IDC ANALYZE THE FUTURE

IDC ANALYST CONNECTION

Sponsored by: Micro Focus

Cyberthreat defenses must evolve and modernize to make organizations cyber-resilient, including the adoption of advanced technologies such as artificial intelligence and security orchestration, automation, and response.

Key Strategies for Managing New Risks in Cybersecurity

November 2020

Questions posed by: Micro Focus

Answers by: Craig Robinson, Program Director, Security Services

Q. Organizations have traditionally had insight into new business risks based on predictable models. How has the global pandemic changed the need to sense for unexpected risks to the business?

A. Enterprise risk management has been turned on its head since the global pandemic arose. Historically, risk management has focused on the physical and financial assets within the virtual four walls of the enterprise. Digital transformation (DX) has caused those walls to fall over recent years, increasing coordination of supply chains and outsourcing agreements for various business functions. The board, chief risk officers, and security teams have struggled with intermittent success to be able to anticipate potential interruptions to their organizations that could now arise from these external business partners.

The growing risk of insider threats as a result of disconnected, disgruntled, or departed employees is increasingly difficult to anticipate. Throw in a global pandemic where entire countries have, at times, been forced to almost completely shut down, along with the sudden shift of work from the relative safety of the corporate office to residential apartments and homes, and you have a recipe for disruption.

Forward-thinking enterprises will need to start adding more domains to their "what-if" predictions. Risk management needs to include anticipating possible business interruptions to business partners, business partners' connections, and back-office technology partners. Global firms, or firms with international connections, will need to start thinking about how resilient they can be when the next big crisis is not necessarily a global pandemic but a crisis that knocks out a particular region's infrastructure for a significant amount of time.

Q. How should detection capabilities evolve and modernize to support business enablement through cyber-resilience?

A. Cyber-resilience is difficult to achieve if the methods used to detect attacks do not evolve to reflect the changes in how and where business activity is occurring. Timely detection of breaches before they become headline-grabbing banners builds trust in the organization. Systematic failures that cause an enterprise to fail to fulfill business obligations lower the level of trust between current and prospective partners and the enterprise.

As businesses expand into new geographies and evolve their product lines, executives are rightfully concerned about the cyber-resilience of the organization, but solutions need to ensure that the enterprise is also accounting for key third-party business partners.

Tabletop exercises need to consider what playbooks must be put together to account for any potential disruption activities from outsourced business functions or supply chain interactions. Service-level agreements should include language that requires a notification when there is a potential disruption to a partner's ability to fulfill contractual obligations. Contextual threat intelligence feeds should include potential and real-time attacks that are targeting sensitive industries and companies that are of importance to the enterprise.

Q. What role does early detection of cyber-related risks and threats play in an organization that is looking to build a cyber-resilient enterprise that can prosper during adversity?

A. The adage "speed kills" certainly applies to how important it is to detect attacks as soon as possible. Rapid detection of a criminal presence in the environment can make the difference between a minor removal of malware versus a serious data breach involving the leaking of substantial intellectual property or personally identifiable information (PII).
A distracted and displaced workforce has become a conduit of successful phishing attacks. Organizations must encourage a culture of self-reporting possible accidental clicks on phishing emails and should consider creating incentives on reporting of potential phishing emails.

Investing in threat intelligence services that can see over the horizon and identify incoming attacks as well as feed digital forensics on attacks as they land can speed up the historically high mean-time-to-respond (MTTR) key performance indicator (KPI). The ability to see attacks before they land is an especially effective defense, as are proactive activities such as patching targeted systems that have been blacklisted.

Organizations should pay special attention to the strategic threat intelligence that a full-featured threat intelligence provider can deliver. This is the sort of information that can feed cyber-resilient teams the key facts about the cybercriminal groups that impact the business, operations, reputation, or sustainable continuity of the enterprise. Understanding potential attackers could give insights into the tactics, techniques, and procedures (TTPs) that are in play.

Q. What role do machine learning (ML); security orchestration, automation, and response (SOAR); and artificial intelligence (AI) play in the new detection paradigm for modern threats?

A. Machine learning is used to distinguish and identify abnormal activity from normal activity. While human analysts can get overwhelmed when too much data needs to be analyzed, ML algorithms perform best when presented with vast amounts of data to analyze and draw insights from. Telemetry from hybrid cloud, 5G-enabled edge locations, email, networks, and endpoints is utilized to feed ML algorithms that can find the proverbial "needle in the haystack."

Artificial intelligence is increasingly utilized either to act independently or to augment human decision making when responding to cyberattacks. Security operations centers (SOCs) are often staffed with fatigued analysts who are overwhelmed with the number of alerts that require investigation. Not all alerts are of equal importance. Just like hospital emergency rooms require a triage nurse to prioritize who is treated first, AI can assist in the triaging of alerts that are of critical importance versus other alerts that can be ignored or tackled at a future time.

SOAR capabilities are key to implement because they can enable the proper response to any attack that lands. When properly refined and tuned to various potential attacks that an organization could face (i.e., ransomware, distributed denial-of-service [DDoS], malware), the SOAR platform can put its automated playbooks into action to quickly respond to the attacks.

Arguably one of the biggest advantages of a SOAR platform is that it lessens the likelihood of human error. Detecting and then responding to threats can be very stressful. A missed keystroke or a skipped step can undermine the response as well as the financial bottom line. Having a proven, properly orchestrated, and automated platform to utilize during stressful times, such as when an enterprise is under attack, is priceless.

Q. What detection elements should organizations put in place in the age of an identity-centric perimeter?

A. Organizations are recognizing that stolen and/or misused credentials are a key contributor to cyberbreaches. Utilizing systems such as multifactor authentication is a relatively quick way to prevent the use of stolen credentials, but other systems are needed to detect credential misuse. In a nutshell, identity and access management (IAM) solutions allow firms to manage the life cycle of an employee or, just as crucially, that of a third-party employed associate. The intelligence behind logging in to a laptop and any subsequent application such as an enterprise resource planning (ERP) suite or a human resource management system (HRMS) should be able to recognize when the identity tied to it has been hired, has been promoted, or is out on vacation so that these activities can be monitored and anomalies can be detected and sent to the appropriate systems for investigation.

The decimation of the traditional network perimeter by the new "work anywhere at any time" reality has caused chief information security officers (CISOs) to start looking at how they can architect their networks and applications to match reality. Implementation of zero trust (ZT) architectures is becoming the answer. The underlying principle of ZT is that the corporate local area network (LAN) is treated as though it were outside the corporate firewall.

Trust is never granted without verifying the identity of the user who is trying to gain access. Trust must be continuously earned and is never assumed. When an identity cannot be properly established, workflows can and should be set up to identify whether this is potentially an attack that deserves further attention.

About the Analyst

Craig Robinson, *Program Director, Security Services*

Craig Robinson is a Program Director within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include IoT security, blockchain services, and threat detection and response services. Mr. Robinson delivers unparalleled insight and analysis, leveraging his unique experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

MESSAGE FROM THE SPONSOR

About Micro Focus

Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges. The ultimate goal of cyber resiliency is to help an organization thrive in the face of adverse conditions (crisis, pandemic, financial volatility, etc.).

Micro Focus develops integrated cybersecurity solutions to enhance your intelligence and cyber resilience and protect against advanced cyberthreats at scale. To learn more about becoming cyber resilient, please take our 360-degree assessment at ***www.cyberresilient.com***.

IDC Custom Solutions

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com