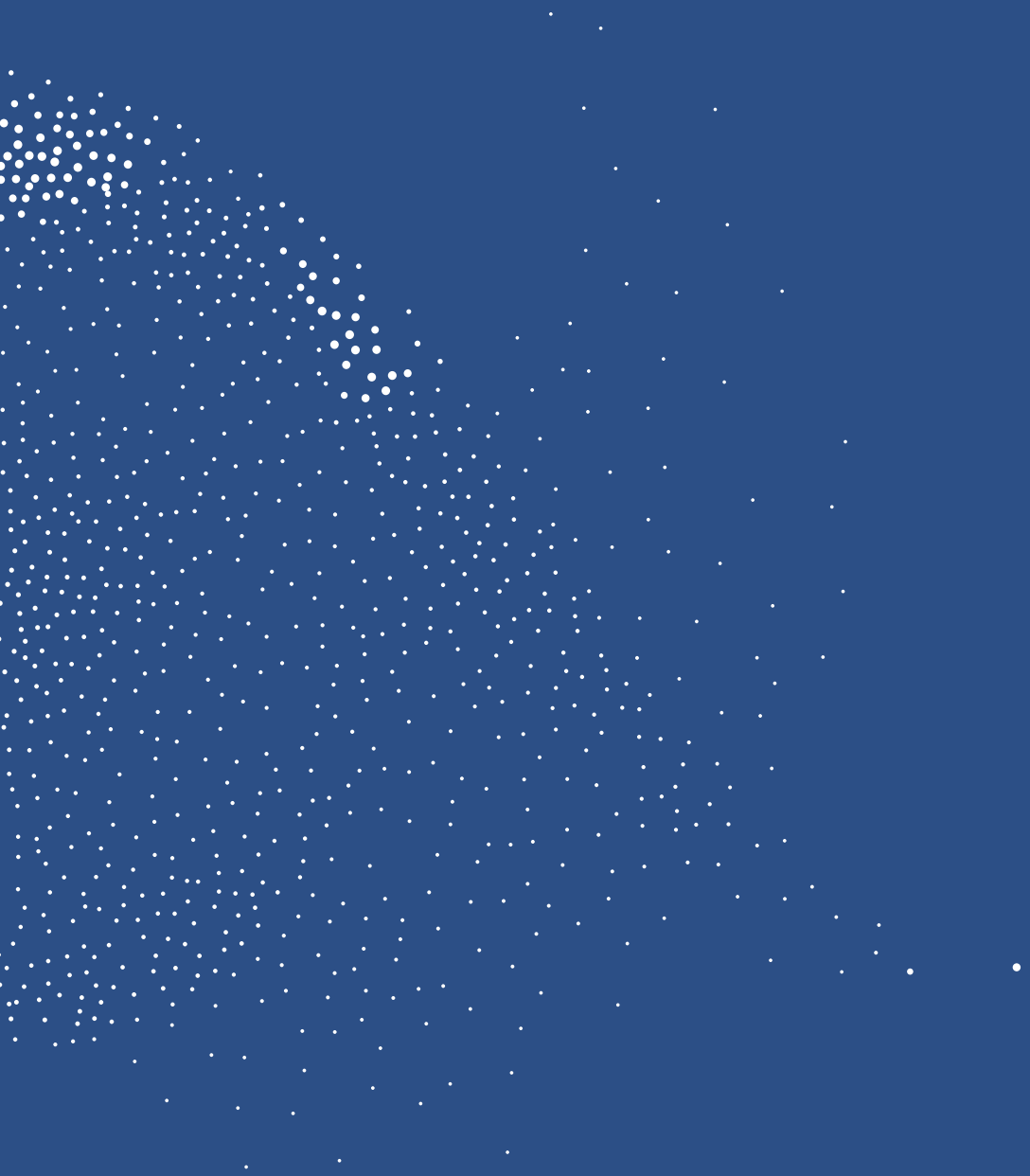
cloudcover®



Detect, Respond, and AI Anticipate

The New Era of CyberSafety™

Reimagine CyberSecurity through Artificial Intelligent SOAR Methodology

White Paper

Executive Summary

As artificial intelligence (AI) becomes more common in everyday life and business, it's also being employed more frequently in cyberattacks. The sophisticated technology that makes it possible for machines to learn from experiences and perform human-like tasks is the same technology that's being used to launch social engineering attacks, develop mutating software that can avoid detection, and monitor networks to detect new vulnerabilities. Hackers are becoming savvier, and it's not enough for companies to use secure network systems that react to malware threats minutes, hours, or even weeks after an attack — not when network devices are being compromised in a matter of microseconds.

