Secureworks

WHITE PAPER

The Benefit of a Clean Sheet for your Security Environment

In an age of constant changes to the regulatory landscape for digital security, testing your environment for existing threat actors might save your organization a lot of pain.

Global and locally governing organisations and private sector bodies have traditionally focused on implementing controls to protect Personally Identifiable Information (PII) with strategies such as 'privacy by design,' which is the process of taking privacy into account throughout the whole development process. While this is valuable, the result can be gaps which can lead to vulnerabilities. It misses programs and processes that have previously been developed without privacy in mind. Pre-validation—a review for existing or historical breaches—can help organizations identify and correct these security gaps to help you build a better, more effective security program.

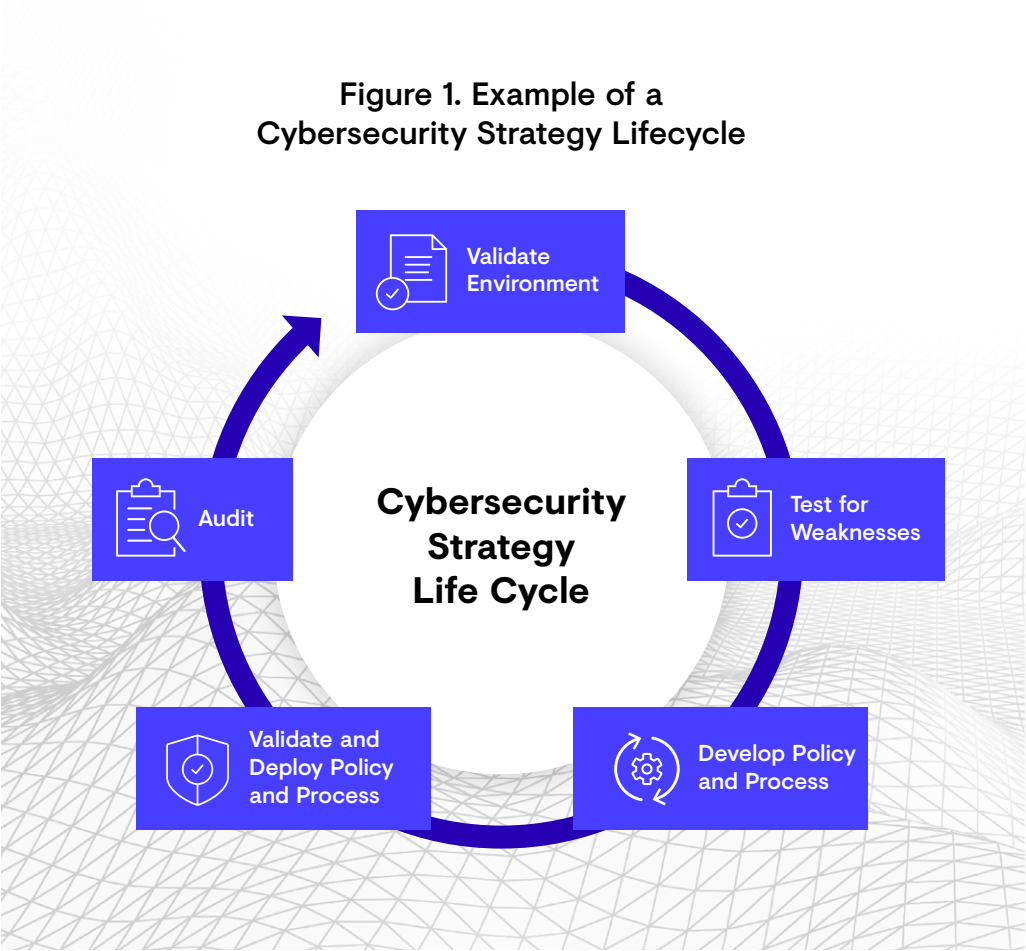
Each year, the mean time for detecting an active compromise (dwell time) changes, however the vast number of published breaches reveal that compromise events occurred months, if not years, prior to detection. Effectively the threat actor had been 'living off the land,' which is defined as a threat actor using an organization's inbuilt systems and software to achieve their goal.

Validation as Part of the Cybersecurity Lifecycle

To describe pre-validation, think of it like buying a second-hand car. If you are about to make a large investment in something that you depend upon heavily, then you are going to have it inspected for issues that could cause you significant pain and cost in the future. Before you make large investments into how you will protect your organization, it is of benefit to make sure there is no existing breach that new investments might miss. Validating that organizations have a clean threat-free environment ensures that the investments made towards future processes and policies are not going to miss a pre-existing breach. This pre-validation work will ensure the effectiveness of an organization's hard work around building out an improved cybersecurity program.

Below, Figure 1 highlights an example of what a cybersecurity strategy lifecycle could look like – you may note its similarity to the Incident Response lifecycle. This is an important comparison because the incident response lifecycle is the treatment of one particular threat, designed to eradicate it from an organization's environment, while the cybersecurity strategy lifecycle gives you a strategy for your entire technology environment.

Figure 1. Example of a Cybersecurity Strategy Lifecycle



It is to the benefit of the threat actor to keep their connection and access to an organization operational for as long as possible, which is why the cybersecurity strategy lifecycle is similar to the incident response lifecycle.

There are many variations out there on the 'kill chain,' a process a threat actor follows to complete the objectives of their attack. Reviewing the kill chain highlights that most of the steps involved are focused on getting into an organization's environment. Getting into the environment undetected presents one of the biggest challenges for online criminals so once they find a way in, they are not going to give up the access they have acquired. Rather, they will keep these back doors open, hiding malware in an organization's environment, ready to be utilized when they decide to launch an attack. Sometimes this can be seen in an organization's environment in the form unusual system issues, such as a user logging over VPN from two different countries just minutes apart. An irregularity like this is often inappropriately referred to as a "glitch." If your organization is experiencing any suspicious network behavior, it could be a sign to contact an incident response specialist.

Testing Before Investing

Threat actors living off the land is a lot more common than you might think. In fact, the vast majority of Secureworks targeted threat hunts result in uncovering threats that existing security solutions have missed, allowing us to help eradicate the threat and eliminate back doors to prevent the threat from returning. Even within some of the most sophisticated security postures, we have seen threats lying dormant, often because the threat existed in the network prior to the security strategy's implementation. This is why validating that a threat doesn't exist in your environment should be the first step in achieving compliance with new or existing security mandates. This will help make certain your organization has a clean bill of health before building out a robust strategy to help reduce overall risk exposure.

With new challenges to cybersecurity practices surfacing all the time, driving greater attention to cybersecurity, activities such as Targeted Threat Hunting should be seen as food for thought as organizations develop methods and processes related to how they will address their cybersecurity requirements.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp