IBM Security
White Paper

October 2017

The awakening of cyber threat hunting: Intelligence analysis for security and risk

Contents

A view of the problem

What if your entire profession revolved around a seemingly unsolvable problem? Imagine issues and crises that never end but can only be managed. This paradigm is something the medical field has dealt with nearly since its inception—an onslaught of disease and injury in a seemingly never-ending cycle.

Over time, physicians evolved their field to deal with threats by creating specialized disciplines. Critical issues are handled by emergency medicine; difficult issues such as neurology and cardiovascular are handled by their own specialties. Epidemiologists and preventative medicine study long-term trends and patterns. Now the profession of modern medicine can apply more tailored solutions to efficiently mitigate issues. It is clear that the medical profession is far more effective today than 100 years ago, prior to the inception of medical specialties.

Similarly, the field of cybersecurity is maturing as it progresses. The new specialty of cognitive analytics is the emerging discipline; aiding the human security analyst in discovering the unknown, and generating insights from disparate data sets with a focus on uncovering advanced threats.

We can learn many lessons from comparing the threats in the cyber domain to that of the field of medicine. This view on creating the discipline of cyber cognitive analysis was inspired by the profession of medicine—a craft where one must constantly learn by doing, continue educational training, and always aspire to become better.

Just a quick glance at the news illustrates the daily drama in the domain of cybersecurity. According to the 2017 Verizon Data Breach report,[1] 1,935 confirmed data breaches and 42,068 security incidents were recorded over a twelve month period—and that was only across 1,003 organizations. How did our public and commercial enterprises arrive at such a dire state of affairs in security? The primary causes for the current security crisis fall into two pillars:

Pillar one—evolution of the threat

- Commoditization of advanced techniques. Typically when experts discuss the breakdown of cyber threats, the 80/20 principle is brought up—meaning 80 percent of cyber actors are generally less sophisticated and the top 20 percent are so advanced that given enough time and resources they will break onto any network. Historically, the top 20 percent of actors were mainly the concern of the defense and intelligence community. Now, the emergence of commoditized threats has spread advanced techniques to a larger audience. Starting in 2006 the emergence of the "Web Attacker" exploit kit brought a packaged suite of tools that any user could operate.[2]
- Sophisticated developers who spent years honing their hacking techniques can now profit from their experience by selling hacking toolkits as a software package. Exploit kits attack known vulnerabilities to deliver malicious payloads of the attacker's choice. New exploit kits are continuously being developed with different attack vectors and infection techniques. At any given time there are dozens of exploit kits available—including Zeus variants, FlokiBot, NukeBot and GM Bot—and the widespread use of these tools has increased the sophistication of tactics, techniques, and procedures among a full spectrum of attackers.
- Rise of the asymmetric threat. In an asymmetric conflict the two conflicting sides may differ greatly in power and capability but are able to continually engage due to the exploitation of key vulnerabilities. Over the centuries, small forces have been able to stifle larger forces by leveraging terrain and tactics. The concept is similar in the cyber domain with a hacker using a low priced laptop, a USD 500 exploit kit3 and some innovative techniques to obtain the ability to penetrate a network where millions have been invested in security. Common examples of asymmetric cyber threats include impacting stock markets by issuing false tweets from a hijacked twitter account or a small group or individual crippling an organization's operations by encrypting critical information with a ransomware attack. The ongoing conflict in the cyber domain has become a human problem with individual hackers continuously outwitting common security systems.

- **Focus on confidentiality.** Effective information security is defined according to three core pillars: confidentiality, integrity, and availability. The confidentiality of data is the guarantee that only those who are properly authorized may have access to a system's information. Integrity of data is the concept that all information within a system is holistic, complete, and free of errors. Availability of data refers to the amount of time a system is functioning, or is available to be accessed by the user.
- Attackers target all of the pillars. They have attempted to disrupt the availability of networks with denial of service attacks, encrypted data to be held for ransom, corrupted data by injecting or changing emails and other data, and violated confidentiality by outright theft of data. The weapon of choice for attackers is generally some type of malware that is delivered via spam emails.
- The IBM® X-Force® Threat Intelligence Index 2017 reported that from 2013 to 2015, 431 million new malware variants were released.[4] This growth hasn't abated as AV-TEST Institute registered 390,000 new malicious programs every day.[5]
- The X-Force report also re-enforces that malware is delivered as attachments in spam, which increased 400 percent in 2016 compared to 2015, and there was a marked increase in the volume of malicious attachments.[6] The malicious programs, such as Trojans, keyloggers, droppers, and ransomware, can allow a hacker to gain remote access to a system, while hiding the connection so it is harder to detect.
- Although cybercriminals impact all security pillars, most security technology, procedures, and frameworks focus on availability and keeping threats away from the perimeter, thus impacting the ability to provide integrity and confidentiality. The security industry needs to have more flexibility to address adversary tactics.

Pillar two—an incomplete security response

- **The wrong security objective.** Most organizations evolved a perspective of security with the objective of 100 percent perfection. In that quest they have made "perfect" become the enemy of "good enough." Security offerings have evolved to create a so-called impenetrable barrier, and for a long time the majority of investment focused on the perimeter. An example of this mindset can be seen in the 2017 Gemalto Data Security Confidence Index where 94 percent of information technology decision makers thought that perimeter security is "quite effective at keeping unauthorized users out of their network."[7]
- The cybersecurity community has not fundamentally changed the way networks have been protected over the past four decades. Much effort has been placed on building the next-generation firewall—expanding the virtual moats and perimeter defenses that surround networks. When an adversary eventually finds a random vulnerability in the complex system, they can move freely in the victim's network. There is usually minimal monitoring and visibility within the network, thus allowing an adversary to move around unseen. For example, if an adversary were to discover an administrator's credentials they could gain unfettered access to all systems because administrator logins are generally not logged by security devices. By focusing too much on keeping the adversary out, most organizations did not emphasize resiliency, thus failing to limit the damage a malicious actor could do.

