Next-Generation Security

The world is interconnected. An event that occurs in one part of the world (e.g., an infected animal for sale at a market introducing COVID-19 to humans) can have dramatic, unexpected consequences everywhere else. All humans are all connected vessels in a common body, and the principle of "oneness" affects everyone whether they are conscious of it or not. The recent pandemic crisis helps humanity to deep dive into the principle of oneness.

Internet space is no different. At first glance, it may seem as if there is no link between the emergence of many weak, typically not-so-secure Internet of Things (IoT) devices and enterprise security; however, these security-weak IoT devices that are unrelated to an enterprise can become potential attack vectors and cause millions of dollars of loss. In 2019, widely reported, well-coordinated activities turned IoT devices into a distributed denial-of-service (DDoS) zombie army[1] used for major infrastructure attacks and caused several large-scale IoT disasters.[2] An old security adage says that security is a chain depending on the weakest link. It is now clear that this chain connects on a global scale. The enterprise security perimeter is disappearing, and it is shifting far beyond the enterprise's boundaries.

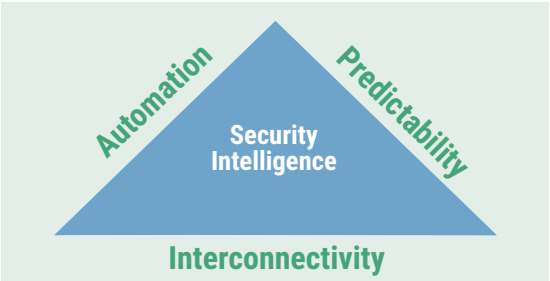
A sound security architecture cannot be designed if the principle of security oneness is not understood. The era of segregated, monolithic enterprise architecture is past. The premise of the security perimeter behaving as a middle-age fortress protecting the enterprise crown jewels is outdated.

Security attacks have become extremely sophisticated, interconnected, automated and better coordinated across the Internet; therefore, a new generation of security intelligence is required.

Interconnected, Predictive and Automated Security Intelligence

The traditional notion of threat intelligence should evolve into a new generation of security intelligence that is interconnected, automated and predictive in nature (**figure 1**).

Figure 1—Security Intelligence Triade



The idea behind this triad is to address modern security challenges by predicting or reacting to security threats in real or near real time and producing a predictive cyberrisk score so that enterprises can prioritize their resources to address highest risk first. This can be achieved using machine learning (ML), big data analytics and automated response playbooks. The building blocks of the security intelligence are presented in **figure 2**.

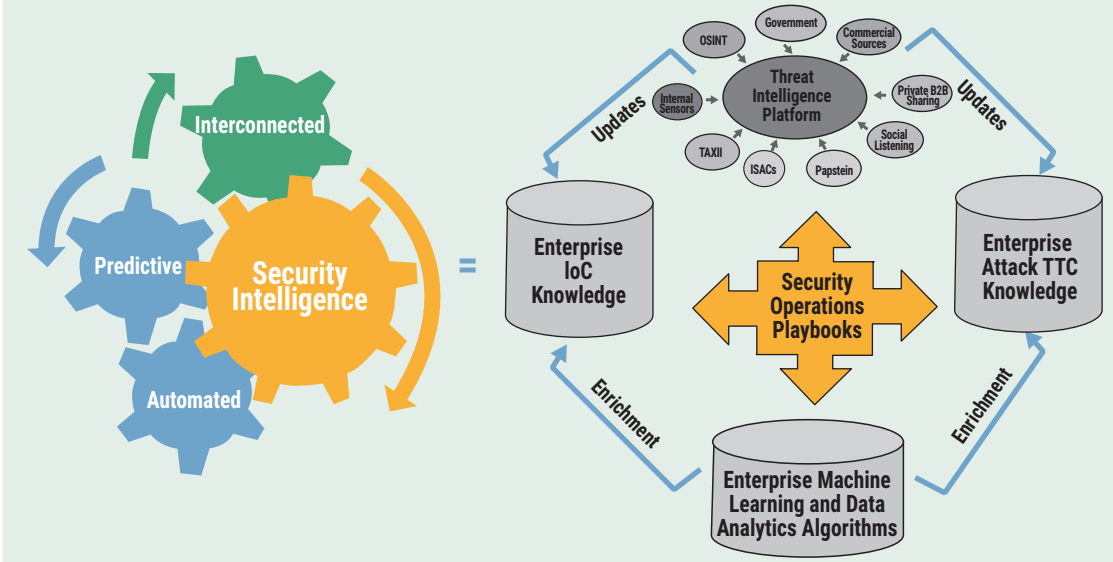
Louisa Saunier, CISA, CISM, CISSP, PMP
Is a security expert, security deal assurance engineer and project/program manager at DXC Technology. She previously held positions as a security officer, auditor, security consultant, and research and development engineer at Hewlett-Packard. She is also a reviewer of the *ISACA® Journal* and author of several patents and articles in the security industry.

