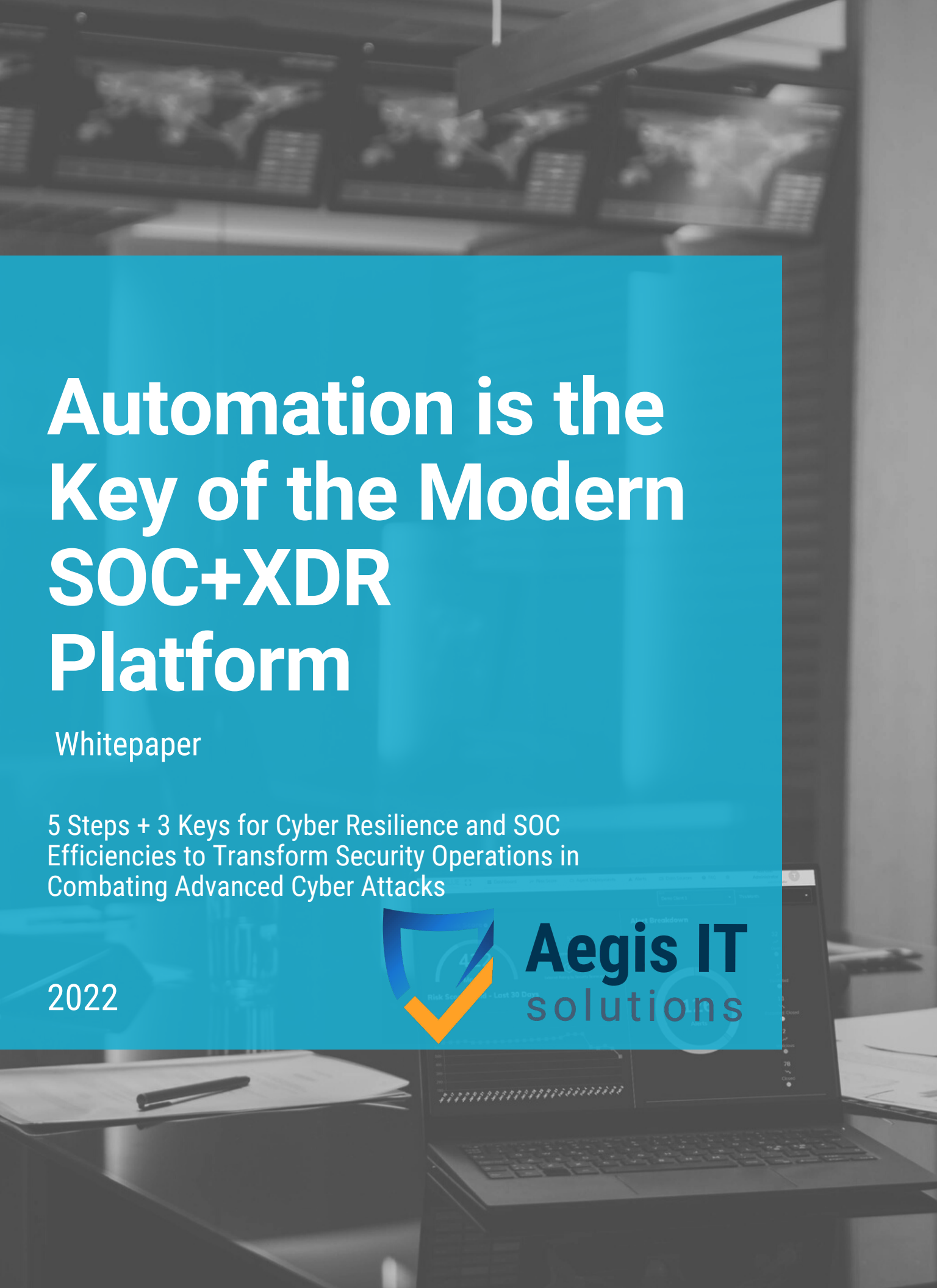


Automation is the Key of the Modern SOC+XDR Platform

Whitepaper

5 Steps + 3 Keys for Cyber Resilience and SOC Efficiencies to Transform Security Operations in Combating Advanced Cyber Attacks

Aegis IT solutions

2022

TABLE OF CONTENTS

A New Generation of Global Disruption

Digital trends and the exponential proliferation of cyber threats resulting from the COVID-19 pandemic has thrust global businesses into a new generation of global disruption. The paralyzing consequences from the increasing cyber-attacks on the economic services, infrastructure and critical services show no signs of slowing down. We only have to look at the 2021 Colonial Pipeline Ransomware attack to see the extent of damage and disruption such attacks can cause.

