Opinion Paper

Prescriptive Security Operations Centers (SOC)

Trusted partner for your **Digital Journey**

Atos

Executive overview

The pace of digital change will never be as slow as it is today as the digital economy will continue to speed up in the upcoming years, unleashing new digital disruptive innovations.

The digital transformation of businesses is growing exponentially because enterprises are attracted by the revenue growth it brings and by the opportunities for new business it generates. Yet, the success of this digital revolution will depend on how quickly and efficiently cyber security evolves to counter increasingly complex, rapid and aggressive threats and to safeguard natively insecure digital innovations.

While the digital revolution is pushing innovation forward, it's also causing the digital threat landscape to expand exponentially and new threats to emerge. It's clear that a shift in paradigm is needed in how to effectively manage cyber security. This is a shift from the traditional in-depth cyber security model based on multiple layers of protection to a new model based on **supercomputing and automation** that uses data to learn from past threats to interpret and prevent future attacks before they strike.

Today it takes on average 191 days[1] to detect data breach in an organisation's environment, reflecting the lack of necessary cyber security expertise, and of effective detection & response capabilities. In this time, vast amounts of information may already have been stolen and entire infrastructures infected and hacked.

In the constant struggle against time, **Prescriptive Security** compresses it, **making time work for organisations instead of against them.**

Prescriptive Security Operational Centers (SOC) will be the next generation SOCs that the digital economy needs in order to innovate securely & steadily. With Prescriptive SOCs, organizations will be able to effectively protect their business assets including valuable business data & customer personal data.

Prescriptive SOC will require **a technological change**, with the convergence of intelligence, big data & analytics- driven security that scrutinize all data generated in its environment, from IT to OT to IoT data. Cybersecurity will shift from a reactive& proactive model to a prescriptive model, focused on analysing analytics patterns in order to identity the next threats & automate the security control responses.

Prescriptive SOC will also require a **cultural change**, where security will need to change its processes to embrace automation & orchestration. As latest research estimates that over 1.8Million cybersecurity jobs will not be fulfilled due to a shortage of resources by 2020, Prescriptive SOC will alleviate this forecast by automating responses and allowing organizations' security experts to focus on advanced detection and threat hunting tasks. It will also introduce new cyber security roles such as Cybersecurity data scientists, to integrate statistical and mathematical models in the SOCs providing innovative mechanisms to detect future cyber-attacks.

[1]Ponemon Institute Cost of Data Breach 2017

Enabling Digital Business

"The companies that mastered digital transformation the best where the ones that integrated Security from the early beginning". This statement has been proven right by hundreds of successful programs and even more failed projects.

Not only Business is redefined – also security is going through the same process. Don´t make the mistake to adopt legacy security to secure digital business. You will need adaptive security framework that combines both conventional security solutions and new situational awareness security solutions to enable continuous security for your business.

By 2020, 60% of digital businesses will suffer major service failures Due to the inability to manage digital risk[2]

What do I need to do to secure the digital business?
We hear, on a daily basis, about data breaches, fraud and even companies pushed out of business due to cyberattacks. Organizations are aware that they need to secure their digital business, but are struggling to understand why certain technological choices are not working.

The road to secure digital transformation is by understanding how your future business should run and identify the security risks that could jeopardize this business. A lot of attacks will only be recognized by comparing the regular business process against the monitored processes. It is core to understand what is right, suspicious or malicious. We believe that organizations must adopt agile & adaptive security frameworks as the cybersecurity threat landscape will undeniably change and the security strategy will need to evolve accordingly.

Depending on the Security risks assessment results, organizations will need to invest in conventional security solutions as well as Security Data Analytics for traffic inspection and the recognition of normal and unusual behavior, with proper attention to the extended enterprise and the cloud.

Organizations will need to question the cybersecurity choices they made until today and will have to seek a 360° Security Visibility, moving further away from the implementation side by side of different security technologies with neither integration nor alignment.

Of course you monitor the cloud environment. But how do you best correlate information across hybrid environments?

You probably already manage an Identity and Access System, but how to build trust in Federated Identity systems with people logging in from various applications with various roles and IDs?

By enhancing the security of your digital business you enhance the security for your partners and their business. Cybersecurity is today a business differentiator and will become a vital business requirement as data protection regulations such as GDPR (General Data Protection Regulation) will go into force.

