XPATTERNS FOR CYBER

THE RULES OF THE GAME HAVE CHANGED

Table Of Contents

Cybersecurity: The Rules Of The Game Have Changed 2

How the Rules Have Changed 2

Why Traditional Tools Fall Short Versus Advanced Persistent Threats 3

It's Time For A New Approach 4

xPatterns' Four Core Capabilities 6

SenseMaking 6

Horizon Scanning 7

Identity Management 7

Network And Operations Management 8

Case Studies 9

CASE STUDY 1: Multinational Corporation Located Overseas 9

CASE STUDY 2: United States Department Of Defense 11

CASE STUDY 3: Healthcare Organization With Interstate Presence 12

Summary 14

© 2015 Atigeo All rights reserved Version # 10

CYBERSECURITY: THE RULES OF THE GAME HAVE CHANGED

There was a time when cybersecurity consisted of taking preventive and mitigation measures against known classes of threats. There would be new viruses, new exploits of vulnerabilities, and new patches to apply; however, apart from some thankfully rare events, threats were symmetric— meaning attackers had the element of surprise, but enterprises had greater resources and more staff.

HOW THE RULES HAVE CHANGED

The threat environment that enterprises face has become *asymmetric*—with attackers that are using fundamentally new tactics, as well as overarching strategies, to attack via any and all available technical and even social channels. Two classes of threats deserving special attention are advanced persistent threats (APTs) and zero-day attacks ("zero days").

Attackers are using fundamentally new tactics, as well as overarching strategies.

APTs and zero days have emerged as the most significant classes of threats to the enterprise. APTs target enterprises with specific infiltration objectives, often motivated by business-related or even political/ideological goals, and are backed by organizations which have grown considerably in sophistication and resources. APTs can result in significant negative financial, reputational, and legal/regulatory consequences. Zero days are particularly dangerous and are part of the APT arsenal; enterprises cannot patch or remediate what neither they nor software publishers know about.

APTs and zero days have emerged as the most significant classes of threats to the enterprise.

Traditional signature-based tools and solutions are simply not capable of detecting APT's and zero days, posing a significant problem for enterprises. New derivative attacks and exploits emerge daily to allow establishment of point of presence *within* an enterprise. As part of the APT, the attacking organization can then silently move around the enterprise's network, compromising devices, seeking intellectual property or sensitive data. The continual discovery of zero-day vulnerabilities gives malefactors a steady supply of new ways to infiltrate and compromise the enterprise.

Traditional tools are not capable of detecting APT's and zero days.

The very nature of APTs are advanced, persistent and have well-resourced command and control behind them. They pose an *asymmetric threat t*oward the enterprise. The organizations behind APTs are:

© 2015 Atigeo All rights reserved Version # 10

- **Persistent** – They can mount continuous, resilient attacks that are prepared and executed over months or years. They are willing to patiently wait for opportunities to exploit vulnerabilities over long timeframes.
- **Intelligent** – They carryout systematic approaches combined with human-augmented intelligence. Stealth attacks are specifically designed to evade detection from traditional security tools by continuously changing their form. These threats are strategically focused on a specific entity to accomplish a key objective. They can include a high number of origination points, targeting greater numbers of system components.
- **Resourceful** – The organizations behind APTs are increasingly well funded, including greater participation from criminal enterprises, terrorists, corporations, political activists, and nation-states.

WHY TRADITIONAL TOOLS FALL SHORT VERSUS ADVANCED PERSISTENT THREATS

Because of the changing, amorphous nature of the threat, traditional approaches are doomed to fail. While signature-based systems do have some value, many of them look at one type of attack in a vacuum and rely on remote updates that are up to 180 days behind the evolving threat. As Cyber is a heterogeneous Big Data challenge, these approaches are at a severe disadvantage in their ability to detect, predict or prevent APTs.

Because of the changing, amorphous nature of the threat, traditional approaches are doomed to fail.