These threats to information security are also becoming more pervasive. Led by the exploitation of smart and Internet of Things (IoT) devices and the increasing innovation of cybercriminals, distributed denial of services (DDoS) attacks over 5 Gbps grew nearly 1,000% over the past year. Attacks under 5 Gbps grew over 250% (Raymone, 2019). Ransomware attacks in the United States are forcing organizations to make tough choices: Either pay a ransom of millions and encourage cybercriminals to continue their practices or refuse and be left with a massive cleanup bill to replace and rebuild an entire IT network.

Security operating center (SOC) teams are managing an incredible number of incoming threats to their data, and they're managing it with a shortage of skilled IT staff. They're also dealing with a shortage of security training and smaller budgets — at the same time that there's added pressure to adopt the popular cyber security technologies. Each of these technologies has its own varying degree of success, no matter how expensive or highly recommended it is.

Many of the chief information security officers (CISOs) and other senior-level IT security executives responsible for establishing and maintaining information and network security are — appropriately — jaded. Even though their stomachs turn when they think about how quickly a cybercriminal could bring their company to its knees, they've been burned plenty of times before. As a result, they've resigned themselves to believe they can only mitigate the hacking, not protect their organizations completely. They feel like a cyberattack isn't a matter of if, but when.

However, organizations can take a proactive, anticipatory approach in the form of security, orchestration, automation, and response (SOAR) technologies — making it possible to have the cyber threat intelligence needed to avoid the inevitable.

SOAR technology signals a significant evolution in cyber security, as it provides a way for SOC teams to hyper-accelerate risk controls to streamline and accelerate the investigation and neutralization of cyber threats. True AI-based SOAR technology offers a way for IT security teams to:

- **Reduce** their risk-management resources, as the technology uses deep learning to detect and eliminate threats to data security in milliseconds — with little human intervention.
- **Detect** and **respond** to threats both ingress and egress faster at their organization's IoT network edge.
- **AI Anticipate** future attacks by identifying anomalous traffic and patterns, correlate and connect data across systems, and perform algorithmic risk analytics on hacker entity in real time.
- Once it learns to AI anticipates, automatically **insert** proactive security code to block a hack or cyberattack — alerting network security technology of the attempt breach and stop the hack.

Table of Contents

Executive Summary 2

Introduction: The Current Landscape — and Approach — to CyberSecurity 4

The Evolution From CyberSecurity to CyberSafety 5

Benefits of SOAR Security: Orchestration & Automation 7

Benefits of SOAR Security: Response 9

Benefits of SOAR Security: Data Egress & Data Leakage Prevention 9

DoS Cyberattacks and Their Effect on Network Security 10

The Frequency of DDoS Attacks 12

The Cloud and Its Contribution to DDoS Attacks 13

How SOAR Technology Offers DDoS Protection 14

The IoT and Its Effect on DDoS Attacks 15

RDoS Attacks and the IoT 16

SOAR Platforms and the Shift From SOC to N-SOC 16

Summary 17

References 19

Introduction

The Current Landscape and Approach to CyberSecurity

Today, organizations are battling complex multi-vector cyberattacks, complicated technology environments, and a growing skills gap, making cyber security awareness and response more complex than ever. Even with a skilled, fully staffed team, it's tough to keep up with the day-to-day threat landscape, changing regulatory compliance mandates, and mounting information security alerts — especially in a quick and efficient manner.