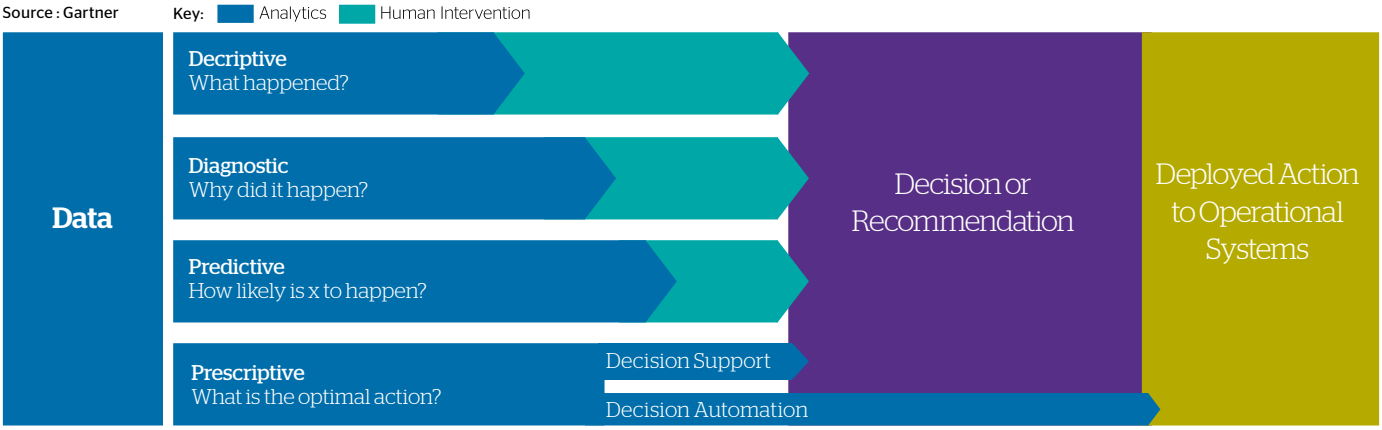
[2]Cybersecurity at the speed of Digital Business, Gartner, 2016

What is
Prescriptive Security?

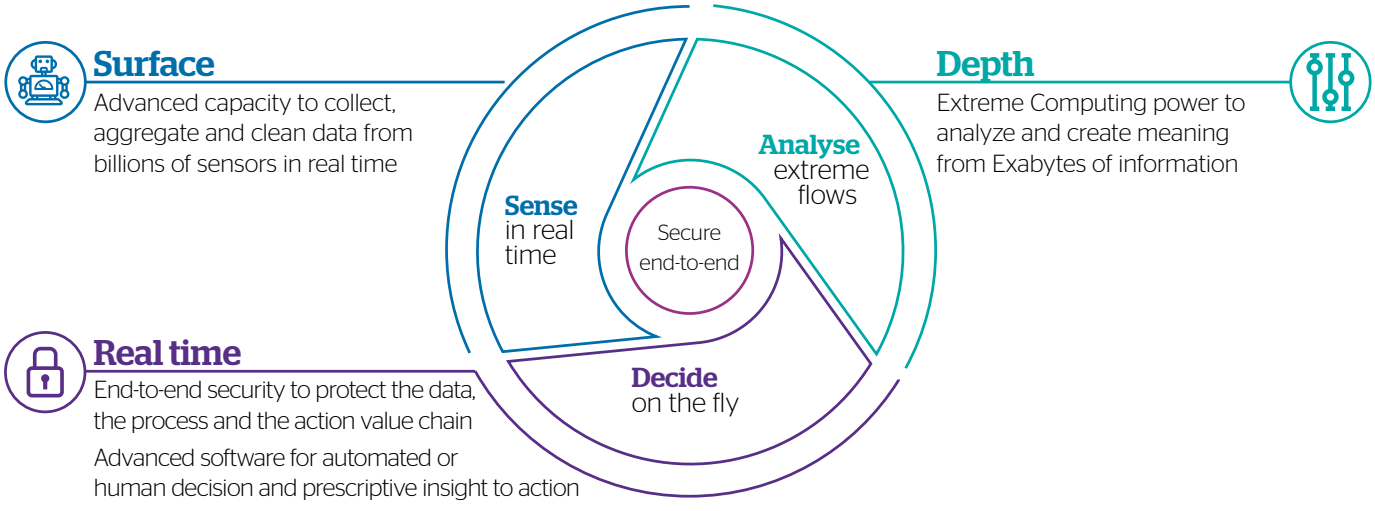
The digital revolution is ongoing, bringing massive changes, and unforeseen risks. Every day, we hear about massive breaches and we wonder whether they could have been preventable.

