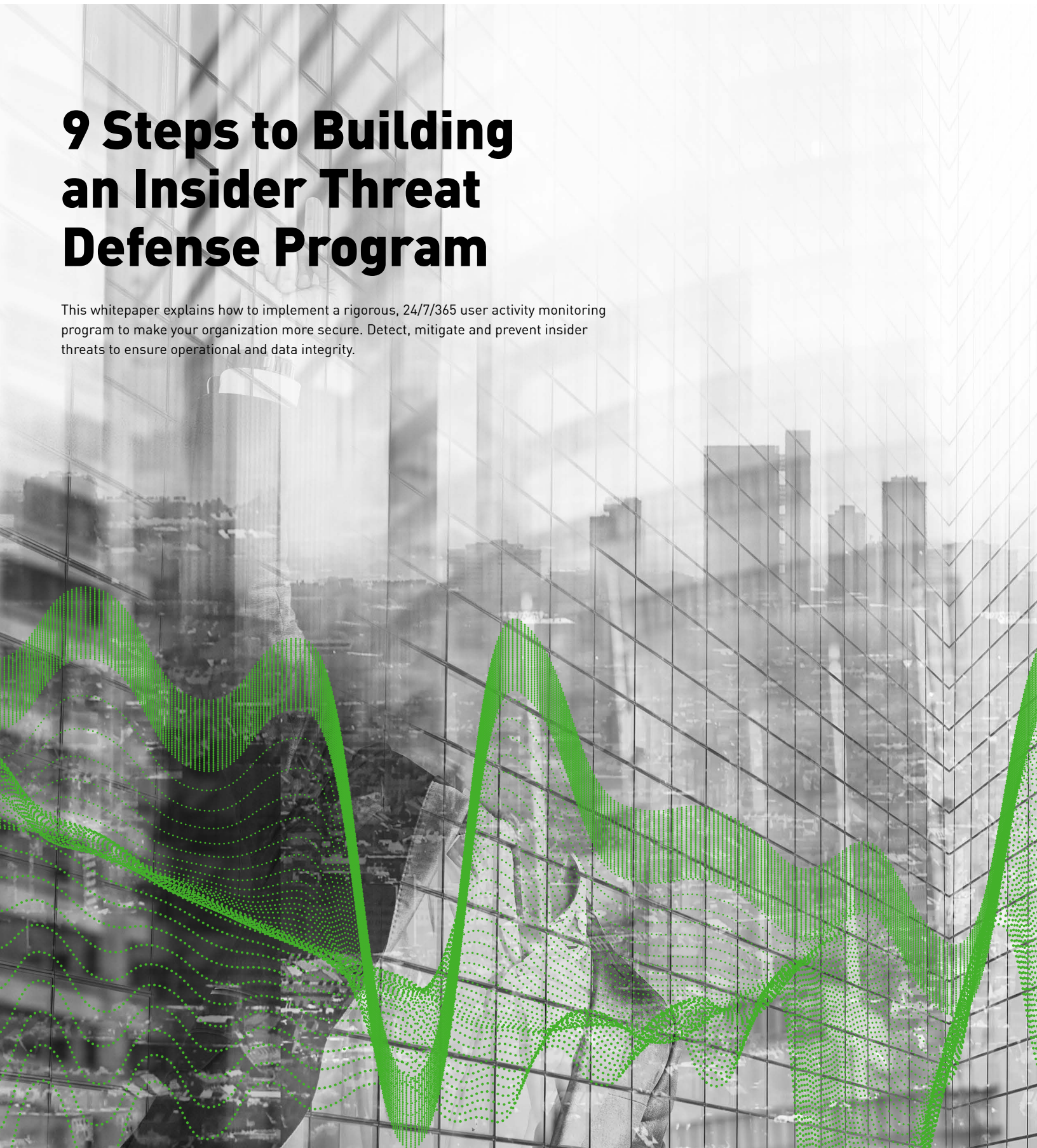
FORCEPOINT
POWERED BY Raytheon

Whitepaper

9 Steps to Building an Insider Threat Defense Program

This whitepaper explains how to implement a rigorous, 24/7/365 user activity monitoring program to make your organization more secure. Detect, mitigate and prevent insider threats to ensure operational and data integrity.



