SECUINFRA

Detect Intruders before They Cause Harm

A wise king never seeks out war, but he must always be ready for it.

Though the age of kings is long gone, the dictum holds its wisdom even in the era of concrete jungles and digital connectivity where threats, in the form of malware, lurk in every corner of a company's digital architecture, and wars are fought on a virtual front.

Very recently, the COO of a large company noticed a breach in his firm's security posture that could put critical data at risk. The company needed specialists in digital forensics, cyber threat detection, and analysis to defend against this targeted industrial espionage attempt. It was at this juncture that SECUINFRA, a seasoned veteran in this domain, entered the fray.

The Digital Forensics and Incident Response (DFIR) experts at SECUINFRA delved deeper into the issue to reveal that it was an Advanced Persistent Threat (APT)—a targeted attack that should be handled by a well-organized response. Over several months, they analyzed the APT's behavior to understand how the attacker infiltrated, what systems were affected, which communication channels were used, what attack methods were chosen, what they were looking for, and more.

After almost half a year of observation, the SECUINFRA team got together to launch a strong response against the APT.

All compromised systems were shut down, and new ones took over; all identified backdoors were closed, and all compromised accounts had been disabled, and new accounts were set into place. While this may seem like a time-consuming process, it only took a few minutes for SECUINFRA to implement its well-organized response, owing to the observation and preparation by the team. "Our forensic experts were engaged for a few more months with the customer and its APT, to ensure we found all backdoors and kicked out the intruder completely," says Ramon Weil, founder of SECUINFRA.

Attacks such as the above are frequent in the modern world. Defending against these digital daggers in the dark can be a nerve-wracking task, especially for organizations that do not know what exactly they need to be protecting from. SECUINFRA is the specialized partner that can detect successful cyber-attacks and compromised systems as early as possible to minimize damages and losses.

Drawing from his expertise in the cybersecurity industry, Weil categorizes clients the company works with, into three broad types. On the one hand, some firms feel insecure and are bothered by news regarding new attacks and breaches—a fear rooted in their lack of resources and know-how in countering cyber-attacks. On the other, are companies that feel secure until an attack occurs and incur massive losses. Then there is the kind that defends itself exceptionally well and is also aware of all measurements to detect and defend against cyber attacks.

SECUINFRA, although

Ramon Weil

initially built to detect successful cyber-attacks, has expanded into DFIR to hunt down perpetrators who pose a threat to the digital security of all clients, no matter the type.

The German company, with its team of well trained and certified cyber defense experts, helps companies fight against economic espionage, sabotage, and large-scale malware campaigns, which prove to be too much to handle for organizations with a low workforce. SECUINFRA, aiming to grow slow yet healthy, researches in the areas of Machine Learning and AI to understand what is possible in the cybersecurity space, and what is not. It uses static methods such as Security Information & Event Management (SIEM) and dynamic methods like network behavior, endpoint behavior, and user behavior analytics to give clients a clear view of what goes on beyond their organization's walls. "With our static methods such as SIEM, we detect well-known attack methods. With dynamic methods such as network behavior, endpoint behavior, and user behavior, we hunt for the unknown," says Weil.

A new offshoot of digital forensics—compromise assessment—is employed by SECUINFRA to find Indicators of Compromise (IoC) within the company's security posture. Using forensic methods and tools, the team looks for indicators of compromise that prove an attacker has successfully exploited vulnerabilities to gain access to the customer's infrastructure. SECUINFRA's compromise assessment goes far beyond by providing a vulnerability scan that highlights weak points in the infrastructure and a penetration test that shows if a penetration tester can use these vulnerabilities to break into the infrastructure. "Our compromise assessment shows if a perpetrator has already exploited vulnerabilities and compromised the customer's infrastructure," says Weil.

Clients can contract SECUINFRA for continuous compromise assessments, to increase their incident response readiness by tracking down compromised systems before more considerable damage occurs. With its services continually improving in their speed and efficiency, SECUINFRA gains knowledge of new IoC by combining its research and lessons learned from its forensics and DFIR engagements, with the exchange of IoC among the other companies in the digital forensics community. "This not only gives us knowledge on new threats but also lets us provide more accurate compromise assessments for early detection of breaches," adds Weil.

It is hard enough for clients to build an organization without having to deal with cyber attacks trying to raze it down. SECUINFRA's many years' experience identifying, analyzing, and defending against cyber attacks is the basis for the development of its unique compromise assessment service. The forensic experts working behind the scenes for this service, and others, are the reason, SECUINFRA has earned the acclamation of being a strong fortress standing tall against cybercrime. ES

"Our compromise assessment shows if a perpetrator has already exploited vulnerabilities and compromised the customer's infrastructure"