Prescriptive Security is exactly about that. Preventing breaches from happening, by leveraging big data & super computing capabilities. Prescriptive Analytics extends beyond predictive analytics by specifying both the actions necessary to achieve predicted outcomes, and the interrelated effects of each decision. It allows taking action quickly for a self-adaptive security

Analytics from Decription to Prescription



Prescriptive Security



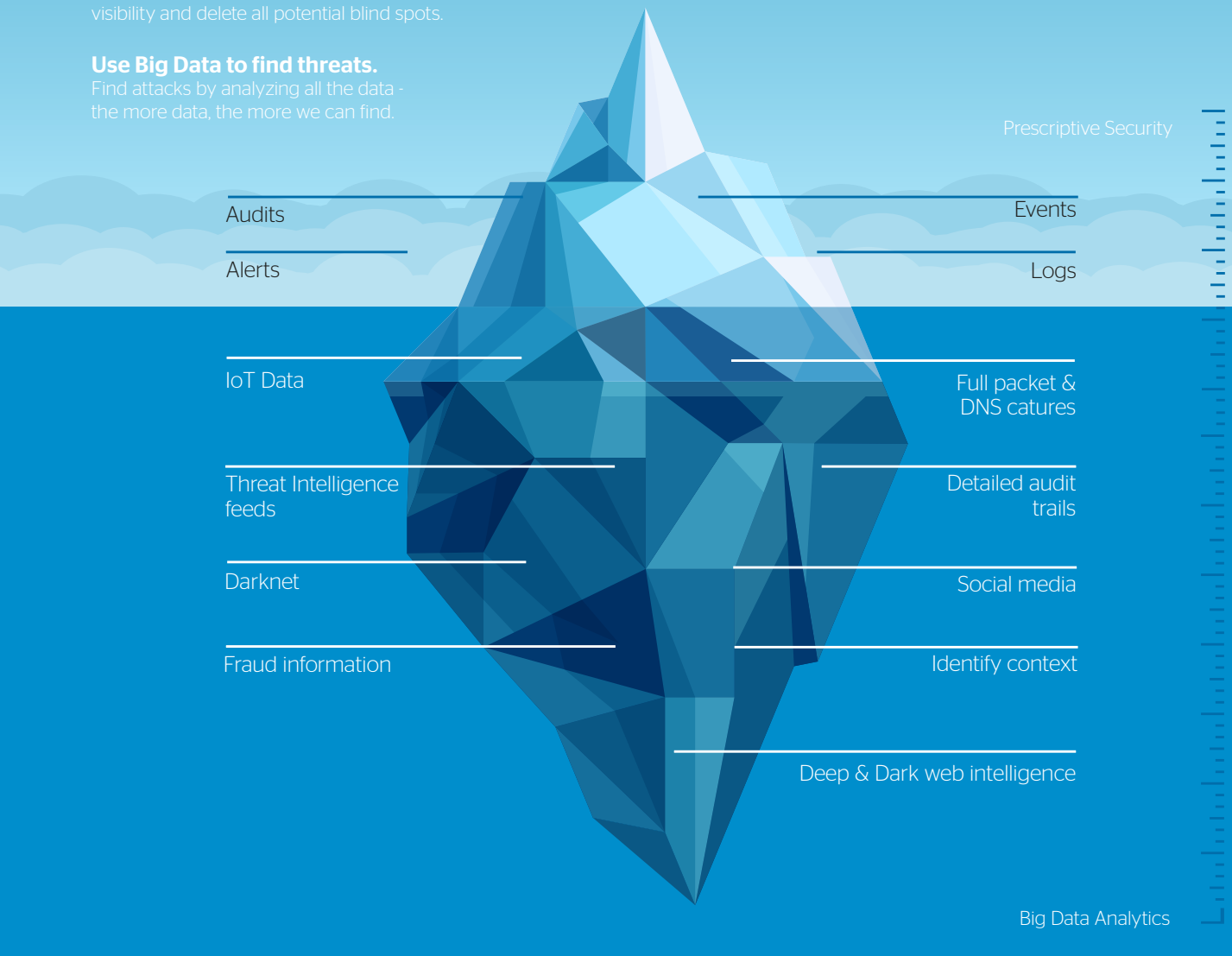
New prescriptive security model

Security has been focused on the tip of the iceberg, focusing on detection & monitoring of specific IT environment of the organizations and waiting for breach attempts to happen.

This approach is prone to error as cyberattacks could originate in none-monitored environments & work their way to the sensitive business assets. It can be easily bypassed as it is based on assumptions & correlation rules.

To win the race against time (detection & response times) Prescriptive security won't look at the tip of the iceberg, but rather leverage big data & machine learning analytics to utilize all data generated everywhere within the organization (as an extended enterprise) and outside the organization, in order to bring 360° security visibility and delete all potential blind spots.

Use Big Data to find threats.
Find attacks by analyzing all the data - the more data, the more we can find.



Why prescriptive SOC is vital for the success of the digital transformation

How would you need less than Prescriptive Security for keeping your assets safe?

Over 3 billion records were publicly leaked in 2016[3], putting in danger sensitive data and raising legitimate questions about the safety of the digital revolution and undermining trusted relationships with customers, partners and stakeholder.

In 2016 87%[4] of organizations reported to suffer at least one cyberattack, yet we believe that cyber threats will continue to grow in size, frequency, and complexity, leading to cybercrime annual costs peaking at 6 Trillion US$ by 2021.

