

Achieve Counter-Insider Threat Program Modernization with Integrated Case Management




Introduction

Cogility's Counter-Insider Threat (C-InT) program solution — a comprehensive, whole-person risk assessment platform integrated with a state-of-the-art case file management system — significantly enhances C-InT program effectiveness. The continuous monitoring and advanced, customizable behavioral analytics provided in the Cogility Cogint C-InT solution is one of two critical components of a mature threat assessment program. The second component is an integrated, end-to-end case file management system.

Program managers understand the challenges of building and managing an efficient C-InT operations team. An effective case file management system helps to ensure consistent threat assessments and facilitates management oversight of workflow efficiency. This white paper describes the key challenges and technology tradeoffs of conventional C-InT and case management approaches — and shows how Cogility's end-to-end approach to whole person C-InT enables organizations to modernize their insider risk programs.

The insider risk assessment process analyzes information relevant to potential risks to identify actions, intentions, motives and capabilities that, when occurring in certain patterns, may negatively impact or harm an organization's mission or assets — either human intellectual or physical. The outcomes of such risk assessments range from no action (if mitigating facts are found) to employee assistance/counseling to disciplinary action to termination, and even legal/criminal prosecution — each of which yield high consequences to the suspected individual.



An effective case file management system helps to ensure consistent threat assessments and facilitates management oversight of workflow efficiency.

Key Challenges

Depending on the incident, creating a thorough risk assessment requires mental agility and attention to detail. It's difficult to address a wide variety of risks and to ask analysts to consistently exercise diligence for every assessment. Since operations teams are staffed by limited resources who possess a limited bandwidth, continuous improvement is an ongoing area of concern. Equally challenging is the need to advance processes and technology in ways that minimize employee turnover, facilitate uniform assessment and terminology, and maximize productivity.

Deploying technology advancements to modernize C-InT programs is a key objective for organizations in both government and large companies. Program leaders need to establish and manage an operations team, maintain technical and behavioral controls and data, ensure policy compliance, define operating procedures, and measure and report on program effectiveness to stakeholders. While these considerations and challenges — and even missteps — can appear daunting, preparation is paramount. This section examines some of the key principles for running an effective C-InT team.

Limitations of Point Solutions and Legacy Systems

“Point” solutions can be useful for many tasks. For example, Microsoft SharePoint is well-suited for managing documents, team knowledge, and collaboration. Microsoft Word is handy for preparing case reports. Email enables communication across teams. Security Information Event Management (SIEM) tools already centralize and manage endpoint, network and cloud event logs. SIEM rules provide degrees of security violation, anomaly, and User Behavior Analysis (UBA). Service desk tools can facilitate workflows. These tools are often used as a starting point for a rudimentary C-InT program. However, over reliance on point solutions and legacy systems results in overburdened case analysts and operations teams, greater delays, and reactive responses to threats.

It is common for operations teams to use and attempt to integrate a variety of tools. The downside of this “daisy chaining” approach is that it is very brittle and disjointed. It is particularly challenging for larger organizations with 10,000+ distributed users and diverse applications to create an integrated and scalable approach. Even with the best documentation, knowledge is lost due to employee turnover. Additionally, this approach is prone to user error. For example, information will often be incorrectly copied between applications, making it unreliable. Information silos will develop when people forget or don't know to share information. Data acquisition and evidence collection is often inconsistent. Tracking and collaborating on cases tends to be disorganized.

Relying solely on point solutions can generate data silos, workload backlogs, alert fatigue, user error, missed threats and lost evidence; it also reduces collaboration and response efficiency.

Legacy C-InT approaches can often demotivate threat analysts and case managers. It is a constant struggle to get the operations team to focus on the highest priority issues first. The team can quickly become inundated with incoming data, alerts and incident reports that generate an ever-growing backlog of work. Some of these notifications and information will be helpful in countering insider risk. However, the majority will not, but instead will create noise, distractions, and unnecessary investigation work.

Measuring and reporting organizational risk, case assessment productivity, and program effectiveness is an on-going endeavor. Supervisors and stakeholders need to understand the effectiveness of their operations team and the C-InT Management program. When the end-to-end process comprises point solutions and legacy systems that are not highly integrated, it is difficult to develop program effectiveness metrics: Assembling metrics and creating reports becomes a manual, resource-intensive, and often inaccurate recurring task that adds work and stress to the entire C-InT organization. Worse, it delays identifying bottlenecks, resolving gaps, and justifying investments.

Overcoming a Reactive Posture

It's far easier to react to insider threat incidents after they happen than to proactively mitigate them. Limiting a program to a reactive posture means, unfortunately, that the harm has already been done. It may even be difficult for leaders, analysts, and stakeholders to imagine how to proactively address detrimental human behavior, such as data exfiltration and workplace violence, before it occurs. This is why many tools on the market, especially those in the user activity monitoring (UAM) category, are reactive.

