GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Creating a Threat Profile for Your Organization

GIAC (GCIH) Gold Certification

Author: Stephen Irwin, stephen.irwin@gmail.com
Advisor: Stephen Northcutt

Accepted: September 8th 2014

Abstract

Developing a detailed threat profile, provides organizations with a clear illustration of the threats that they face, and enables them to implement a proactive incident management program that focuses on the threat component of risk. Organizations are facing new types of advanced persistent threat (APT) scenarios that existing risk management programs are not able to evaluate completely and incident management programs are not able to defend against. This paper provides information about how to expand existing risk management models to better illustrate APTs and provides a framework on how to gather threat related information so that detailed threat profiles that include APTs can be developed for organizations. These threat profiles can be used by an organization's risk management team to record information about threat actors, scenarios, and campaigns that may have been launched against them. The threat profiles will provide incident management teams with threat intelligence information that they can use to analyze individual threat scenarios or threat scenario campaigns and enable them to anticipate and mitigate future attacks based on this detailed knowledge about the threats.

© 2014 The SANS Institute Author retains full rights.

1. Introduction

Organizations are facing an increasing trend where threat scenarios from advanced persistent threats (APTs) are becoming more sophisticated and prevalent, and organizations are struggling to be able to defend against them. This paper provides information for organizations' risk and incident management teams about how to develop detailed threat profiles that include information about APTs and threat campaigns.

A threat profile includes information about critical assets, threat actors, and threat scenarios. A threat scenario is an illustration in which one or more threat actors can mount one or more threat actions in an attempt to compromise an identified critical asset by exploiting both vulnerabilities and inadequate safeguards (Dziadyk, 2011). A threat scenario campaign is a series of related threat scenarios that are used together as part of an APT for a common objective. An organization's threat profile includes all of this threat information and presents a clear and detailed illustration of how each of these components are used together.

This paper references the Common Criteria security concepts and relationship figure from the *General Model for Information Technology Security Evaluation* and expands this figure to illustrate how APTs can be integrated. This model illustrates the relationships between the components that should be evaluated when determining risk (Common Criteria, 2005). This paper focuses on the asset, threat agent, and threat components of the model but also references vulnerabilities. It specifies which data attributes to collect for assets, threat actors, and threat scenarios so that organizations can organize threat information into a standardized format. This addresses the current challenge of inconsistent data element, format, and terminology usage. This paper incorporates elements, formats, and terminology from various sources and uses the most common ones to propose a consistent framework for recording threat information.

The Lockheed Martin *Intelligence-Driven Network Defense Informed from Analysis of Adversary Campaigns and Intrusion Kill Chains* paper and some of the more recent industry papers, such as Verizon's *2014 Data Breach Investigations Report* and the Mandiant's *M Trends – 2014 Threat Report,* illustrate that threats are not to be viewed as single events. Rather, they are often related to a number of other threat

© 2014 The SANS Institute Author retains full rights.

scenarios that form a campaign of threats and attacks against an organization (Hutchens et. al., 2011), (Verizon, 2014, April), and (Mandiant, 2014, April).

2. Current Threat Assessment Limitations

The *Security Concepts and Relationship* context figure provided by Common Criteria represents the relationship between the components that determine risk. This figure illustrates that security is concerned with the protection of assets from threats, where threats are characterized as the potential for abuse of protected assets (Common Criteria, 2005, August). Figure 1 illustrates Common Criteria's high level security concepts and relationships.

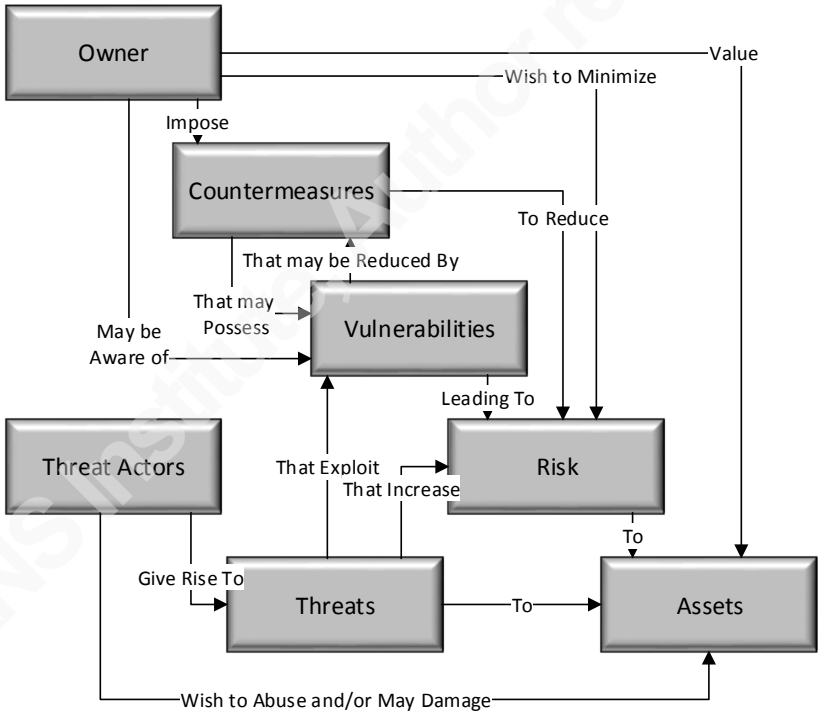


Figure 1 - Security Concepts and Relationships

Building on the Common Criteria two dimensional representation of the security concepts and relationships, this paper adds a third dimension to emphasize that when assessing advanced persistent threats (APT) it is beneficial to identify the related threat scenarios that constitute the full threat scenario campaign. Figure 2 shows an overview of the expanded model. (Note: For visual clarity, not all relationship links have been included.)

Stephen Irwin, stephen.irwin@gmail.com

© 2014 The SANS Institute Author retains full rights.