Kemal A. Delic
Is a senior visiting research fellow at the Center for Complexity and Design at the Open University (Milton Keynes, United Kingdom). He is the cofounder of AI-Inc, Ltd. and a lecturer at the University of Grenoble (Grenoble, France) and University of Sarajevo (Sarajevo, Bosnia and Herzegovina). He previously held positions as a senior enterprise architect and senior technologist and scientist at Hewlett-Packard.

Enjoying this article?

- Read *ISACA® Tech Brief: Threat Intelligence. www.isaca.org/Threat-Intelligence*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 2—The Security Intelligence Building Blocks



Traditionally, threat intelligence is based on known static indicators of compromise (IoCs) such as malware signatures, malicious Internet protocol (IP) addresses, malicious domains, a URL that references suspicious content, a file hash using a malicious executable and a text code of a malicious email message. Many traditional security tools rely on IoCs such as antivirus using malware signatures, intrusion prevention systems (IPS) using static expert knowledge, and traditional security information and event management (SIEM) systems using static correlation rules. They are mostly reactive in nature, valid for limited periods of time, generate too many false positives and are not efficient for zero-day, polymorphic threats and threat hunting.

Knowledge about adversary groups and attacks is captured in the tactics, techniques and procedures (TTPs). TTPs are collected to represent adversary behavior by analyzing individual incidents and understanding the attacker's tradecraft. MITRE ATT&CK is a well-known curated knowledge base for TTPs.[3] TTPs can be embedded in security tools and platforms for enterprise security gap assessment to enable security response automation (e.g., in security orchestration, automation and response [SOAR] platforms) or used in red teaming and threat hunting. More and more security products are embedding TTP knowledge or dynamically linking with TTP repositories. TTPs can be used as tools to construct and test behavioral analytics, e.g., user and event behavioral analytics [UEBA] to detect adversarial behavior within an environment.

Interconnectivity is an important aspect of security intelligence, as it allows IoC and TTP repositories to be continuously updated from threat intelligence feeds.

Methods need to be put in place to uncover emerging attacks, detect advanced persistent threats (APTs), and uncover dynamically, in real time, new IoCs and new TTPs. This can be achieved by using ML and big data analytics. By analyzing high volumes of network traffic and logs, organizations could discover behavioral anomalies, correlate individual incidents and analyze the security incidents, setting a context. This would reduce false positives of traditional tools (e.g., SIEM) and allow organizations to respond to attacks in real time. Organizations also could reduce alert fatigue and time to remediate by automating time-consuming actions typically performed by security operation teams (SOCs). ML learning algorithms can continuously enrich an organization's knowledge about emerging IoCs and TTPs. This enrichment process could run in real time, near real time or as the result of a batch processing.