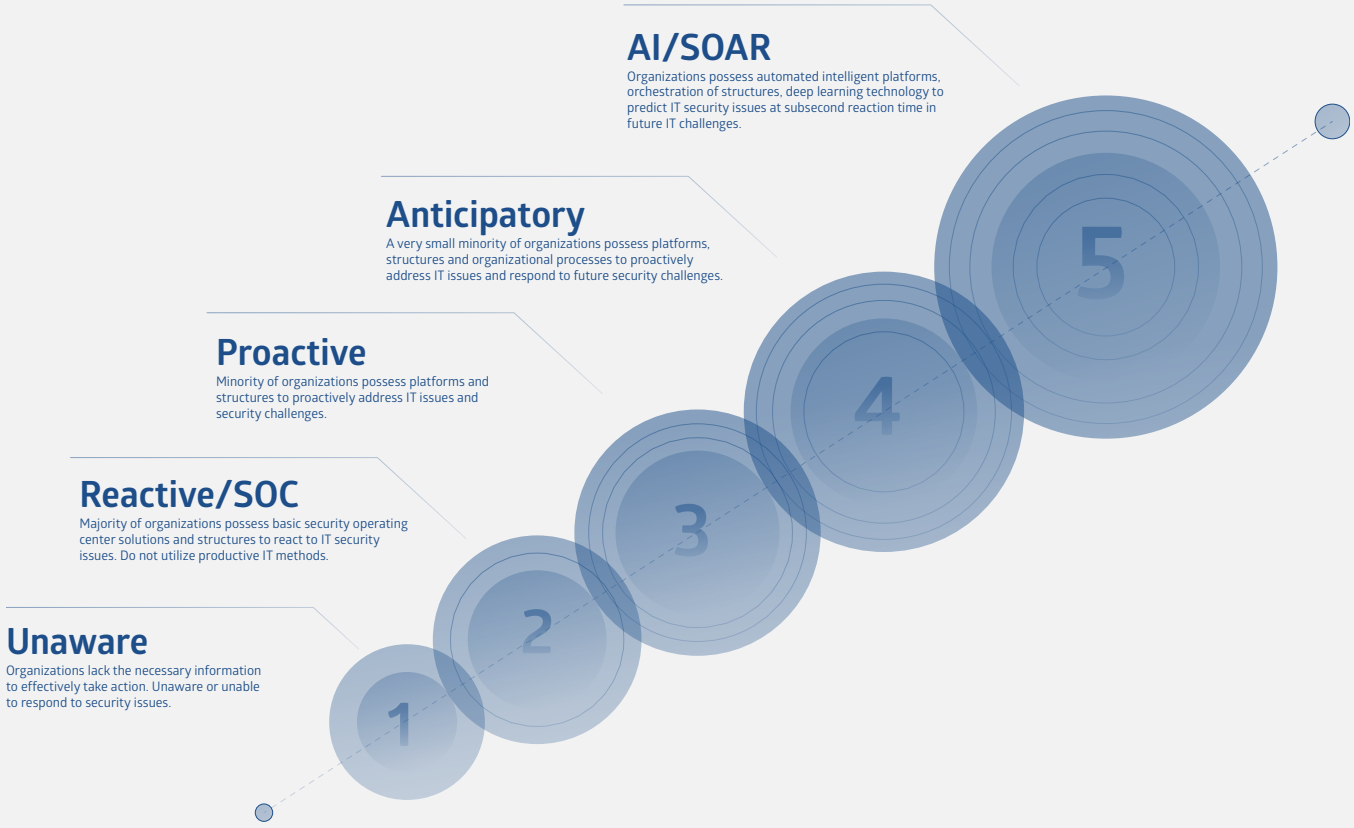
To manage new hacking threats, organizations must take a holistic view of their network data ecosystem and choose the best way to ensure digital data security. Today's cybercriminals have a variety of motivations, using hacking as a form of financial gain, protest, spying, and even as a form of fun or a challenge — and they've also started to use artificial intelligence to carry out attacks that can overcome or work around data security commands and control at lightning speed.

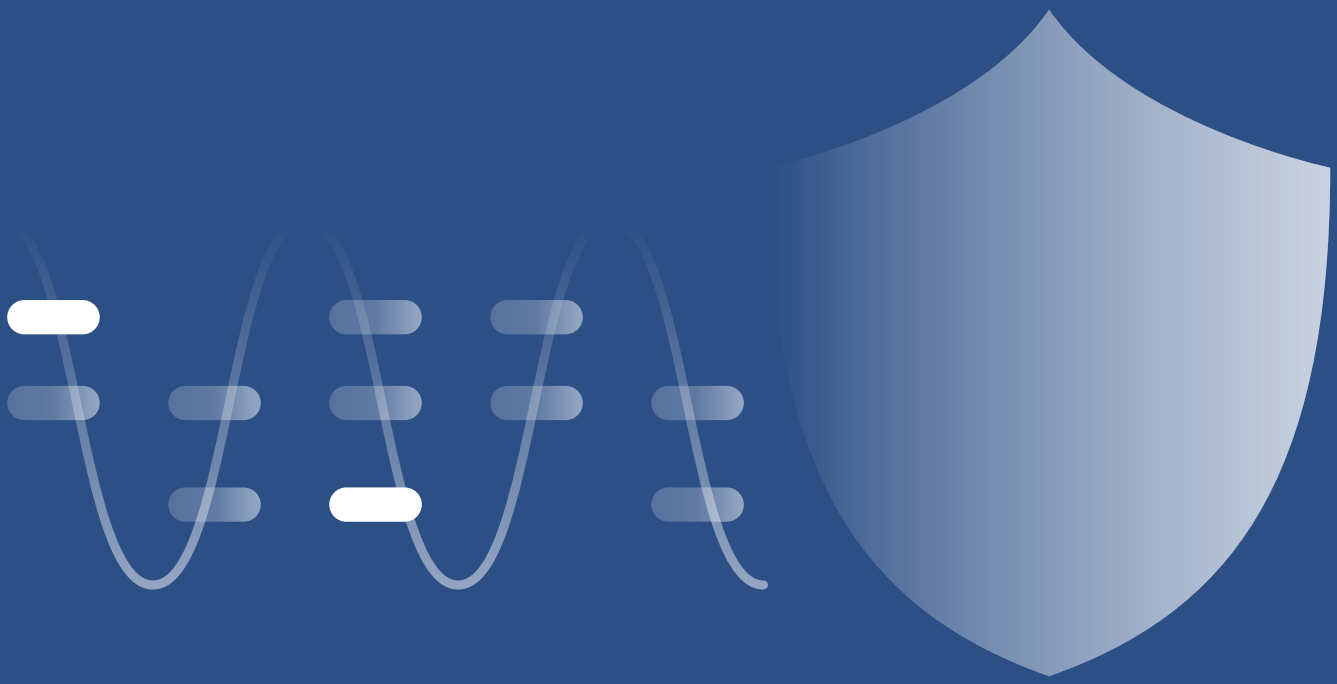
That's why anticipatory responses are critical to an organization's network security. **Automated intelligence (AI) and security, orchestration, automation, and response (SOAR) technologies are more than simply the next generation of cyber security awareness — they're the next evolution.**

