sponsored feature

Ravid Circus
Is vice president of products at Skybox Security

Indicators of Exposure and Attack Surface Visualization

It is undeniable that IT systems have become enormously complex, and they continue to be influenced by rapid changes that are redefining networks, such as deperimeterization, mobile devices, virtual environments, Software as a Service (SaaS) and the Internet of Things (IoT). This growing complexity is occurring in an environment where resources are limited and regulatory requirements are forcing senior management to demand more information, leaving security practitioners scrambling to communicate the state of their security across departmental silos and to business executives and the board.

Enterprises need to think of their entire network infrastructure—physical, virtual and cloud—in the same way that attackers do: a very large, diverse and geographically dispersed attack surface (all the ways in which IT systems and networks are vulnerable to attack). All too often though, security practitioners have no means of viewing the attack surface that they are protecting in its entirety; therefore, they rely on a dangerously narrow perspective to identify, prioritize and remediate that which they believe are critical vulnerabilities. Typically, these tasks are done in crisis mode and with little context of precisely how those vulnerabilities may or may not pose an actual threat.

This narrow perspective is changing with the emergence of visualization tools that give security practitioners unprecedented views of their attack surface and subsequently greater insight into how to best address threat exposures that put enterprises at risk. Such tools combine attack path modeling with advanced threat reporting (the ability to correlate threat intelligence with vulnerabilities found in the enterprise) and analytic engines that automatically prioritize vulnerabilities and generate alerts. This article describes the foundation of such tools and the concept of indicators of exposure (IOEs) as the critical underpinning of attack surface visualization.

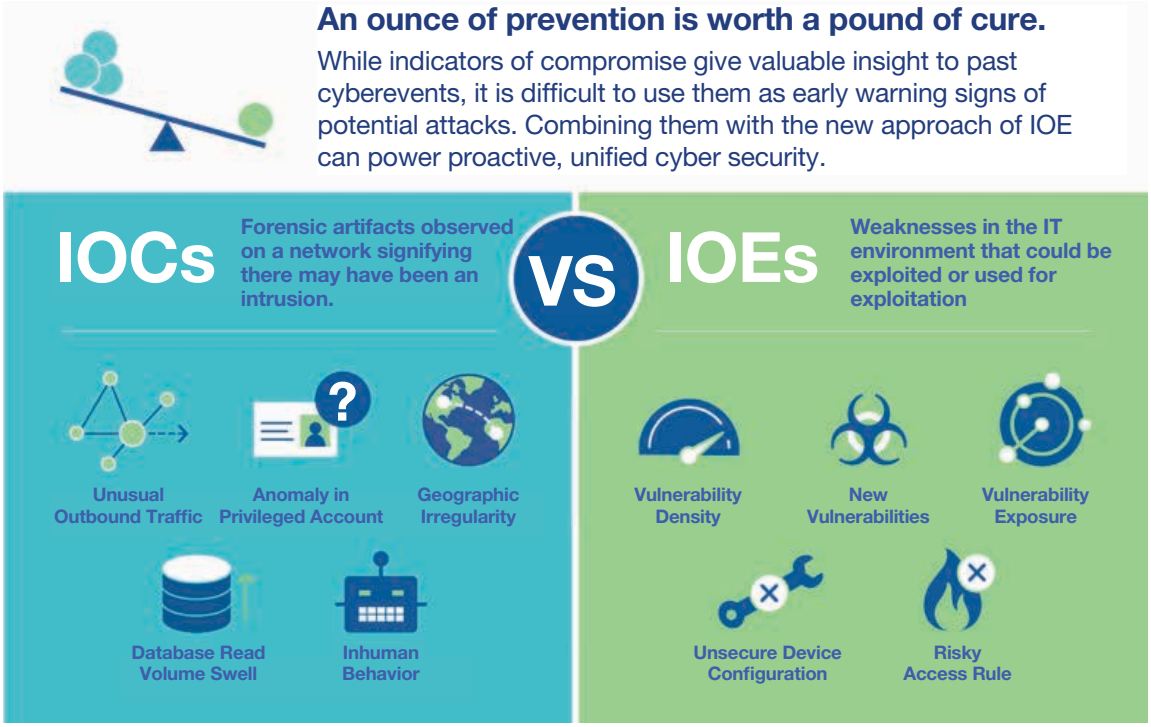
Understanding Indicators of Exposure—The Ounce of Prevention

Since the emergence of the Google Aurora attack in 2010,[1] advanced persistent threats (APTs) have dominated cyber security headlines, making security practitioners ever more aware that attacks against their networks are no longer a matter of if, but when. Security teams have quickly expanded their use of attack detection tools that are armed with advanced capabilities to identify indicators of compromise (IOCs) and used to mount a rapid response to limit damage.