Another important aspect of enterprise security intelligence is the creation of playbooks for orchestrating and automating security operations. This turns security threat knowledge into an automated action (e.g., quarantine an endpoint device and get forensic images, blacklist phishing links, shut down the network port, kill a process). The ability to uncover new threats should be combined with the ability to provide automated or semi-automated response and continuously enhancing SOC playbooks.

Next generation security intelligence will encompass and go beyond traditional cyberthreat intelligence as it becomes more predictive, automated and interconnected.

Application of Machine Learning to Cybersecurity

The most valuable use cases of ML in cybersecurity are:

- **Predict new IoC patterns**—Machine intelligence can uncover new IoCs by applying deep learning models over large sets of data. These models can learn the characteristic of malicious patterns (e.g., malware signatures, bad URLs and intrusion detection patterns). The more data that are available, the better IoC detection capability is over time. For instance, by providing thousands of examples of known malicious and non-malicious URLs, a machine intelligence approach can extract key features (structure) from these URLs to build models that can discern potential malicious vs. non-malicious URLs.[4] ML capability can detect completely new IoCs and push them to enrich the enterprise's IoC knowledge.
- **Intrusion detection using UEBA**—By employing machine intelligence, deviations from normal behavior can be extracted in real time and evaluated by ML algorithms. UEBA algorithms compare the current behavior with the standard one, detect anomalies by applying some rules (e.g., unusual day of week, time of day, volume or country for a user), assemble anomalies and aggregate the risk of all detected anomalies (entity risk aggregation). UEBA algorithms reduce false positives, prioritize security alerts and improve SOC team efficiency.[5]

- **Uncover new TTPs**—Machine intelligence could provide insights into the profiles of attack groups by inspecting historical patterns and predicting potential future activities. ML could help build or maintain attacker profiles. These profiles can be sent back to TTP knowledge repositories and further fuel the cybersecurity war craft.
- **Rank aggregation or cyberrisk scoring**—By assigning a rank to all detected potential vulnerabilities and threats in an enterprise's network, the enterprise could prioritize remediation activities and security incident responses.

"ANOTHER IMPORTANT ASPECT OF ENTERPRISE SECURITY INTELLIGENCE IS THE CREATION OF PLAYBOOKS FOR ORCHESTRATING AND AUTOMATING SECURITY OPERATIONS."

Security Intelligence and Managed Security Service Providers

Most managed security service providers (MSSPs) have their own threat intelligence repository (to suit the services they provide), even if it is not exposed directly to customers. Many of them augment their threat intelligence with ML, big data analytics and

> WITH BIG VOLUMES OF DATA COMING FROM MANY CUSTOMERS AND SENSORS ACROSS THE GLOBE, MSSPS CAN STAY AHEAD OF EMERGING THREATS, UNDERSTAND TRENDS ACROSS MILLIONS OF USERS AND DEVICES, AND BUILD AND CONTINUOUSLY UPDATE THEIR THREAT INTELLIGENCE.

behavior-based analytics based on large volumes of data fueling their own data lake. Many MSSP solutions start embedding ML capabilities to evaluate the activity of users and other entities and discover changes to their normal behavior using the UEBA algorithms mentioned above. UEBA capabilities could be added to enhance traditional security tools and services such as endpoint protection, standard SIEM, intrusion detection and prevention, secure email gateways, and web application firewalls.

With big volumes of data coming from many customers and sensors across the globe, MSSPs can stay ahead of emerging threats, understand trends across millions of users and devices, and build and continuously update their threat intelligence. Big MSSP players behave as the concentrators of security data or a constellation of sensors on a global scale; the more data are fueling the MSSP service, the better predictability of their security knowledge and the better security protection. This is shown in **figure 3**.

The real power and competitive advantage come with the possibility to predict and stay ahead of security threats. This is fully true for an MSSP, but the same is applicable to any enterprise.