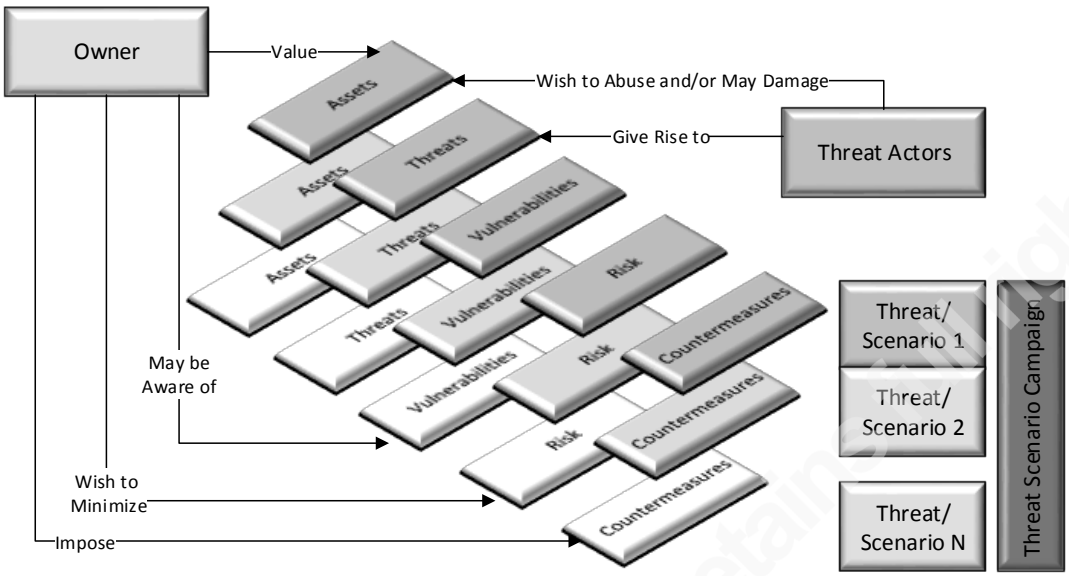


Figure 2 - Security Concept and Relationship Model Expanded for APT

3. Asset Categorization

While performing a Threat and Risk Assessment, the assets are assessed to determine the impact from a compromise that affects confidentiality, integrity, and availability. The Federal Information Processing Standards Publication (FIPS) provides guidance on security categorization of information and information systems (FIPS, 2004, February). Categorizing the organization's critical assets into a structured asset list with a standardized set of attributes provides: consistency in how multiple projects protect the common set of assets; completeness, as assets are less likely to be overlooked; accuracy, flexibility and scalability. The categorization can be updated when required.

3.1. Asset Attributes

Tangible assets should be included in the organization's asset list. This list may include, but is not limited to, information in all forms and media, networks, systems, material, and real property. From an IT security perspective, an organization's personnel should also be considered assets as social engineering attacks may be launched against them. Threat scenario campaigns may target multiple assets and launch different attacks against the assets until the threat actors have reached their final objective. Some of the compromised assets are leveraged to further penetrate the network. The motive of the threat actors will determine what their objective target asset is. For example, a state-

© 2014 The SANS Institute Author retains full rights.

sponsored threat actor wishing the exfiltrate information will be searching for data assets. Hacktivists who intend to cause harm and destruction will search for a server or service to disrupt and compromise to cause a denial of service.

An organization can categorize the assets that are to be added to their asset list using the attributes listed in Table 1.

Table 1 - Asset Attributes

Attribute		Description
Unique ID		A unique ID for each asset should be assigned. Examples of a unique numbering scheme include information assets - CA.IN.01, network assets - CA.NT.01, and subsystem assets - CA.SS.01.
Description		A description of the asset that is meaningful to a business owner.
Ownership		Identification of the individual or organization who owns the asset.
Location		Physical and/or logical location information of the asset.
Security Categorization		Impact or injury assessment of confidentiality, integrity and availability is performed during a security categorization process to create a statement of sensitivity for the critical assets in the organization.
C	**Confidentiality**	Confidentiality impact assessment of High, Medium, or Low
I	**Integrity**	Integrity impact assessment of High, Medium, or Low
A	**Availability**	Availability impact assessment of High, Medium, or Low
Value		Monetary value of the assets.

3.2. Commonly Compromised Asset Characteristics

IT Assets that are commonly compromised and used during attacks include, but are not limited to, servers, network components, user devices, storage media, people, network and system design specifications, and VPN configurations. Critical information assets, which are usually the final objective of the threat actor, include intellectual property, product development information, manufacturing processes, business plans, policies, emails, organization charts, and user credentials.

Stephen Irwin, stephen.irwin@gmail.com

© 2014 The SANS Institute Author retains full rights.

Verizon states that threat actors target and compromise servers more than user devices, but user device compromises are increasing. Obtaining user credentials is a main objective of threat actors as this allows them to compromise other nodes in the network. Verizon states that the theft of intellectual property and data, such as network and system design specifications, is at its highest level. Some of this data, would be obtained during initial attack steps to be used in future attacks to obtain further information (Verizon, 2014, April). Mandiant supports this finding by reporting that threat actors have an increased interest in comprehensive network reconnaissance and are attempting to obtain assets such as network documents, organization charts, system documents, and VPN configurations. Mandiant states that data theft includes product development information, manufacturing processes, business plans, policies, emails, user credentials and network information (Mandiant, 2013, April) and (Mandiant, 2014, April). The CyberEdge Group states that the most vulnerable assets in an organization's IT infrastructure are mobile devices such as smartphones, tablets, and laptops (CyberEdge Group, 2014). Symantec states that the individuals most likely to be targeted by spear-phishing campaigns are personal assistants, people working in media, and senior managers. This report also states that there is an increasing trend in private information breaches as the value of this information has increased (Symantec, 2014, April).

4. Threat Gathering

There are many sources of threat information that can be used by the organization. There are also tools and standards that should be considered.

4.1. Sources of Threat Information

There are internal and external sources of threat information that are available to an organization. Some of the external sources are free of cost, and others are available by paid subscription. When reviewing the different external sources, it is important to be aware of any potential biases that some industry papers may have if they are provided by a vendor whose business model is to sell and support security products. It is also important to be cognizant that some papers are focused on data incidents and breaches, some are focused on vulnerabilities, and some are focused on all IT compromises.

Stephen Irwin, stephen.irwin@gmail.com

© 2014 The SANS Institute Author retains full rights.

4.1.1. Internal Sources

An organization has numerous potential internal sources of threat data that may provide timely and applicable threat information. Systems logs from intrusion detection and prevention systems, firewalls, and data loss prevention systems may be a rich source of threat information. Any existing computer incident forensics, physical security, and threat and risk assessment reports should also be reviewed.