- **Too much data and too many tools.** Just obtaining the proper data for network visibility is an enormous task. Now, the modern network has massive amounts of tools and data storage recording every log, alert, and heartbeat. There is so much data that a single analyst can spend a lifetime sifting through the disparate sources to discover relevant events. Compounding the issue of too much data is the confusing array of security tools, which must be constantly maintained and configured. The information security team may very well have the indicators and solutions about a cyber attack, but the complexity of existing solutions make it difficult to discover answers in real time and to distinguish between what is important and what is just noise.
- **Not enough experienced personnel.** Both the public and private sector are rapidly seeking to swell their cybersecurity ranks with qualified personnel, but there are simply not enough trained persons. The US Bureau of Labor Statistics states that in 2015 there were 209,000 unfilled cybersecurity positons with about 40,000 of those specifically being for information security analyst positions. When candidates are found it takes time with many positions being open for six months or more. There has been a dramatic increase in educational opportunities and training geared towards the development of security professionals, however it will take considerable time to reduce the skills gap as the demand for cybersecurity jobs is expected to grow by 37 percent by 2022.[8] It will take even longer for the cadre of security analysts to become proficient through experience. Without a skilled team it is very difficult to keep up with the constant security operations.

Roles, responsibility and terminology

To begin a cognitive driven approach we must define the lexicon and outline specific roles. Much like the field of medicine began to specialize to attack complex problems, so must the security industry. Cybersecurity must be thought of as a profession with formal training, qualifications, and continuing education. The first such differentiation that must be drawn is between the operational aspects of security and the eventual product which is created. Thus, we should define the difference between *analysis*, *analytics*, *cognitive*, *and intelligence*.

Analysis is the examination, inspection, and investigation of relevant data in order to reach a conclusion. Generally, this process is human-led and a manual process.

Analytics is the systematic and procedural computational analysis of data or statistics in order to produce a result. Generally, this process is automated and heavily assisted by a computer.

Cognitive is the thought processes involved in the acquisition and understanding of knowledge, decision making, and problem solving. It is rooted in facts and not in emotions.

Intelligence is the ultimate result of the collection of valuable information produced in a format in which a decision or conclusion can be reached.

In this context, analysis and analytics are the *operational process* of data examination. The *product* of such a process is deemed *intelligence*, with the purpose of allowing a decision maker to gain valuable insight from otherwise confusing randomness.

Now, we must examine the difference between information *security* and *cyber analysis* (Figure 1). The term *information* security generally refers to operations conducted to strengthen the core of organizations architecture and *cyber analysis* refers to the examination of advanced threat.

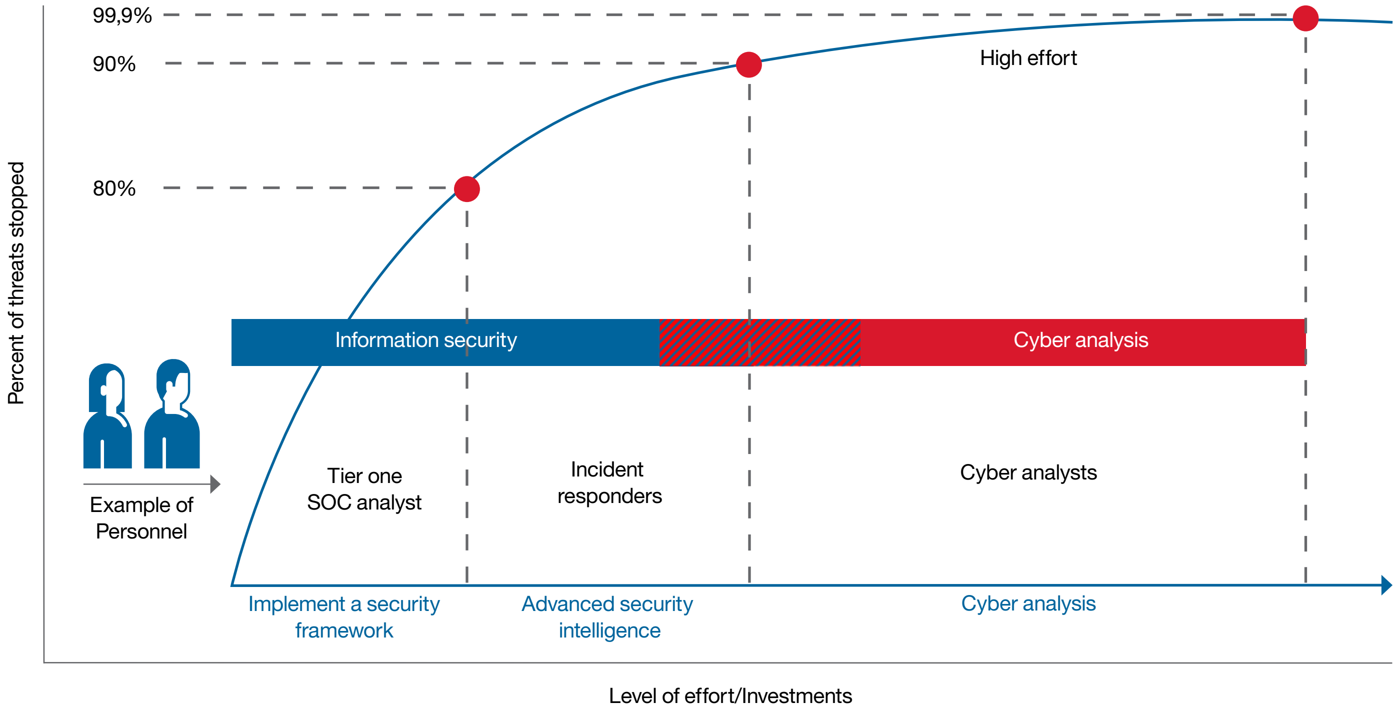


Figure 1: The difference between the domain of information security and cyber threat analysis.

In order to attack the full cyber threat spectrum an organization must embrace both information security and the natural evolution of cyber analysis which includes the use of cognitive tools, and is commonly called "Cyber Threat Hunting." Information security creates a foundation of security with a framework and builds upon that with some specialization and technology. Eventually, the security process evolves into cyber analysis with long-term research and ecosystem visibility concerning malicious actors. Drawing from the medical analogy, information security becomes the hygiene and triage of critical issues. Cyber analysis is analogous to medical and laboratory research, which examine more sustained issues (Table 1).

