Executive overview

The pace of digital change will never be as slow as it is today as the digital economy will continue to accelerate in the coming years, unleashing new digital disruptive innovations. Be prepared!

The digital transformation of businesses is growing exponentially because enterprises are attracted by the associated revenue growth, 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 to effectively manage cyber security going forward, a paradigm shift is needed. This will be 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\textsuperscript{1} to detect data breach in an organization’s environment, reflecting the lack of necessary cyber security expertise, and of effective detection and 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 organizations instead of against them.

Prescriptive Security Operations Centers (SoC\textsuperscript{2}) will be the next generation SOCs that the digital economy needs in order to innovate securely and steadily. With Prescriptive SOCs, organizations will be able to effectively protect their business assets including valuable business data and customer personal data.

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

The Prescriptive SOC will also require a cultural change in the security organizations to change its processes to embrace automation and orchestration. As latest research estimates that by (2022) over 1.8 million cyber security jobs will remain unfilled due to a shortage of resources. Prescriptive SOC will alleviate this forecast shortfall 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 cyber security data scientists, to integrate statistical and mathematical models in the SOCs providing innovative mechanisms to detect future cyber attacks.

---

\textsuperscript{1} Ponemon Institute Cost of Data Breach source

---

\textsuperscript{2} Prescriptive Security Operations Centers
Enabling Digital Business

“The companies that mastered digital transformation the best were those that integrated Security from the early beginning”.

This statement has been proven by hundreds of successful programmes and even more by those that failed.

Today both businesses and security itself are being redefined. Don’t make the mistake of applying adopt legacy security solutions to secure digital business. Business will need an adaptive security framework that combines conventional security solutions with new situational awareness security solutions to enable continuous security for your business.

By 2020, at least one major safety incident will be caused by an IT security failure, leading to significant injury².

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 cyber attacks. 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 to understand how your future business should run and identify the security risks that could jeopardize an optimum model. Many attacks will only be recognized by comparing the regular business process against the actual, on going processes: it is core to understand what is right, suspicious or malicious. We believe that organizations must adopt agile and adaptive security frameworks as the cyber security threat landscape will continue to 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 (hybrid, private, public).

Organizations will need to challenge the cyber security choices they made to date and to seek a 360° Security Visibility, moving further away from the implementation 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?

By enhancing the security of your digital business you enhance the security for your partners and their business. Cyber security 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 Gartner source
Prescriptive Security Operations Centers
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 and supercomputing 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 enables taking action quickly for self-adaptive security.

Analytics from Description to Prescription

<table>
<thead>
<tr>
<th>Data</th>
<th>Key</th>
<th>Analytics</th>
<th>Human Intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptive</td>
<td>What happened?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Why did it happen?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Predictive</td>
<td>How likely is it to happen?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prescriptive</td>
<td>What is the optimal action?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Deployed Action to Operational Systems

Decision or Recommendation

Decision Support

Decision Automation

Prescriptive Security

Surface

Advanced capacity to collect, aggregate and clean data from billions of sensors in real time

Real time

End-to-end security to protect the data, the process and the action value chain

Depth

Analyze extreme flows

Secure end-to-end

Secure extreme flows

Advanced software for automated or human decision and prescriptive insight to action

End-to-end security to protect the data, the process and the action value chain

Sense in real time

Decide on the fly

Extreme computing power to analyze and create meaning from Exabytes of information

Source: Gartner
Security has been focused on the tip of the iceberg, focusing on detection and monitoring of the IT environment, waiting for breaches to happen.

This approach is prone to error as cyber attacks could originate in un-monitored environments and work their way to the sensitive business assets. It can be easily bypassed as it is based on assumptions and correlation rules.

To win the race against (detection and response) time, Prescriptive Security leverages big data and machine learning analytics to utilize all data generated everywhere within the organization (as an extended enterprise) and outside the organization, to bring 360° security visibility and cover 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

85 percent of organizations acknowledged they were unable to identify anomalous behavior across cloud applications.³

We believe that a shift in cyber security paradigm is necessary to move from the traditional in-depth security model of multiple layers of protection to self-adaptive security based on raw computational power and automation.

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 cyber criminals are becoming more organized.

In one quarter, over 18 million new malware samples were 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 and time. An organizations’ best option is to proactively hunt for threats, identifying the vulnerabilities in their environment before the cyber criminals do.

Threat Intelligence will need to cover the entire attack surface and attack vectors, and organizations will need to watch and hunt for OT, IT and 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 enable the detection of unknown threats before they reach the organization.