Security Intelligence Defense Framework

At the heart of the Security Intelligence Defense Framework proposed here is the enterprise data lake (**figure 4**). The data lake ingests security and nonsecurity data coming from different internal or

Figure 3—MSSP: A Constellation of Sensors on a Global Scale

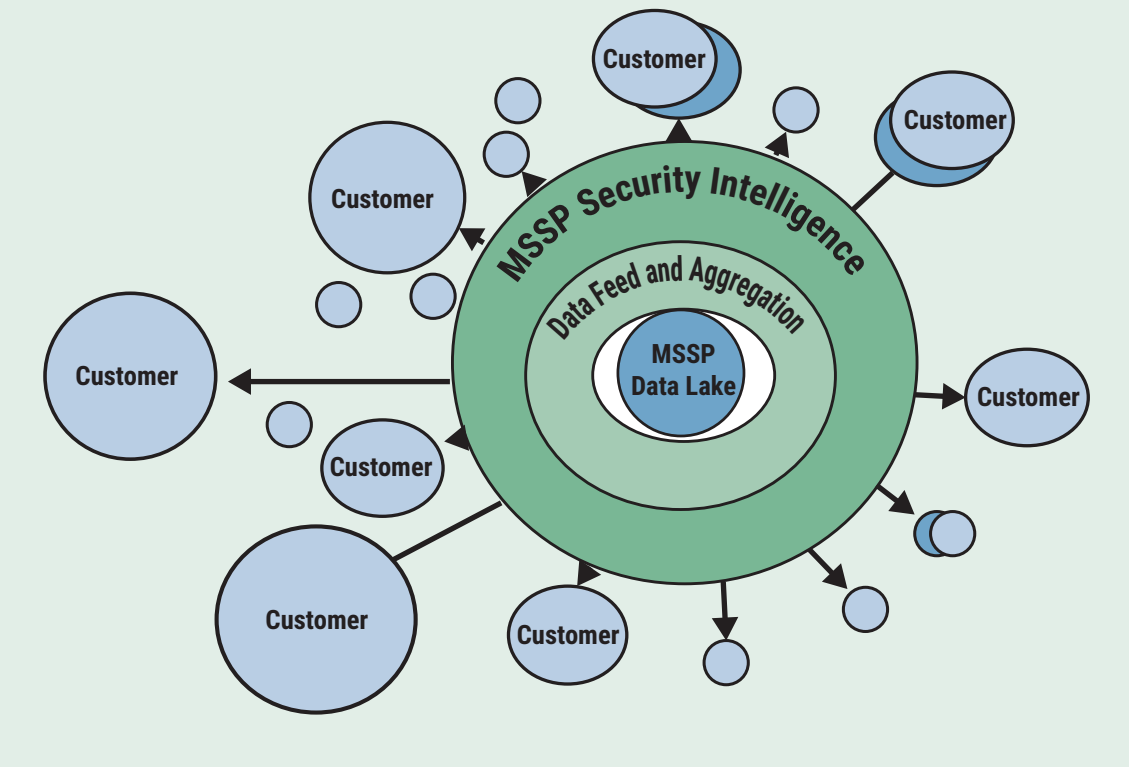
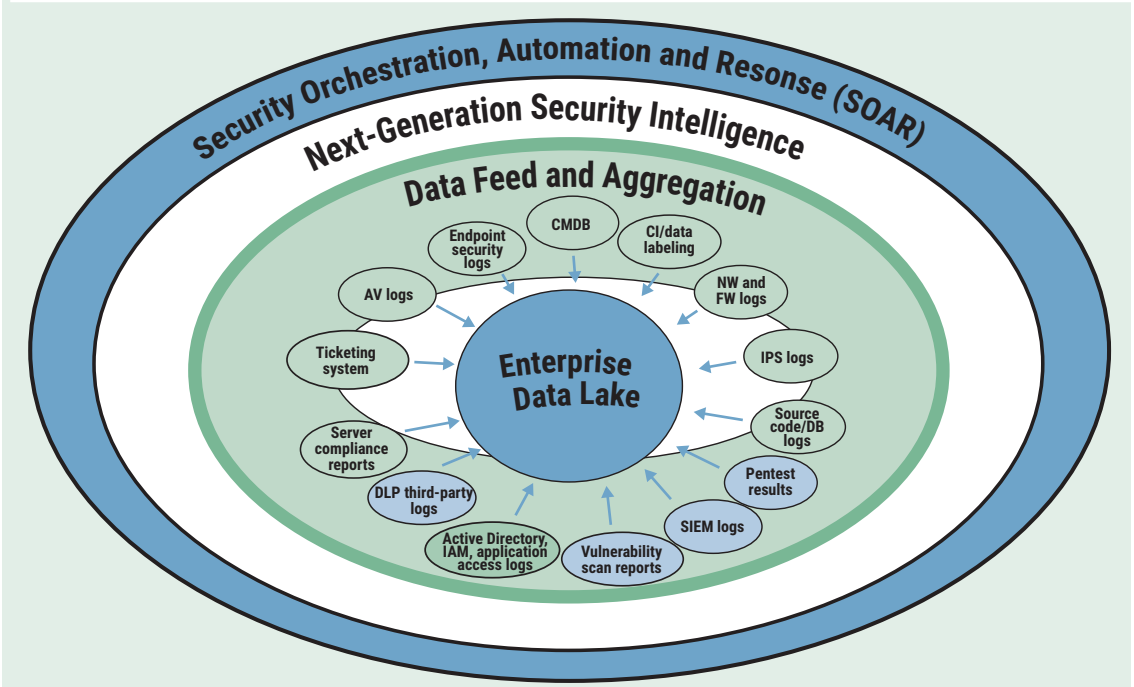