TYPE OF SECURITY	LEADING VENDORS	KEY DATA SOURCES	USES ABOVE THE PROXY DATA
IDS and Firewall	Fortinet, Palo Alto Networks	Incoming traffic flow and requests	Limited
Endpoint Detection and Response (EDR)	Websense, Sophos, Blue Coat, FireEye	Internal endpoint traffic, point to point	No
Application and Network Performance	NetScout	Internal network and application traffic	No
SIEM	HP, Symantec, IBM	Alerts and event data (not packet-level)	Limited

© 2015 Atigeo All rights reserved Version # 10

APTs are asymmetric threats because they are specifically designed to circumvent traditional security solutions. They capitalize on the following disadvantages to increase the asymmetry between them and their target's security solutions:

APTs are designed to circumvent traditional security solutions.

- Visibility is limited to below the proxy data. Solutions lack visibility outside of the network, which is where attackers reside, making it difficult or impossible to characterize and identify the sources of attacks before they occur.
- Point solutions are highly prone to false positives and false negatives.
    - Threats are specifically designed to evade detection by navigating between the gaps of existing tools (IDS, EDR, SIEM, etc.). They do this by continually moving and evolving across traditional security boundaries[1]. This renders traditional security perimeters ineffective against APTs.
    - Point solutions are limited in their ability to integrate their insights across a uniform view. SIEMs are used to aggregate data; however, they lack the ability to find complex patterns across all of the solutions. Insights from SIEMs are further obscured by the overwhelming number of false positives and negatives.
    - Point solutions often require customer security policies which are difficult to continually update and contribute to an overwhelming amount of alerts, typically multiple orders of magnitude beyond that which can be effectively closed.
- Threat closure cycles that are spiraling out of control.
    - Policy- and rules-based security solutions lack the descriptive capability to describe APTs, which make detection difficult if not impossible. A static set of policies and signatures cannot identify polymorphic threats, i.e. threats that are designed to continuously change their form to avoid detection.
    - Further exacerbating this problem is that each enterprise has unique characteristics that require custom policies, integration and tuning to maintain the efficacy of each security solution. This requires the continuous attention of highly skilled security professionals and makes it very difficult to keep policies coordinated and up to date.

IT'S TIME FOR A NEW APPROACH

xPatterns for Cyber provides multi-vector and multi-spectrum lifecycle protection against zero-day and Advanced Persistent Threats (APTs) that transcends "signature-less" detection, with the

xPatterns for Cyber provides multi-vector and multi-spectrum lifecycle protection against zero-day and Advanced Persistent Threats.

[1] Traditional detection approaches suffer from combinatorial explosion

© 2015 Atigeo All rights reserved Version # 10

ability to infuse proven tradecraft into Internet security. xPatterns for Cyber not only provides a cyber "readiness" approach that evolves current cyber "hygiene" strategies, it also identifies and protects against threats that others miss. It reduces or eliminates key points of asymmetry between APTs, zero day attacks and recommends remediation for the enterprise. In addition to the specific cyber analytics models, xPatterns for Cyber is now the industry's first real intelligent system that self improves with human feedback to detect adversaries who are constantly changing their tactics. This unique ability is made possible through xPatterns' Cooperative Distributed Inferencing (CDI) engine, which learns over time and self-optimizes through a hybrid approach of maximizing hard rules and soft rules from heterogeneous sensors, both supervised and unsupervised.

xPatterns for Cyber is the industry's first real intelligent system that self improves with human feedback to detect adversaries who are constantly changing their tactics.

xPatterns for Cyber goes far beyond the scope of conventional cybersecurity solutions by offering the following features:

xPatterns for Cyber goes far beyond the scope of conventional cybersecurity solutions.

- True global insight
    - Incorporates data from above the proxy, Dark Web/Tor, social media, known APTs and other sources. These are the sources of data where adversaries leave information trails, conduct illegal transactions and plan attacks.
- Real-time, global cross-sectional deep analysis
    - Real-time, near-real-time, and forensic analysis across temporal, spatial, thematic (context) and semantic dimensions simultaneously. Processes terabytes per hour with payload transparency and deep analysis. This enables detection of threats that move and evolve across traditional security boundaries.
    - Reduces false positives by validating threats across critical signals.
- Dynamic rules and predictive models
    - Increases operator efficacy by five to ten times, by providing fast, intuitive insights into vulnerabilities of current policies of existing security solutions, enabling them to be updated effectively. Existing security assets and spend are fully leveraged.
    - Advanced predictive models that dynamically adapt and can identify complex polymorphic threats that evolve quickly.
    - Enables baseline *global and local network* operations to be described by soft, hard, and absolute rules, which are continuously and automatically updated by xPatterns.

