anomalies. After further analysis, the cyber intelligence analyst could correlate that account information with other link analysis sources to determine that the account owner also has ties to a foreign military or intelligence service, or even a terrorist organization. Moreover, by leveraging other information sources, the analyst may also determine that this particular individual also has ties to other bank accounts, ISPs, communications devices, and individuals that are threats due to association with groups that have nothing to do with cyber, but are still of interest. This “next level” of analytical processing is a critical necessity, and it is ultimately made possible by analysts empowered with the right tools, doctrine, and access to data. Through multi-INT event correlation and event enrichment—the inclusion of context and experience—the cyber analyst can develop a more comprehensive understanding of a potential threat or attack.

Cross-Domain & Cross-Agency Intelligence

To support cross-domain and cross-agency collective intelligence, Informatica’s Low-to-High™ (L2H™) solution, based on RulePoint, simplifies analyst workflow by facilitating the monitoring and management of data across one or more low-side security domains, and by providing automated alerts and intelligent transfer of data to high-side security domains. Informatica’s L2H solution automatically monitors key low-side data sources on behalf of analysts, provides high-side alerts based on key events, and automatically assists with getting new, changed data into the appropriate, accessible form on the high side.

The L2H solution performs event detection and response across multiple security domains. This includes monitoring resources on a low-side network, such as RSS feeds, sensors, e-mail accounts, etc., and delivering information-rich notifications to interested users on high-side networks. High-side situational awareness is provided via the following key solution features:

- Automatic high-side notifications based on low-side events (user-defined rules)
- Automatic movement of data to high-side networks using existing data transfer infrastructure
- User-defined filters and high-level event detection rules on low-side networks (as required)
- User-defined alerting and complex event detection rules on high-side networks
- Automated monitoring of conditions of interest on low-side networks

Scenario

Observation & Collection	Correlation & Detection	Routing & Dissemination	Planning & Responding	Description: The following operational use case provides an illustrative example of how RulePoint and Low-to-High provide an event-driven collective intelligence solution for the cyber analyst. Multi-INT, cross-domain, cross-agency alerting, along with collaboration and tipping/cueing capabilities, are described. Mission: Identify key personnel within a "cyber warfare" network and then communicate this information to appropriate channels to initiate the proper response. Analysts: Cyber Analyst (CA) Network Analyst (NA)
√	√			CA uses RulePoint to create personalized rules that monitor relevant intelligence sources (CYBINT, OSINT, GEOINT, HUMINT) and correlate the identity of likely threats.
√				Actor in Dambula, Sri Lanka begins host attack within an agency's honeynet; i.e., two or more networked servers ("honeypots") used to capture, detect, and isolate malicious or unauthorized system use.
√				NA identifies a potential cyber threat by using a set of monitoring and forensic tools across the honeynet. These tools provide profiling and evidentiary data using packet inspection, identification of Denial of Service (DoS) attempts, capturing SQL injection attempts, tracing failed login attempts, and an assortment of other detailed forensic signatures.
√				Upon detecting a network anomaly, the NA or low-level monitoring tool transmits potential cyber threat data to RulePoint.
√	√			CA's rules within RulePoint automatically correlate the incoming cyber threat data with relevant field reports, internal databases, and other sources of intelligence.
	√			Conditions of interest are triggered within RulePoint indicating:
	√			• Cyber threat is correlated with other past events in the same geographic area.
	√			• Suspect is identified as having online aliases on popular Internet sites such as rezamal7 (Facebook) and mebeonez (Twitter).
	√			• Threat originated from an Internet Service Provider (ISP) located in the same geographic area as the suspect's last known location.
	√			• ISP is owned by an individual that has an association with suspect Salam Azer (aka: mebeonez) and other suspects on a cyber watch list for the geographic area.
	√			• Threat is highlighted as possible state-sponsored activity due to the associations between the ISP, the actual suspect, and the ties to organized activity identified over the last several months.
		√		RulePoint instantly generates threat alerts, initiates automatic processes, and performs necessary updates such as the following:
		√	√	• Alert is delivered to the CA's workstation, within the Informatica Real-Time Alert Manager™, that includes contextually relevant data and possible actions to initiate such as drill down, escalation, and further dissemination.
		√		• Link analysis database is updated with new associations.
		√		• GIS view and associated database are automatically updated with new coordinates and contextual annotations from additional data sources.
		√	√	• Target profile database is updated to ensure continuous refinement of future cross-correlation processes. Updates include IP address, host name, alias, associations, geolocation, ISP, and more.
		√	√	• Collaboration is initiated using instant messaging among watch officers, cyber analysts, and network analysts to expedite transfer of knowledge of the threat, share new details, and coordinate a response.
	√	√	√	• Rules are activated on other RulePoint systems for low-side (open source) or high-side (profile and/or biographical) analysis.
			√	Based upon the alert and the contextual information, the CA may take many actions:
			√	• Initiate a follow-up investigation (task workflow) and collection request (tipping and cueing).
	√	√	√	• Relay and/or escalate alert and collected data to other RulePoint systems or other analysts across the community using cross-domain (low-to-high or high-to-low) capabilities.
	√		√	• Update centralized and/or personalized watch lists to ensure time-sensitive detection in the future.

Conclusion

The new cyber security processes described here begin to define an "over-the-horizon" cyber defensive and offensive posture that proactively detects and denies threats and guides preemptive counterattacks when required. By persistently analyzing all sources of available and relevant intelligence, and not just traditional security event data, and by automatically identifying and correlating unique dependencies and relationships among disparate events, RulePoint maximizes the precision of decisions, responses, actions, and consequence management.

RulePoint puts the power and potential of event-driven collective intelligence into the hands of the cyber analysts. Analysts use a simple and natural language to express conditions of interest. Self-service analytics provide an automated capability for data computation. Alerts and responses can be rendered in an unlimited number of ways and environments. Cross-domain intelligence analysis can be automated to ensure that analysts receive only the data in which they are interested from across all accessible networks.

Collective cyber intelligence is the foundation by which cross-agency events, alerts, and tipping/cueing provide a unified, force-multiplied, and coordinated response to cyber threats. A strong policy of deterrence is dependent upon the United States's ability to collect, analyze, and share all sources of intelligence when formulating appropriate defensive postures and offensive responses. This asymmetric cyber warfare threat is committed, creative, and patient; the United States must respond with greater commitment, patience, and intellectual and technological resourcefulness in order to be victorious.

Learn More

Learn more about the Informatica Platform. Visit us at www.informatica.com or call
+1 650-385-5000 (1-800-653-3871 in the U.S.).

About Informatica

Informatica Corporation (NASDAQ: INFA) is the world's number one independent leader in data integration software. The Informatica Platform provides organizations with a comprehensive, unified, open, and economical approach to lower IT costs and gain competitive advantage from their information assets. Nearly 4,000 enterprises worldwide rely on Informatica to access, integrate, and trust their information assets held in the traditional enterprise and in the Internet cloud. Visit www.informatica.com.

INFORMATICA®

Worldwide Headquarters, 100 Cardinal Way, Redwood City, CA 94063, USA
phone: 650.385.5000 fax: 650.385.5500 toll-free in the US: 1.800.653.3871 www.informatica.com

Informatica Offices Around The Globe: Australia · Belgium · Canada · China · France · Germany · Japan · Korea · the Netherlands · Singapore · Switzerland · United Kingdom · USA