With the rapid digital transformation that is shaping the economic future, criminal groups, hackers, hacktivists, and rogue governments have become more sophisticated with their advanced methods and tools. Cybercriminals will use highly sophisticated malware that can be hidden inside legitimate software updates. This will not only allow attackers to infiltrate systems to access sensitive data but also spread the malware across every industry including individuals.

Never before have businesses around the global network been faced with such damaging cyber incidents and cybercrimes, costing an estimated $6 trillion in 2021 and is expected to reach $10.5 trillion by 2025. Experts predict that the threat of cyber-attacks on critical infrastructure is imminent which will pose major challenges for both private and government sectors.

Potential 'real' threats to private and government infrastructure include:

- Defense – military bases, command centers, satellites, nuclear, communications, defense systems
- Government – access to classified information and data, manipulation of political information and influencing presidential outcomes
- Public and Private – disruption to critical hospital life support, schools, universities and education/training facilities
- Mining and Gas – disruption to supply and global stock prices
- Energy – potential to disrupt global energy supply
- Oil – manipulation and control of global oil prices
- Communications – telecommunications, digital, misinformation
- Finance – potential to shut down the global economy, crypto scamming, manipulation and control of the global stock market
- Shipping – disruption to the global supply chain
- Digital – misinformation, AI hacking, Deepfakes, scamming, terrorist and criminal activity

Experts and researchers in cybersecurity predict that the sophistication, frequency and intensity of ransomware attacks will significantly increase in 2022 and beyond. Businesses and organizations that hold sensitive data will become the main targets for cybercriminals. Industries such as finance and healthcare are at high risk along with companies who have sensitive product data including intellectual property.

Future Challenges for SOC in a Digitized and AI World

Global digitalization and artificial intelligence (AI) have become the new normal, catapulting the world into chaos with cyber events, threats and attacks becoming more sophisticated and frequent. Post-Covid has seen us survive many challenges and experience digital transformation at a rapid pace.

The world was forced into remote working, increasing our dependence on digital technologies. While this may be seen as positive to many who have embraced their new digital lives in the security of their own homes, it has also opened opportunities and a backdoor for cybercriminals to use new sophisticated tools and advanced methods on their victims. This opportunity has resulted in new tactics used to exploit the vulnerabilities of individuals, small businesses, and organizations.

A new era of AI hackers will be upon us before we realize it and the world will face a war of artificial intelligence algorithms that will cause global disruption and damage on many levels. The future of cyber warfare is another complex challenge that will need to be confronted. Despite current methods and tactics used to protect national and international security, it may not be enough to combat future security threats.

How governments respond will be determined by two crucial factors: technology tools and the cyber mindset. Another factor that we cannot ignore is that state and non-state actors who collaborate for global domination will pay hackers to upload viruses that will paralyze communication, defense systems and critical military infrastructure.

The cyber threat landscape is evolving at a rapid pace and there is a need for intelligent strategies to be implemented to keep up with emerging and potential threats. SOC is faced with ongoing operational challenges and costs, skill shortages and too many unwarranted alerts.

Businesses and organizations need to build cyber resilience and find smart solutions by implementing intelligent technology systems, training staff and processes that will help reduce the risks and impact. A more comprehensive approach must involve organization affinity, process formalization and automation.

Organization Infinity

To achieve organization infinity, strategies and guidelines are needed to plan and implement an integrated SOC, incorporating control systems, corporate systems, and physical security. Currently, many organizations still work with individual systems which can be challenging when correlating all the data to determine threats, and by the time they do, it is too late.

Process Formalization

Process formalization is key when it comes to auditing and reporting controls. It will not only help monitor your company's performance efficiency but will ensure that all policies and procedures meet legal requirements. Failure to have good controls in place will not only fail to meet the needs of an organization, but it will also impact the bottom line. If there is a lack of documentation and process not only will it fail to pick up any inconsistencies, auditors will consider it non-existent.