	Medical		**Security**	
	Threat example	**Mitigation Strategy**	**Threat example**	**Mitigation Strategy**
Tier One-Hygene	Common hospital associated infections	Washing hands, wearing masks and scrubs	Commodity threat, individual hackers with widely-used tools	Changing passwords, removing unused services, patching
Tier Two-Specialization	Emergent situations (like chest pain, gunshot wound)	Creation of critical care and preventative medicine discipline	Organized crime, semi-tailored fraud and crimeware tools	Visibility, monitoring, alerting, response, real-time security analytics
Tier Three-Research	Genetic diseases and cancer	Research and tailored genetic treatments	Advanced Persistent Treat, nation-state, high resources	Cyber analysis, threat inteligence trend analysis, campaign trecking

Table 1: This table depicts an analogy between the medical and cyber professions and how they developed mitigation strategies in order to mitigate various levels of threat.

Both the information security and cyber analysis dimensions require the operations of analysis and analytics. Human operators and analysts exist in both, examining data and alerts. Also, both dimensions use automated tools to assist with analytics and statistics — mainly to help automate repetitive actions. Cognitive systems act as a trusted advisor by processing much more data than a human can to uncovering new insights, patterns and security context. At the end of the process, both an information security and cyber analyst produce intelligence — the ultimate product or conclusion to help a leader make decisions. The intelligence products may vary in scope and scale. An information security analyst may be interested in a specific alert where a machine reverted to a vulnerable state. A threat hunter may look at the aforementioned event as one data point in a long-term trend.

In all of these cases, supplementing the investigations with a cognitive system expands and increases the accuracy of the intelligence available, which ultimately can lead to better informed conclusions.

The following definitions illustrate the differences between information security and cyber threat hunting:

Security analysis
The art of aggregating, correlating, and automating IT-related data in order to detect, discover, and understand information security threats. Much of this process is performed with automated tools that rely on algorithms and pattern recognition.

Cyber analysis
The art of human-led analysis of security and non-security related data from logical and physical domains in order to research trends, discover anomalies, provide context, create relationships, and uncover hidden issues.

Cyber intelligence
Evidenced-based knowledge and actionable advice concerning security related issues.

Security intelligence
Actionable information derived from the analysis of security-relevant data available to an organization.

The lexicon can vary between organizations because the field of cyber analysis and cyber threat hunting are emerging disciplines. Much like the field of medicine continually refines terms among the community, so will the profession of cyber. Some of the initial efforts in cyber analysis began in government organizations as a natural extension of the military intelligence process. As such, practitioners in the government sector tend to refer to the combined process of security analysis, cyber analysis, and threat research as “cyber intelligence.” This generally stems from the fact that government entities utilize an intelligence cycle as a means of fusing all data and creating products. Within the private sector, cyber analysts are also being referred to as cyber threat hunters in that they sift through data hunting for signs of attacks.

Case studies in the shortcomings of the current approach

The cyber domain is under a constant threat from malicious actors spanning the range of amateur hacktivists to nation-state actors. When discussing cyber threats it is important to keep in mind the two factors of an actor’s capability and intent. For example, a malicious actor may have the most advanced tools, but the motivation to use them in only the rarest of circumstances. Historically, there has been a distinct divide between actors with advanced capability and the intent to target the private sector. Similarly, actors with the intent to attack private entities lacked the tools, technology, and personnel to affect information networks. In the past few years we have seen a seismic shift in advanced threat profiles, which are of great concern to the private sector.

Attacks using low capability and high intent can still have the same damaging impact of a high capability actor. Due to the nature of the asymmetric cyber threat, organizations must protect against clever low capability attacks as well as high-impact sophisticated events.

The following are two case studies: one of the 2014 Sony Pictures attack, which outlines a high capability event. The other is a study of the successful 2016 attack against the Society for Worldwide Interbank Financial Telecommunication (SWIFT) banking network that resulted in the heist of tens of millions of dollars. The attack that compromised the payment process used relatively unsophisticated techniques to great effect. These studies show that an advanced actor can exist on a network unnoticed for months without being detected by common security approaches. It also shows that by not incorporating the human aspect of security into analysis, a low capability actor can easily penetrate a system and cause considerable damage.

Case study: the Sony attack

On November 25th 2014, reports began to surface that Sony Pictures was being attacked by a ransomware linked to a group calling itself the Guardians of Peace.[9] Five days later, the FBI assists in the investigation and eventually releases a warning about the wider use of destructive malware. In the coming weeks hundreds of gigabytes of Sony's files were posted in a series of bundles in public forums and contained personally identifiable information, sensitive correspondence, and salary information.

On December 3rd 2014, Bloomberg News released an article describing an early examination of the malware found in the Sony network. An early examination of the malware makes it clear the hackers had become familiar with the Sony network beforehand. Analysis of the code found the names of Sony's internal servers as well as credentials and passwords needed to connect to the network. The malware was used to communicate with IP addresses in Europe and Asia, which is common for hackers trying to obscure their location. This may indicate hackers lived in the network for months.

On December 19th 2014, the FBI released an official update on their investigation,[10] concluding that the North Korean government was responsible for the attack. Reports indicate that's North Korean hackers had access to the network for months. Though the initial infection vector remains unknown, it is believed to be a targeted spear phishing campaign. Hackers used the malware BKDR_WIPALL.A-F in the Sony attack. This backdoor contained a list of user names and passwords, which it used in its attempt to grant access to the system root folder of an infected machine. The backdoor arrived on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. As a result, malicious routines of the dropped files are exhibited on the affected system. It connects to certain websites to send and receive information. In early February 2015, Sony announced that initial remediation costs would be around USD 15 million.

Case study: next-generation bank heist

On February 4th 2015, the Federal Reserve Bank of New York processed four requests to transfer USD 101 million from the Bangladesh Central Bank to banks in the Philippines and Sri Lanka. The transactions were handled in accordance with the procedures and credentials governed by SWIFT—an international consortium that operates a trusted and closed computer network facilitating the transfer of funds between member banks around the world. Although the transfers seemed out of the ordinary they were allowed to proceed because the credentials were valid and the New York bank was not able to receive replies to their queries to Bangladeshi authorities.[11]

The autopsy of this operation discovered that the unknown assailants introduced malware, most likely a Remote Access Trojan (RAT), into the victim's computer systems a few weeks before the plan was executed. The malware was able to collect user credentials and the infiltrators then observed the processes on electronic funds transfers. After collecting sufficient information, the fraudsters finally launched their operation. Understanding the mechanism also allowed the hackers to remove a critical system file and disable the printer that recorded each money transfer request,making it harder for the bank to see the transfers before they could be halted.[12]