Figure 4—Security Intelligence Defense Framework



external sources. The more data available from different sources, the better security prediction and insights about emerging threats inside and outside the enterprise. Then, data source aggregation is implemented by connecting various security and nonsecurity data sources to the enterprise data lake. Data can take the form of alerts, logs, incident information, application access logs, data loss prevention (DLP) logs and SIEM logs.

The next layer centralizes and continuously enriches the enterprise's security intelligence knowledge. This layer interconnects various external or internal threat feeds augmented with predictive and automated response capabilities. Powered by ML and big data analytics over the large data sets ingested at the data aggregation layer, the primary objective here is to continuously update the TTPs and IoCs in real time, near real time or as the result of batch processing. The enterprise security intelligence knowledge is, therefore, continuously enriched with uncovered emerging threats, ongoing attacks, new IoCs and TTCs, new threat detection algorithms, and updated security operation playbooks (**figure 1**). "Combining automation and machine intelligence will enable increased use of predictive analytics to anticipate and mitigate threats earlier and more effectively."[6]

The top of the framework is the SOAR layer. Fueled by the predictive and interconnected security intelligence knowledge from the previous layer, it allows the organization to orchestrate and automate security operations based on workflows and playbooks. Security threat detection from the security intelligence layer triggers workflows involving the SOC team and the security incident response team (SIRT) and provides automated or semi-automated responses to security events.

Security Intelligence Interconnectivity

Interconnectivity is an important aspect of the security intelligence notion introduced here:

> *The globalization and increasing complexity of modern cyber security operations have made it virtually impossible for any organization to properly manage cyber threats and cyber incidents*

> THE DOMAIN OF THREAT INTELLIGENCE SHARING IS STILL DEVELOPING, AND THE ADOPTION OF INTEROPERABLE PROTOCOLS AND APIS IN THREAT INTELLIGENCE PLATFORMS HAS A LONG WAY TO GO.