© 2015 Atigeo All rights reserved Version # 10

- Auto remediation with xPatterns CDI engine
    - Ability to detect polymorphic threats and dynamic adversaries along with remediation actions
    - Leverages human inference sensor to allow users to provide absolute, hard and soft rules based on the review of the threat results and remediation actions
    - Given user feedback and rules, xPatterns CDI continuously optimize sub-sequent results
    - When ready, customer can turn on auto-remediation actions

XPATTERNS' FOUR CORE CAPABILITIES

xPatterns for Cyber empowers the enterprise by surfacing critical insights and remediation paths across four major capabilities:

- SenseMaking
- Horizon scanning
- Identity management
- Network and operations management

These capabilities are designed to minimize time to relevant insight and remediation, while providing deep insights across multiple, disparate internal and external sources. The workflow is designed to bridge strategy, tactics, and operations across the organizational hierarchy, from the CISO down to those working at the front lines. It has been tested, deployed, and validated at the United States Department of Defense and other government agencies.

xPatterns for Cyber surfaces critical insights and remediation paths across four major capabilities designed to minimize time to relevant insight and remediation, while providing deep insights across multiple, disparate internal and external sources.

SenseMaking

SenseMaking is a required capability for enterprises to understand the context of critical decision-making in complex, dynamic environments. xPatterns for Cyber is designed to provide a new level of SenseMaking by identifying anomalies and issues across disparate security systems, networks, external data sources, the Dark Web and enterprise data. The breadth and depth of these insights goes beyond traditional security to provide insight and alignment across all phases of portfolio management, impact analysis, situational understanding, and customer analytics.

xPatterns for Cyber is designed to provide a new level of SenseMaking by identifying anomalies and issues across disparate security systems, networks, external data sources, the Dark Web and enterprise data.

© 2015 Atigeo All rights reserved Version # 10

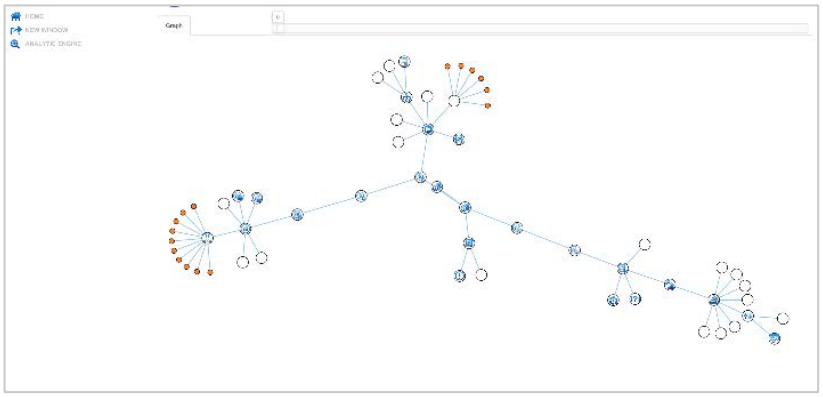

Figure 1: SenseMaking capabilities across network

Horizon Scanning

To predict threats, core capabilities must derive insights from multiple external sources. xPatterns' Horizon Scanning capability surfaces insights from social network and media sources to analyze data and social sentiments for indications and warnings about potential events. Horizon templates are available to capture megatrends in marketing, technology, science, and other fields.

xPatterns' Horizon Scanning surfaces insights from social network and media sources to analyze data and social sentiments for indications and warnings about potential events.

Figure 2: Horizon scanning across attack types

Identity Management

Identity Management is a critical capability for determining the source and methodology of threats. xPatterns for Cyber supports and monitors multiple data security chains to forecast future loss and operational impact, from external and insider threats. It also recommends interdiction and prevention of adversarial courses of action.

xPatterns for Cyber supports and monitors multiple data security chains to forecast future loss and operational impact, from external and insider threats.