Contents

EVERY ORGANIZATION NEEDS AN INSIDER THREAT DEFENSE PROGRAM

Insider threats pose high risks to all enterprises. No organization, regardless of size, industry or region, is immune. With all the advantages that the digital age has brought us — and they are many — it has also brought a rise of highly damaging data breaches, from both internal and external sources. But regardless of the source, all threats eventually come from the inside. Early and clear recognition of the signs and indications of insider threats is, therefore, a key part of defending your network from crippling data breaches and data theft. The challenges of identifying and defending against insider threats are significant and include:

Too much access to critical data

Widespread, uncontrolled remote access to your organization's critical data and users with too much and unnecessary access and privilege to networks and data lead to your critical data being:

- More accessible — and exposed — than ever before
- Subject to theft using a simple thumb drive or single click on an email or URL
- Ripe for exploitation via malware unleashed by a careless user

Too little user supervision and control

Most enterprises lack the supervision and control they need to prevent insider-caused data breach incidents. In many cases, organizations are losing critical data and don't even know it. That risk comes in many forms:

- Employees connecting to the enterprise network, both inside and outside the office, often far away from the eyes of supervisors
- Liberal Bring Your Own Device (BYOD) policies
- Business partners with too-broad data security permissions
- An expanding network of third-party contractors

In response to these challenges, well-informed supervision and behavioral context is critical.

You should know that:

- An insider threat defense program involves people, processes and technology
- You can't rely on an assumption of good behavior or best intentions
- You need to gain context around user behavior to know who is accessing your data, for what purpose and where that data is going

NINE STEPS TO BUILDING YOUR INSIDER THREAT DEFENSE PROGRAM

A successful insider threat program requires a process that includes these nine steps:

1. **Formally Establish Your Insider Threat Program**
2. **Create a Business Case**
3. **Assemble Your Team**
4. **Involve Stakeholders Early and Often**
5. **Give Education and Awareness Training to All**
6. **Incorporate Governance and Oversight**
7. **Select the Auditing and Monitoring Solution**
8. **Launch Your Insider Threat Program**
9. **Keep People Interested and Engaged**

MANAGEMENT, USERS AND TECHNOLOGY: THE GOLDEN TRIANGLE OF SECURITY AND BUSINESS ENABLEMENT

The 9 steps in this whitepaper outline how management, users and technology security objectives must align with — and enhance — the organization's business objectives. This means that the program must NOT disrupt productivity, overburden your IT staff or hurt your reputation. Finally, the program must be policy-driven from the highest level and made a part of user behavior. Note that in the following 9 steps, technologies for access and activity monitoring play a crucial, but supporting role.

According to the 2015 Vormetric Insider Threat Report:

93% of U.S. enterprises polled believe they're vulnerable to insider attacks—almost twice the number from 2013.

Figure 1. Source: 2015 Vormetric Insider Threat Report

1. Formally Establish Your Insider Threat Program

A strong insider threat program doesn't just happen. Management must launch the program overtly, with direction and big-picture support from the C-suite on down. That will empower program leaders to move forward, even in the face of institutional inertia or operational delays. Any other approach threatens to make your program a low priority or even irrelevant. Be aware of regulation and mandates that require insider threat programs; such as National Industrial Security Operating Manual (NISPOM) Change Order 2.