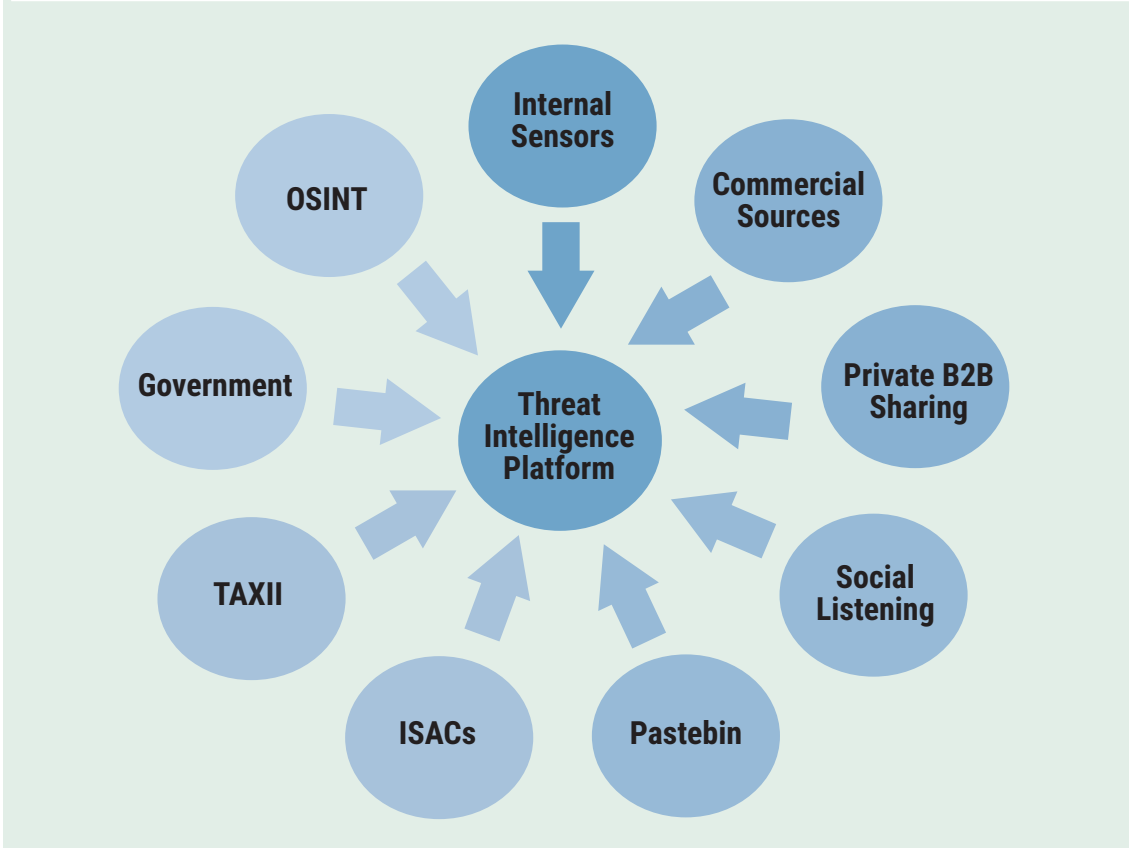
without leveraging various collaboration instruments with different partners and allies.[7]

One approach is to integrate a threat intelligence platform using one or more external threat intelligence feeds and ensure that there are continuous updates of the threat intelligence knowledge based on open protocols and application programming interfaces (APIs). This allows for "always on" security protection. Many threat intelligence solutions offer machine-readable intelligence that can integrate seamlessly with the various security products an enterprise already is using, and an increasing number of solutions are adopting open-source standards, making it easier than ever to share data across platforms.