As the digital threat landscape continue to expand exponentially and new threats to emerge, we believe that a shift in cybersecurity paradigm is necessary to move from the traditional in-depth security model based on multiple protection layers to self-adaptive security based raw computational power & automation.

We are building the next generation of Security Operation Centers (SOC) with our Prescriptive SOC services, bringing together predictive security and automation—powered by supercomputing.

Prescriptive SOC services detect more persistent, weaker signal malicious activity by means of behavioral and predictive analytics. But it does not stop there.

The Prescriptive SOC instructs the security components in the adaptive environment controlled by it to adapt and recover from threats; they are put to contribution to hunt for threats upon their detection and then guided through elimination of those.

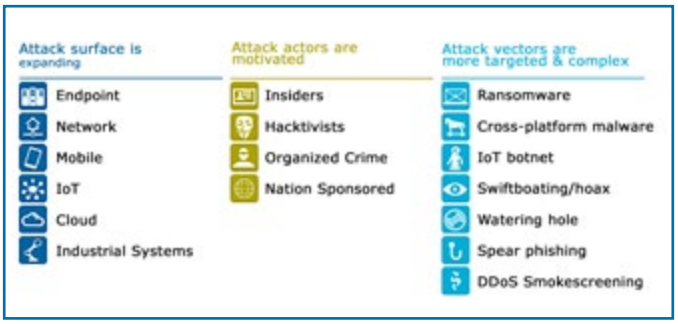
Prescriptive SOC to face the ever evolving Threat landscape

It is no secret that the threat landscape has been increasing exponentially as the adoption of new technologies such as IoT , Big Data, Cloud computing are expanding the attack surface and cybercriminals are becoming more organized.

In one Quarter, over 18 Million new malware samples are captured, with zero-day exploits expected to rise from one-per-week in 2015 to one-per-day by 2021.

It is a race against complexity & time and organizations' best option is to proactive hunt for threats, identifying vulnerabilities in their environment before the cybercriminals.

Threat Intelligence will need to cover the entire attack surface & attack vectors, and organizations will need to watch & hunt for OT, IT & IoT threats. By integrating such threat intelligence capabilities in Prescriptive SOC, threat intelligence is no longer a separate technology watch process managed through alert bulletins, but an integrated part of the SOC where Threat intelligence Feeds give actionable risk scorings and allow to detect unknown threats before they reach the organizations.



[3] IT Governance UK December 2016 report
[4] Bitglass Threats Below the Surface Report April 2017 Report

Prescriptive SOC to optimize cybersecurity resources

Cybersecurity professionals in all organizations are facing an increasing volume of cyberattacks. Cyberattacks that are not only growing in volume, but also in complexity & pervasiveness. Add to that, the shortage of security resources which is expected to grow year on year and reach a gap of 1.8 Million security experts by 2022. Organizations will then have to counter an increasing volume of cyber-attacks with a limited number of resources.

Prescriptive SOC by introducing artificial intelligence and automatic response will optimize the usage of cybersecurity professionals who will now be able to automate response to common cyberattacks, and focus on the more complex & persistent ones.

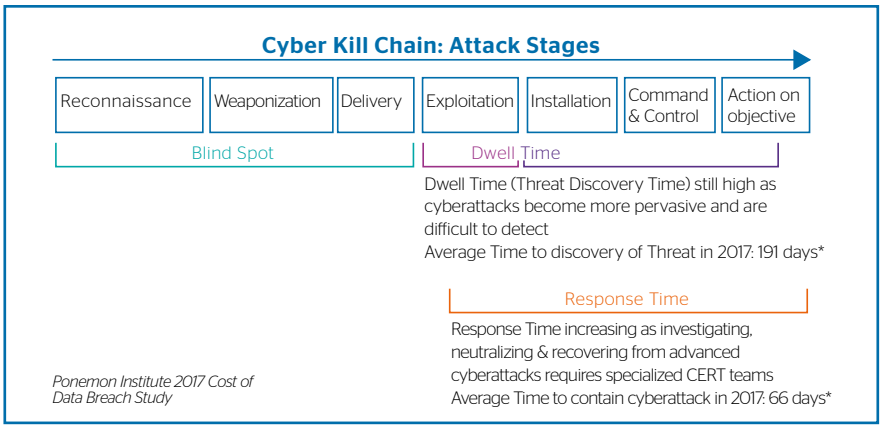
Prescriptive SOC to reduce dwell time & response time