© 2015 Atigeo All rights reserved Version # 10

Figure 3: Identity Management identifies strong and suspected links across complex entity relationships, spanning internal networks, Dark Web, and other sources

Network and Operations Management

Effective network and operations management is the foundation of detection and remediation. xPatterns for Cyber provides a cohesive picture empowering end users with situational awareness, pattern detection, and threat prediction. It is designed to provide effective and near-instantaneous insights into the following:

- Exfiltration monitoring and analysis – identifies exfiltration attempts and ongoing breaches in real time
- Blacklist and Dark Web cross-filters – integrates 3rd party and proprietary blacklists, simultaneously cross-filtering against key Dark Web activity
- Threat prediction analytics – global and local threat predictions

xPatterns for Cyber provides a cohesive picture empowering end users with situational awareness, pattern detection, and threat prediction.

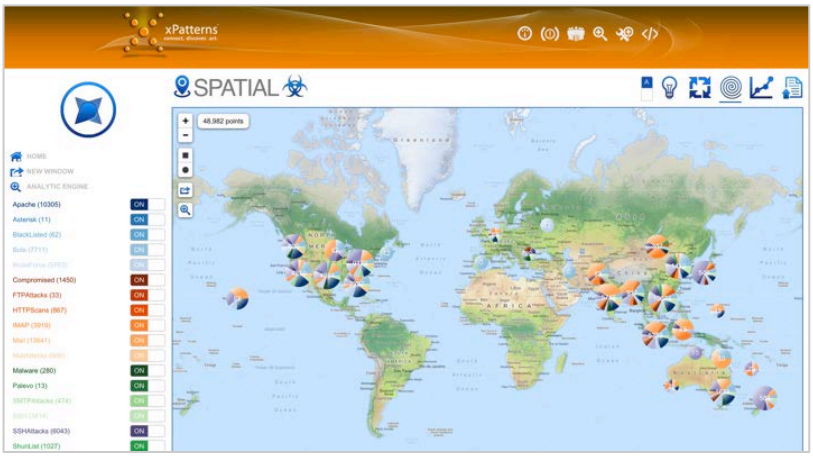

Figure 4: Network and Operations Management

© 2015 Atigeo All rights reserved Version # 10

CASE STUDIES

CASE STUDY 1: MULTINATIONAL CORPORATION LOCATED OVERSEAS

An organization located outside the United States had been relying on traditional point solutions; however, they were still suffering from severe security threats. It was increasingly clear the combination of these solutions were not providing them with adequate protection. Appliance fatigue and reliance on traditional signature detection were pinpointed as root causes of inadequate security.

The combination of traditional point solutions was not providing them with adequate protection.

Traditional vs. xPatterns for Cyber

Their security posture was based on the simple: "see something, do something" model. This meant if they saw something, they would:

- Identify that "something" as potentially malicious or not (average 6 hours per alert) at 26,000 alerts per hour.
- Analyze large volumes to isolate real threats and correctly identify them (additional 4 days)

Once identification was verified, to remediate the threat, they would:

- Develop a signature (2 hours) per signatures
- Test the signature (3 hours)
- Deploy the signature (at least 8 hours)

TASK	TRADITIONAL SOLUTION	XPATTERNS FOR CYBER
Total threats identified	26,323 in 4 days	Over 30,000
Time to identify alerts	6 hours	Milliseconds
Time to validate candidate	4 days	Milliseconds
Time to develop signature	2 hours	N/A

© 2015 Atigeo All rights reserved Version # 10

Time to test signature	3 hours	N/A
Remediation deployment	Weeks/Months	**Hours/days to implement remediation against single APT**
Total hours per signature	5 days	**Identified 12 APT threat vectors in milliseconds**

These metrics are from when the customer was performing at peak response times. Even at peak response capabilities, the attack vector would have been rotated out (obsolete), by the time the signature was implemented. The customer's threat lifecycle was measured in weeks, while attackers were executing within hours. This made their efforts effectively obsolete in the majority of cases. Point solutions were a source of vulnerabilities across the following dimensions:

- **Alerts overload** – Suffering from tickets/issues overload. They were generating 26,323 alerts per hour from packet flow monitoring, taxing their analysts with a never ending queue of isolation queries and this was set to increase over time.
- **Overwhelmed skilled analysts** - They simply had too few analysts to cover the number of potentially viable tickets/issues. At their closure rates and number of alerts, hundreds if not thousands of analysts were required. In addition, training could not keep up with attacks.
- **Obsolete closure rates over 100 times longer than the threat lifecycle** – Threats are able to penetrate and infiltrate within hours, far shorter than the current detection and remediation timeframe of days to weeks. This rendered defenses obsolete. The time and conversion of closure rates were getting worse, not better. Elongated workflows and closure rates were ideal for IT but not for cybersecurity.

The customer's threat lifecycle was measured in weeks, while attackers were executing within hours.

Point solutions were a source of vulnerabilities.

With xPatterns for Cyber

xPatterns for Cyber provided an autonomous response model, deploying models that are trained to identify likely sources of threats. xPatterns for Cyber discovered over 36,000 candidates to their 26,323, and isolated the 12 they should focus on in a few milliseconds. To save more time, we deployed a simple model that identified the number of distinct clients (by their IP addresses) visited by each machine in a day, and when the number of clients

© 2015 Atigeo All rights reserved Version # 10

exceeded a fixed number per day, an autonomous response would blacklist the IP address until it was investigated by an analyst.

Security operators quickly leveraged xPatterns for Cyber to establish a protocol for acceptable behavior and expected conduct on the network. When a machine steps outside of that range it is either blocked automatically or isolated and scrutinized to determine if it should be blocked. With xPatterns for Cyber, the customer's skilled analysts spent less time sifting through long lists of possible threats to determine their legitimacy and more time actually responding to the most critical threats.

In military terms, the customer was using obsolete WWI trench-warfare techniques to defend against sophisticated enemies employing asymmetric, low-intensity attacks. With the help of xPatterns for Cyber, the customer now has the agility to identify and neutralize the biggest threats in real-time.

With the help of xPatterns for Cyber, the customer now has the agility to identify and neutralize the biggest threats in real-time.

CASE STUDY 2: UNITED STATES DEPARTMENT OF DEFENSE

This organization inside the United States Department of Defense was looking to fuse their network operations with cyber operations through an effective tipping and cueing mechanism. The goal was to create a fused Cyber Common Operational Picture.

The solution was to deploy a Tier 0 platform that was able to take:

- SCCM feeds for CVE
- Netflow
- Data loss prevention
- Active scanning
- Real time packet capture

Before xPatterns for Cyber

The solution approaches they were considering would have required several months of work by teams of five to ten people to build, integrate, and test. During the long implementation period, the organization would have been subject to constant attacks potentially entailing massive losses.

© 2015 Atigeo All rights reserved Version # 10

With xPatterns for Cyber

By choosing xPatterns for Cyber, the customer was able to have protection in place in a matter of days, not months. xPatterns for Cyber immediately detected and neutralized threats that the customer was not aware of. The customer used the solution to analyze events and heterogeneous data, and was able to implement further defenses:

- Established a system to patch vulnerabilities based on priority ranking.
- Built a prediction model that identified patches that are likely candidates for upgrade up to one year in advance.
- Identify candidate devices using configuration management databases to prioritize trouble tickets for devices contributing to network latency.
- Correlate above-the-proxy threat intelligence with data loss prevention point solutions to rapidly homogenize and create policies at the edges of the network.
- Conduct in-situ analytics on data residing at the edge, obviating the need to pass large amounts of data to a central data lake; only lightweight analytic summaries are passed to the centralized hub.

By choosing xPatterns for Cyber, the customer was able to have protection in place in a matter of days, not months.

All told, the hub-and-spoke deployment saved the customer roughly 1,500 man-hours of implementation time and revealed previously unknown threats. Furthermore, xPatterns for Cyber delivered the benefits of a big data platform without the latency issues associated with massive ingestion. The result: a unified cyber operational picture that enhanced the organization's situational awareness.

xPatterns for Cyber delivered the benefits of a big data platform without the latency issues associated with massive ingestion.