Several works aim at formalizing security incident and threat knowledge sharing among different actors, taking into account the repercussions of sharing sensitive data.[8]

Threat Intelligence Sharing Standardization Efforts
As highlighted by researchers, "considerable efforts have been put during the last decade to standardize the data formats and exchange protocols related to Threat Intelligence."[9] Existing efforts classify standards into different areas including configuration guidance, vulnerability alerts, threat alerts, and risk and attack indicators.[10] Structured

Figure 5—Threat Intelligence Platform and Feeds



Threat Information eXpression (STIX) language seems to have become the *de facto* standard for describing threat intelligence data and has the largest adoption.[11]

However, the domain of threat intelligence sharing is still developing, and the adoption of interoperable protocols and APIs in threat intelligence platforms has a long way to go. The majority of platforms primarily focus on the sharing of basic indicators of compromise and not so much on adding intelligence.

Threat Intelligence Feeds

There are multiple threat intelligence feeds to which an enterprise can subscribe to nourish its IoC and TTP repositories (**figure 5**). A good approach is to get feeds from both open-source (i.e., communitywide, nonprofit organizations that provide a central resource for gathering threat intelligence knowledge) and closed-source (e.g., public, private and unindexed from dark or deep web) feeds.[12] It has been estimated that "the public part of the internet only makes up approximately four percent of all data online. The remaining 96 percent belongs to the deep and dark web."[13] Paid feeds can provide data gathered from closed sources such as the dark web. Open-source feeds, on the other hand, are free, but need to be manually curated. Country-specific, military-specific cyberattacks happening at a geographical level can be gleaned from government intelligence feeds. Gathering of information through social media platforms, such as Twitter, LinkedIn and Facebook, is called social listening. Pastebin (a text repository for storage/copy/paste allowing access via API) is a great source of threat intelligence information. Some known feeds are MITRE ATT&CK,[14] Alien Vaults, ThreatConnect, open-source intelligence (OSINT), STIX and Trusted Automated eXchange of Indicator Information (TAXII)–based platforms, and information sharing and analysis centers (ISACs). ISACs as nonprofit organizations deserve special attention, as they allow for closer cooperation between the private and public sector and are supported by both the US government and European legislation and the European Union Agency for Cybersecurity (ENISA).[15]

Threat Intelligence Platforms

Threat intelligence platforms (TIPs) are content management systems that aggregate intelligence data from different threat intelligence feeds, normalize them, prioritize the sources, carry out some data curation and organize data into a single platform. One of the essential features of TIPs is the ability to set up alerts and notifications based on the data so that security analysts can react quickly to an attack.[16] Another key feature is the TIP ability to be extended by external sources.[17] Threat information should be both human and machine readable, and the sharing mechanism must allow threat intelligence sharing between the platform and different stakeholders.[18] TIPs can also be integrated into other security systems such as SIEMs, web application firewalls (WAFs), end-point detection tools, DLP, IPS, firewalls and email gateways.

> "THE ADVENT OF SOAR TECHNOLOGIES MAY BECOME A BIG CORNERSTONE IN SECURITY OPERATIONS AND, THEREFORE, A WIDER ADOPTION OF SOAR BY ENTERPRISES IN THE NEAR FUTURE MAY BE EXPECTED.

Next-Gen SOC

The security intelligence defense framework in **figure 4** allows for a new approach toward traditional Security Operation Centers (SOCs) and security incident response (SIR) teams leading to the so-called next-gen SOC. Time-consuming activities such as analyzing logs, reports and alerts can be automated. Alert fatigue could be reduced significantly because many false positives could be eliminated, thus allowing the SOC/SIR teams to work smarter. For example, traditional SIEM alerts could be combined with non-real-time processing activities making it possible to rank alerts and set priorities for the SOC team. Remediation activities could be partially automated to reduce security incident response time.

This would make it possible for more proactive actions, reducing the time to contain or stop the attack and allowing for faster remediation. New SOC roles appear such as security data analysts and ML model maintainers. The next-gen SOC can combine SOC, SIRT and threat-hunting activities where the borders of these (currently distinct) activities start disappearing.