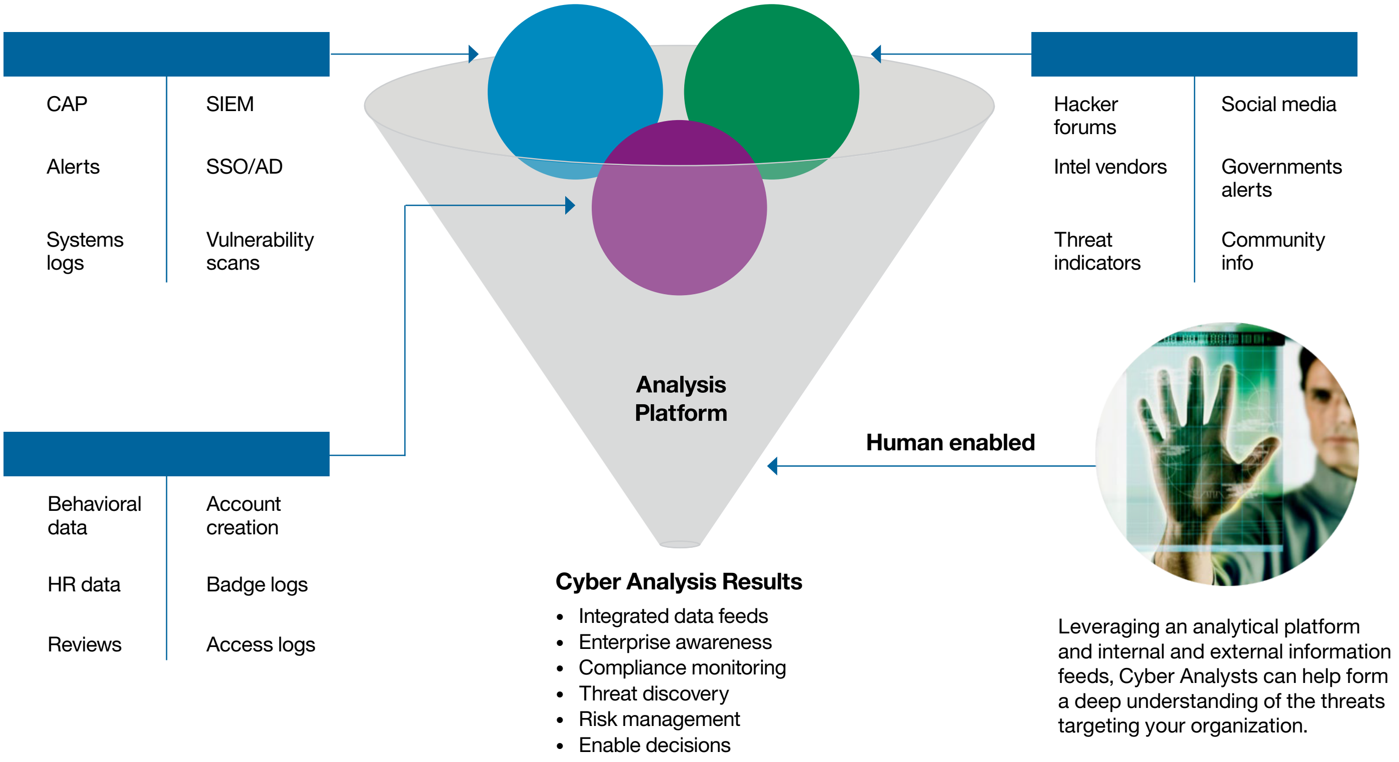
The incident could have been much worse in that the hackers submitted dozens of transactions but due to typos in the request documents all but four were rejected. However, the incident is significant because it caused international financial institutions to question the system used to process millions of daily communications. Investigators revealed that the malware used in the heist was almost identical to one used to infiltrate banks in Ecuador, Vietnam, and the Philippines.

Investigations into the hack uncovered how the criminals were able to acquire credentials, understand the bank's processes, and try to avoid detection. However, the examination also discovered lax security at the Bangladesh Central Bank. Their network was not protected by a firewall, thus making the implantation of malware much easier. In many of the recent high-profile data breach cases, it is evident that the victim organization lacked resiliency in the network. Harkening back to our medical analogy, this is the equivalent to getting a small paper cut where a virus can get in and eventually dying as a result of missing the symptoms of an infection. For this specific case detecting the malware in January 2015 could have prevented the events of February 2015.

Concepts of intelligence operations: the new approach

Cyber threat hunting is one of the newest fields in the security profession. The emerging discipline blends aspects of intelligence analysis, information security, and forensic science. Network traffic and system logs are a foundational data source for cyber threat analysts, but they must also consider external and human generated sources of information. By using cyber analysis, one can detect infiltrations faster, regardless of their source. Pairing advanced analytic and cognitive platforms with a human is the most effective way to detect an infiltration.

Cyber hunters excel in finding unique patterns among massive datasets. Consider the four phases of a hacker's attack: reconnaissance, scanning, exploitation, and persistence. If an organization consolidates systems logs and network traffic, analysts can sift through the data at each phase. Analysts can link associated events among multiple sources and replay how an attack occurred. Tracing patterns over time, analysts can determine the signature of a scan and assign it to specific actors. This will help predict when an attack will occur. Traffic from backdoor beaconing can be found quickly and blocked at the gateway. The source of data will be irrelevant; analysts can just as easily identify traffic from an insider threat as they can from Internet-based attacks. Consider the SWIFT heist example described above, perhaps with a holistic intelligence analysis and information sharing approach the theft would not have occurred due to an analyst identifying the initial pattern.



Cyber Analysis Results

- Integrated data feeds
- Enterprise awareness
- Compliance monitoring
- Threat discovery
- Risk management
- Enable decisions

Leveraging an analytical platform and internal and external information feeds, Cyber Analysts can help form a deep understanding of the threats targeting your organization.

Figure 2: The various components that feed the cyber threat analysis process.