The Evolution of CyberSecurity to CyberSafety

In practice, CyberSecurity is reactionary — incidents such as hacks and data breaches are responded to after they occur. CyberSafety, on the other hand, is proactive, anticipatory - i.e predictive preparedness with the help of AI/SOAR.[1]

CyberSecurity Evolution Model





The basis for CyberSafety was formed by combining software-defined networking (SDN) methods with security automation and automated intelligence. Traditional networking is quickly being replaced by SDN capability that enables dynamic programmable networks — a new, promising approach to designing, building, and managing more secure networks.

While SDN allows for more flexible network security management (Vizy'ary and Vykopal, 2014), the real answer lies within today's SOAR orchestration, automated intelligence, and deep learning "risk-aware" security. The combination of the two will outpace the conflict between cyberattacks and cyber defense systems.

SOAR platforms aren't new to the network and information security space — the U.S. Patent Office has issued several new patents in recent years that fully embrace SOAR systems, methods, and architecture. One patent, No. U.S. 10326777 B21, covers the Internet technology used to identify threats, orchestrate and automate security, and apply AI-based proactive responses.

SOAR technologies employ these three key elements:

- **Orchestration methodologies** that interface with multiple cyber security technologies to prevent an attack
- **Automated security technology** that uses data science to automatically write a new security mitigation rule
- **The ability to prevent a polymorphic attack within seconds or minutes** by inserting that rule into an exact area of code – without human intervention

Benefits of SOAR Security

Orchestration & Automation

AI is based on the principle that algorithms can understand, analyze, and perform cognitive-assigned tasks effectively — and can augment the human "decision" in the learning process to bolster situational risk awareness and further perform specific assigned tasks.

Automated AI-based deep learning in SOAR technology allows for:

- Instantaneous machine learning
- The ability to "hunt and deflect" threats
- Predictive threat management
- A commingling and streamlining of the alert process
- The reduction of workflow barriers
- Enhancement of human efficiency, making the issue of IT security (staffing shortage) less severe

Automated orchestration within SOAR platforms offers the ability to:

- Integrate disparate software systems
- Improve and enable measurement of SOC productivity
- Alleviate skills gaps and staffing shortages
- Improve speed of the data breach notification process
- Enable guide responses to complex attacks
- Have greater visibility through a unified dashboard

> **Where we really see the benefits and capabilities of SOAR's orchestration and automated intelligence capabilities is in the effects of a delayed response to a data breach — not only in time wasted, but also cost.**

A few sobering statistics: Ponemon Institute 2020 “Cost of a Data Breach” study

These numbers speak volumes.

> **By the time a breach has been discovered, the damage has often already been done — the criminals responsible had unlimited access to your database and intellectual property through your software systems, and the personal and private information of millions of customers has been compromised.**

Benefits of AI/SOAR Security

Response

What makes SOAR technology a particularly unique answer to cyber threat intelligence is its "Response" attribute. This represents three proactive risk attributes — risk aware, react, and respond.

In each of (our) SOAR modes, inspection, analytic, and action, we automatically insert new proactive security code to prevent a cyber attack and alert the data security technology of the attempted breach, stopping it at the first packet handshake. This is the point when a small segment of information, called a packet, is initially sent to a computer or a device.

Data Egress & Data Leakage Prevention

One of the most overlooked data security vulnerabilities is data egress — often referred to as data leakage prevention. Data egress refers to data leaving a network in transit to an external location (the opposite being data ingress).