CASE STUDY 3: HEALTHCARE ORGANIZATION WITH INTERSTATE PRESENCE

This massive healthcare organization inside the United States wanted to fuse their national network operations with cyber operations through the deployment of a cybersecurity solution. Their goal was to protect their patients and their brand with a prediction, protection, detection and remediation platform.

Before xPatterns for cyber

The organization had a nationwide network of hospitals and clinics and its IT infrastructure was highly vulnerable to cyber-attacks. The organization was in talks with providers of conventional cybersecurity solutions, but was discouraged by their high cost and long implementation time. In addition, the solutions they were

The organization was discouraged by the high cost and long implementation time of conventional cybersecurity solutions.

© 2015 Atigeo All rights reserved Version # 10

offered did not provide them with the ability to rapidly identify the most critical attacks and remediate them in real-time.

With xPatterns for Cyber

The customer turned to Atigeo to provide a unified situational awareness platform that would deliver comprehensive security intelligence while providing real-time updates to their newly formed Special Operations Center. The customer is now using xPatterns for Cyber to identify, prioritize, and respond to modern security threats. xPatterns for Cyber was configured to operate as a Tier 0 analytic hub with universal spokes, ingesting the following data:

- PCAP
- Wide-area network flow
- User reporting and trouble tickets
- Active Directory data
- Firewall activity
- Microsoft System Center Configuration Manager and Patch Management
- ITSM/Service Management
- Device and facilities data
- Network port data
- DHCP management
- External IP space
- Security information and event management (SIEM) data

With xPatterns for Cyber in place, the customer could rapidly surface previously undetectable events, prioritize signatures, and forecast unmatched and unmasked IP addresses. Once identified in real-time, these artifacts are passed to a SIEM tool for rapid payload inspection through its playback and transparency capabilities. Threats are channeled into a repeatable forensic capability for further automation and to close the response gap. Events that had previously gone undetected or had been lost in the flood of alerts were now surfaced, prioritized, and remediated. xPatterns for Cyber yielded:

- Effective time management and rapid forensic analysis of significant threats rather than an endless list of incidents needing to be reviewed.

Events that had previously gone undetected or had been lost in the flood of alerts were now surfaced, prioritized, and remediated.

© 2015 Atigeo All rights reserved Version # 10

- A flyaway team that was able capture PCAP locally for analysis at the hub to prioritize a national rollout strategy while reducing costs for a healthcare “extraprise” rollout.
- An effective threat intelligence team working deep in the Dark Web, zone fields, and social media to provide “left of bang” early warning and threat forecasting.
- A global cyber dashboard which included
    - A strong authentication and gradient-trust model for privileged users and access policies
    - A unified critical vulnerability and patch management strategy
    - Effective scanning and indicators of compromise response strategy
    - Round-the-clock monitoring of overall network effectiveness by instrumenting availability, performance, and quality to generate a “cyber scorecard”
    - A global high-value asset list that ensures proactive security practice and focused active and passive defense postures
    - Monthly privileged access reviews to reduce the impact of user error and insider threat
    - Daily above-the-proxy incident reviews for increased threat intelligence, situational awareness, and policy review

This massive N-tier hub-and-spoke deployment provided this national healthcare organization with a military-grade cyber defense at a far lower cost than conventional solutions. xPatterns for Cyber integrated existing point solutions, embracing and extending them through an effective Tier-0 integration methodology. This extended the life of the point solutions by turning them into active sensors for the effective defense of their patients and their brand.

SUMMARY

xPatterns for Cyber provides two major advantages:

1. It is an extensible and expandable security solution. It is powered by xPatterns, a complete big data analytics platform, proven in healthcare, finance and government. It can be easily deployed for additional advanced security applications, while leveraging best-in-class proprietary and open-source data science and engineering technologies. Atigeo frequently upgrades the xPatterns platform, providing a high-level of insurance against obsolescence.

xPatterns for Cyber is an extensible and expandable security solution powered by a complete big data analytics platform.

xPatterns for Cyber is easily deployed for advanced security applications while leveraging best-in-class proprietary and open-source data science and engineering technologies.

