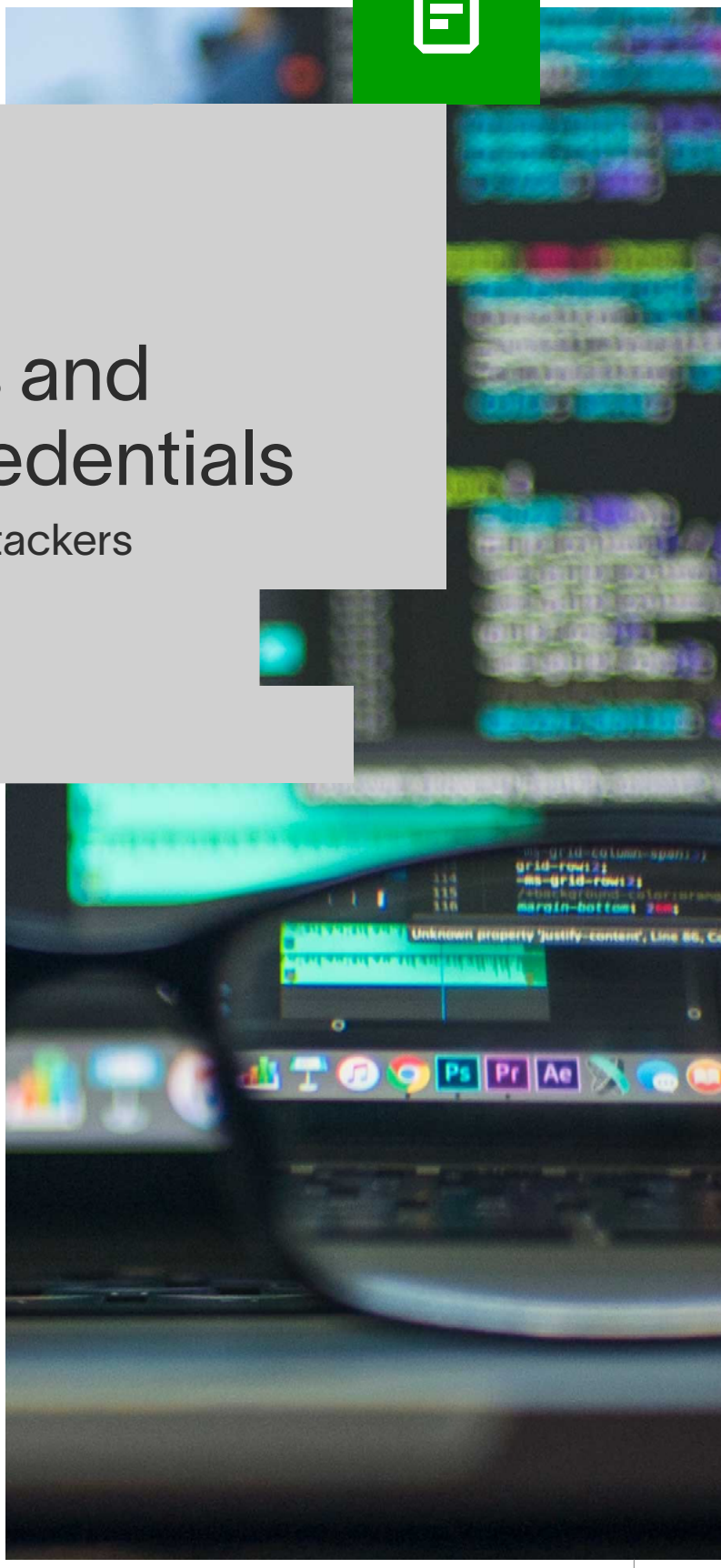
exabeam

TUCANA CYBER SECURITY SOLUTIONS

Checklist

Insider Threats: Malicious Insiders and Compromised Credentials

Whether it's angry insiders or attackers for profit, here are checklists for detecting and addressing them.



Defending against insider threats is more than just picking the right security solutions. It's also defining and creating a security program that pulls people, processes, and technology together to effectively defend against these kinds of threats.

An insider threat is malicious activity against an organization that comes from user credentials with legitimate access to an organization's network, applications, or databases. These credentials can be current employees, former employees, or third parties like partners, contractors, or temporary workers with access to the organization's physical or digital assets. They can be privileged or service accounts that have automated download functions or normal activities that have been compromised by an identity-based attack. While the term is most commonly used to describe illicit or malicious activity, it can also refer to any user account which causes harm to the business. The following checklist is meant to be a guide when defining an insider threat or insider risk defense program.

Malicious Insiders

A malicious insider is an employee or contractor who knowingly looks to steal information or disrupt operations. This may be an opportunist looking to sell confidential information, re-use secrets in a new job opportunity, or a disgruntled employee looking for ways to disable an organization or punish and embarrass another employee.