Next-gen SOC will:

- Know better, as it will discover and contain attacks in real time
- React faster, as it will make use of security orchestration and automated workflows, from automated alert creation and triage to a full-blown SOAR solution and automated response.
- Be smarter, as it will benefit from a faster and more accurate event analysis enabled with ML and data analytics in real time, near real time and batch processing.

The advent of SOAR technologies may become a big cornerstone in security operations and, therefore, a wider adoption of SOAR by enterprises in the near future may be expected.

Conclusion

Security attacks have become interconnected and better coordinated on a global scale; therefore, they require a new generation of security intelligence that is interconnected, predictive and automated in nature. New threats should be dealt with using a new set of technologies: ML and big data analytics. An innovative security intelligence defense framework should enable enterprises to make use of an actionable, trifolded security intelligence, fueling the next-gen SOC to make use of security intelligence interconnectivity, intelligence automation and predictability.

The application of ML to cybersecurity challenges is still in its early stages and important advancements are needed in the near future. Development and adoption of open protocols for the sharing of security intelligence knowledge needs to grow as well to allow a global response to security threats that are happening on a global scale. The interoperability of the security intelligence knowledge and integration of APIs and open protocols will become an important driver for security vendors and will turn into a key criterion for the enterprise defense strategy.

The era of siloed security seems definitively gone. Everyone is connected in an insecure world. A sound security architecture cannot be designed if the principle of security oneness is not understood. Only interconnected, predictive and automated security intelligence will augment capacities of organizations to operate in an increasingly dangerous world. The only realistic option toward enterprise security is the interconnectivity and automation of the security intelligence knowledge augmented with ML and big data analytics to turn security intelligence knowledge into a predictable and proactive cyberdefense strategy.

Authors' Note

The opinions expressed here are the authors' and do not necessarily reflect those of their employers.

Endnotes

1 Bracy, J.; "The IoT Zombies Are Already at Your Front Door," The International Association of Privacy Professionals, 29 September, 2016, *https://iapp.org/news/a/how-poorly-secured-iot-devices-can-take-down-your-website/*
2 O'Donnell, L.; "Top 10 IoT Disasters of 2019," Threatpost, 23 December 2019, *https://threatpost.com/top-10-iot-disasters-of-2019/151235/*
3 MITRE ATT&CK, *https://attack.mitre.org/*
4 *Op cit* Bracy
5 Jou, S.; "Best Practices for Deploying and Utilizing UEBA: Improve Your Security Operations with Real-World AI," BrightTALK, 16 April 2019, *https://www.brighttalk.com/webcast/288/353391/best-practices-for-deploying-and-utilizing-ueba*
6 Saunier, L.; K. Delic; "Corporate Security Is a Big Data Problem," ACM Ubiquity, July 2018, *https://ubiquity.acm.org/article.cfm?id=3158348*

7 Hernandez-Ardieta, J., *et al*.; "Information Sharing Models for Cooperative Cyber Defence," 5th International Conference on Cyber Conflict (CYCON 2013), 2013, *www0.cs.ucl.ac.uk/staff/G.SuarezdeTangil/papers/2013cycon.pdf*
8 *Ibid*.
9 Chantzios, *et al*.; "The Quest for the Appropriate Cyber-Threat Intelligence Sharing Platform," 2019
10 Skopik, F.; *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level*, CRC Press, USA, 2017
11 Structured Threat Information eXpression (STIX), *https://stixproject.github.io/*
12 Recorded Future, "Five Threat Intelligence Solution Use Cases," 23 January 2019, *https://www.recordedfuture.com/threat-intelligence-use-cases/*
13 *Ibid*.
14 *Op cit* MITRE ATT&CK
15 The European Union Agency for Cybersecurity (ENISA), *Information Sharing and Analysis Center (ISACs): Cooperative Models,* Greece, 2018
16 Sauerwein, C.; C. Sillaber; A. Mussmann; R. Breu; "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives," WI2017 Conference
17 *Ibid*.
18 *Ibid*.