4.1.2. External Sources

There are many external sources of threat information that an organization can use. These sources include federal government intelligence sources, international government intelligence sources, industry specific threat reports, industry community members sharing threat information at conferences, free and subscription based third party threat reports, and free and subscription based third party threat feeds.

Some examples of free third party threat reports include Verizon's annual *Data Breach Investigations Report*, Mandiant's annual *M Trends Threat Report*, Symantec's *Internet Security Threat Report*, Microsoft's semi-annual *Microsoft Security Intelligence Report*, and Sophos' annual *Security Threat Report*. Many vendors are now publishing threat reports.

Other reports of threat trends include FireEye's *Definitive Guide to Next-Generation Threat Protection*, Lockheed Martin's *Intelligence Driven Computer Network Defense Information by Analysis of Adversary Campaigns and Intrusion Kill Chains*, U.S. Defense Security Services', *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*. Sources of continuous threat updates include the SANS Internet Storm Center, Sophos, and Symantec.

4.2. Tools and Standards

There are tools and standards that an organization can use to capture and exchange threat and incident information. Some of the tools and standards are more strategic and risk based, while others are more tactical. It is important to review a number of options and choose the solution that meets the organization's specific requirements. The SANS Reading Room paper *Tools and Standards for Cyber Threat Intelligence Projects* provides an overview of a number of the tools and standards. The paper includes

© 2014 The SANS Institute Author retains full rights.

an overview of Verizon's Vocabulary for Event Recording and Incident Sharing (VERIS), the three Mitre standards (CybOX, STIX, TAXII), the Traffic Light Protocol (TLP), Managed Incident Lightweight Exchange (MILE), Open Indicators of Compromise (OpenIOC) Framework, Open Threat Exchange (OTX), and Collective Intelligence Framework (CIF) (Farnham, 2013, October).

4.3. Continuous Engagement

An organization should be continuously engaged and up-to-date on tactical threat information as well as strategic threat trends. Some of the options that can be considered include biweekly internal threat conference calls, attending semi-annual industry security conferences, and maintaining a security awareness and training program.

5. Threat Actor Classification

It is important to understand the characteristics of threat actors. Threat actors have evolved from the 1970s when they used simple computer viruses and phone phreaking attacks to annoy their victims, to computer hacking in the 1980s which used modems to access target computers, to the script kiddies in the 1990s who used the Internet to deface websites. Threat actors in 2014 are highly trained and incorporate sophisticated attack techniques. Hacking is now a multi-billion dollar industry for cyber criminals and provides opportunities for threat actors to exfiltrate data for political and corporate gains. Verizon states that threat actors are getting better and faster at what they do at a higher rate than defenders are improving at their trade (Verizon, 2014, April).

5.1. Threat Actor Attributes

Table 2 uses the following attributes to characterize threat actors: name, description, relationship, region of operation, motive, intent, capability, target victim, action, target asset, and objective.

Table 2 - Threat Actor Attributes

Attribute	Description
Unique ID	A unique ID should be assigned to each threat actor, e.g. TA.E.01.
Name	This attribute provides a standardized name for the threat actor.

© 2014 The SANS Institute Author retains full rights.

Attribute	Description
Description	This attribute provides a description of the threat actor.
Relationship	This attribute provides an assignment of whether the threat actor is external to, internal to, or a partner of the organization. External threat actors are generally cyber criminals, state-sponsored threat actors, or hacktivists. Internal threat actors are usually systems administrators, end users, or executives and managers. Partners are third party organizations that have business relationships with the organization.
Region of Operation	Region of Operation describes the geographic location of the threat actor. Different papers use different regional breakdowns. Kenneth Geers provides a regional assignment for state sponsored threat actors as follows: Asia-Pacific, Russia/Eastern Europe, Middle East, and The West (United States and Europe) (Geers, 2013, September). The U.S. Defense Security Service 2013 Targeting U.S. Technologies provides a much more detailed regional breakdown for state sponsored threat actors as follows: Africa, East Asia & the Pacific (China), Europe & Eurasia (Russia), Near East (Iran, Syria), South Central Asia, and Western Hemisphere (N/S/C America) (Defense Security Service, 2012, October). Verizon provides the following regional breakdown: East Asia, Eastern Europe, Western Asia, North America, Europe, and Southern Asia (Verizon, 2014, April). The regional assignments are generally consistent between the sources, and the organization will need to standardize on a specific regional assignment which aligns with the threat sources that best meet its business needs.
Motive	A threat actor will have a specific motive for the attack or threat. External and internal threat actors may attack for financial gain, espionage, or ideological reasons. Internal threat actors and partners may have no motive if the incident is accidental.
Intent	A threat actor will have an intent which may include deliberate,

© 2014 The SANS Institute Author retains full rights.

Attribute	Description
	malicious, competitive, or accidental reasons.
Capability	The capabilities of the threat actor can have multiple sub-attributes including technical strength, financial support, political support, size, intensity, persistence (time), stealth (ability to hide), and access to target. Sandia National Laboratories provides threat metrics and models for characterizing threats in a consistent and unambiguous manner, and provides many of the threat attributes it uses to profile a threat (Sandia National Laboratories, 2012, March).
Target Victim	This attribute provides the name of the industry that is typically the target of threats from this threat actor. Reports such as the Verizon Data Breach Report use the North American Industry Classification System (NAICS) to classify industries.
Action	A description of the action that the threat actor performs provides a description of the tools and methods of attack used. Actions will be reviewed in detail in section 6.1.
Target Asset	This attribute provides a list of the assets that the threat actor typically strives to obtain or access. This includes assets that are compromised at interim stages of an attack campaign to access the final objective and the critical assets that are the final objective. The target assets are from the list that was described in section 3.1.
Objective	The objective of the threat actor refers to the ultimate asset that the threat actor wishes to access or compromise.

5.2. Threat Actor Characteristics

The CyberEdge Group states that with respect to threat actors, organizations are more concerned about malicious insiders than they are with external threat actors. However, with respect to threats, the report states that organizations' concern about external threats outweighs that for internal threats by a ratio of approximately 2.5:1; and that organizations are more concerned about the type of threat action than they are about the source of the threat (CyberEdge Group, 2014). It seems inconsistent that the concern

© 2014 The SANS Institute Author retains full rights.

for threat actors and threat scenarios does not align. This suggests that some organizations have not developed a clear threat profile.

