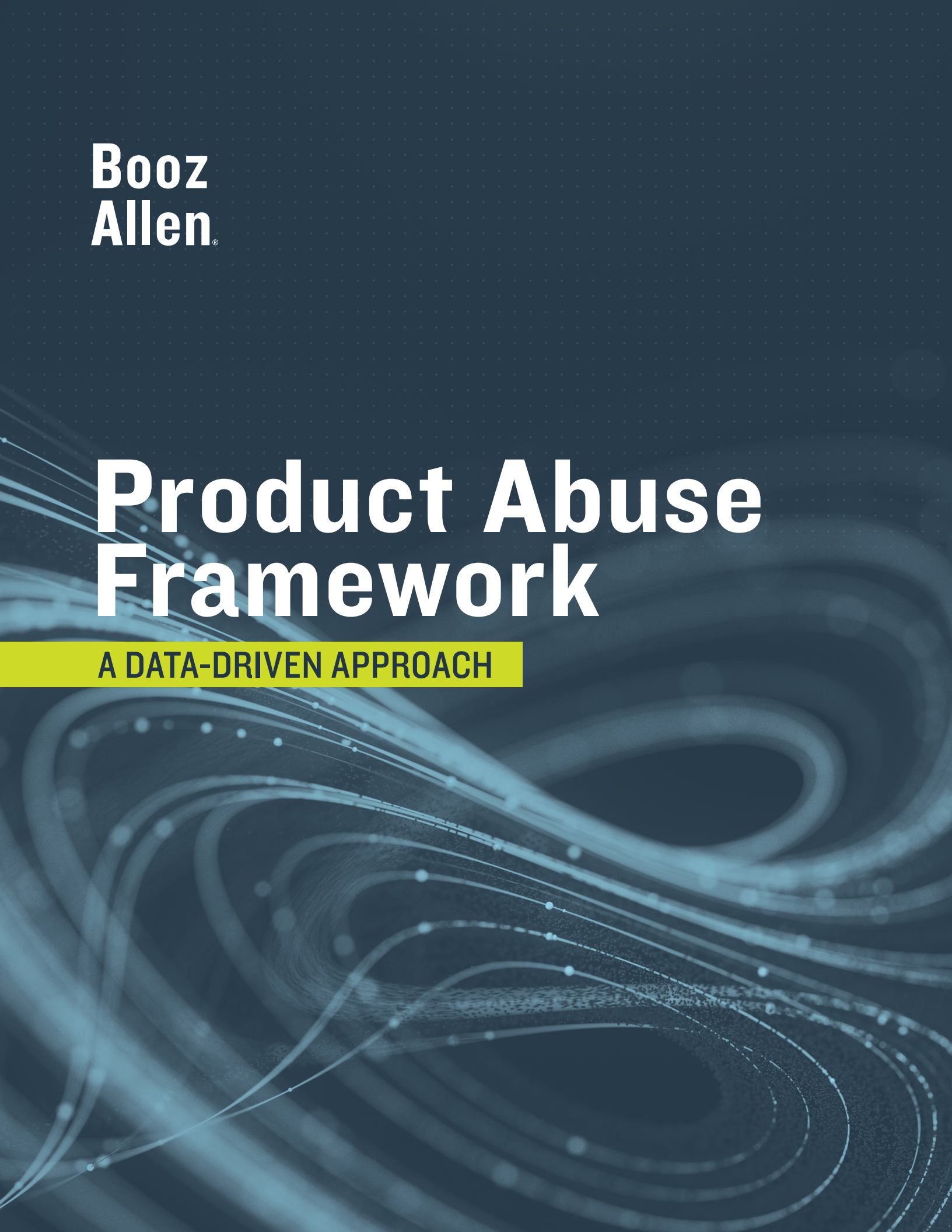
Booz Allen®

Product Abuse Framework

A DATA-DRIVEN APPROACH



TRADITIONAL RISK APPROACH: A GROWING PROBLEM

From the vantage point of the C-suite and the boardroom, it can be hard to tell that an organization's cybersecurity and fraud risk management efforts are poorly integrated. Disparate teams put in place countless controls, giving the appearance of multi-layered protection. The result is often a patchwork with gaps that hackers and fraudsters can easily discover and exploit. This means cybercriminals can maliciously monetize the business' internet-facing products like web-based portals, application programmable interfaces (APIs), and mobile applications. Such malicious activity is known as product abuse.