- **Validate personnel**
  - The organization ensures a trusted workforce by fully vetting employees prior to granting them access to assets and by implementing procedures to alert on behavior indicative of insider threats once onboard.
  - Vet all personnel, regardless of role (full-time employee, part-time employee, contractor, partner, etc.) before granting access to organizational assets.
  - Create a vetting program and define levels of access for each role type.
- **Continuous monitoring**
  - Employees and assets are monitored to obtain visibility for purposes of uncovering actions that are indicative of a threat and may negatively impact the organization.
  - Use relevant security solutions to monitor users.
  - Scrutinize signs of threats like resignations and abnormal activity as defined by security solutions.
  - Leverage relevant security solutions for fraud by monitoring and reporting transactions and communications.
- **Analysis**
  - The analysis across multiple platforms and sources, capable of providing actionable alerts, is conducted to identify behaviors and interactions that may be indicative of a threat.
  - Use security solutions that provide user activity monitoring (UAM), behavioral analytics, and data loss prevention (DLP) to provide a complete picture of both asset and insider actions and behaviors.
- **Investigation**
  - Behaviors, actions, and insider threat indicators are examined and fully explored to determine the level of threat, and then mitigated in accordance with established policies, business objectives, risk tolerance, and regulatory requirements.
  - Coordinate between security teams, HR, legal, and other business units to determine how to ensure a seamless, secure exit that removes network assets and investigates final activities.
  - Create an insider risk center of excellence (COE) led by CSO and include dedicated management, SME, analyst, and investigator support.
- **Insider risk assessment**
  - The organization's priorities, asset impacts, vulnerabilities, and threats are identified and used to measure insider risk to support business operations and security resource allocations.
  - Define a logical process to identify, assess, and communicate the risk of insiders and then, develop a formal policy to address risk and allocate resources for tools and people.
- **Compliance and reporting**
  - Insider risk management personnel, processes, and procedures are formally managed and reviewed for compliance with established legal, privacy, policy, and regulatory requirements.
  - Identify, document, and communicate operational parameters with formal metrics and plans that align with key regulatory requirements.
  - Create quarterly compliance reports for legal and risk with relevant information as defined by insider threat program and legal.

Compromised Credentials

Compromised credentials are when a legitimate user's credentials have been obtained by a malicious actor either directly or via trojan malware, and are used to access sensitive information. This typically happens via phishing scams or by clicking on links from malware. Compromised credentials could also happen as a result of a negligent insider — an employee who did not follow proper IT procedures such as someone who left their computer without logging out, or an administrator who did not change a default password, failed to apply a security patch, or inserted an infected USB into their computer. Compromised credentials are used as a "home base" for cybercriminals, from which they can move laterally, scan file shares, create new accounts, escalate privileges, access or infect other systems, and more.

Compromised Credentials, contd.

- Governance and strategy
  - Assign an Insider Threat Director (ITD) role to serve as central coordination and communication point, leading the insider threat working group and reporting to the CSO or CRO.
  - The organization's ecosystem, structure, objectives, policies, and procedures are defined, and regulatory, legal, and operational requirements are understood and inform the management of insider risk.
  - Define cross-functional owners for each component.
  - Set metrics and specific tasks for each component to ensure objectives are met.
  - Ensure each component owner is part of an insider threat working group.
- Training and awareness
  - Insiders are provided with threat awareness education and are trained to perform their insider risk-related responsibilities, consistent with related policies, procedures, and agreements.
  - The workforce is trained on regulations, expectations, codes of conduct, conflict resolution processes, and the policies and procedures supporting each.
  - Ensure insider threat training explores the various types of insider threat personas and is continually updated and expanded.
  - Engage and inform employees of current regulations, security threats, and practices with regular updates and education.
- Asset identification and prioritization
  - The organization's assets are identified, prioritized, and managed consistently with the organization's insider risk strategy, including trading systems, financial applications, and SWIFT network access.
  - Create a formal program to identify and define critical assets.
  - Establish an asset identification process that captures relevant information like asset type, asset owner, authorized users, access, usual behavior, and locations.
  - Map sensitive data flows.
- Entitlement control
  - Entitlements to assets and associated facilities are limited to authorized users, processes, or devices, and to authorized activities and transactions.
  - Audit entitlements to sensitive information regularly to ensure unnecessary access privileges don't exist and reduce the number of devices with access.
  - Audit account names and creation dates — particularly for new accounts created outside the standard IT practices.
  - Take into account non-static insiders like temporary employees, contractors, and business partners as they may have access to sensitive information.
  - Review and shut off access to systems and data in a timely manner for departing employees.

About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in Next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit

exabeam

TUCANA CYBER SECURITY SOLUTIONS
www.tucana.com info@tucana.com