The following sections provide threat actor characteristics that have been gathered and synthesized from numerous industry sources. The following threat actors have been profiled: cyber criminals, state-sponsored actors, hacktivists, systems administrators, end users, executives, and partners.

5.2.1. Cyber Criminals – External

Table 3 provides characteristics of a cyber criminal threat actor.

Table 3 - Cyber Criminal Threat Actor Profile

Name:	**Cyber Criminal**
ID: TA.E.01	
Description: Cyber criminals hack computer systems for financial gain.	
Relationship: External	**Region of Operation:** Eastern Europe, North America
Motive: Financial gain	**Intent:** Deliberate, Competitive
Capability: High technical capability, well-funded, large number, stealthy, patient and persistent, and high intensity.	
Target Victim: Financial, Retail, Food Industry.	
Action: Cyber criminals and state-sponsored threat actors often use the same tools but will usually leave a different attack footprint. Financially motivated criminals will not be as persistent as espionage motivated state-sponsored threat actors who wish to maintain control within a target for a long period of time. These threat actors will use tampering (physical), brute force (hacking), spyware (malware), capture stored data (malware), adminware (malware), RAM scrapers (malware).	
Targeted Asset: Automatic Teller Machines (ATM), Point of Sale (POS) controller, POS terminal, Database, Desktop.	
Objective: Steal credit card numbers, bank information, and social media and email account information and sell them on the black market.	

© 2014 The SANS Institute Author retains full rights.

5.2.2. State-Sponsored Threat Actors – External

As stated by Kenneth Geers, state-sponsored threat actors have distinctive motivations and types of threat actions used (Geers, 2013, September). Table 4 provides characteristics of a state-sponsored threat actor.

Table 4 - State-Sponsored Threat Actor Profile

Name:	**State Sponsored Threat Actors**
ID: TA.E.02	
Description: State-sponsored threat actors are individuals employed by a government to penetrate commercial and/or government computer systems in other countries. Their goal is to perform cyber espionage, compromise data, sabotage computer systems, and even commit cyber warfare. Some nation-states have been purported to hire cybercriminals to perform some of their cyber-attacks. Kenneth Geers provides the following overview (Geers , 2013, September): • Asia-Pacific: Home to large, bureaucratic hacker groups such as the "Comment Crew" who pursue many goals and targets in high-frequency, brute-force attacks. China, the largest threat actor in this region with 1.35 billion people, has the ability to overwhelm cyber defenses. China's attacks are not the most sophisticated, but the brute force capabilities are effective. • Russia/Eastern Europe: These cyber-attacks are more technically advanced and highly effective at evading detection. Russia's attacks are the most complex and advanced, and are stealthier than Chinese attacks. There is more focus on Zero-day exploits. • Middle East: These hackers are dynamic, often using creativity, deception, and social engineering to trick users into compromising their own computers. The malware is not as sophisticated as others, but the delivery and installation are often performed in creative and sophisticated ways. • United States: The United States uses the most complex, targeted, and rigorously engineered cyber-attack campaigns to date. The attacks require a high level of financial investment, technical sophistication, and legal oversight	

© 2014 The SANS Institute Author retains full rights.

which, all combined, make these attacks stand apart from the others.	
Relationship: External	**Region of Operation**: Asia Pacific (China), Russia/Eastern Europe, Middle East (Iran, Israel), United States
Motive: Espionage and Ideological	**Intent**: Deliberate, Malicious, Competitive
Capability: Highly capable technically, well-funded, very large number of attackers, stealthy, very patient and persistent, and high intensity.	
Target Victim: Public, Manufacturing, Professional, Transportation	
Action: Phishing (social), Backdoor (malware), Command & Control (CC), Malware/Hacking, Export Data (malware), Downloader (malware), Stolen Credentials (hacking)	
Targeted Asset: High-Level Employees, Laptop/Desktop, File Server, Mail Server, Directory Server	
Objective: Credentials, Internal Organizational Data, Trade Secrets, System Information.	

Stephen Irwin, stephen.irwin@gmail.com

© 2014 The SANS Institute Author retains full rights.

5.2.3. Hacktivists – External

Table 5 provides characteristics of a hacktivist threat actor.

Table 5 - Hacktivist Threat Actor Profile

Name:	**Hacktivists**
ID: TA.E.03	
Description: Hacktivists are individuals or groups who use digital tools to perform cyber-attacks on targets for political ideological reasons.	
Relationship: External	**Region of Operation**: Western Europe, North America
Motive: Ideological	**Intent**: Deliberate, Malicious
Capability: Moderately capable technically, moderately well-funded, moderate number of attackers, low level stealth, less patient and persistent, and moderate intensity.	
Target Victim: Public, Information, Other Services	
Action: SQL Injection (hacking), Stolen Credentials (hacking), Brute Force (hacking), Backdoor (malware), Denial of Service (DoS).	
Targeted Asset: Web Application, Database, Mail Server	
Objective: Typical cyber-attacks performed by hacktivists include website defacement, redirects, information theft, and virtual sit-ins through distributed denial-of-service attacks. Desired data includes personal information, credentials, and internal organizational data.	

© 2014 The SANS Institute Author retains full rights.

5.2.4. System Administrators/End Users/Executives & Managers – Internal

Table 6 provides characteristics of internal threat actors.

Table 6 - Sys. Admin. /End Users/Executives & Managers Threat Actor Profile

Name:	**System Administrators/End Users/Executives & Managers**
ID: TA.I.04	
Description: Verizon states that The CERT Insider Threat Center focuses research on insider breaches. It determined that, in more than 70% of the IP theft cases, insiders stole the information within 30 days of announcing their resignation (Verizon, 2014, April). Symantec reports that accidental exposure of information grew significantly in 2013, is responsible for 28% of data breaches, and is ahead of theft and loss and just 6% behind hackers as a cause of data breaches (Symantec, 2014, April).	
Relationship: Internal	**Region of Operation**: World
Motive: Financial gain	**Intent**: Deliberate, Malicious
Capability: Varies from advanced to low.	
Target Victim: Target Organization.	
Action: Varies from accidental exposure to deliberate exfiltration of information using privileged access and privilege escalation.	
Targeted Asset: Intellectual property and trade secrets of the organization.	
Objective: **System administrators** will abuse access privileges and smuggle exfiltrated data out on unapproved devices. **End users** often are involved in accidental data loss. **Executives and managers** are often targets of Spear-Phishing and are also responsible for deliberate data exfiltration when they leave an organization. Verizon highlights that most of the data is exfiltrated within 30 days of an executive announcing their resignation (Verizon, 2014, April).	