Hackers and fraudsters are in constant contact with online business tools designed to enable customers to log into accounts, set up and manage new accounts, enjoy seamless experiences involving third-party businesses, and make purchases. Cybercriminals are always testing controls, probing for information, and exploring the limits of actions that can be performed using the accounts and data at their disposal.

ALIGNMENT ON STRATEGY

Businesses often have a mix of edge or network controls, application layer controls, identity and access management (IAM), and anti-fraud or risk models. The control layers are owned by different organizational verticals, which makes it difficult to share data between the control layers and set unified strategies that streamline decisions. The three pillars of product protection traditionally used by organizations are information security, identity and access management, and fraud risk management. The ownership of the controls within a respective pillar creates gaps in the continuity and completeness of intelligence that could be shared among the control layers for more effective detections and mitigations.

Some organizations may have a simple model where the chief information security officer (CISO) organization is responsible for edge/network controls, application layer controls, and product identity and access management. The fraud risk management organization owns the models and processes to stop fraudulent activity. However, many organizations have multiple stakeholders/organizations controlling the multiple layers. Moreover, the CISO organization frequently has different goals than the fraud risk management organization and such a disconnect can potentially create significant challenges.

THE OWNERSHIP OF THE CONTROLS WITHIN A RESPECTIVE PILLAR CREATES GAPS IN THE CONTINUITY AND COMPLETENESS OF INTELLIGENCE

EXAMPLES OF MALICIOUS ACTIONS

- **Account takeovers** enable unauthorized access to an account that can result in the collection of personally identifiable information (PII), protected health information (PHI), transactional data, and other sensitive information
- **Account enumeration** determines if an identifier to an account exists such as username, email address, or phone number
- **Credential or card stuffing attacks** validate credentials or debit/credit card information
- **API vulnerabilities** let adversaries collect and correlate relationships between accounts on social media or other platforms where users communicate
- **Two-factor authentication (2FA) bypass** uses account takeovers of other products to bypass 2FA by gaining access to an email address or phone number

The CISO organization deploys controls to ensure that products do not have vulnerabilities and to protect availability from disruptions such as distributed denial-of-service (DDoS) attacks, while the fraud risk management organization focuses on reducing the financial impact that adversaries cause with account takeovers or synthetic/fake accounts that support illicit activity within the product. Misalignment often occurs when the two organizations use their controls and resources to address two distinctly different problem sets. What is missing is accountability for preventing the abuse of internet-facing products—actions that might appear legitimate but are malicious. Such actions might include downloading account data, transactional information, health records, and more. Accountability can take the form of coordination of objectives and key results (OKRs), data management requirements, or documentation of the control architecture.

To address these challenges, ***businesses can work to create alignment between the CISO and fraud risk organization***, so they work together to create a strategy to meet their own business needs while focusing on preventing abuse that falls in between their two goals. Creating such alignment can also help reduce losses associated with abuse within the products, such as account takeovers and fake accounts that launder money, create scam websites, and produce propaganda. Organizations can strengthen their management of these risks by assigning oversight to a single organizational leader, such as the chief risk officer (CRO) or chief operating officer (COO) organization, to provide a clear, direct strategy that needs to be in place to ensure all stakeholders are aligned and unified in their approaches.

IMPROVED METRICS FOR VISIBILITY INTO THREAT ACTIVITY

Traditional cybersecurity metrics are insufficient for managing product abuse risk and would benefit from the alignment on strategy. In fact, relying on these traditional metrics can create a false sense of robust risk management when the organization lacks significant opportunities to counter these risks with greater efficiency and effectiveness. Adversaries can take advantage of gaps in controls and visibility caused by organizational misalignment and communication issues, specifically in information security, IAM, and fraud risk management. To combat these issues, organizations should explore opportunities to use data-driven approaches to measure the amount of pressure being put on controls, which will be referred to as threat pressure, and in turn, use a model to measure the effectiveness of any control protecting the product during a specific time (i.e., day, week, or month). These approaches should establish common OKRs to support aligning on what the effectiveness of a control means and measuring against it. Opportunities to deploy approaches will be discussed in the following sections.

> RELYING ON TRADITIONAL METRICS CAN CREATE A FALSE SENSE OF ROBUST RISK MANAGEMENT

ALIGNMENT CREATES ADDED VALUE

Alignment to the same mission and strategy between control layers enables more than just consistency. It also helps to pull together decision-making, control mapping, and control data. Control owners may not understand when their controls are straying from their baselines as they may have an incomplete picture from a data perspective to attack traffic that is making it past their controls. In turn, the control owners and the oversight organization need to unify control data sources to identify patterns when controls are allowing malicious traffic through to the next layer. This will help solve the problem of knowing the effectiveness of their controls at any given time.

Measuring the effectiveness of controls is difficult, so organizations rely on metrics shared by their vendors or perform penetration tests to determine the effectiveness. These metrics are only a point-in-time attestation to the effectiveness of controls. To create a holistic approach to measuring effectiveness, organizations should consider the method provided below that aims to assess risks to control performance in near-real time.

MORE ON CONTROL EFFECTIVENESS

To accurately quantify the effectiveness of controls protecting an environment and therefore measure the risk of the system, organizations need to create solutions consisting of robust logging and analytics. The solutions should be capable of tracking the control activity across a session to fully understand the responses to malicious activity. Logging and correlation of activities should occur on sessions detected/mitigated by controls and sessions that were not prevented, resulting in the intended malicious activity, such as an account takeover. It is difficult to measure the effectiveness of any controls without a consolidated view of all malicious sessions, as any metric would be operating in a vacuum. A single pane of glass allows the organization to understand the effectiveness of controls at a given point in time, thus keeping up with evolving tactics, techniques, and procedures (TTPs) and the potential deterioration of controls.

Figure A shows traditional methodologies used by organizations to set risk ratings based on the coverage and effectiveness of controls in their environment. Coverage is typically static; however, the effectiveness of a control changes depending on the TTPs used by adversaries and the pressure (or volume) of requests being made on the control. Booz Allen labels this volume of traffic as threat pressure. Think of increased threat pressure as a multiplier to the likelihood variable in traditional risk equations *(i.e., RISK = IMPACT * LIKELIHOOD)*.

CONTROLS	*COVERAGE*	*EFFECTIVENESS*	*RATING*
A	**50%**	**50%**	**GREEN**
B	**100%**	**99.9%**	**RED**

Figure A: *Traditional risk ratings*

Consider how the equation changes if *Control A* is sitting in a segmented network zone with compensating controls and limited access, and *Control B* protects an executive's mailbox containing sensitive business information.

Does the risk equation change when the executive goes from their baseline of receiving five malicious emails per month to 1,000 malicious emails in a week?

At 99.9% effectiveness, the pressure would increase the likelihood of a significant security incident and may change the risk rating. The threat pressure concept allows organizations to increase the fidelity of their alerting, improve threat hunts on relevant activity, and provide trending to threat-related activity targeting specific controls, systems, assets, or individuals.

MEASURING THE LEVEL OF THREAT PRESSURE PROVIDES VALUE AS IT RELATES TO:

- Increased pressure may **increase** a control's risk profile
- Clusters of adversarial activity will **inform** leadership on the state of targeting by adversaries against the organization
- Increased pressure can help **prioritize** alerting or provide support to security/fraud incidents
- Utilization of data-driven approaches to **contextualize** the level of abuse a threat is performing on the system

THREAT PRESSURE IN ACTION FOR PRODUCT ABUSE

Applying the threat pressure concept provides visibility into abusive product activity and can help to reduce risk. As previously mentioned, measuring control effectiveness and threat pressure is partial if all control data is unavailable for analytical modules to process. The recommended solution is to ensure an appropriate platform, such as a cloud environment, is created to store all relevant control log data across the edge/network controls, application layer controls, identity and access management, and anti-fraud/risk models. Another option is to ensure that the control data is logged within the security information and event management (SIEM); however, our experiences suggest that the analytics and logging may cause issues with SIEM performance given the large volume of data and analytics required. This allows organizations to comprehensively document the controls across products with the support of the aligned stakeholders.