Where does the cyber threat analysis discipline fit into the modern Security Operation Center (SOC)? Overall security operations are divided temporally into the areas of tactical, operational, and strategic. In each phase of operation, analysts may produce data and intelligence, which inform decisions. The full security spectrum and key functions are defined as follows:

Tactical phase. The intelligence produced from this phase is mainly useful for security operators in the day-to-day fight. Most commonly seen tools in this field are threat feeds or indicators of compromise (IOCs). This phase can be sub dived into *current operations* (0-24 hour horizon) and *future operations* (1-5 days). *A tier one analyst* is usually the key role in current operations, where events of interest are constantly examined and triage is performed to determine critical events. A tier one analyst may have between one and fifteen minutes to examine each event of interest. A tier two analyst accepts cases from tier one and performs in-depth analysis to determine what actually happened and if an event of interest may be an incident. A tier two analyst may use a system incident and event monitoring (SIEM) tool is assist in this function. The tier two function may span across one to five days in order to examine interesting activity. This may be the equivalent in the medical field to emergency room operations.

Operational phase. This phase attempts to determine the nature of the attack, using advanced forensic analysis. Incident responders or reverse engineers are the key personnel in this phase, using artifacts such as hard drive images, full-session packet capture (PCAP), or malware reverse engineering to determine exactly what happened in an incident. They may use security intelligence or forensic tools to assist in this function. Sometimes, forensic evidence must be collected and analyzed to support an official investigation. This phase attempts to determine what went wrong in an incident and produce intelligence to prevent future problems.

Strategic phase. This phase attempts to look at a larger ecosystem of data in order to provide insight into threats, vulnerabilities, and adversary TTPs. The process of cyber threat hunters will combine cyber news feeds, signature updates, persona data, incident reports, threat briefs, and vulnerability alerts to eventually produce cyber intelligence. Intelligence from the strategic phase can help senior leadership make key decisions about security investment—it answers who is attacking me, and why? Intelligence about threat actors attacking similar organizations may be fed into the tactical and operational phases in order to make operations more efficient.

The strategic phase opens the aperture of data and examines issues across much longer timelines. This would be the equivalent in the medical field to long-term research on genetic diseases. Imagine some cancers, which take a long time to reveal noticeable symptoms. There may however be underlying indicators or identifications which hide just below the "noise floor." By conducting research to identify the combination of seemingly normal indicators, physicians may be able to discover hidden cancer before it progresses to a dangerous stage.

There can be a wide variety of use cases in cyber analysis and associated platforms. In the simplest use case, consider efficiency with a 100,000 to 1 reduction ratio of events to correlated incidents. On the surface, this sounds impressive, but many organizations can generate 2 billion events per day. This will leave that company's security team with 20,000 incidents per day to investigate. Traditional SIEM correlation may reduce noise down to such a degree that important correlations are missed. A cyber analysis platform that can utilize the experience of trained human experts and cognitive-aided machine processing may quickly identify important latent activity.

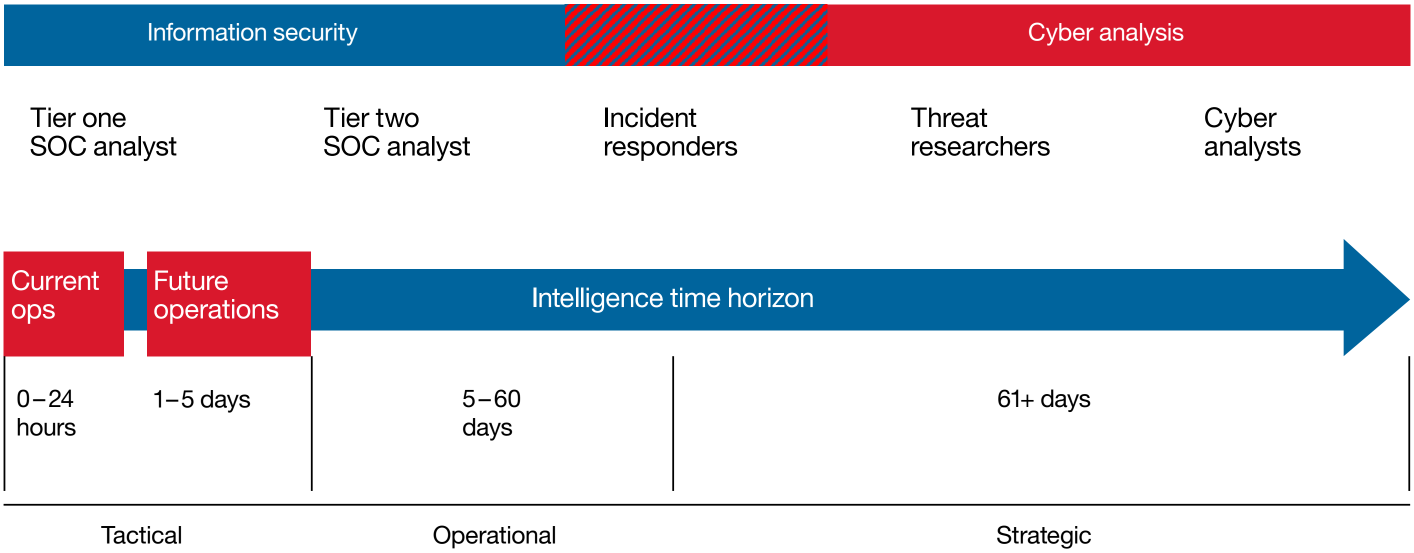
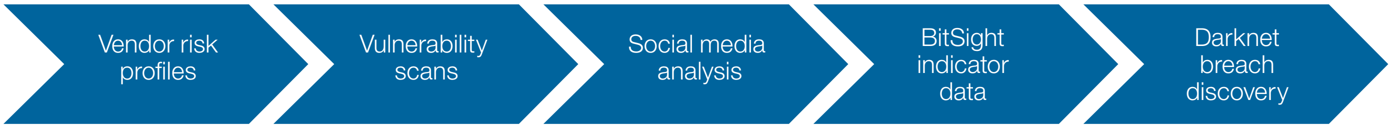


Figure 3: The intelligence time horizon as it applies to information security and cyber threat analysis.