© 2014 The SANS Institute Author retains full rights.

5.2.5. Partner

Table 7 provides characteristics of a partner threat actor. The partner's network may also be used by other external threat actors as an initial access point to the target's network.

Table 7 - Partner Threat Actor Profile

Name:	**Partner**
ID: TA.P.05	
Description: A partner is an organization that the target organization is in a trusted partnership with. This partner may provide services to the target organization. This may be a hosting facility, cloud provider, or any other service provider.	
Relationship: Partner	**Region of Operation**: World
Motive: Financial gain, competitive advantage	**Intent**: Accidental, Deliberate
Capability: The trusted partner relationship may provide network connectivity from the partner to the target organization's network. Mandiant states that attacks against outsourced service providers have increased as this provides threat actors with an initial foothold and may be a stepping stone to obtain access to the final target organization (Mandiant, 2014, April). Symantec states that indirect (partner) attacks are increasing and attacks against cloud providers will become more dangerous. This is consistent with increases in watering hole attacks (Symantec, 2014, April).	
Target Victim: Target Organization.	
Action: The trusted partner relationship may provide network connectivity from the partner to the target organization's network. There is an increasing trend where hackers are using the partner as an initial jump point to access the target organization's network.	
Targeted Asset: Intellectual property and trade secrets for exfiltration. Services to disrupt if attempting to deny services.	
Objective: Exfiltrate intellectual property, trade secrets or disrupt services.	

© 2014 The SANS Institute Author retains full rights.

6. Threat Analysis

This section discusses how to gather, organize and analyze threat information, and use this information to develop threat scenarios that are relevant to a specific organization. A number of threat actions are presented to help classify threat scenarios in a consistent manner.

The Verizon VERIS framework is used to illustrate threat actions, but an organization can choose any format that suits its business and security needs. The Lockheed Martin attack sequence phase concept is introduced as well, as it provides an excellent framework to illustrate the details of a multi-phased attack campaign (Hutchens et. al., 2011). A number of threat trend references that capture threat trends that exist in today's fight against cyber-attacks have been included in this section.

6.1. Threat Actions

Threat actions describe what threat actors do or use to cause or contribute to a security incident. Every incident has at least one, but most will be comprised of multiple actions. VERIS uses 7 categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error, and Environmental. VERIS provides additional attributes, including Variety and Vector (path of attack) for all categories, Vulnerabilities for hacking and malware, Target for social attacks, and Location for physical attacks. An organization can use, modify, or enhance this structure to meet business and security requirements.

6.1.1. Malware

Malware is any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent. Examples include viruses, worms, spyware, keyloggers, and backdoors (VERIS).

Steve Piper provides a simplified view of the threat landscape by grouping cyber-attacks into two broad categories: traditional threats and next-generation threats. Traditional threats are known threats and can often be detected by IPS devices, firewalls, and anti-virus solutions but remain very effective at compromising systems. Traditional threats include malware such as worms, trojans, viruses, spyware, botnets, social engineering attacks, buffer overflows, and SQL injections. Next-generation threats are

© 2014 The SANS Institute Author retains full rights.

unknown threats and include zero-day threats, advanced persistent threats, polymorphic threats, and blended threats (Piper, 2013).

6.1.2. Hacking

Hacking is defined within VERIS as all attempts to intentionally access or harm information assets without authorization by circumventing or thwarting logical security mechanisms. Included in this category are brute force attacks, SQL injection, cryptanalysis, and denial of service attacks (VERIS).

6.1.3. Social

Social tactics employ deception, manipulation, and intimidation to exploit the human element, or users, of information assets. Included in this category are pretexting, phishing, blackmail, threats, and scams (VERIS). Internal threat actors may use physical observation such as shoulder surfing. External threat actors perform profiling from social media sites. They then send phishing emails or compromise a public Web site as part of a watering hole attack.

6.1.4. Misuse

Misuse is defined as the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended. Included in this category are administrative abuse, policy violations, and use of non-approved assets. These actions can be malicious or non-malicious in nature. Misuse is exclusive to parties that enjoy a degree of trust from the organization, such as insiders and partners (VERIS).

6.1.5. Physical

Physical actions encompass deliberate threats that involve proximity, possession, or force. Included in this category are theft, tampering, snooping, sabotage, local device access, and assault (VERIS).

6.1.6. Error

Error broadly encompasses anything done or left undone incorrectly or inadvertently. Included in this category are omissions, misconfigurations, programming errors, trips and spills, and malfunctions. It does not include something done or left

© 2014 The SANS Institute Author retains full rights.

undone intentionally or by default that later proves to be unwise or inadequate (VERIS). This may include not changing the default password.

6.1.7. Environmental

The Environmental category not only includes natural events such as earthquakes and floods but also hazards associated with the immediate environment or infrastructure in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions (VERIS).

6.2. Attack Sequence Phases

This section uses the Lockheed Martin's attack kill chain to provide the framework used to integrate the assets, threat actors, and threat actions together and to illustrate comprehensive threat scenarios in a multi-stepped phased attack sequence. The Lockheed Martin paper presents 7 steps which include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions and Objectives (Hutchens et. al., 2011). This paper has added an 8th step called Covering Tracks.

6.2.1. Reconnaissance

Reconnaissance is the phase of an attack where an attacker finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities (SANS, Glossary). Internal threat actors may use physical observation such as shoulder surfing coworkers. External threat actors profile from social media sites and target online profiles. They use this information in their phishing email attacks or as part of a watering hole attack.