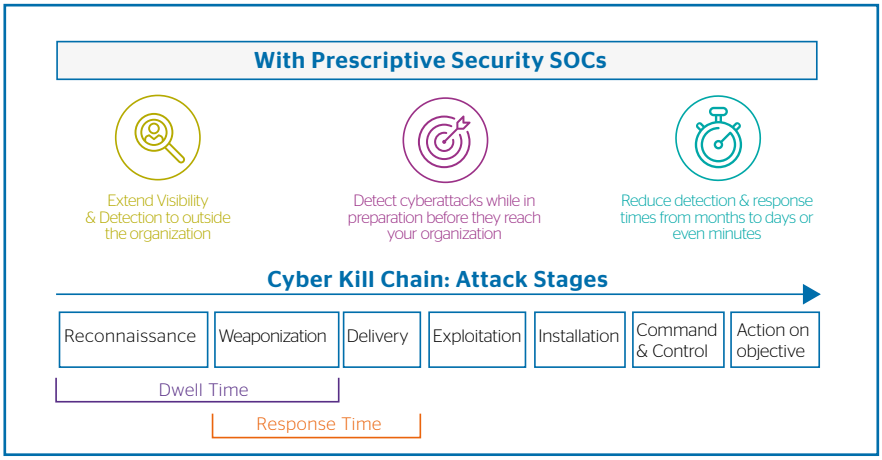
Time is on the side of the adversary. An adversary that's patient, persistent and creative. We're fighting against human ingenuity and attackers aren't playing by the same rules as we are. The Cyber Kill chain illustrates how organized cyberattacks are started with reconnaissance phase where cybercriminals extensively research and harvest information on targeted victim to the action on objective phase where cybercriminals take actions to achieve their objectives, by collecting data, encrypting and extracting information from the victim environment, etc.

The Dwell time has been increasing steadily in the past years, as cyberattacks become more pervasive and complicate the detection of compromise. The response time has been increasing as well, especially the associated costs to recovery.

Only Prescriptive SOC, can change the current operational models of protection, detection& response in order to considerably reduce the dwell time and improve the response time with the adoption of Threat hunting, Threat intelligence, machine learning & response automation.

Instead of thinking in the days and months it takes to detect and correct threats, with Prescriptive SOC, we can neutralize in real-time emerging threats and prevent future attacks from breaching systems in the same way.





Prescriptive SOC:
Building the Next Generation SOC

Security Operation Centers will need to undergo in-depth transformation in order to implement Prescriptive Security Analytics. This transformation will require

Analytics and machine learing

We can reduce cybercrime by using supercomputing to learn from historical data and putting algorithms in place in response to this learning. A data lake powered by high performance storage and analytics software makes it possible to collect, aggregate and access high volumes of data. Prescriptive Security analytics integrate all key elements in the environment (from the Internet of Things, operational technology and information technology) and leverage threat intelligence gathered outside the organisation (surface web, the dark and deep web, social media and partners' feeds) to proactively block upcoming cyberattacks.

Optimized human resources

Prescriptive Security can optimise an organisation's cyber security resources and free them from spending valuable time detecting threats and then acting on them. This means that cyber security teams can focus their resources where most needed.

Automation

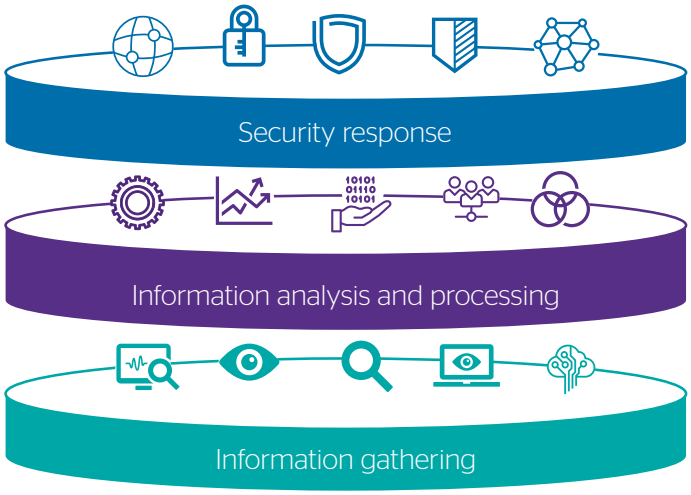
When threats are detected, a response must be instant. Prescriptive Security minimises the need for human intervention by using automation to expedite a clean-up, not only resolving the threats but also analysing their root causes and protecting against them in future. Automation means resolution happens faster and more efficiently, freeing up resources.

People, organisation and operations

State of the art Security Operations model within Atos can be represented as a Control Tower where data gathering is the foundation above which sit the many exploitation, analysis and processing techniques which allow the identifications and response to the security threats.