ESSENTIAL INGREDIENTS OF AN INSIDER THREAT PROGRAM

- **Policies.** Leadership must establish clear rules for BYOD, social media, Web surfing, transferring work materials to home computers and so on. Without stated policies, you can't hold employees accountable.
- **Processes.** Training in insider threat best practices should be a part of every new hire's orientation and reinforced on a consistent basis.
- **Technology controls.** These controls limit users' access to systems and data based on assigned roles. Project-based access is cut off when the project is complete.
- **Risk management.** Identify the enterprise's mission-critical data. What are the crown jewels that must be protected? Develop a risk-management plan for each one.
- **Auditing and monitoring.** All of the above measures are preventative in nature. Auditing and monitoring supports a broader, more comprehensive insider threat program.

It is crucial that you designate a leader for your insider threat program. The appointment of an Insider Threat Program Senior Official (ITPSO) will define roles and responsibilities for the team, assigning duties for prevention, detection and response. And he or she will be the one to step up when an issue or incident arises.

The ITPSO must also ensure that the insider threat program comprises policies, processes, training and awareness, technical controls and risk management, as well as auditing and monitoring. Auditing is key because it will measure the effectiveness of the program.

2. Create a Business Case

Creating a business case for your insider threat defense program not only gives the program budgetary legitimacy within your organization, but also institutionalizes the processes. Metrics to leverage include:

- Return on Investment (ROI) projections (such as forecasting financial losses due to a breach)
- Risk assessments to determine what needs to be protected
- Risk-compliance summaries for:
  - o Payment Card Industry Data Security Standard (PCI DSS)
  - o Financial Industry Regulatory Authority (FINRA) audit trail
  - o Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - o Other applicable regulations

3. Assemble Your Team

Team members must bring to the table an eclectic range of technical skills and knowledge. They must be well-versed on relevant laws and regulations, and should be proficient with forensics. An important aspect of the team's insider threat program is training. This training must include sessions on dealing with privacy concerns and protections. Those sessions will cover appropriate monitoring, as the project team must operate with a great deal of trust.[1] Before any training takes place personnel should be thoroughly vetted and relevant non-disclosure agreements should be signed.

4. Involve Stakeholders Early and Often

While stakeholders will definitely bring their own requirements, they may also bring in funding, too. (Combining requirements and funding also serves to protect from creating unfunded mandates and helps to foster wider investment in program success.) Stakeholders include board members, the legal department, IT network security teams, the CIO, HR, internal audit and union leadership. Once requirements are identified, address all conceivable issues in presentations — with a realistic action plan — so that everyone moves forward with common goals and expectations.

ACTION STEPS FOR ELEVATED USER AWARENESS

CERT's "Common Sense Guide to Mitigating Insider Threats" has emerged as an industry standard for program implementation. Among its recommended actions:

- Launch a security information and event management (SIEM) system to log, monitor and audit user activity.
- Detect activities outside the users' normal scope of duties via phone/network logs and other sources.
- Review accounts regularly to verify that all are still active and necessary.
- Perform ongoing audits of user accounts created and passwords provided.
- Require all system administrators to change passwords when a fellow administrator leaves his or her job.*
- Monitor and control remote access from all endpoints, including mobile devices.
- Incorporate threat awareness and prevention policies into comprehensive termination policies.
- Develop a baseline of normal network device behaviors.
- Inventory IT assets and routinely assess their present-day role and relevance.

** System administrators fall into the special insider sub-category of "privileged user." For more about the oversight of these users, see the Forcepoint white paper, "Privileged Users: The Threat from Within" https://www.forcepoint.com/resources/whitepapers/privileged-users-threat-within.*

1 For an outstanding training reference, we recommend the "Common Sense Guide" and other research from CERT. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

5. Give Education and Awareness Training to All

All employees must become aware of the need and value of data security and learn the terminology of insider threat protection. This will help prevent destructive or even malicious behavior. For administrators and analysts, auditing — which is part of the education process — provides recognizable events, influences and activities that create the telltale footprint of potential insider threats: Why is that staffer calling up a Word doc titled, "Resume"? Why is he/she on their personal email account all the time during office hours?