The following are other use cases that utilize cyber analysis:

- **Whaling campaigns.** By combining email metadata, threat indicator feeds, and web proxy logs, cyber analysis can uncover a spearphishing campaign against a large company's top tier executives, known as whaling. This activity must be discovered through analysis and is not obvious in the individuals' feeds alone.
- **Beaconing activity.** Analysts may discover odd open port activity outbound to various locations as a starting point. Examining proxy logs and correlating with external data, analysts can discover the initial source of infection and perhaps the precise data that was compromised.
- **Discover hidden RDP sessions.** Analysts may see anomalous Remote Desktop (RDP) sessions occurring at regular intervals. Pulling in HIPS, IDS, and firewall logs, analysts can discover where perimeter security failed to detect a remote exploit that was allowed to execute on internal systems.
- **Internal botnets.** Analysts can combine proxy logs, firewall logs, and IDS datasets. Through visualization and discovery within these datasets, an internal botnet controller may be found proliferating through an internal business network. The infected machine may beacon out to a malicious command and control node through encrypted sessions looking like normal traffic.
- **Insider threat.** Examining HR databases, administrator records, and a business intelligence database, analysts can discover terminated employees who still maintaine unrevoked high-level administrator access. Additionally, analysts can use temporal analysis to quickly determine which employees consistently access critical systems during off hours.
- **Vendor risk management.** Some large organizations may have tens of thousands of vendors utilized for various types of services. Mature security programs will attempt to understand the risk of these vendors, but often have difficulty prioritizing which pose the highest risk. Figure 4 depicts how a cyber analysis process will make the vendor risk process more effective.



A security vendor risk management team interviews and records information about vendors. Reports contain pages of information detailing infrastructure and protection.

Periodic vulnerability scans are conducted against vendor's servers which contain sensitive company information.

Constantly analyze various social media feeds for malicious actors discussing potential threats against vendors.

BitSight provides real-time data concerning botnet and other vulnerability activity stemming from a vendor's infrastructure. The data service provides a real-time risk rating for each vendor.

By mining various darknet data feeds, the security team may discover indicators of a breach concerning one of the vendors who may contain sensitive company data.

Figure 4: An analytics process to help identify a company's most at-risk vendors.

Proof points with IBM i2 Enterprise Insight Analysis

The human analyst is the crucial component to the cyber analysis process. The analyst will use intuition and experience to discover hidden threats and develop patterns of threat activity over time. In order to maximize an analyst's capability and multiply work capacity, a mature security organization must use a data analysis tool to enrich, produce, visualize, and analyze information. IBM uses IBM i2® Enterprise Insight Analysis (EIA)—an open, interoperable, extendable, and scalable solution that helps organizations accelerate the data to decision process by enabling them to perform analysis and advanced analytics at scale and with critical speed.

The following are specific cyber analysis and threat hunting uses cases created i2 EIA:

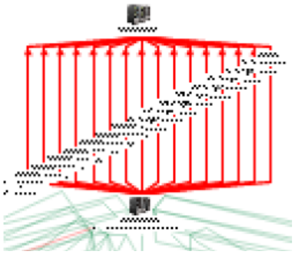
Unify the SOC analysts: connecting the dots over time

Issue: What hidden activity is hiding among datasets? How do you condense disparate events over time?

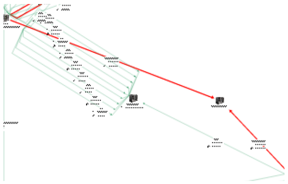
Why this is difficult: Advanced actors may use low and slow techniques to remain obfuscated.

i2 Enterprise Insight Analysis cyber solution: Advanced actors may use low and slow techniques to remain obfuscated.

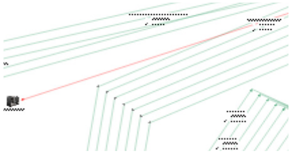
Part of cyber analysis is hunting for patterns, searching for the typically undetectable—the unknown unknowns. Imagine a typical SOC with multiple analysts that work over 2-3 different daily shifts. There may be even five different personnel allocated for each position. An analyst may notice an interesting event and then dismiss it as a benign anomaly. Another analyst on a different shift may notice a similar event with some correlated properties but not identify the similarities between the issues. These hard to detect anomalies are perhaps signs of "low and slow" attacks, which are very difficult to detect. Let's examine four separate events that if discovered by separate SOC analysts may appear unrelated:



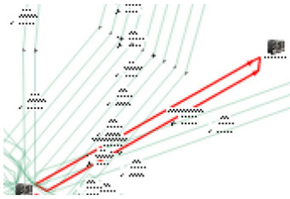
Strangle mail traffic: an analysts notices email traffic originating from a DHCP server on an unusual port.



Port 81 traffic: HTTP network traffic is recorded on port 81; sometimes this is associated with TOR.



LDAP traffic on port 80: an analyst noticed LDAP traffic on Port 80 rather than 689 as usual.



Outbound FTP: strange outbound FTP traffic is discovered in the network on Port 20.

Figure 5: Four seemingly unrelated anomalies could signal a "low and slow" attack.

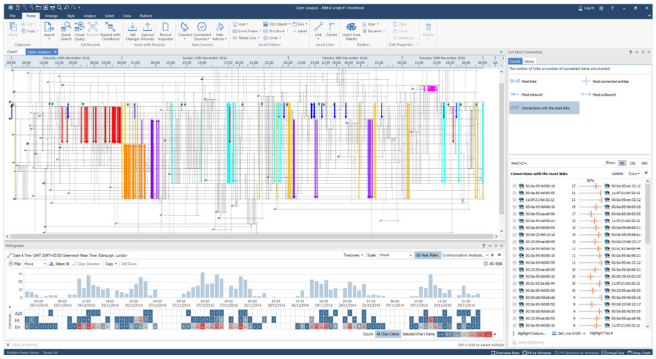


Figure 6: As a way of seeing into the unknown, i2 EIA helps the analyst discover issues unfolding over a longer time horizon.

Tracking threat Campaigns: Predict who will attack you…and when

Issue: Who is attacking me? Where am I most vulnerable? When will an attack potentially occur?

Why this is difficult: Data on actors and attack vectors will come from disparate sources in silos.

i2 EIA cyber solution: Advanced analytics, such as social network analysis, visual query tools, data fusion.