Egress traffic is a term used to describe the volume and substance of traffic transferred from a host network to an outside network through everyday actions like:

- Sending outbound emails
- Cloud uploads
- Transferring files to external storage
- Web uploads
- Removable hard drives

Cybercriminals are always looking for sensitive, proprietary, or easily monetizable information — and so are competitors, nation states, and malicious insiders. These criminals use various data exfiltration techniques, such as backdoor Trojans or built-in Windows tools like Windows Management Instrumentation to steal or expose sensitive data.

Data loss is a serious issue on its own — but imagine the amount of data traveling across a manufacturing supply chain from one manufacturer to several wholesalers or customers. Infiltrating the data egress of just one manufacturer or organization can have a devastating impact on hundreds of companies.

SOAR technology provides successful data protection and recovery as well as proactive network security awareness for effective security of data egress within a network system.

DoS Cyberattacks and the Effects on Network Security

In addition to assisting with data leakage prevention, SOAR technology can also prevent denial-of-service (DoS) cyberattacks — attacks that can have profound effects on the network security of businesses in the public and private sectors.

DoS cyberattacks continue to increase in number and complexity (Mahjabin et al., 2017), due to the proliferation of Internet of Things (IoT) devices that are part of our daily lives, as DoS attacks are the most common and easiest to implement of IoT systems.
DoS cyberattacks fall into two categories — basic and distributed.

Basic DoS Attacks

A cyberattack where the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely disrupting the service of a host connected to the internet. The denial of service is typically accomplished by flooding the service with unnecessary requests to overload the system — preventing some or all of the legitimate requests to be fulfilled.

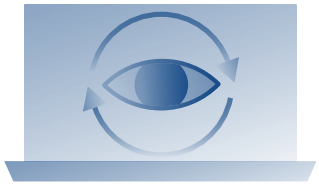
Distributed DoS (DDoS) Attacks

A more complex cyberattack where multiple aspects of computer architecture are compromised (e.g., synchronized attack of a target such as a server, website, or other network resource), causing a denial of service for the users of a targeted resource.

A DDoS attack is hard to stop by using ingress filtering and makes distinguishing legitimate user traffic difficult, as it's spread across multiple points of origin.

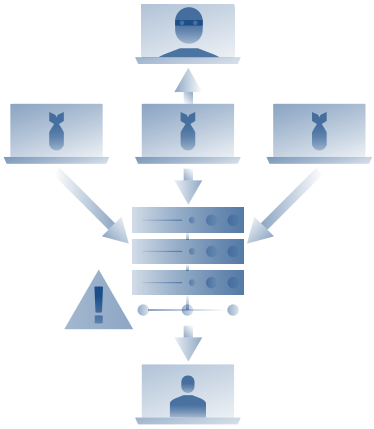
The main location of a DDoS attack is through a web server or proxy server. It can be manual, semiautomatic, or automatic and is usually in some form of complex multi-vector attack to drop the packets, which exceed threshold limits arising from one or more sources (Mahjabin et al., 2017). The targets of these attacks can be an in-home user, private businesses of any size, or a government agency — and the victims can be any organization from an e-commerce site to an internet service provider (ISP).

Within a DDoS attack, cybercriminals typically employ three strategies:



Botnet Attack

A DDoS attacker creates a command-and-control server to comment a network of bots. A bot, or zombie, is a computer or networked device under the control of an intruder.



Network-Centric Attack

Network-centric, or volumetric attacks, overload a targeted resource by consuming available bandwidth with packet floods.

Protocol Attack

Protocol attacks target the network or transport layer protocols, using flaws in the protocols to overwhelm targeted resources. With this type of attack, network resources are made unavailable to their intended users by any of the DDoS attacks by successfully disrupting the host's connection to the internet — temporarily or indefinitely.

The Frequency of DDoS Attacks

DDoS attacks continue to increase, advancing in both style and severity — and recent trends indicate we can expect to see more of the same in the future (Chadd, 2018). The DDoS landscape is driven by a range of actors, from malware authors to opportunistic entities offering services for hire. They're a busy group, constantly evolving new technologies that enable new services while using known vulnerabilities, preexisting botnets, and well-understood attack techniques.

Here are a few numbers that underscore the seriousness of DDoS attacks and why DDoS protection is so important:

50%
Percentage of organizations that say they have been victims of a DDoS attack (Belding, 2019)

1,000+
Percentage of those organizations that say they've been hit multiple times (Belding, 2019)

967%
Increase in DDoS attacks 100Gpbs and higher in Q1 2019 compared to Q1 2018 (Raymone, 2019)

51%+
Number of attacks that target three or more vectors (Raymone, 2019)

587Gbps
Largest DDoS attack measured in 2019 — an increase of 70% over the largest attack measured in 2018 (345Gbps) (Raymone, 2019)

42%
Percentage of those organizations that say they've been hit multiple times (Belding, 2019)

257%
Increase in DDoS attacks under 5Gbps in 2019 over 2018 (Raymone, 2019)

The Cloud and Its Contribution to DDoS Attacks

Cloud providers have profound opportunity in the marketplace due to the many benefits of cloud computing: fast deployment, pay-for-use, lower cost, scalability, rapid provisioning and elasticity, and many others. This has been especially true during the COVID-19 pandemic. According to Flexera's 2021 State of the Cloud Report, nine out of 10 companies accelerated their cloud adoption, driven by the rapid change of work environments as well as a focus on business continuity.