Centralized location for IT security assessment, processing and response

Operations
Cyber analysts and experts
Threat analysis
Advanced correlation
Business intelligence
Behavioral analysis
Statistical analytics
Network and building monitoring
IS crisis coordination
Security awareness
R&D
Security information and events management



Services
Cyber defence
Cyberwarfare
Incident response
Offensive security
Compliance monitoring
Information analysis reports
Digital forensics
Data leak protection

Information
IT/OT logs
Network raw data
Threat intelligence
VOIP
DB
SCADA
Vulnerability assessment
Antivirus
GRC
CCTV

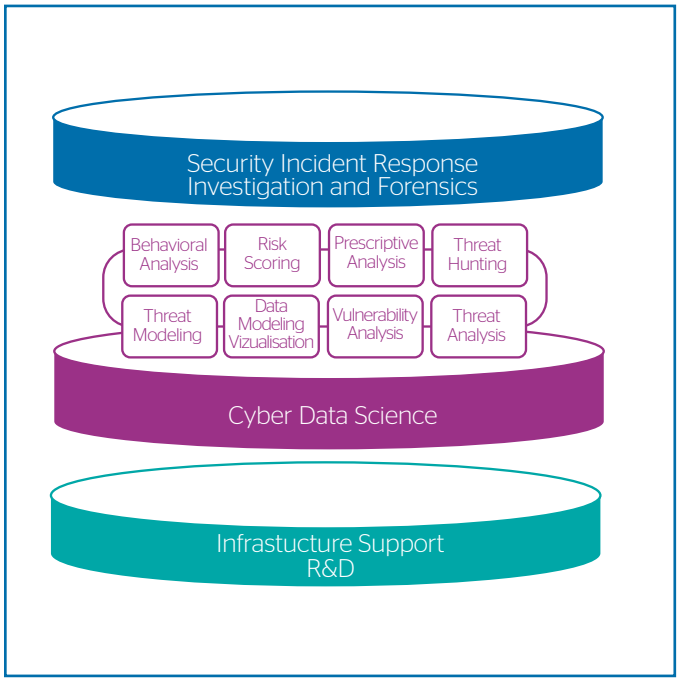
The central use of Big Data Analytics, Machine learning and threat models in the toolset of Prescriptive SOC makes the Information analysis and processing layer reliant on highly qualified personnel to run and maintain these. In fact, the Big Data & Analytics tools alone or misused can be ineffective ; for instance, they can produce false negatives while generating for your already challenged SOC more workload from processing their false positives.

The cyber data scientists play an essential role in making this toolset efficient in the mission that it has been designed for – detecting and rapidly responding to security threats. The data scientists will apply their expertise in many areas:

- The Data scientists will have to do the governance of the production models. That means that they have to put in place a process to continuously evaluate the models' performances in order to do an update when needed.
- They need to create custom visualizations or data queries to a detection scenario specific to businesses, assets or threat vectors.
- They will have to communicate the result and collaborate with non-data scientists experts

Depending on the data feed and the function, the cyber data scientists are in turn Vulnerability analysts, Threat analysts, Event and Incident Analysts, Investigation analysts, Malware Analysts and Threat hunters. Backed by infrastructure teams and by the R&D departments, they keep the Prescriptive system at its best performance.

Looking at it from the human resourcing challenge perspective, the more sophisticated and fine grained the diagnosis is, the higher expertise is required to qualify the results, maintain the system and continously improve and supervise the system underlying intelligence. Expert staff is limited and time to build staff skills and experience is longer than the time it is getting to push their limits. Regulations are making it more difficult as, in some instances, they dictate specific accreditations and nationalities. This is where an important role is played by Prescriptive security in handling this challenge. By automating and speeding many of the response operations, the SOC staff , upskilled and properly trained, is available and capable of taking on the data science functions backed with the right Big Data & Analytics Subject Matter Experts.