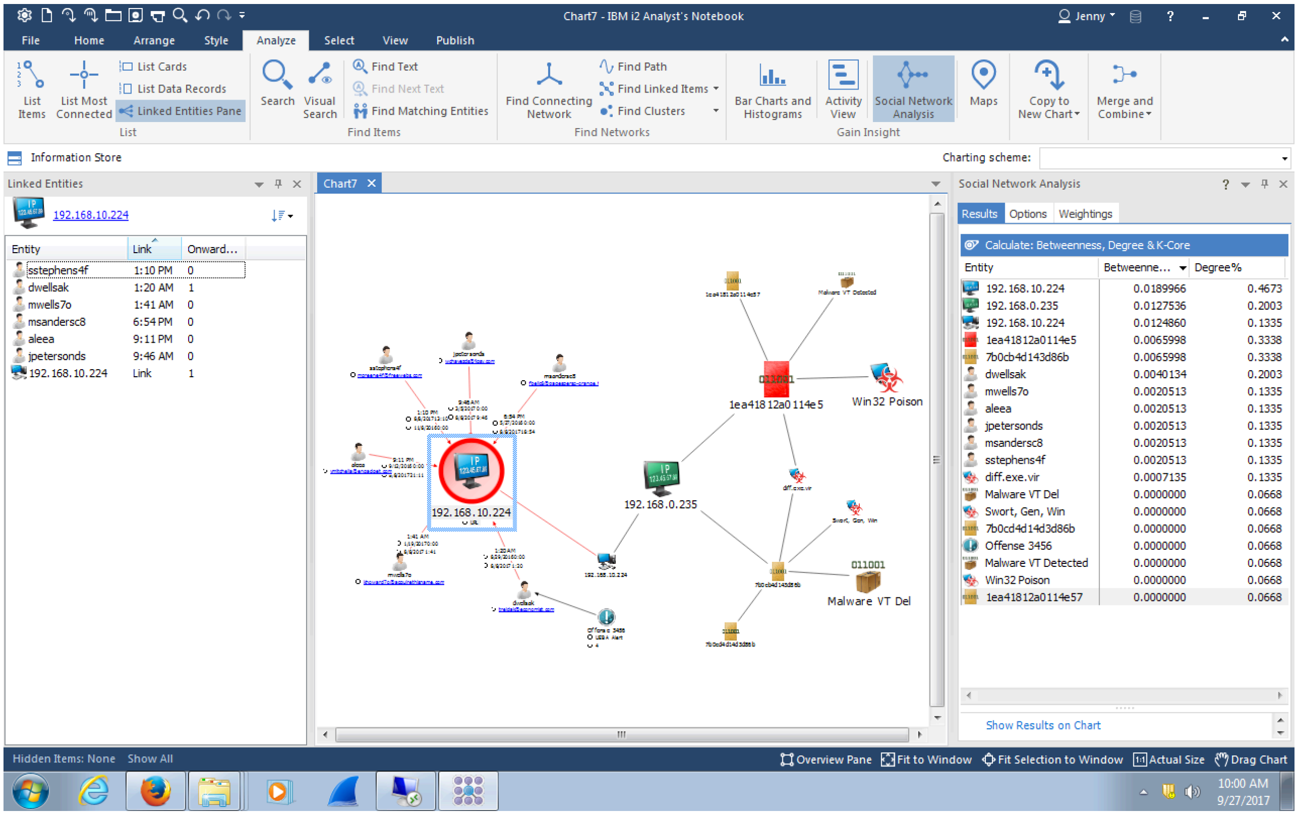
One of the key differentiators of a cyber threat analysis platform is the ability to take all the external security data and compare to an organization's internal security operations. This perspective is a critical function for an internal cyber intelligence team to make all the data in the security ecosystem relevant and actionable to an organization. i2 EIA enables this component of strategic analysis by enabling the ingesting of multiple data sources and providing an advanced analytic tool.

The complete picture: an analyst using i2 EIA discovers that these events are related. All the anomalies are connected to DHCP servers initially infected by malware. The malicious actors used one server to send phishing attacks to users in the network. Once the individual users were infected, FTP sessions are established with a C2 server and data is exfiltrated. The sophisticated actors used odd ports to mask connections to C2 nodes and hide internal traffic.

Open up the aperture. Unstructured and structured source data are imported automatically from public, deep web, vendor, and social media sources. IBM i2 EIA can automate this process. In forums, actors will discuss tactics and post claims on targets they attack. Hackers will often reuse screen names between legitimate and dark web sites. This correlation can be used to understand relationships between individuals otherwise hidden. STIX/TAXI type data may also be ingested concerning historical attacks, which reveal patterns..

Understand the who and the how. Automated social network analysis tools allow analysts to see threat actor interpersonal relationships, movements, techniques, and procedures. An analyst may discover geo IP address information connected to threat actors, which can be used by the security team to identify threats. Understanding the industries targeted by a particular group and how they penetrated associated defenses can be compared against the organization's current security state.

Figure 7: Social network analysis tools



Linked Entities

192.168.10.224

Entity	Link	Onward...
sstephens4f	1:10 PM	0
dwellsak	1:20 AM	1
mwells7o	1:41 AM	0
msandersc8	6:54 PM	0
aleea	9:11 PM	0
jpetersonds	9:46 AM	0
192.168.10.224	Link	1

Social Network Analysis

Results | Options | Weightings

Calculate: Betweenness, Degree & K-Core

Entity	Betweenne...	Degree%
192.168.10.224	0.0189966	0.4673
192.168.0.235	0.0127536	0.2003
192.168.10.224	0.0124860	0.1335
1ea41812a0114e5	0.0065998	0.3338
7b0cb4d143d86b	0.0065998	0.3338
dwellsak	0.0040134	0.2003
mwells7o	0.0020513	0.1335
aleea	0.0020513	0.1335
jpetersonds	0.0020513	0.1335
msandersc8	0.0020513	0.1335
sstephens4f	0.0020513	0.1335
diff.exe.vir	0.0007135	0.1335
Malware VT Del	0.0000000	0.0668
Swort, Gen, Win	0.0000000	0.0668
7b0cd4d14d3d86b	0.0000000	0.0668
Offense 3456	0.0000000	0.0668
Malware VT Detected	0.0000000	0.0668
Win32 Poison	0.0000000	0.0668
1ea41812a0114e57	0.0000000	0.0668

Figure 8: Automated social network analysis tools help analysts reveal deeper connections.

In all of the above cases, the cyber threat hunter can use IBM cognitive capabilities to uncover hidden patterns and connections buried in disparate data sets. The IBM i2 QRadar® Offensive Investigator app brings together elements of i2, QRadar, and IBM Watson™ for Cybersecurity by pushing QRadar data directly into the i2 Analyst's Notebook, allowing the built-in visualization, analytics, and mathematical modeling resident in i2 to correlate anomalous security events with unstructured data. By proactively correlating seemingly unrelated events and details, the threat hunter can gain a comprehensive understanding of the threat, the threat actor, and potentially uncover indicators of the adversary executing portions of the malicious operation and stop it prior to completion.