As Benjamin Franklin said, “An ounce of prevention is worth a pound of cure.”[2] IOCs can be used to identify the hallmarks of attacks in progress, such as unusual outbound traffic, anomalies in privileged accounts and geographic irregularities. Certainly, tools to detect and respond to IOCs have their rightful place in any security tool kit, but a singular focus on detection and response can take security attention (and budget) away from the proactive measures that reduce the chance of an attack occurring in the first place. If security leaders maintain such a narrow focus on IOCs and do not have a strategic plan in place for minimizing the factors that can lead to them, then the enterprise will forever be in firefighting mode.

IOEs are the factors that can lead to an attack and should be identified alongside IOCs. IOCs represent an artifact of an attack; IOEs highlight the preconditions that make an exploit more likely (**figure 1**). By combining IOEs into a single, dynamic

Figure 1—Indicators of Compromise vs. Indicators of Exposure



Source: R. Circus. Reprinted with permission

view, security practitioners gain the advantage of access to a comprehensive representation of their enterprise attack surface. This level of attack surface visibility and analysis of the IOEs that contribute to it constitute a game changer for security managers and chief information security officers (CISOs).

Identifying Indicators of Exposure

IOEs describe security weaknesses that are particular to an enterprise network and can be exploited by an attacker. It is not enough to only catalog a list of vulnerabilities. Consideration must be given to those vulnerabilities that are not only exposed to a potential attack, but also put key assets at risk. IOEs are determined by analyzing multiple factors, i.e., events as opposed to observing a single one. An unexpected firewall rule change is an event, but an unexpected firewall rule change that opens up an access path to a critical asset is an IOE. By linking together IOEs with an understanding of network topology and assets, enterprises can discern which attack vectors are most likely to be exploited in a multistep attack.

Working with identified IOEs rather than raw vulnerabilities and other risk data also allows security teams to use the power of contextual analysis to determine actions that will significantly reduce the size of their attack surface with less effort than a “fix everything” approach.

A Working Set of IOEs

Research shows that most attacks exploit known vulnerabilities where a patch has been available for months or even years.[3] In addition, a variation of the 80-20 rule is in effect for vulnerabilities. The top 10 vulnerabilities accounted for 85 percent of successful exploit traffic, while 900 different vulnerabilities accounted for the remaining 15 percent.[4]

Attack risk tends to cluster around common exposure factors, which can be grouped into five of the most prevalent IOEs:

- Vulnerability exposure encompasses all vulnerabilities that are exposed and can be used in an attack vector. Contributing factors include vulnerability assessment, network context and security controls. Vulnerability exposures are ranked by risk and exposure level. Direct exposures are ranked ahead of second-step exposures. Vulnerability exposure contains an advantage over a standard Common Vulnerability Scoring System (CVSS)-based ranking, which does not account for unique network context or potential for multistep attacks.
- New vulnerabilities are all vulnerabilities that were identified in the past 30 days and ranked by risk. Contributing factors include vulnerability assessment, threat intelligence and time. It is worth noting that 59 percent of enterprises scan every 30 days (or less frequently), so recent vulnerabilities are more likely to be unpatched and available to exploit.[5]
- Vulnerability density is a high concentration of vulnerabilities in a particular network area and indicates an increased likelihood that an adversary will attempt repeated attacks on several of those vulnerabilities to achieve a successful breach. Contributing factors include vulnerabilities, vulnerability severity and network asset groups. Vulnerability densities can also indicate that security managers need to scrutinize the vulnerability remediation process in a particular area.
- Unsecure networking or security device configurations include networking or security device configurations that violate policy or create security gaps. Contributing factors include violations, severity and network asset groups. This IOE is ranked by the severity of the configuration policy violations, using the highest-severity configuration policy violation in each network asset group.
- Risky access rules in firewalls and networking devices encompass a variety of rules in firewalls or networking devices that could allow attackers to reach critical assets. Contributing factors include access violations, network device rule violations and access path analysis. This IOE is ranked by highest severity and number of violating rules.

The list of possible IOEs can be expanded to include commonly employed attack techniques and their combination of factors that are likely to lead to exploit.

Role of IOEs in Attack Surface Visualization

Understanding the nature and location of possible exposures is key to understanding the attack surface. Unfortunately, at any point in time, an enterprise can have hundreds of thousands of IOEs to manage, and that amount of data quickly becomes overwhelming. Therefore, prioritization and coordination of limited resources are critical.