The increase in targeted attacks that has been reported in most of the industry papers suggests that the threat actors are performing more detailed reconnaissance activities on their target organizations and are able to focus their attacks to gather information about these targets. Symantec reports a 42% increase in targeted attacks where the primary motivation was expected to be industrial espionage and data exfiltration (Symantec, 2013, April). Symantec reports a 28% decrease in targeted attacks where they are returning to levels seen in 2011. Symantec has observed that the attacks have become more focused as the attackers have streamlined their attack methods. The volume of distinct email phishing campaigns increased by 91% in 2013. However, the

© 2014 The SANS Institute Author retains full rights.

average number of attacks per campaign has decreased. The number of recipients of spear-phishing campaigns is decreasing, but the campaigns are lasting longer and are more focused and persistent (Symantec, 2014, April).

Verizon reports that social attacks have increased by 400% between 2012 and 2013, and this trend is continuing in 2014. Phishing jumped to being the third most common threat action compared with its ninth place standing in 2012. This is mainly due to an increase in targeted espionage attack campaigns, as the majority of espionage attacks used social attacks (Verizon, 2013, April) and (Verizon, 2014, April).

Phishing is used as a first step to gain a foothold into the target's environment. Email is the most common vector for launching a Phishing attack. Spear-Phishing attacks are most often targeted at senior employees, such as managers and executives. However, there is an increasing trend where privileged users, such as system administrators, are being targeted. Mandiant also reports that Spear-Phishing using an email vector increased in 2013 and that drive-by attacks are more advanced (Mandiant, 2014, April).

6.2.2. Weaponization

Weaponization refers to adapting something so that it can be used as a weapon. Lockheed Martin reports that client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents increasingly serve as weaponized deliverables. Threat actors with deliberate intent to harm may use a combination of compromised JavaScript, PDF files, or Microsoft Office files that are attached to a Phishing email and sent to a targeted user or group of users in the organization (Hutchens et. al., 2011). The intent is to exploit vulnerabilities in an operating system or application. Microsoft states that the two most common exploits are against HTML/JavaScript and Java. These attacks are often used to get the initial compromise into the network before applying a command and control component (Microsoft, 2013).

6.2.3. Delivery

The delivery phase is the phase used to deliver the weaponized exploit to the target. System exploits are typically delivered through a remote Web exploit or through a local email exploit as an attachment. In the case of remote delivery, such as Web drive-by

© 2014 The SANS Institute Author retains full rights.

downloads, no user interaction is required beyond visiting the Web page. Local delivery often requires social engineering to initiate the necessary interaction needed to complete the exploitation. External threat actors with deliberate intent to harm may compromise one or more public web sites which initial reconnaissance activities highlighted as being often accessed by target users. Malware may then download to the users' machines and send authentication credentials to the threat actor or provide the threat actor access to the target environment

Verizon, Mandiant, Symantec, and Google report that there is an increasing trend where threat actors compromise common public web sites that are used by targeted users. Symantec reports that 67% of malicious sites are legitimate web sites that have been compromised and infected with malware. This is known as a watering-hole attack. The malware may perform a number of malicious tasks including capturing user credentials, cookies, and system information. These attacks are used to gain a foothold into the target's environment. They are often used by financially motivated and espionage motivated attackers and are part of a social engineering attack. Verizon and Mandiant report that email is the most common delivery vector for phishing attacks (Verizon, 2014, April), (Mandiant, 2014, April), (Symantec, 2014, April), (Google, 2014, August). Lockheed Martin reports that the three most prevalent delivery vectors are email with malware attachments, malware compromised websites, and USB removable media (Hutchens et. al., 2011).

6.2.4. Exploitation

Once the weaponized exploit has been delivered, it will begin to attack the vulnerabilities in the operating system or application. This may allow the attacker to execute code, such as command and control code, which will enable the malware to connect to the attacker's command and control servers and download more code (Hutchens et. al., 2011).

Microsoft states that non-Microsoft applications have been the subject of the highest vulnerability disclosure, followed by operating system vulnerability disclosures. Lockheed Martin states that threat actors may leverage an operating system feature, such as auto-execute, to trick the targeted user into launching a malware installation. Verizon

© 2014 The SANS Institute Author retains full rights.

reports that the most commonly compromised assets are user workstations, devices, and servers. Microsoft states that, in a normalized dataset, older operating systems have a higher malware infection rate. Consumer home computers have an 18% malware encounter rate compared to approximately a 10% encounter rate for enterprise computers. Specific malware tools encountered tend to differ between home and enterprise computers. The usage pattern for home users and enterprise users is different. Symantec states that mobile vulnerabilities are increasing particularly on Android operating systems but there are still very few attacks launched against mobile devices (Microsoft, 2013, July), (Hutchens et. al., 2011), (Verizon, 2014, April), (Symantec, 2014, April).

6.2.5. Installation

Installation and exploitation are tightly aligned as malicious code must be installed in order for it to exploit a vulnerability. Malicious code is executed enabling the code to be installed on the compromised system. Visiting a compromised Web page may be all that is required to become compromised and infected by a remote exploit of a malware payload. Phishing emails originating from a threat actor may contain malicious attachments or may contain hyperlinks that, when clicked on by the target, open a Web browser or other applications such as Adobe Reader, Microsoft Word, or Excel. Web browsers may be redirected to hidden links which assess the Web browser for vulnerabilities and download Trojan downloader malware. This malware may be used to communicate back to the threat actor who is running the attack.

Verizon states that direct installation of malware by an attacker who has gained access to a system is the most common vector for deploying malware. This is a change from past trends where the attacker attempted to get the victim to install the malware. However, users can and will be exploited in order to install malware that will allow a threat actor persistent access to the targeted environment (Verizon, 2014, April).

6.2.6. Command and Control

Once the threat actor has successfully installed the required malicious code, the malware will usually attempt to establish communication back to the threat actor's command and control server. This outbound connection is often an SSL/TLS encrypted

© 2014 The SANS Institute Author retains full rights.

session. Once a communication session has been established, the threat actor can send commands remotely to further compromise and control the infected host and network.

6.2.7. Actions and Objectives

It is unlikely that the end-user device initially breached contains the strategic data that the threat actor is ultimately after. The threat actor will often use this device as an initial point to launch additional attacks against other systems and devices in the network, and move laterally to other nodes in the network with the intent to access the ultimate target host that stores the final objective data.