Automation

Automation is the ultimate efficiency for a SOC. The processing of automation and optimization will not only optimize your security posture but will help decrease time from threat detection to remediation. Expertise and human skills can be augmented to increase the time to detect and respond, which will not only increase productivity it will improve job satisfaction, team function, and give an organization a huge return on investment

Transitioning to Cyber Resilience

An optimized, integrated SOC architecture will collect data, integrate, and analyze all alerts to provide greater situational awareness. From an intelligence-driven approach to incident management, this has proved to be most effective for dealing with advanced threats.

2022 is the year for cyber resilience. The world has now reached a crucial turning point where cyber resilience is defining the cyber landscape. Support for cyber resilience has resulted in a major shift to a cyber mindset where businesses and cyber leaders are having to respond in a swift and timely manner when confronted with cyber challenges. To fit in with the current and future cyber landscape there needs to be a clear focus on cyber resilience and risk which experts say is driven by three key factors: environmental, social and governance (ESG); governance, risk, and compliance (GRC); and operational resilience.

Environmental, Social and Governance (ESG)

With a focus on communities, people and customers organizations need to be committed to responsible and sustainable business practices. The objective is so organizations can contribute to a world where better outcomes are more beneficial to the world we live in. This can be achieved by developing innovative cyber technologies, offsetting carbon emissions, and improving staff awareness, education, and training to empower the next generation of a global cyber workforce.

Organizations also have a responsibility to the rest of the world by aligning themselves with the UN Sustainability Goals which include:

- Responsible production and consumption
- Clean and affordable energy
- Quality training and education
- Improved health and wellbeing
- Sustainable work practices and economic growth
- Pro-active climate action

Governance, Risk and Compliance (GRC)

Governance, risk and compliance strategies are crucial in driving organizations forward. By investing in GRC and implementing the right strategies for your business, it will benefit sustainability and long-term growth. providing you meet the expectations of stakeholders and meet regulations. By designing processes and frameworks that deliver best practices over the long term along with commitment and the right investment you will still manage to meet the expectations of stakeholders whilst meeting regulatory and industry standards.

Operational Resilience

With the increasing cyber challenges there has never been a more crucial time than to plan and prepare, respond and recover from cyber events and attacks. Not only is it best practice but having a cyber resilience strategy in place will ensure organizations can operate at minimal risk levels and disruption to processes and workflow practices.

A successful cyber operational resilience plan is built on solid risk assessments that can anticipate the threat level an organization is likely to experience. These include both internal through an organization's own staff and external threats from data breaches through to ransomware attacks.

5 Steps to Achieving Future SOC Efficiencies

Step 1: The Identity Function - Auditing and Assessing to Reduce the Risks from Tool Sprawl

Tool sprawl refers to the redundancy and system complexity associated with the unnecessary use of new IT tools and outdated systems. This can be debilitating to an organization, as it creates inefficiencies and siloed data. Frustrated cyber tech teams spend longer repair times and there is usually a failure to meet end-user requirements. Auditing the tools portfolio is the best way to prevent tool sprawl from affecting organizations by conducting a tools portfolio audit. Management who evaluates the tools portfolio must have insight into the value of each tool, along with the costs of maintaining each tool and the potential gaps within the system.

Tools portfolio audits are critical to the successful functioning of a business as it is essential to create a streamlined digital transformation. Auditing the tools portfolio can solve the problem by using a three-step process:

1. Inventory current tools and your organizational requirements
2. Consolidate tools portfolio
3. Implement an ongoing monitoring strategy

Management must first assess and evaluate current toolsets and re-consider what is necessary and what is not.

Step 2: Automating Capabilities + Orchestrating Workflows

There is an increasing challenge in organizations to meet their security goals due to manual, time-intensive tasks. Teams work in a silo and find it hard to function as one cohesive unit to actively orchestrate security initiatives and demands. Cumbersome manual processes also contribute to the delays in approvals and remediations. Other challenges include manual and incorrect incident prioritization and delays in remediation due to manual handover to different teams.