Enterprises need a means of consolidating and analyzing data from dozens of security controls and other sources to create a visual, interactive model that links network topology, network connections, business units and organizational hierarchy, i.e., an attack surface visualization tool with IOEs. With such visualization, senior management and technical security teams can more easily understand the security posture of the enterprise and make more informed decisions.

At the highest level, IOEs should be viewed in a simple, representational picture of the attack surface that is mapped to geography, business units, asset types or other logical structures. Different types of users are able to view the data in the manner most appropriate to their needs. For example, a security team that is responsible for manufacturing operations views a map consisting of the enterprise factories, while a team that is responsible for regional data centers views geographic locations or network architecture. Trending information should also be available for each view, giving security leads important information about the progress that has been made in alleviating risk exposures for a specific aspect of the network.

Attack surface visualization can also help tremendously in security management of cloud

or hybrid IT environments where it is even harder to evaluate the interaction of the virtualized components with the physical world. For a complete picture of the attack surface, security information must be integrated from physical and virtual environments, and from cloud services. Security visualization shows the applied policy within virtual networks, analyzing access into and out of the network (north-south traffic), and access within the virtualized data center (east-west traffic). This visualization can also ensure that policies within the virtualized environment align with policies covering the rest of the network. As an example, contextual analysis of the east-west movement of data must be readily available to control access to, for example, financial data, which may need to be managed differently from manufacturing data.

Role of IOEs in Prioritizing and Remediating Risk

With any large data set, prioritization is critical when evaluating early signs of security weaknesses. Customized filters are beneficial for focusing the efforts of security teams on severity levels above a specific threshold or on specific types of IOEs. This focus avoids the risk of too many false positives, which cause individuals to waste their efforts chasing unprioritized alerts instead of addressing the truly serious issues. In addition, vulnerabilities should be assessed beyond the one-dimensional critical or medium severity ranking. A critical vulnerability might be effectively neutralized in a relatively easy manner through modifications in configurations and existing security controls, while a medium vulnerability on a business-critical asset and behind a misconfigured firewall can create a dangerous exposure to attack. The context of vulnerabilities in relation to the business is key. Security practitioners should always use contextual analysis to determine the existence of a vulnerability and its importance, considering the possible exposure of key enterprise assets or information, under a variety of compliance regulations such as the US Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and the European Union General Data Protection Regulation (GDPR).

Finally, to turn high-level analysis into remediation action, an attack surface visualization tool should enable a user to easily and intuitively drill down from the attack surface view to greater levels of granularity where the user can fully evaluate potential actions. For example, a security manager identifies hot areas of the network when viewing vulnerability density at the highest level and then drills down to understand the set of vulnerabilities that are the greatest contributors to those hot spots. The user then zooms in further to identify the individual hosts or devices and actions that will have the greatest impact on vulnerability density.

Figure 2 shows how IOCs and IOEs are used in the attack life cycle.