Keep in mind that users are more receptive to a teacher than a dictator; an engaging approach of sharing lessons learned will help you to better connect with employees.[2] You want them to understand how the way they are using technology is enabling insider incidents. Ill-intentioned users definitely understand this, and they can cover their actions well. That's why education is so critical.

6. Incorporate Governance and Oversight

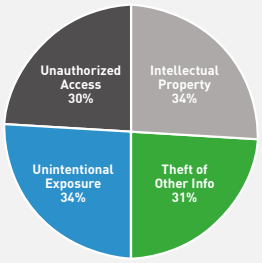
It is imperative for the legal team and senior management to define the appropriateness of the various tools and authorities to be entrusted. Policy controls are needed to ensure that the auditing and monitoring system is executed properly.

The following three "rules" of governance and oversight will help you achieve this goal:

- The "No Cowboys" Rule. Ensure that audit policies are properly authorized, approved and carried out so that leaders of the program can't abuse their privileges. Internal governance rules are very important. No organization needs a "cowboy" who creates a litigation nightmare by going beyond reasonable boundaries. (For example, a customer's insider threat program analyst fixated on a senior manager without any justifiable cause — it was strictly personal. This poor behavior was discovered through review of the analyst's auditing logs.)
- The "No Fishing" Rule. A valid business objective must directly support all generated audit records. Keep the inside threat team focused so they don't "go fishing" with pointless, unproductive excursions that may violate your policies, regulations or the law.
- The "No Ignore" Rule. All of the well-executed auditing and monitoring amounts to nothing if you lack governance policies that specify what the team should do when risks are detected. Members must know exactly how to report an incident. Program leaders need to know the proper response and remediation steps to take. In addition, the team and upper levels of management should review the risk-management process and ask: Are we effectively but fairly responding to individual cases? What enterprise-wide policies and training should be developed to address the risky user behaviors that we've uncovered?

2 For curriculum materials support, start with all of the terrific research at CERT. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

THE DAMAGE DONE TO ORGANIZATIONS EXPERIENCING AN INSIDER-CAUSED BREACH



34% Unintentional exposure of private or sensitive data.

34% Intellectual property theft.

31% Theft of other proprietary information including customer and financial records.

30% Unauthorized access to/ use of information, systems or networks.

Figure 2. Source: CERT Insider Threat Center at the Carnegie Mellon University Software Engineering Institute

7. Select the Auditing and Monitoring Solution

The technology you choose must detect user activity anomalies within your information systems. It must also be compatible with your IT architecture and establish trusted, enterprise-ready technical capability. But there are additional subtleties. Consider these questions:

- Will it scale as the program matures?
- Will it support confidentiality among multiple users of the system?
- Does it allow you to implement a risk-based model of detection with granular policy rules?
- Will it produce output that even non-technical managers can understand?
- Will it allow you to see activities and their full context?

This last point is especially relevant. Without context, your tools will create more questions than answers. False alarms will sometimes be connected to perfectly harmless activity.

For example, picture this scenario: A Human Resources employee is logging into a highly sensitive finance department system late at night. She hasn't received a raise in three years and has expressed resentment about this to superiors. Although she never travels for work, she's logging in from a foreign nation.

Is an unauthorized intrusion underway?

Not necessarily. She's on vacation overseas and has been collaborating with finance on a new company-wide pay-grade evaluation, and is checking on a file — something she forgot to do before she left.

The upshot: Tools must enable your insider threat analysts to build contextual awareness, so you get more answers from your insider threat program instead of more questions.

8. Launch Your Insider Threat Defense Program
Establishing an insider threat program is a culture shift. It introduces your organization to a new way of doing business. Inform stakeholders at every step — but especially this one — as this project will always involve a mix of technical and non-technical resources and personnel. To reduce implementation time, model your auditing/monitoring approach in a lab using virtualization technologies. Your technology vendor should be able to supply implementation templates that will help minimize deployment disruption.