At this stage of the attack, the threat actor may also have obtained valid authentication credentials that will enable them to access additional systems by escalating privileges. The threat actor will likely perform direct installation of command and control malware such as Trojans and Backdoors. As stated by Lockheed Martin, these compromised hosts will beacon out to the Internet and will usually require manual interaction rather than conduct activities automatically. Lateral movement does not necessarily involve the use of malware or tools other than those already supplied by the compromised host operating system such as command shells, VNC, and Windows Terminal Services (Hutchens et. al., 2011).

Once the threat actor has access to the host that has the data they wish to exfiltrate and has reached their final objective, they must be careful not to be detected when transferring the data. They need to ensure that they do not generate an unusually high volume of network traffic. They will often send the data in smaller chunks, and compress the data into a number of files such as password-protected RAR files. They may encrypt these files to help bypass an organization's data loss prevention controls. They will ensure the server to which they are sending this exfiltrated data with cannot be linked to them. The threat actor may use cloud-based staging area virtual hosts that can be destroyed after the data has been extracted.

6.2.8. Covering Tracks

The best time for an organization to detect and analyze an APT attack is while it is still in progress, as threat actors are extremely good at covering their tracks. Threat actors will often plant malware to distract incident responders; use network file shares,

© 2014 The SANS Institute Author retains full rights.

and delete the compromised files after they have been extracted from the staging servers; delete a cloud-based staging server; and delete the malware used at the initial point of entry. Mandiant states that the average time period that a threat actor maintained access to a target's environment was 365 days. The longest time they maintained access was 4 years and 10 months. Some threat actors will cover their tracks for some of the attack and then publicize their findings to everyone (Mandiant, 2013, April).

7. Creation of Threat Profile

This section uses the information from the previous sections to provide a sample of a threat scenario campaign. An organization's threat profile will include multiple threat scenario campaigns, which will be tailored to be applicable to the organization. When creating threat scenario campaigns, the organization will select critical assets, threat actors, and threat scenarios. This process will be repeated for each scenario. To construct the threat scenarios in a consistent format, the attack sequence phases that were outlined in section 6.2 will be used.

7.1. Threat Scenario Campaign – Exfiltrate Industrial Trade Secrets

This threat scenario campaign focuses on an external threat actor who is motivated to exfiltrate information to improve their industrial trade posture. This threat scenario campaign is composed of three critical asset, one threat actor and three threat scenarios.

7.1.1. Asset Categorization

Table 8 - Executive Laptop

Asset ID.		***CA.SS.01 – Executive Laptop***
Attribute		**Description**
Description		Executive Laptop with Windows 7 & Adobe Reader
Ownership		Manufacturing Executives, COO, VP, Directors
Location		Executive wing of head office.
Security Categorization		
C	Confidentiality	Confidentiality impact assessment - **High**

© 2014 The SANS Institute Author retains full rights.

I	Integrity	Integrity impact assessment - **High**
A	Availability	Availability impact assessment - **Medium**
Value		Monetary value of the assets.

Table 9 – Corporate Wiki and File Servers

Asset ID.		***CA.SS.02 – Corporate Wiki and File Server***
Attribute		**Description**
Description		Corporate Wiki application and File Server with Windows 2008 Server and VNC remote access software.
Ownership		Organization
Location		Data Centre.
Security Categorization		
C	Confidentiality	Confidentiality impact assessment - **High**
I	Integrity	Integrity impact assessment - **Medium**
A	Availability	Availability impact assessment - **Medium**
Value		Monetary value of the assets.

Table 10 – Manufacturing Process Trade Secrets

Asset ID.		***CA.IN.01 – Manufacturing Process Trade Secrets***
Attribute		**Description**
Description		Manufacturing Process Trade Secrets in PDF, Word, and Excel file formats.
Ownership		Manufacturing Executives, COO, VP, Directors
Location		Company file server.
Security Categorization		
C	Confidentiality	Confidentiality impact assessment - **High**
I	Integrity	Integrity impact assessment - **High**
A	Availability	Availability impact assessment - **High**
Value		Company trade secrets. Competitive advantage.

© 2014 The SANS Institute Author retains full rights.

7.1.2. Threat Actor

Table 11 - State-Sponsored Threat Actor Profile

Threat Actor ID.	***TA.E.02 – State Sponsored Threat Actor***
Description: Individuals employed by a government (not necessarily their own) to penetrate commercial and/or government computer systems in other countries to compromise data, sabotage computer systems, and commit cyber warfare.	
Relationship: External	**Region of Operation**: Asia Pacific (China)
Motive: Espionage	**Intent**: Deliberate, Competitive
Capability: Highly capable technically, well-funded, very large number of attackers, stealthy, very patient and persistent, and high intensity.	
Objective: Credentials, Internal Organizational Data, Trade Secrets, System Data.	

7.1.3. Threat Scenario #1 – Establish Foothold

Table 12 - Threat Scenario #1

Threat Campaign	***TC.01 – Exfiltrate Industrial Trade Secrets***		
Threat Scenario	***TS.01 – Establish Foothold***		
Asset ID.	***CA.SS.01***	**Threat Actor ID.**	***TA.E.02***
Phase	**Description**		
Reconnaissance	Threat actor performs social reconnaissance using social networking sites to obtain information about the target user population. The threat actor may also attempt to obtain information about the organization structure. The focus is to obtain company executive contact information. **Action.Social.Social_Media_Profile**		
Weaponization	Threat actor creates PDF malware that will be used to obtain user credentials from compromised user. **Action.Malware.PDF_Malware**		
Delivery	Threat actor uses email to deliver a Spear-Phishing attack with PDF malware attachment to target users, COO, VP & Directors of Operations. **Action.Social.Phishing**		
Exploitation	Target users' unpatched Adobe Reader software is the asset that will be compromised. The exploitation is executed when one or more phishing email recipients clicks on PDF malware.		

© 2014 The SANS Institute Author retains full rights.

Installation	Target users receive, open, and execute PDF malware attachment and their workstations become compromised.
Command & Control	Not applicable.
Actions & Objectives	Threat actor has compromised **CA.SS.01** asset & established foothold.
Covering Tracks	Not applicable.