Effective Security Orchestration and Automation Response (SOAR) solutions automate security operations and integrate security tools and systems to streamline the security process, enabling optimal outcomes. SOAR helps in customizing workflows for your team and ensures more collaboration opportunities between teams. Organizations can also accelerate security programs and maximize efficiencies by reducing Mean Time to Detect and Respond while mitigating risks.

The capabilities of SOAR integrate independent security technologies and streamline processes whilst automating workflow and driving threat analysis. It offers a combination of automation, security orchestration, and AI-driven threat intelligence platform capabilities to identify vulnerabilities and exploits for effective cyber incident response.

Enhanced AI-driven threat detection and support includes:

- Automated remediation
- Integrated security solutions
- Automated cyber incident enrichment
- Automated threat intelligence
- Interactive investigations
- Referenceable knowledge
- Optimizing Mean Time to Detect and Mean Time to Respond
- Lowered costs through reduction of manual operations

Automation gives SOC teams the edge they need to proactively enhance their threat hunting capabilities.

Step 3: Automated Cyber Resilience

According to Dr. Ponemon, founder of the Ponemon Institute, automated cyber resilience starts with vigilance and visibility. The combination of transparency, a cyber mindset and adopting a security culture, organizations need to have the ability to observe, monitor and respond to current technologies in place. In addition, business processes enable organizations to identify the best tools that will prioritize their responses. By adopting vigilance and visibility, organizations will be better prepared and enable them to minimize risks, complexities and build a strong future-forward cyber resilient SOC.

According to SANS, the key factors for success in building a successful SOC, includes:

- Collecting the most important logs and network data
- Building, training, and empowering a diverse team
- Creating playbooks and managing detection use cases
- Using threat intelligence to focus your budget and detection efforts
- Threat hunting and active defense strategies
- Efficient alert triage and investigation workflow
- Incident response planning and execution
- Choosing metrics and long-term strategy to improve the SOC
- Team member training, retention, and prevention of burnout
- SOC assessment through capacity planning, purple team testing, and adversary emulation

Optimizing Security Operations

Organizations need to continuously evaluate existing practices, security architecture and practices. By optimizing your SOC, it will increase management efficiency and productivity, and incident detection. It can also be useful for integrating and implementing a hybrid, both in-house and virtual. SOC's must meet industry standards, legal and compliance requirements, and it is the organizations' interest to address security measures in order to keep the SOC functioning at an optimal level.

The first step to optimizing SOC is assessing and analyzing existing tools, systems, processes, and security teams. The second step is to evaluate how effectively these work together to detect system compromises and carry out detection and incident response functions. The third step is to automate steps once and to then be able to re-assess and make improvements to functions including detection, incident response and increasing the time to mitigate threats.

The Operational Cybersecurity Leader

As cyber-attacks become more sophisticated and more expensive for organizations, there needs to be a shift to view security operations from the point of view of cyber criminals, if they are to protect sensitive information and data. No matter how advanced vulnerability tools and software become, data breaches will always happen, and the key is to stay ahead of the game. With the technologies available requiring more time, training and knowledge, the global shortage of cybersecurity staff, the migration to cloud, and legal and regulatory compliance are complicating matters.

With SOC teams, typically made up of IT experts, all trying their best to make a difference, there is the constant challenge of protecting information and fighting attackers. There needs to be more leaders who oversee the overall architecture, networks, systems and people, and put policies and frameworks in place, to ensure the SOC is operating at an optimal level.

The SANS Institute has come up with an Operational Cybersecurity Executive triad which was designed to help organizations and leaders build, grow, and sharpen their cyber team.

High-level, cyber resilience is critical to the integrity, efficacy, and survival of SOC, to combat ever-evolving cyber threats and attacks. If an organization has a strong cyber resilience, it will be able to effectively detect, prevent, contain, and recover from a complex matrix of serious threats to its cyber architecture and data.

Organizations are quickly developing and improving cyber resilience by continuously revising security protocols, policies, procedures and implementing new technologies to enable greater effectiveness and efficacy. By building a strong cyber resilient SOC, organizations will not only have a better chance of surviving the challenging cyber landscape, but it will also create a more resilient workforce.

SOC would not function without the skilled staff to manage the cyber security architecture. It is important to keep them empowered, motivated, trained and rewarded in an effort to retain them. The most important aspect is the main points to be implemented into a cyber framework: people, technology, policies, and procedures.