Call to action: critical success factors to remember

In order to enable success in cyber analysis programs, organizations must embrace a risk management strategy. The true purpose of intelligence is always to inform decision makers when making decisions. Cyber intelligence produced from cyber analysis should be used strategically in order to make risk mitigation decisions about cyber threats. The following concepts are key features, which will enable a cyber analysis program. The establishment of an analytical platform such as i2 EIA can enable the following critical components of a mature security intelligence program.

Advanced threats are real and growing

As seen in the many examples above, the cyber threat from advanced actors, such as nation-states, are now a reality in the private sector. More importantly, the advanced tactics procured by top tier adversaries tend to become commoditized among less-skilled criminal groups when the information becomes public. Attacks that require greater resources such as social engineering will become more common as breaches continue. Organizations must understand that anyone can become a target of advanced attacks, and not just meet the minimum security standards to counter common malware. It is important to shift resources to structured intelligence analysis in order to better counter stealthy advanced threats.

Don't forget the easy stuff

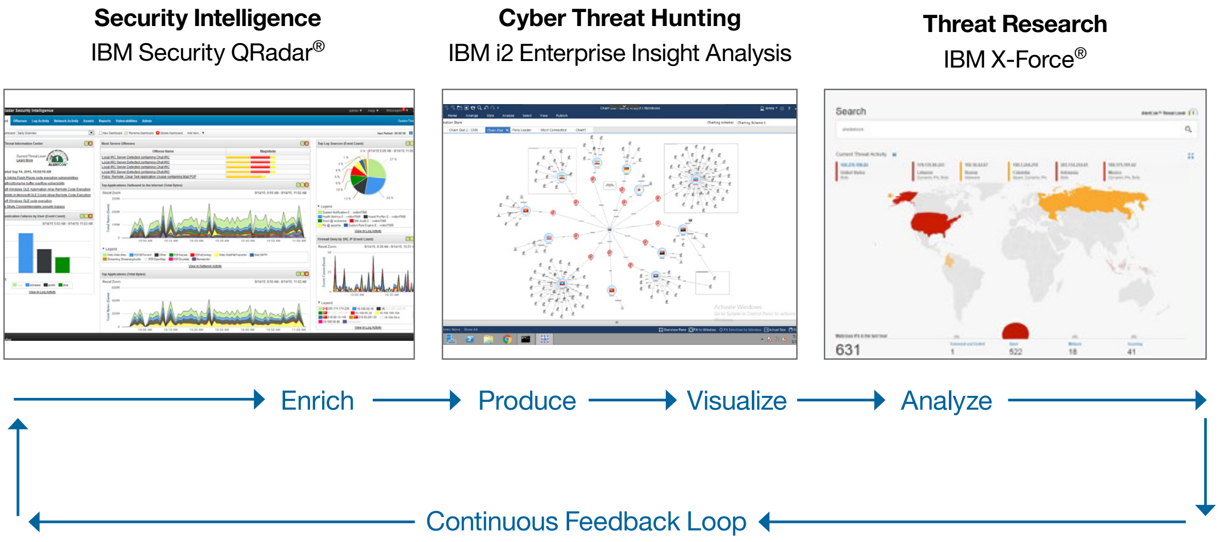
Contrary to popular belief, simple security controls are the most effective way to deter a majority of the threat actor spectrum. Malicious cyber actors have limited resources and just like anyone else, they will direct assets to what has the greatest return on investment. Organizations with proper security controls will likely be overlooked for easier targets. The Center for Internet Security's (CIS) Top 20 Critical Security Controls document has five controls that are considered quick wins. These controls offer substantial and immediate risk reduction against very common attacks without requiring major policy or technical changes to the organization's environment. These simple risk reducers include patching, standard system configurations, and limited administrative controls. Use of a cyber analysis platform a can enforce each component of a security framework.

Security is an "ecosystem"

Some law enforcement officials mention the phrase "using a network to fight a network." Organizations must build the connective processes between the security teams, cyber analysts, and external threat researchers. One of the key mitigation tactics against top tier actors is the participation in industry specific intelligence sharing groups. More complex actors will tend to use similar tactics and common traits shared among their targets or campaigns. By changing code or tactics just slightly, malicious actors can stealthily bypass most detection technology. With access to an intelligence-sharing network, "an attack on one organization is an attack on all." Information security professionals can share what they are seeing when an attack occurs and distribute indicators of compromise and compare them against vulnerabilities inside of a cyber analysis platform.

It's important to find out why an attack occurred

When an advanced attack occurs against an organization it is vital to understand why the infiltration was successful. There may be multiple dimensions which led to the attack from a policy control failure, to lack of technical detection capability. The best way to identify the root cause is to trace a decision tree, back-tracking the original attack to understand the underlying human decision which led to the issue. These indicators can be detected in the future by an analysis platform to prevent a future attack using similar techniques.



Security Intelligence
IBM Security QRadar®

Cyber Threat Hunting
IBM i2 Enterprise Insight Analysis

Threat Research
IBM X-Force®

Enrich → Produce → Visualize → Analyze →

Continuous Feedback Loop

Figure 9: IBM i2 Enterprise Insight Analysis cyber threat analysis is most effective when integrated with security intelligence and external research.

What’s next?

Learn more at www.ibm.com/cyber-threat-hunting

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] 2017 Verizon Data Breach Report

[2] www.threattracksecurity.com/resources/white-papers/exploit-kits-cybercrimes-growth-industry.aspx

[3] https://securityintelligence.com/commercial-malware-makes-a-comeback-in-2016

[4] IBM X-Force Threat Intelligence Index 2017, March 2017 page 21

[5] www.av-test.org/en/statistics/malware

[6] X-Force page 10

[7] www.news.europawire.eu/data-security-confidence-index-companies-under-invest-in-technology-that-adequately-protects-their-business-654321456890/eu-press-release/2017/07/13

[8] www.business2community.com/cybersecurity/booming-job-market-3-reasons-cybersecurity-jobs-will-reign-supreme-01434850#GQ6QQW3CgXv7sDAc.97

[9] www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202

[10] www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[11] www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

[12] www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know

Please Recycle