There are many advantages of cloud services, but they're also a ripe target for hackers, as massive amounts of data are being stored within cloud computing services and centers. In many cases, cloud technology divides the "as-a-service" offering without substantially changing the off-the-shelf hardware and/or software — a divide that comes at the expense of security.

> **There are many advantages of cloud services, but they're also a ripe target for hackers, as massive amounts of data are being stored withing cloud computer services and centers.**

How SOAR Technology Offers DDoS Protection

DDoS attacks are considered to be one of the most serious threats to internet availability, given that the Internet's resilience is coming down to a fraction of a second. **The microsecond response offered by SOAR technology makes it one of the only weapons that can thwart DDoS attacks and offer DDoS protection.**

The benefit of SOAR technology in the cloud is that it offers an organization the ability to implement AI-driven cloud security — an orchestrated solution that enables the exchange and coordination of relevant security controls concerning known threats, shared communities, and external security vendors — creating a holistic view of cyber threat intelligence suitable for automated decision making. The technology helps organizations use new intelligence updates to empower accurate, proactive cloud security automation.

In addition:

- New complex and multi-vector DDoS attacks are short in duration — 63% of them last under five minutes. Relying on human intervention means a too-late response.
- An "everyday" DDoS attack can't be defeated in the traditional internet gateway security solutions, e.g., firewalls, intrusion prevention systems, and others.
- On-demand, cloud-based DDoS protection and scrubbing alternatives can't achieve successful mitigation with the low-volume, short-duration attacks that regularly impact organizations.

The SOAR platforms and technology that employ AI machine learning and microsecond response to irregular traffic and patterns, correlate data security across multiple systems, and perform behavioral analytics will outpace the "co-evolutionary" war of DDoS cyberattacks vs. cybersecurity (verbal citation, Demopoulous, 2019).

The IoT and Its Effect on DDoS Attacks

Over the past decade, computer architecture and networking has changed from localized servers and desktops contained within four walls to a world filled with mobile devices (Donner, 2019). The internet was created using insecure networking and switches and routers that ensured high-capacity traffic handling over a protocol-based network. Security was an afterthought — one that was only considered with the arrival of encryption and private networking.

The advent of low-capacity traffic-handling internet-connected devices, or IoT, devices are not part of traditional computing networks. They're everywhere and are transforming both our personal lives and the way we do business (Donner et al., 2019).

As beneficial as they are, IoT devices do have some drawbacks — the biggest is that they're a common weapon in incredibly destructive DDoS attacks. These devices are soft targets for cybercriminals and other aggressors due to their lack of fundamental data security controls. The firmware in most IoT devices doesn't have the same level of protection as the operating systems running on most computers — meaning they can be easily hacked and added to botnets, which are used to launch attacks against organizations.

> **IoT devices are soft targets for cybercriminals and other aggressors due to lack of fundamental data security controls. The firmware in most IoT devices doesn't have the same level of protection as the operating systems running on most computers — meaning they can be easily hacked.**

IoT devices are rapidly diversifying, creating an enormous problem when interconnecting multiple highly heterogenous networked entities (Mahjabin et al, 2017). These devices aren't always designed with security in mind, and at the same time, cyber threats become potentially more harmful as they develop algorithms that become pervasive in affecting aspects of everyday use of mobile devices (Donner et al., 2019). This perfect storm is leading to more frequent, complex, and massive DDoS attacks that can shut down an organization's operations (Mahjabin et al., 2017; Tabassam, 2017; Donner et al., 2019; Cimpanu, 2019).

SOAR technology can stop these attacks by creating an unbreachable perimeter around the entire network, including the individual IoT network devices.

RDoS Attacks and the IoT

Ransom denial of service (RDoS) attacks are becoming more common as cybercriminals hang out on the edge of networks to launch their assaults, attempting to extort money from their victims. In these attacks, the criminal will typically send a message to the victim demanding a ransom.

If the victim refuses to pay, the attackers threaten to harm infrastructure or expose private personnel information. Paying, on the other hand, encourages more of the same behavior, with similar actors returning to extort again and again.

Recently, 22 Texas cities found that their municipality software had been infiltrated by hackers — the cities shared the same outsourced contractor. The hackers demanded $2.5 million (Allyn, 2019). As long as there's a digital dependency on IoT devices — especially mobile devices, these kinds of attacks will continue to happen.