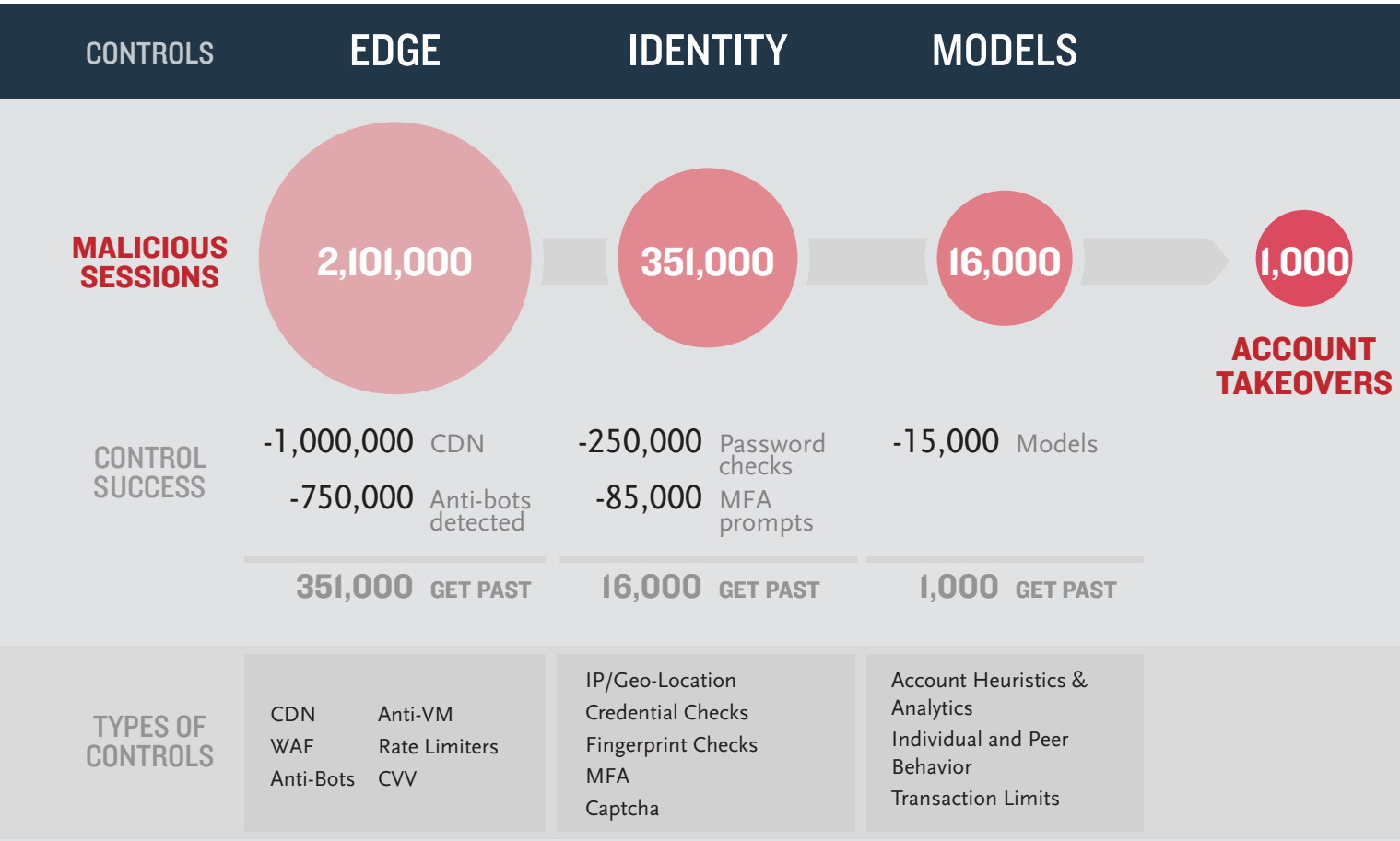


Figure B: *Threat pressure filtering*

Monitoring and alerting should be applied using analytics to identify changes in control activity over time. For instance, a rise in password failures could correlate to a drop in mitigations by the prior control, such as an anti-automation control or rate limiting, and indicate that an attack campaign has found a way to bypass the prior control(s). This alerting allows for threat hunting and forensic teams to have actionable insights into malicious activity relevant to product security from the threat pressure. Teams use actionable insights from the analytics to reverse engineer how attacks exploit a process vulnerability or other techniques to bypass controls with a data-driven approach. The data-driven approach provides stakeholders with true positives to research.