Step 4: Augmenting Security Teams with AI and ML-Driven Intelligence

In an innovation-digital business world, Artificial Intelligence (AI) and Machine Learning (ML) are future game-changers. Integrating AI and ML into systems will eliminate human error for a fraction of the cost. This will allow for the augmentation of faster analysis of data, problem-solving, risk assessment and decision-making, allowing organizations to optimize their workflows and work smarter. Organizations can leverage the power of AI and ML-driven intelligence enabling a smooth transition into the next era of digital transformation. Systems can be built to provide highly effective, intelligent solutions that run on advanced AI and ML algorithms, processing data to generate data-driven insights for better decision making.

AI and ML are the next-generation technology solutions. SaaS can help organizations combine AI with human intelligence to build, implement, adopt, and utilize AI and ML solutions that can process enormous data faster to achieve successful business outcomes. Not only will this enable organizations to keep up growth whilst meeting the demands of the future cyber landscape, but it will also optimize their SOC, allowing for automated workflows and performance.

Step 5: Building and Optimizing Security Operations Building a Future-Forward SOC

With the increasing sophistication of threats and complexity of systems and networks, the global cybersecurity skills shortage, organizations need to have the expertise and resources available to build an effective SOC. The SOC of an organization is made up of a high-level security team who analyze and respond to daily alerts and multiple security incidents. With the rapid digital transformation, it has become more difficult for SOC's to build a solid team and keep up with the demands of securing their network and architecture.

According to SANS, Operational Cybersecurity Leaders should be able to have:

- An understanding of all security controls
- The ability to implement security controls
- The access to audit security controls
- Management skills to effectively create a comprehensive vulnerability management model
- The ability to guide and assess the threats that need attention
- Continually grow the security operations, in turn saving money, time, and hours of wasted effort and frustration

It is time for change and having an operational cybersecurity leader will take the organization to the next level and ensure continuous optimization of all operations.

SANS Institute: the successful formula for operational cybersecurity leaders

3 Keys for Successful SOC Transformation

Key 1: Attack Surface Management (ASM) – Protect the Data That Matters Most

Time is critical for attack surface protection (ASM). Time, automation at scale and solid processes help eliminate data breaches faster for a stronger security. These three important points are critical for the success of ASM. When attackers find something before you do it will be exploited. At any given moment, organizations need to have the ability to identify and report before attackers find the opportunity to attack. Slow attack surface mapping and the prioritization of risks are usually the primary problem when it comes to protecting data.

Finding ways to contextualize assets and risks as well as focusing on decreasing the time it takes to find networks, cloud environments and applications is a crucial part of ASM. Security teams are already under pressure and finding it hard to keep up with the demands and threats. Staff need to be empowered with automated processes and solutions that accelerate attack surface management process so expertise can be leveraged on the important matters.

Key 2: SOAR – Orchestrate Across Your Product Stack

Security, orchestration, automation and response (SOAR) is critical in the face of ever- evolving threats, a global shortage of qualified and experienced cyber staff, and the need to monitor cyber threats and manage workflows, SOAR orchestrates across product stacks whilst rapidly detecting and responding to attacks. It optimizes the quality of intelligence, improves the efficacy and efficiency of SOC, captures and streamline information and knowledge, and enhances incidence response.

Optimizing quality intelligence

Combatting sophisticated cyber security threats requires a deep understanding of the tactics that attackers use, including their techniques, procedures, and the ability to identify compromising indicators. By integrating and validating data from a range of different sources, including security technologies such as intrusion detection systems, firewalls, UEBA and SIEM technologies, SOAR helps security operation centers to have an intelligence-driven focus. This assists security teams in contextualizing incidents, accelerating incident detection, and response making better informed decisions.

Optimizing efficacy and efficiency of SOC

Managing many different security technologies can put massive pressure on security teams. Not only do systems need constant monitoring to ensure their ongoing performance and integrity, but the excessive number of daily alerts can result in alert fatigue. The constant use between multiple systems, costs effort and time, as well as increasing the risks of human error. SOAR solutions semi-automate and automate day-to-day tasks of security operations, and present intelligence and controls through ML and AI all in one platform, reducing time and effort. SOAR improves an organization's capacity to address incidents and its productivity ensuring processes are handled more efficiently without the need to hire more manpower. The philosophy of SOAR is to work smarter not harder.