SOAR Platforms and the Shift From SOC to N-SOC

An effective Security Operation Center (SOC) has three key interrelated components: a cyber security platform, people, and process (Crowley, 2019). In the past, a fully functioning SOC would allow companies to monitor, detect, and investigate threats 24/7.

> **SOCs require human interaction to stop a cyberattack, and in this microsecond world, that isn't fast enough — even for the most skilled IT team.**

However, SOCs require human assistance — and that can be both expensive and difficult to find. Another problem is that SOCs require human interaction to stop a cyberattack — and in this microsecond cyber world, that isn't fast enough. It's tough to do this kind of data protection quickly and expertly, even for the most skilled IT team. There are too many components of the threat landscape to manage — increasingly complex IT environments, changing regulatory compliance mandates, and mounting security alerts.

With SOAR technology, companies can adopt a N-SOC, or No-Security Operation Center. A SOAR platform is able to act as the ongoing operational component of enterprise network security, including microsecond risk awareness, reaction, and reporting factors. For these reasons, it reduces the financial burden of an SOC and creates a more fluid and instantaneous way to stop, contain, and prevent cyberattacks.

Summary

Today's internet search landscape is constantly evolving and becoming increasingly complex — and it's difficult for security operation teams to keep up. AI-based SOAR technology offers a solution for cyber security awareness — its anticipatory capabilities operate in microseconds and augment the need to rely on human interaction.

The arrival of SOAR technology comes at a critical moment in cyber protection, where:

- The **cost of cyber security is increasing**, yet a company's bottom line would be even more severely impacted financially by a data breach.
- The **pressure is growing** to adopt new technologies, yet budgets for security operation centers are shrinking.
- The **threat landscape is becoming saturated and dangerous**, yet there's a shortage of skilled IT professionals.

Even if you have a robust and skilled IT team, they're no match for a DDoS cyber attack that can take an entire network down in less than a second.

At the same time, cyber threats themselves are becoming more pervasive because of the quick proliferation of IoT devices — devices that help companies operate more efficiently but often with little regard to their data security risks. It's easy for malware to compromise networks or for a hacker to gain access through them and steal critical information once IoT devices are on a network. This ease is leading to more frequent and complex attacks — and massive data breaches.

SOAR technology can transform an organization's security operation by:

- **Protecting the edge of a network from hackers** attempting to use IoT devices as their infection host by creating a defensive-aware barrier at the edge and encircling a company's entire network.
- **Helping network administrators and security operations teams optimize their ability to detect and respond to cyber threats** faster, quantify key performance indicators, and reduce their day-to-day workload through improved risk intelligence, mitigation, and reporting.
- **Using their instantaneous risk-aware/reaction/report capabilities to understand and mitigate anomalous behavior** on the network, automatically responding to the threat – reducing dwell time of a breach target.

Today's networks need an AI-augmented approach to manage their data security in microseconds. SOAR platforms are an important aspect of any advanced cyber security strategy — making it possible to monitor networks and perform the necessary actions to protect data from potential threats.

It's the technology that's needed for organizations to confidently make the leap from merely reacting to cyber threats and data breaches to preventing them in the first place — CyberSecurity reimagined as CyberSafety.

CloudCover® has long been a champion of AI-driven SOAR technology. Our goal is simple: to help CISOs find a better solution to their cyber security challenges and sleep better at night. Our CyberSafety CC/B1 Platform™ can mitigate cyber theft in microseconds.

Contact us to learn more and see a demo.

Acknowledgements

The author is thankful to Jim Libersky, Robert Demopoulos and Marc Weintraub for their support and technical assistance during the writing of this paper.

References

Allyn, B. 2019. 22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault. https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-innewfront-of-cyberassault

Bayern, M. 2018. Advanced DDoS attacks up 16% from last year: Watch for these methods. https://techrepublic.com/article/advanced-ddos-attacks-up-16-from-last-year-watch-for-thesemethods

Belding, G. 2019. Threat Hunting for DDoS Activity and Geographic Irregularities. InfoSec. https://resources.infosecinstitute.com/category/enterprise/threat-hunting/iocs-and-artifacts/threathunting-for-ddos-activity-and-geographic-irregularities/#gref

Chadd, A., 2018. Network Security. (7): 13–15.

Cimpanu, C. 2019. No municipality paid ransoms in 'coordinated ransomware attack' that hit Texas. https://www.zdnet.com/article/no-municipality-paid-ransoms-in-coordinatedransomware-attack-that-hit-texas

Crowley, C. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. SANS Institute. https://www.sans.org/media/analyst-program/common-practicessecurity-operations-centers-results-2019-soc-survey-39060

Demopoulos, R. 2019. CTO CloudCover USA. Minneapolis MN.