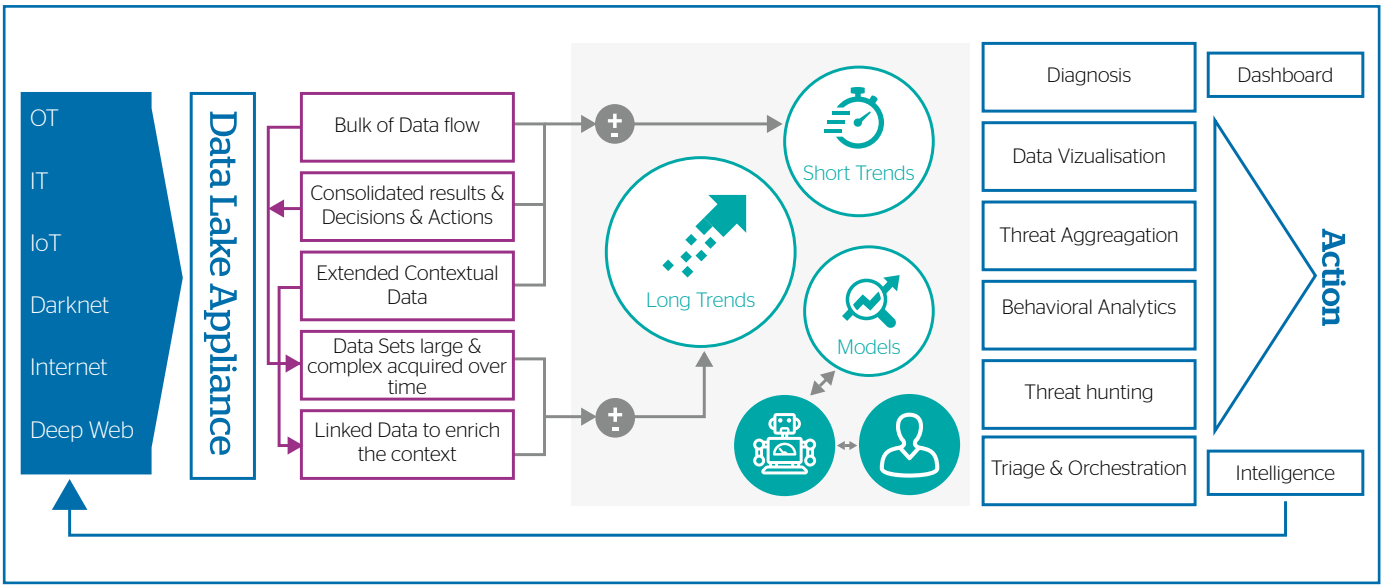


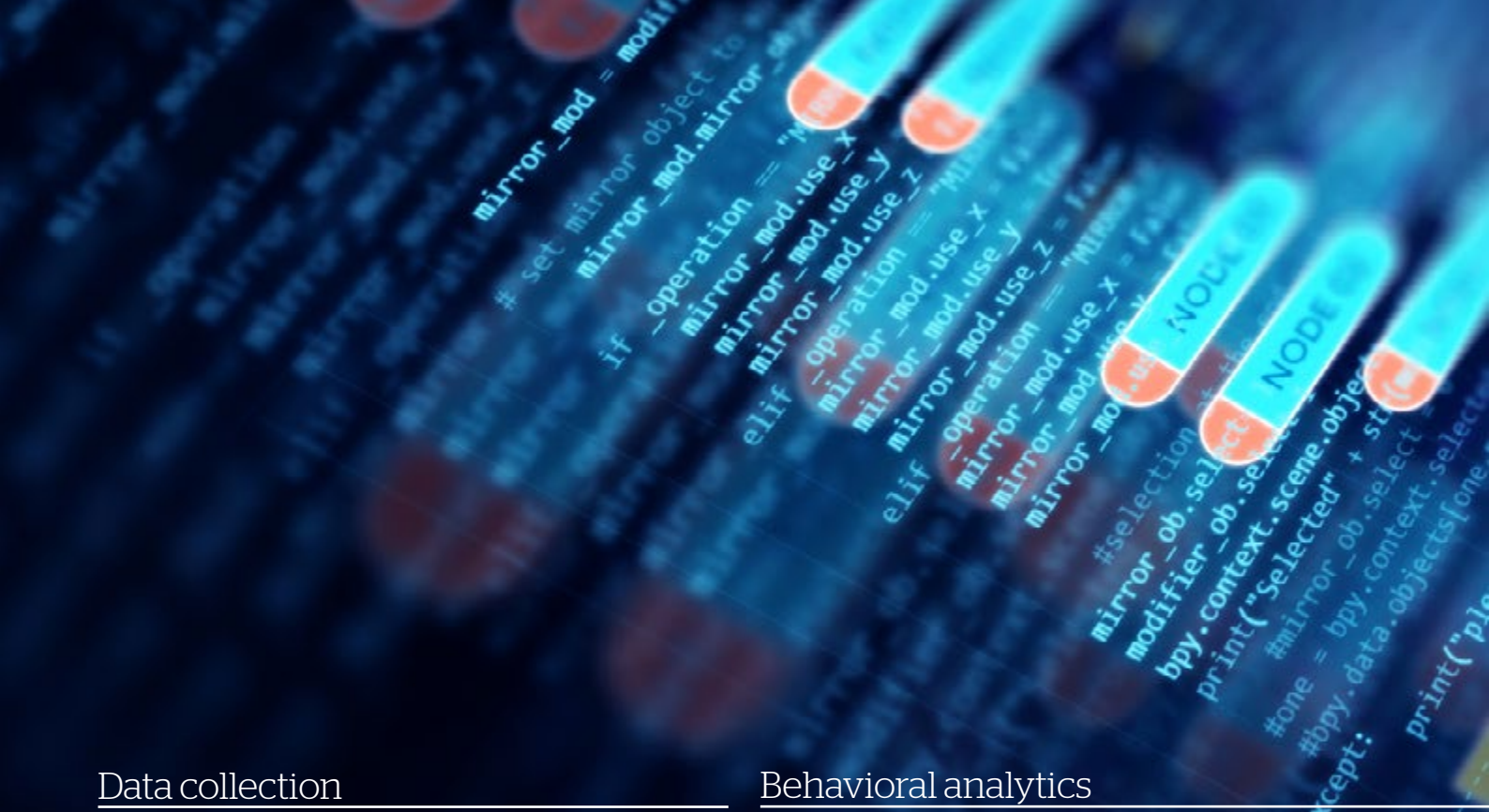
Big Data Analytics
for the success of the digital transformation