7.1.4. Threat Scenario #2 – Penetrate Network

Table 13 - Threat Scenario #2

Threat Campaign	***TC.01 – Exfiltrate Industrial Trade Secrets***		
Threat Scenario	***TS.02 – Penetrate Network & Exfiltrate Data***		
Asset ID.	***CA.SS.02***	**Threat Actor ID.**	***TA.E.02***
Phase	**Description**		
Reconnaissance	Threat actor performs network scans from compromised workstation and maps corporate network. **Action.Hacking.Scans**		
Weaponization	Threat actor downloads a Trojan and keylogger to the workstation. **Action.Malware.Trojan , Action.Malware.Keylogger**		
Delivery	Threat actor uses the beaconing SSL/TLS connection from the malware on the workstation. **Action.Malware.Trojan**		
Exploitation	Previously compromised PDF vulnerability to access workstation.		
Installation	The threat actor installs the Trojan and keylogger.		
Command & Control	The keylogger malware on the compromised workstation/laptop sends authentication credential information to the threat actor.		
Actions & Objectives	Threat actor uses the stolen authentication credential information to access the organization's wiki repository storing the Manufacturing Process Trade Secrets. The threat actor will use remote access software VNC software found on the server to access the file system.		
Covering Tracks	Not applicable.		

7.1.5. Threat Scenario #3 – Exfiltrate Data & Cover Tracks

Table 14 - Threat Scenario #3

Threat Campaign	***TC.01 – Exfiltrate Industrial Trade Secrets***
Threat Scenario	***TS.03 – Exfiltrate Data & Cover Tracks***

© 2014 The SANS Institute Author retains full rights.

Asset ID.	***CA.IN.01***	**Threat Actor ID.**	***TA.E.02***
Phase	**Description**		
Reconnaissance	Not applicable.		
Weaponization	Not applicable.		
Delivery	Not applicable.		
Exploitation	Not applicable.		
Installation	The threat actor uses the existing remote access software that is on the server to install command & control software.		
Command & Control	The C&C software will be used to setup a secure TLS session to a cloud service.		
Actions & Objectives	Threat actor compresses the trade secret data files into small password-protected RAR files and begins to exfiltrate the data using a TLS session to a cloud service.		
Covering Tracks	Threat actor will delete the RAR files after they have been extracted from the staging servers, delete the cloud-based staging server, and delete the malware used at the initial point of entry.		

8. Conclusion

Implementing a threat profile for an organization will help the risk and incident management teams to be better prepared to handle the APT campaigns that may be launched against the organization. The threat profile will illustrate one or more related threat scenarios and associate these scenarios to threat scenario campaigns. This will allow the risk management team to assess the risk of a series of related threat scenarios as part of the threat scenario campaign. It will also allow the incident management team to analyze related threats and be better prepared to anticipate future attacks. This improved threat intelligence will enable the organization to implement safeguards to mitigate the risk of anticipated attacks before they occur. The detailed threat profile also provides a clear illustration of how attacks are launched and how safeguards can be implemented to thwart the attack. It is important that business leaders understand that supporting a proactive approach to incident management to fight these APTs will be beneficial to the organization.

Stephen Irwin, stephen.irwin@gmail.com

© 2014 The SANS Institute Author retains full rights.

9. References

Common Criteria (2005, August). Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.3, CCMB-2005-08-001. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf

CyberEdge Group (2014). 2014 Cyberthreat Defense Report, North America & Europe. Retrieved from http://cyber-edge.com/wp-content/uploads/2014/01/CyberEdge-2014-CDR.pdf

Defense Security Service (2012, October). 2013 Targeting U.S. Technologies, A Trend Analysis of Cleared Industry Reporting. Retrieved from http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf

Dziadyk, W. (2011, September), Harmonized TRA (HTRA) Methodology – Limitations. Retrieved from http://www.bdpro.ca/wp-content/uploads/2012/05/Harmonized_TRA_Limitations_13Sep2011.pdf

Farnham, G. (2013, October). Tools and Standards for Cyber Threat Intelligence Projects. Retrieved from http://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

Federal Information Processing Standards Publication (FIPS) (2004, February). FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems. Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Geers, K. (2013, September). FireEye Labs, World War C: Understanding State-sponsored Motives Behind Today's Advanced Cyber Attacks. Retrieved from http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/new-fireeye-report-world-war-c.html

Google, (2014, August). The Google Transparency Safe Browsing Report. Retrieved from http://www.google.com/transparencyreport/safebrowsing/?hl=en

Hutchins, E. M., Cloppert, M. J., Amin, R. M. (2011). Lockheed Martin Corporation - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and intrusion Kill Chains. Retrieved from

© 2014 The SANS Institute Author retains full rights.

http://www.lockheedmartin.ca/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Mandiant (2013, January), APT1 Exposing One of China's Cyber Espionage Units. Retrieved from https://www.mandiant.com/resources/mandiant-reports/

Mandiant, (2014, April), M Trends – 2014 Threat Report. Retrieved from https://www.mandiant.com/resources/mandiant-reports/

Mandiant, (2013, April), M Trends – 2013 Threat Report. Retrieved from https://www.mandiant.com/resources/mandiant-reports/

Microsoft, (2013, July), Microsoft Security Intelligence Report, Volume 15. Retrieved from http://www.microsoft.com/security/sir/archive/default.aspx

Piper, S. (2013), Definitive Guide™ to Next-Generation Threat Protection, 2013, Published by CyberEdge Group, LLC. Retrieved from http://www2.fireeye.com/definitive-guide-next-gen-threats.html?x=FE_BLOG_IC

Sandia National Laboratories, (2012, March), Cyber Threat Metrics. Retrieved from http://www.osti.gov/scitech/biblio/1039394

SANS, Glossary of Security Terms. Retrieved from http://www.sans.org/security-resources/glossary-of-terms/

Symantec, (2013, April), Internet Security Threat Report. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Symantec, (2014, April), Internet Security Threat Report. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

VERIS, The Vocabulary for Event Recording and Incident Sharing (VERIS). Retrieved from http://veriscommunity.net/index.html

Verizon, (2014, April), 2014 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/DBIR/2014/

Verizon, (2013, April), 2013 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Stephen Irwin, stephen.irwin@gmail.com

© 2014 The SANS Institute Author retains full rights.