Formalizing and unifying data sources allow organizations to measure the effectiveness of controls. For example, in ***Figure C***, the total number of malicious sessions observed is 2,101,000. Each control's effectiveness is measured by the number of sessions acted upon divided by the total volume of traffic coming into that control.

CONTROLS	*MITIGATED SESSIONS*	*CONTROL EFFECTIVENESS*
CDN	1,000,000 / 2,101,000	**46%**
ANTI-AUTOMATION	750,000 / 1,101,000	**68%**
PASSWORD	250,000 /351,000	**71%**
MFA	85,000 / 101,000	**84%**
MODELS & RULES	15,000 / 16,000	**94%**

Figure C: *Control effectiveness for a given control*

Decision makers can set baselines on control effectiveness for each layer using data observed over time rather than point-in-time testing or assumptions. It allows the stakeholder to appropriately assess the accepted risk levels for how those controls operate.

One caveat is the presence of false negatives, or control actions on non-malicious traffic, in the control logs. Organizations need to understand their false positive and false negative rates, as inaccurate actions by controls would impact perceived control effectiveness. The good news is the collection of log sources, and associated analytics, makes it easier for organizations to assess their controls' impact on legitimate user activity. This is because the control data is in one place; therefore, the correlation of event data across layers can help determine if false negatives exist.

FOCUSING ON TACTICS, TECHNIQUES, AND PROCEDURES

Identifying controls and associated logs allows organizations to pursue how their controls map to tactics, techniques, and procedures (TTPs) for product abuse. The MITRE ATT&CK framework is commonly used by information security programs to identify gaps in controls and enable threat-hunting activities; however, this same concept can be used by organizations to assess controls for product abuse. Booz Allen has been developing a TTP framework for reference to support research into product abuse. It was developed to understand the TTPs Booz Allen has observed and documented through client engagements and external threat intelligence.

> ORGANIZATIONS CAN USE THE MAPPING OF TTPS TO CONTROLS TO SCRUTINIZE HOW DIFFERENT ATTACKS ARE EVOLVING

Figure D provides a high-level view of the product abuse TTP framework; however, each technique is broken down into sub-techniques to provide more granularity into attack patterns. For example, under the "Resource Development->Obtain Crimeware," sub-techniques that need to be accounted for in reducing abuse, especially automated abuse, include "Black Box Credential Stuffing Crimeware," "Configurable Credential Stuffing Crimeware," "Headless Browsers," "Anti-Detect Browsers," and "Mobile Emulators." Each sub-technique includes descriptions of tools used for these observed attacks and suggested detection techniques.

TTP FRAMEWORK FOR PRODUCT ABUSE

RECONNAISSANCE	RESOURCE DEVELOPMENT	DEFENSE EVASION	PERSISTENCE	DISCOVERY	COLLECTION	IMPACT
Active scanning	Acquire infrastructure	Abusive elevation control mechanism	Account Manipulation	Account discovery	Adversary-in-the-middle	Application denial of service
Gather identity information	Compromise accounts	Access token manipulation	Create account	Browser information discovery	Automate collection	Attrition of accounts
Gather product information	Compromise infrastructure	Anonymized, distributed IP infrastructure	Established device personas	Control discovery	Data from information repositories	Brand and reputational damage
Gather victim network information	Compromised financial instruments	De-obfuscate / decode files, code, or information	Precision through proxies	Honeypot evasion	Input capture	Data manipulation
Probe and validate information	Compromise identities	Direct access to origin servers	Valid accounts	Software discovery	Manual collection	Financial losses/fraud
Search closed sources	Develop crimeware	Establish trust			Screen capture	Network denial of service
Search victim owned websites	Establish Accounts	Masquerading				Regulatory Notifications
Search open technical databases	Establish accounts	Third party and business integrations				
	Obtain crimeware	Valid accounts				

Figure D: *Product abuse TTP framework for organizations to map TTPs used by adversaries targeting internet-facing products.*