Donner, H., Steep, M., and T. Peterson. 2019. Crossing the Urban Data Layer: Mobility as a Data Generating Activity. Stanford School of Engineering Disruptive Technology and Digital Cities Program.

Flexera. 2021. State of the Cloud Report. https://info.flexera.com/CM-REPORT-State-of-the-Cloud

Johnson, J. 2019. Cybersecurity maturity model lays out four readiness levels. https://searchsecurity. Techtarget.com/tip/Cybersecurity-maturity-model-lays-out-four-readinesslevels?src+5923837&asrc+EM_ERU_116181485&utm

Mahjabin, T., Xao, Y., Sun, G., and Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, vol. 13, 12.

Nazario, J. 2008. DDoS attack evolution. Network Security (7): 7–10.

Netscout, 2019. NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report (WISR).Paul, F. 2019. "Six IoT predictions for 2019". Network World. https://www.networkworld.com/article/3330738/six-iot-predictions-for-2019.html 174

Ponemon, L. 2020. Cost of Data Breach. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/en/pdf

Raymone, A.D., 2019. Major DDoS attacks increased 967% this year. https://www.techrepublic.com/article/major-ddos-attacks-increased-967-this-year

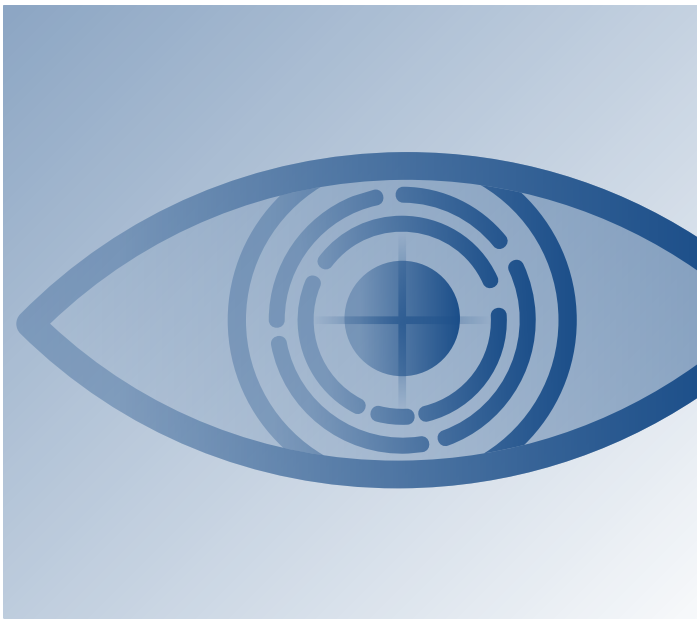
Su, J. 2019. Why Cloud Computing Cyber Security Risks Are On The Rise: Report. Forbes. https://www.forbes.com/sites/jeanbaptiste/2019/07/25/why-cloud-computing-cyber-security-risks-are-onthe-rise-report/#1d28acf85621

Tabassam, J. 2017. Security and Privacy Issues in Cloud Computing Environment. J Inform Tech Softw Eng., 7:5.

Vizv´ary, M., and J. Vykopal. 2014. Future of DDoS Attacks Mitigation in Software Defined Networks. In., Monitoring and Securing Virtualized Networks and Services. (8): 123–127.

1 - US Patent Office No. US 10326777 B2 / 8,832,833 / 8,973,143 covers the internet technology used to identify threat, security orchestrate, automate, and apply incident response utilizing its SOAR technology to automatically generate in millisecond, custom rules directing one or more of its defensive module technologies to prevent subsequent communication traffic from specific sources from infecting a customer's protected network.

C3C™



The Current Landscape — Approach to CyberSecurity

Today, organizations are battling complex multi-vector cyberattacks, complicated technology environments, and a growing skills gap, making cyber security awareness and response more complex than ever. Even with a skilled, fully staffed team, it's tough to keep up with the day-to-day threat landscape, changing regulatory compliance mandates, and mounting information security alerts — especially in a quick and efficient manner.

To manage new hacking threats, organizations must take a holistic view of their network data ecosystem and choose the best way to ensure digital data security. Today's cybercriminals have a variety of motivations, using hacking as a form of financial gain, protest, spying, and even as a form of fun or a challenge — and they've also started to use artificial intelligence to carry out attacks that can overcome or work around data security commands and control at lightning speed.

That's why AI-based anticipatory responses are critical to an organization's network security. Automated intelligence (AI) and security, orchestration, automation, and response (SOAR) technologies are more than simply the next generation of cyber security and cyber risk awareness — it is the "re-imagine" next generation.[1]