© 2015 Atigeo All rights reserved Version # 10

2. Ready-to-deploy cybersecurity-specific applications and workflow. We have taken our combined decades of experience in real-world warfare (counterterrorism, asymmetrical warfare) and cybersecurity (DoD, enterprise) to map a powerful, but generic big data platform to the key capabilities and workflow required for cybersecurity.

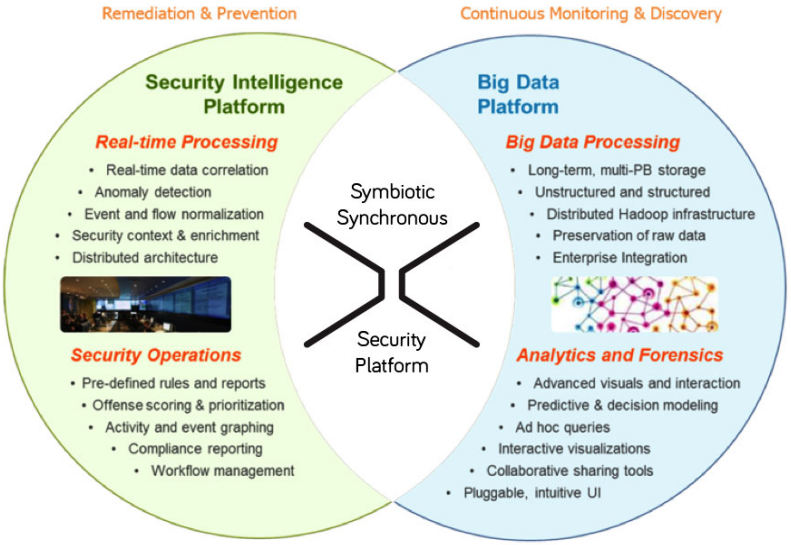

Figure 5: xPatterns for Cyber is based on xPatterns, a complete Big Data analytics platform that has proven at real-world, petabyte-scale deployments across healthcare, government, and financial applications

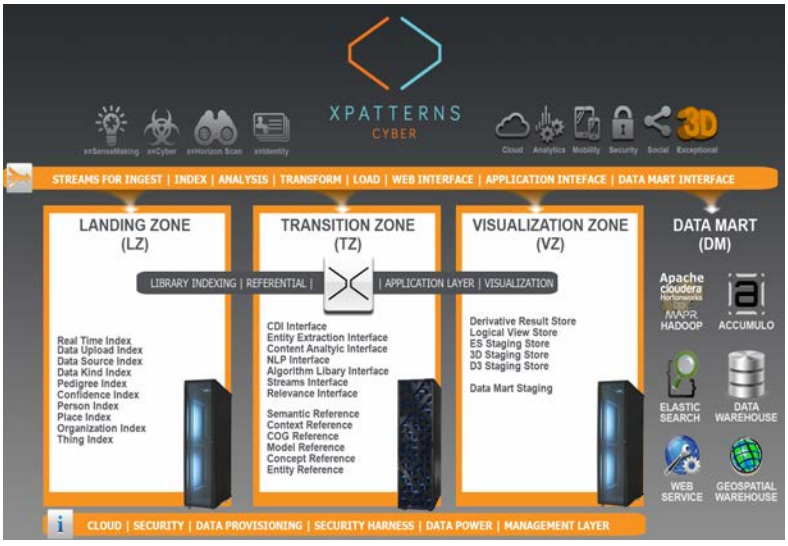

Figure 6: xPatterns for Cyber maps xPatterns big data analytics into a cybersecurity-specific workflow that embodies years of experience fighting against APT and zero-day security threats. This workflow and can be expanded with specialized applications through RESTful APIs.

xPatterns for Cyber offers ready-to-deploy cybersecurity-specific applications and workflow.

xPatterns for Cyber is based on xPatterns, a complete Big Data analytics platform that has proven at real-world, petabyte-scale deployments across healthcare, government, and financial applications.

© 2015 Atigeo All rights reserved Version # 10