The Threat Landscape is continuously changing (it’s a race against complexity & time)

<table>
<thead>
<tr>
<th>Attack surface is expanding</th>
<th>Attack actors are motivated</th>
<th>Attack vectors are more targeted &amp; complex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>Insiders</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Network</td>
<td>Hacktivists</td>
<td>Cross-platform malware</td>
</tr>
<tr>
<td>Mobile</td>
<td>Organized Crime</td>
<td>IoT botnet</td>
</tr>
<tr>
<td>IoT</td>
<td>Nation Sponsored</td>
<td>Cryptojacking</td>
</tr>
<tr>
<td>Cloud</td>
<td></td>
<td>Watering hole</td>
</tr>
<tr>
<td>Industrial Systems</td>
<td></td>
<td>Spear phishing/ whaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DDoS Smokescreening</td>
</tr>
</tbody>
</table>

³ Bitglass Report: Less than half of enterprise have visibility into external sharing, DLP policy violation in the cloud
Prescriptive SOC to optimize cyber security resources

Cyber security professionals in all organizations are facing an increasing volume of cyber attacks. Cyber attacks that are not only growing in volume, but also in complexity and pervasiveness. Add to that the shortage of security resources which is expected to grow year on year and reach a gap of 18 million security experts by 2021. Organizations will then have to counter an increasing volume of cyber attacks with a limited number of resources.

By introducing artificial intelligence and automatic Responses, Prescriptive SOCs will reduce the raw requirement for, and optimize usage of cyber security professionals who will be able to automate response to common cyber attacks, and focus on the more complex and persistent ones.

Prescriptive SOC to reduce dwell time and 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 cyber attacks start with reconnaissance phase where cyber criminals extensively research and harvest information on the targeted victim to the objective phase where cyber criminals 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 cyber attacks become more pervasive and complicate the detection of compromise. The response time has been increasing as well, together with the associated costs to recovery.

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

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

By introducing artificial intelligence and automatic Responses, Prescriptive SOCs will reduce the raw requirement for, and optimize usage of cyber security professionals who will be able to automate response to common cyber attacks, and focus on the more complex and persistent ones.

Prescriptive Security Operations Centers
Prescriptive SOC
Building the Next Generation SOC

Security Operations Centers will need to undergo in-depth transformation in order to implement Prescriptive Security Analytics. This transformation will require: The central use of Big Data Analytics, Machine Learning and threat models in the toolset of Prescriptive SOC’s.

**Analytics and machine learning**
We can reduce cyber crime 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 organization (surface web, the dark and deep web, social media and partners’ feeds) to proactively block upcoming cyber attacks.

**Optimized human resources**
Prescriptive Security can optimise an organization’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 minimizes the need for human intervention by using automation to expedite a clean-up, not only resolving the threats but also analyzing their root causes and protecting against them in future. Automation means resolution happens faster and more efficiently, freeing up resources.

**People, organization and operations**
State of the art Security Operations model within Atos can be represented as a Control Tower where data gathering is the foundation upon which sit the many exploitation, analysis and processing techniques which allow the identification 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 event management

**Services**
- Cyber defence
- Cyber warfare
- 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

---

Prescriptive Security Operations Centers
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 and Analytics tools alone or misused can be ineffective. For instance, they can produce false negatives 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 undertake the governance of the production models. That means that they have to put in place a process to continuously evaluate the models’ performances and apply refinements 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 optimum performance.

Looking at it from the human resourcing challenge perspective, the more sophisticated and fine grained the diagnosis, the higher the expertise required to qualify the results, maintain the system and continuously improve and supervise the system’s underlying intelligence. Expert resources are limited and time to build skills and experience is longer than the time it is taking to push them to 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, are available and capable of taking on the data science functions backed with the right Big Data and Analytics Subject Matter Experts.
Big Data Analytics
Enabling successful digital transformation

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

The concrete advantages

- 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 the numbers and thence 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, endpoints, network devices and applications and for orchestrating the execution of the prescriptive response.

Security Operations Centers need to adopt new and advanced tools to process the increasing volume of data and to detect and mitigate cyber-attacks.

Data visualization

Security analysts and Threat analysts are presented with a graphical perspective that deeply enhances the brain’s capacity to identify the underlying and relevant data. Timely access to full and aggregated context data speeds and augments the accuracy of the event qualification thus reducing dramatically both 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 see 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.

Data collection

Atos Data Lake allows the collection and storage 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.
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 unstructured, 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).

These data are 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 enable 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 scoring 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 are available to further act on the event until 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 search 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.

Prescriptive Security
How do we manage the change?

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

Powering the Prescriptive SOC with Big Data capabilities, automation and orchestration will enable organizations to proactively protect their businesses, preventing attacks from happening, containing pervasive attacks and even hunting for threats before they become cyber attacks.

Keeping up with 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 Cyber Security Portfolio Director

**Zeina Zakhour**  
Global CTO  
Atos Cyber Security
About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 73 countries and annual revenue of around €13 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, Telecommunications and Transportation. 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

Let’s start a discussion together