Enhancing Incident Response

Rapid incident response is critical in minimizing the risk of breaches, disruption, and damage they can cause. SOAR reduces the mean time to detect and mean time to respond by enabling rapid security alerts that can be remediated and resolved in a matter of minutes. SOAR also automates playbooks allowing blocks on an IP address on an IDS system or firewall and can immediately suspend user accounts and infected endpoints from a network.

Streamlining reporting and capturing knowledge

SOC teams spend an unnecessary amount of time managing cyber events, documenting incident response procedures, and writing reports. By integrating intelligence from a range of sources and into custom-built dashboards, SOAR can help organizations minimize mundane tasks and paperwork whilst improving communication between the frontline and C-suite.

By automating procedures and tasks, SOAR allows organizations to capture and retain key knowledge. This allows teams to prioritize and perform tasks faster and focus on all threats in a timely manner, minimizing the risk of damage and disruption.

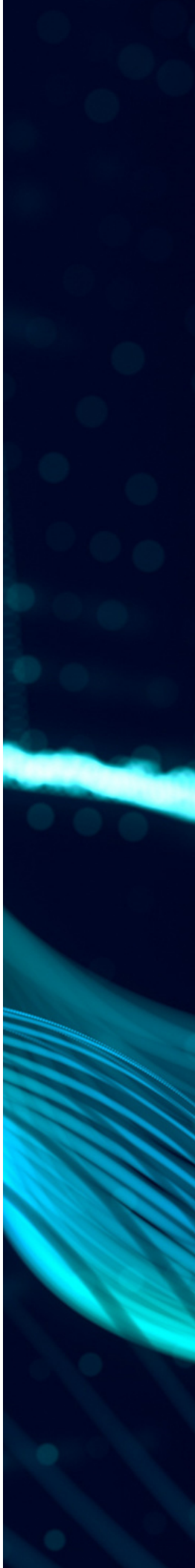
Key 3: XDR – The Evolution of MDR

The emergence of automation and ML processes has had a significant impact in the cyber security arena. It has reduced the response time to changes, improved language processing, security optimization and big-data processes. Managed Detection and Response (MDR) has been built to identify and contain before damage is done. The early detection of compromised user/endpoints is key.

The demands and expectations of cybersecurity leaders has increased considerably to successfully monitor endpoints and find detection active response solutions. There needs to be more awareness on the management level to counter cyber threats and their damage potential. Demands and pressures are continuously increasing and MDR still remains the best tool to help organizations in a fruitful and effective manner.

Extended detection and response (XDR) which evolved from managed detection and response (MDR), delivers more efficiency and efficacy in the detection, investigation, and response to threats. XDR is the new future-forward cyber threat-centric security prevention with an integrated streamlined approach incorporating analysis, workflows, and security data ingestion across an organization's entire security stack. XDR aims to enhance visibility around advanced and hidden threats whilst unifying responses.

XDR's aim is to collect and correlate data from endpoints, networks and email, cloud workloads, prioritizes and analyze them all in one platform. XDR coordinates and extends the value of siloed security tools, unifying and streamlining security analysis, investigation, and remediation into one consolidated platform. As a result, XDR will dramatically accelerate security operations by improving threat visibility and reducing TCO security team burden.



The AWS, AZURE, and OFFICE 365 Solution

The Most Important Tools in One Place

SOC's experience plenty of tool sprawl and when software isn't integrated, valuable time is lost in the detection and response process. Instead of multiple solutions, a single cloud-based SOC and SIEM platform allows you to:

- Monitor systems, applications, and workloads, whether physical or virtual, anywhere in a network, whether in a data center, in a private cloud, or across one or more public clouds
- Scale on-demand instead of being required to re-architect solutions as an organization grows
- Eliminate hardware costs by moving off expensive hardware and removing the administrative costs required to maintain the solution
- Get real-time alerts on security incidents
- Serve as the basis for risk analysis and audits
- Consolidate and manage security and event log data
- Automate compliance reporting
- Increase time to value with fast implementation and updates

AWS

API integration with Amazon Web Services (AWS) enables ultra-fast event gathering and monitoring to get log files from AWS S3 buckets with SQS notification. Monitoring the security events in the AWS cloud infrastructure is critical to detect and mitigate cyber threats before they lead to a major cyber incident or a data breach.