Once you implement the program, track its impact on your business processes. For instance, did document download time increase after the launch? To assess impact, you can (discreetly) designate one department for implementation and another department as a placebo. Both groups are told they are being brought into the monitoring initiative, but only one really is. That should help you determine the real impact on systems and users..

9. Keep People Interested and Engaged
People forget about benefits that they don't see or understand. This underscores the importance for the program leader to continually demonstrate to management that the resources required to monitor user activity are paying dividends by:

- Reducing the risk of the accidental insider threat
- Identifying inefficient processes or poorly implemented technical controls
- Detecting malicious insiders who pose an intentional threat to the organization

Regular reporting of program activity, success stories, challenges and maturity ensure that business units appreciate the value of the investment. And don't overlook the deterrence benefit of keeping the workplace informed of ongoing user activity monitoring. Prevention is the best medicine; when it comes to insider theft and data breaches, where costs can run into the millions of dollars, an ounce of prevention is definitely worth a pound of cure.

DON'T WAIT — IGNORING INSIDER THREATS ONLY INVITES MORE!

Organizations of all sizes are now aware of just how much damage an insider can do. Most of the major recent data breaches, from Target Stores to the federal government's Office of Personnel Management, were caused by insiders. Can your organization afford to have its intellectual property, marketing plans, customer information and other critical data stolen on any given day?

For a successful deployment of your insider threat defense program, enlist the counsel of experts. Working with the right security partner will enable your program faster and help you to avoid unnecessary costs and mistakes.

APPENDIX

THREE ARCHETYPAL INSIDER THREAT PROFILES

All risky users have authorized access to the network. Otherwise, they diverge into the following three profiles:

The Malicious User

The malicious insider intends to cause your organization harm. This includes staffers who are passed over for a promotion, know they're about to get fired or have developed a grudge against a boss or coworkers. This type of employee seeks payback. They might also be third-party users who have been bribed by an outside adversary or have grown bitter over the pending termination of a contract.

Regardless of the user's full time or contract status, look for classic tip-off behaviors that can indicate trouble. The Federal Bureau of Investigation (FBI) offers some examples: taking proprietary information without need or approval, expressing increased interest in matters unrelated to their defined duties or connecting to the network remotely from unusual places at unusual times.[3]

The Unintentional Threat

Unintentional insiders don't know any better, but they should; they are causing your organization harm by their actions. These users can be tricked into downloading malware and introducing it into the network. They can lapse into sloppy habits, such as sending corporate materials to their home computers on vulnerable private email accounts. Of course, they can also simply lose mobile devices or USB drives that end up in the wrong hands.

Consider the impact of your organization's culture in creating or enabling these threats. A security-conscious Research and Development (R&D) team will have well-considered policies dictating secure computer usage; users receive regular training on acceptable use of technology, and acknowledge via logon warning banners that their activity is subject to monitoring. They realize that no one should ever share a password.

By contrast, a digital marketing startup might mistakenly follow the approach of "we trust everyone to do the right thing." It might keep security practices loose out of a desire to maintain a competitive edge for recruiting and retaining talent.

The Rule Bender

Rule benders fall somewhere in between the prior two profiles. Their actions are intentional, yet not maliciously so. They realize that IT is enforcing network security policies to counter increasingly sophisticated and well-funded attacks. But rule benders conclude that the added layer of protections are unnecessary, overly alarmist or simply too inconvenient. They consider themselves and their work as being above it all, and decide on their own when to follow security protocols — and when to circumvent them.

As they grow more comfortable with circumvention, rule benders begin to adopt it as their default setting. For example, they develop the habit of sending proprietary information outside the company without encryption. Or they may rely on saving data to external drives and USB sticks to take their work home. The risk is that those tools make it nearly impossible to distinguish dangerous behavior from harmless, work-related shortcuts.

3 https://www.fbi.gov/news/stories/how-to-spot-a-possible-insider-threat

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2014-027 [WHITEPAPER_9_STEPS_INSIDER_THREAT_EN] 200040.030117