Organizations can use the mapping of TTPs to controls to scrutinize how different attacks are evolving, especially when utilizing threat pressure to research changes to malicious product sessions. The combination of data-driven alerting and threat modeling is a powerful tool for organizations to focus on legitimate threats within their product ecosystem. For example, organizations could refer to the diagram to determine how their controls effectively reduce risk from both a tactical and strategic point of view regarding credential stuffing attacks on web-based login portals for customers. Adversaries use several tactics and techniques to carry out credential stuffing attacks, such as collecting compromised credential sets, acquiring IP infrastructure for proxying traffic, and using crimeware (customized or purchased) to make the requests. A basic review of controls would identify if organizations had visibility into compromised credentials, the ability to use threat intelligence data and other means for IP reputation, and inspect client requests to identify the latest crimeware employed to carry out credential stuffing attacks. Additional work should be performed regularly as new techniques emerge to visualize the gaps in controls, or the change in the effectiveness of controls, to key stakeholders and leadership.

EXAMPLE STRATEGIC ALIGNMENT BASED ON IDENTITY

As noted earlier, we recommend organizations assign oversight to a single organizational leader, such as the CRO or COO organization, to help align on a strategy to protect internet-facing products. The following section shows how the oversight leader can create a strategy for protecting customer accounts.

Aligning monitoring and controls in an identity-centric manner allows organizations to understand the impact of threat pressure and implement responses consistently. This is regardless of the subject of an attack being an individual account or API. Understanding that there is increased pressure on a web portal by new crimeware is important. However, that is only a partial solution. To mitigate the risk, identifying and alerting related to the population of impacted accounts needs to be in place. In addition, ensuring other products or services are aware of the affected accounts allows them to adjust their risk posture without disrupting the user population.

Logging and event monitoring should be implemented uniformly to ensure the accounts can be identified and linked across platforms and services. Advanced platforms or services can consume this data to provide the context for risk decisions. At a minimum, operational teams will be better equipped to threat hunt and prevent monetization of attacks at the account level.

NEXT STEPS

This paper provides recommendations to help organizations methodically counter the abuse of their internet-facing products. Here is a recap of the recommended actions:

- **Stakeholder alignment:**
  - Document the key stakeholders who are responsible for controls that protect internet-facing products.
  - Identify an executive to provide oversight to protect the organization's products.
  - Develop a unified strategy across the control layers.
- **Control mapping:**
  - Identify all controls for internet-facing products.
  - Aggregate the control logging into a centralized data lake/store for analytics.
- **Tactics, techniques, and procedures (TTPs):**
  - Document the TTPs that are observed within the organization's products and ecosystem.
  - Identify where there are control gaps or weaknesses for TTPs relevant to the organization.
  - Continually update the documentation as new techniques and sub-techniques emerge.

These recommendations provide data-driven approaches to enable key stakeholders and leadership with the details to make informed decisions about risk. The decision to implement a control or make major architectural changes without the data is difficult to justify to other stakeholders for financial and technological support.

The CISO organization should be a catalyst to call for the alignment of stakeholders, controls, and data sources to prevent unauthorized or unintended access to an organization's data / records. This initiative should be performed in collaboration with the chief risk officer, and backed by the chief financial officer, to scope the risks, identify measurable impacts, and stress the importance of mitigating to support the business' strategic objectives. Organizations should also consider involving the business intelligence function in the development of better metrics that take fraud prevention and abuse of products into account to inform cyber and risk management investments. These metrics will impact the ability of organizations to adopt data-driven cybersecurity approaches that advance business objectives.

BAH-2024-10-28

SOURCES

https://www.security.org/digital-safety/account-takeover-annual-report/

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account

https://owasp.org/www-community/attacks/Credential_stuffing

https://technologymagazine.com/cloud-and-cybersecurity into-the-breach-breaking-down-3-top-api-security-breaches

https://www.securityweek.com/6-ways-attackers-are-still-bypassing-sms-2-factor-authentication/

https://attack.mitre.org/techniques/T1111/

TO LEARN MORE, CONTACT BOOZ ALLEN:

infosec@bah.com

BoozAllen.com/Commercial

BAH-2024-10-28

Booz Allen®

ABOUT BOOZ ALLEN HAMILTON

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining 110 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: Empower People to Change the World®.

BAH-2024-10-28