Access logs contain detailed information about the requests made to these services. VPC flow logs capture information about the IP traffic going to and from network interfaces in AWS VPC. ELB access logs capture detailed information about requests sent to the load balancer. CloudTrail logs contain events that represent actions taken by a user, role or AWS service.

Customizable Data Analytics Platform

- Complete visibility of digital infrastructure and cloud monitoring
- Compliance requirements
- Indicators of attack
- Suspicious AWS console login, such as login from a rare location
- Permission elevation or new account created
- AWS CloudTrail logging being disabled

AZURE

A direct and streamlined API integration with Microsoft Azure, enables ultra-fast event gathering and monitoring of log events. Quickly uncover suspicious activities like brute force attacks on a user login, unexpected infrastructure creations / deletions, or high alert density from a particular resource group. With a built-in API, it's possible to correlate cloud-based data with data from on-premises sources (such as Active Directory) to add entity context information and analyze the end-to-end activities of users. This includes a tightly coupled correlated integration between multiple Microsoft Azure components, collecting data from Microsoft Office 365.

Detecting Threats Before It's Too Late

- Monitor user activity, sign-ins, and audit logs via Azure Event Hubs
- Recognize sensitive data movement along with suspicious login activity
- Monitor unauthorized and/or unexpected activities
- Catch privilege misuse or compromise within organizations
- Detect unauthorized sharing and data exfiltration
- Spot suspicious login attempts by location
- Uncover brute force login attempts to Office 365

OFFICE 365

Security challenges are growing as every company and its users migrate business-critical data and operations to Office 365 cloud apps, including SharePoint Online, OneDrive for Business, and Exchange Online. Security concerns include data loss or leakage, data privacy, unauthorized access, account takeover, phishing and more. These cyber-threats can be inflicted by external attackers or negligent or malicious insiders with legit privileges.

Up To Date Alerts and Monitoring

The Aegis IT Solutions platform provides comprehensive monitoring for various Office 365 operations such as Active Directory, SharePoint, OneDrive, authentication: users and access, resource sharing, mail and file operations, and mobile device management.

SOC-as-a-Service Differentiators

Features and Benefits of SOC-as-a-Service

Capabilities and service level quality can vary widely between SOC-as-a-Service providers. Potential buyers of cybersecurity services should look for SOC-as-a-Service providers that can offer the following:

Simplified Setup and Installation

SOC-as-a-Service providers should have detailed and tested plans, procedures, and timelines for starting the service. This will include briefing and training designated members of the supported organization.

Reliable Anomaly Detection and Reduced False Positives

The SOC-as-a-Service provider should be able to demonstrate that the service can accurately and quickly detect cyber anomalies and cyberattacks. False positives can significantly impact the reliability, efficiency, and credibility of the service, and the provider should be able to demonstrate how false positives are minimized.

Intuitive Dashboards

Ideally, the dashboards should be easy to navigate. An overall risk score to allow personnel without cybersecurity experience to quickly assess the overall state of cyber health is a huge value add.

Robust Logging and Analysis

The service should include log collection, aggregation, and analysis to support regulatory compliance and review by examiners, assessors, and auditors.

Responsive Cybersecurity Specialists

This is the most important aspect of a SOC-as-a-Service provider. Buyers should be looking at the qualifications, training, tenure, and certifications of the organization's cybersecurity experts. The provider should be able to offer references from other clients.

> ***"There's no silver bullet solution with cybersecurity, a layered defense is the only viable defense."***
> *- James Scott, Senior Fellow, ICIT*

Aegis IT solutions

Aegis IT Solutions is a software company with an innovative SOC|XDR-as-a-Service for 24/7 network monitoring, cloud security, data privacy and compliance backed by our U.S. based SOC.

We detect cyber threats before you have been breached. Our SOC-as-a-Service platform is designed to monitor your cloud, network, and endpoints. Our modern SOC-as-a-Service is built on innovative machine learning and autonomous execution.

Ready to start protecting your company?

Request a Free Consutation