Prescriptive Security pushes forward the limits of a tri-dimensional paradigm. It needs to increase detection surface, velocity and decrease reaction time. By using Big Data Analytics and super computing systems, it also effectively optimizes the cost factor

- Increase detection surface (volume and variety) and velocity of Decision
  - Big Data Analytics increases the speed of apprehension and reaction by detecting attacks in early stages and speeding the decision.
- Reduce cost of storage and compute power needed for Cyber Security in the New Age (90% of the data is less than two years old)
  - Increased performance of single boxes and taking advantage of flexible parallel distributed computing
- Reduce cost of man-power

Powered by Atos Big data and McAfee technologies, Prescriptive Security relies on high performance Analytics to implement 360° visibility of the environment, Active Real-time Response capabilities for immediate propagation of threat indication throughout the environment end-points, network devices and applications, and for orchestrating the prescriptive response as it gets executed.





Data collection

Atos Data Lake allows to collect, store on a vast storage space, as well as compute, distribute and analyze data using an industrialized analytics software suite, validated and pre-integrated on an appliance with Hadoop distribution.

Data vizualization

Security analysts and Threat analysts are presented with a graphical perspective that deeply enhances the brain capacity to get the underlying and relevant data. Access to full and aggregated context data timely speeds and augments the accuracy of the event qualification thus reducing dramatically the false positives and negatives. Security Compliance and Risk Managers, have the ability to access advanced dashboards displaying the KPIs they need to measure the security posture of their environment and to measure the effectiveness of the implemented security controls.

Investigation analysts are presented with powerful ground for forensics, and ability to filter and seek data to know what happens in real time or at a specific time frame Geo positioning contextualizes the analytics and visualization experience to provide an unmatched perspective on the posture of the environment sites, behavior of the user populations or the profiling of offenders.

Threat aggregation

Prescriptive Security looks at threats holistically. Its foundational Data Lake powered by high performance Bullion storage and Analytics software makes it possible to collect, aggregate and access high volumes of threat intelligence concerning the IT, OT and IoT, structured and structured, external (feeds, social media, dark and deep web..) and internally produced by the security active components on the network (endpoint, network and application side security devices).

This data is aggregated and transformed into actionable intelligence by populating an aggregated Intelligence repository, distributing qualified intelligence and enabling Active Response

Behavioral analytics

Data Lake Analytics with 3rd party software allow making sense of machine data, sensors data, structured and unstructured data. This broad data collection combined with batch and real time processing using Machine learning and modeling of hundreds of threat scenarios allows detecting, measuring and scoping anomalies. Integration of such detection and scoring with the SIEM provides the SOC with a unified risk view to prioritize and qualify the anomalies. Drill down capabilities to investigate the anomalies with the exact combinations of behaviors and profiles is then available to further act on the event till its resolution

Threat hunting

With nearly unlimited retention of logs and events, it is made possible to hunt in historic data for newly discovered and characterized threats. Prescriptive Security Operations Center use Data Lake Analytics to continuously searches for Indicators from different sources making even years' long persistent attacks possible to trace. Real time threat hunting is also made possible with the McAfee Data Exchange layer which wraps newly detected indicators and sends them to the active security components on the network to trace down and act upon affected systems

How do we manage the change?

As detailed through this paper, the adoption of Prescriptive Security Operation Centers will require organizational, technological & cultural changes.

Powering the prescriptive SOC with Big Data capabilities, automation & orchestration, enables organizations to proactively protect their business, preventing attacks from happening, containing pervasive attacks and even hunting for threats before they become cyberattacks.

Keeping up with the disruptive innovations is a challenge, securing the associated digital businesses is even more difficult. With Prescriptive SOC, organizations will be able to implement effective cyber security measures that protect them against the threats of tomorrow.

Scalability

Big Data Capabilities

Machine Learning

Data Visualization

One Platform for all Services

Talk with
our experts

Farah Rigal
Global SOC Transformation
Program Director

Thomas Erben
Global Cybersecurity
Portfolio Director

Zeina Zakhour
Global CTO
Atos cybersecurity

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, TelecommunicationsTransportation.
The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
ascent.atos.net

Let's start a discussion together

For more information: **marketing@atos.net**

CT_170629_SKR_ATD_Opinion Paper