Zero-day Attack Scenario

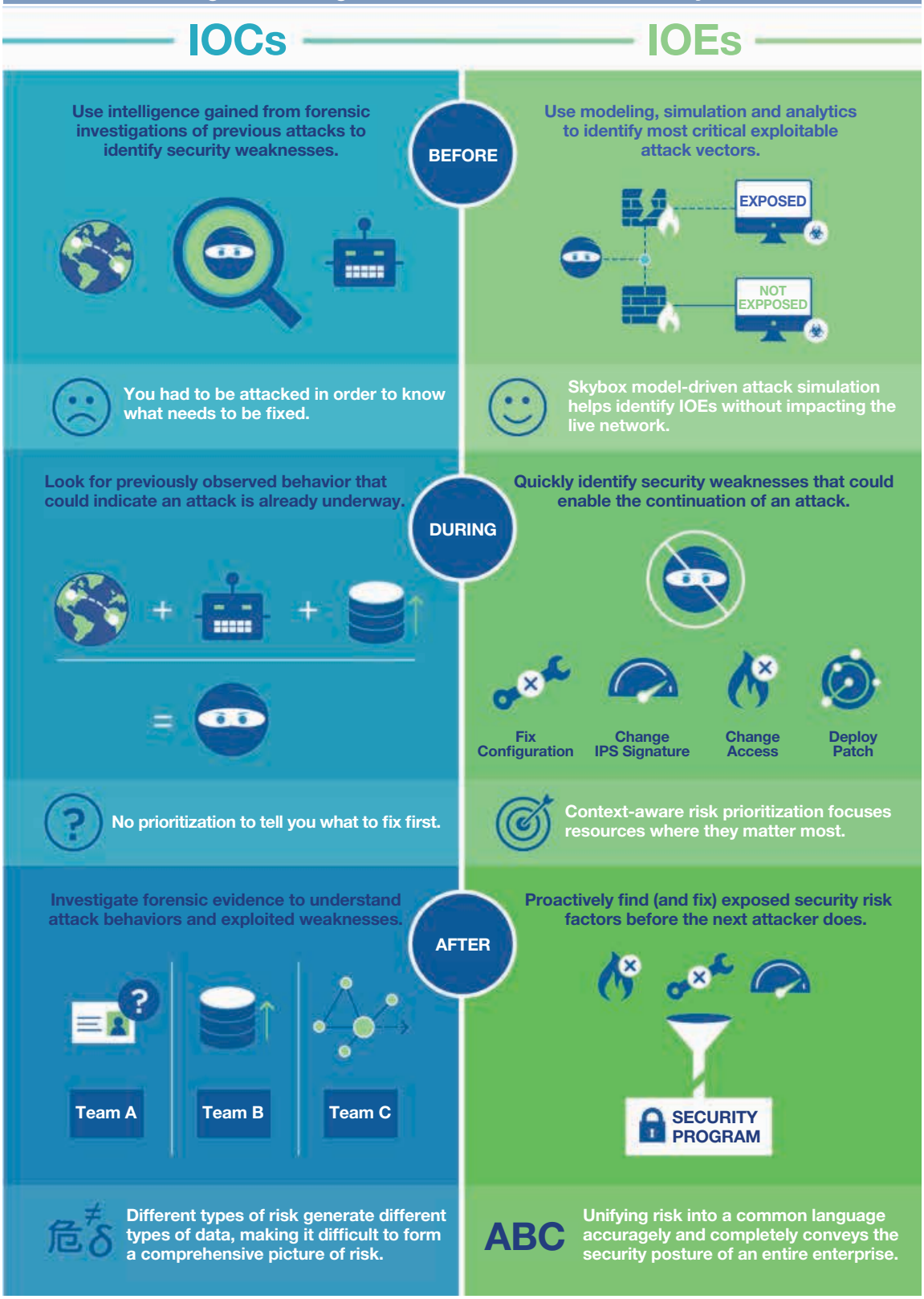
When discussing IOEs, it helps to place them in the context of a real-world scenario. To illustrate, take zero-day attacks, in which time is of the essence. Security teams must identify vulnerable hosts within minutes and neutralize attack vectors immediately. The 2016 news reports describing the simultaneous exposure of network vulnerabilities that were discovered by the US National Security Agency (NSA) and the malware code that was needed to exploit those vulnerabilities highlight the need for quick action.

The following timeline is an example of such a zero-day situation for an enterprise using an attack surface visualization tool with IOEs:

1. Zero-day vulnerability is announced. Immediate knowledge of susceptibility is required, so a real-time attack surface model is pulled up.
2. IOEs are updated in minutes through a reanalysis rather than a rescan of the network, which can take days to complete.
3. Filters are applied to identify only those IOEs containing the newly discovered vulnerability.
4. The ability to drill down to the host or device level provides security teams with the precise information that they need to perform the necessary remediation.

The assets that are most exposed to the attack can be attended to as highest priority. The attack that could threaten the livelihood of an enterprise can be quickly and effectively thwarted.

Figure 2—Using IOCs and IOEs in the Attack Life Cycle



Source: R. Circus. Reprinted with permission

The Network Security Pendulum

For years, the pendulum of network security has swung between the extremes of prevention and reaction. A happy medium that incorporates both is needed. Such an approach combines close attention to IOCs with close attention to IOEs—because simply knowing that security has been compromised is no longer enough. Security practitioners must be able to redress attack vectors before they can be exploited. A complete understanding of the attack surface is fundamental to both, requiring a solution that combines an intuitive, visual representation at every level with the ability to drill down into specific assets and the vulnerabilities within those assets. Attack surface visualization tools with IOCs and IOEs provide this solution.

Endnotes

1 Ayers, P.; "Cybersecurity: Issues and ISACA's Response," lecture, Jacksonville ISACA Chapter, Jacksonville, Florida, USA, June 2014

2 Goodreads Inc, "Benjamin Franklin," *www.goodreads.com/quotes/247269-an-ounce-of-prevention-is-worth-a-pound-of-cure*

3 Verizon, *2016 Data Breach Investigations Report*, 2016, *www.verizonenterprise.com/verizon-insights-lab/dbir/2016/*

4 *Ibid*.

5 Skybox Security Inc., "2015 Enterprise Vulnerability Management Trends Report," 29 April 2015, *www.skyboxsecurity.com/resources/report-2015-enterprise-vulnerability-management-trends*