Legacy SIEM and UAM tools can centrally capture violations and generate alerts that are based on anomaly inference. SIEM and UAM will allow information security and insider threat teams to monitor user and system access and actions within physical, endpoint, network, and cloud systems. While these solutions provide a needed layer of defense, they are limited and do not provide a proactive, whole person approach. The first limitation is they are only effective at notifying personnel after an incident has taken place or enough of a material anomaly has been inferred, which means they are reactive by nature. Secondly, they exclude human behavioral risk indicators found in reports maintained by HR, law enforcement, and publicly available sources. It's important to understand that the toolset you choose will either enable a proactive posture or limit an operations team to a reactive one.

Traditional monitoring tools that generate alerts based on technical anomalies or violations are not sufficient to support proactive mitigation of insider risk.

Piecemeal Program Metrics

Team leaders report to supervisors and stakeholders who need to understand the effectiveness of their operations team and the C-InT Management program. Measuring and reporting organizational risk, case assessment productivity, and program effectiveness is an on-going endeavor. However, this is difficult, if not impossible, to achieve, when the end-to-end process comprises point solutions and legacy systems that are not highly integrated. This lack of integration means that assembling metrics and creating reports for stakeholders becomes a manual, resource-intensive, and often inaccurate recurring task that adds work and stress to the entire C-InT organization. Worse, it delays identifying bottlenecks, resolving gaps, and justifying investments.

Programs with “daisy chained” point solutions and legacy systems require manual collection and calculation of metrics from each tool, which consumes time and resources and yields inaccurate performance evaluations.

Pitfalls of In-House Engineering

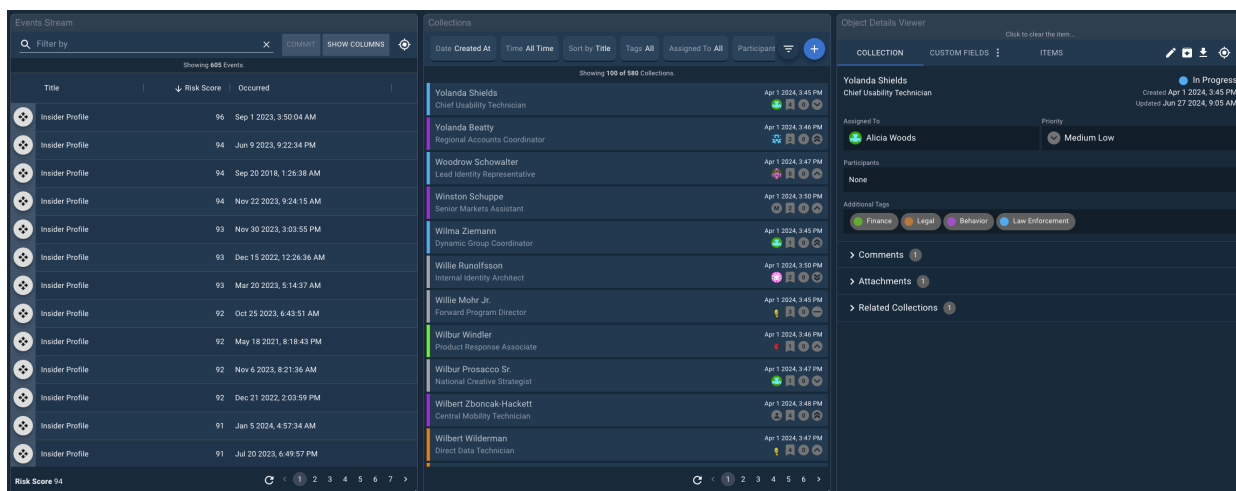
Engineers often build proprietary databases, services, and applications to support a home-grown solution. This approach can allow organizations to have greater control over what is built and to create a unique solution that satisfies the insider threat team's needs, but there are significant drawbacks. Software engineers are an expensive and limited resource, which makes building in-house insider threat management applications expensive to develop and maintain. Build times can take months if not years, engineering estimates are often inaccurate, and miscommunication errors in relaying subject matter experts and C-InT team requirements are common. Over-engineering databases and services that query data on a highly periodic basis can prove to be a costly, resource consumption mistake as well. Finally, maintaining a high-quality codebase throughout typical engineering turnover has a big impact as key talent could exit the organization at any time.

Cogility's Integrated C-InT Solution

Cogility's C-InT solution, powered by our Coglynt Continuous Intelligence platform, was designed to provide a fundamentally different approach to C-InT and case management. It transcends conventional SIEM and UAM by providing a platform that delivers whole-person risk profiling that factors in behavioral indicators in addition to technical indicators of insider risk. This allows operations teams to mature their C-InT capabilities, gain more comprehensive operational oversight, increase analyst productivity, and to achieve a proactive posture.

End-to-End, Built-for Purpose Solution

Cogility Coglynt provides an end-to-end C-InT solution that applies flexible data ingestion, real-time data analysis, behavioral analytics, and risk scoring to modernize program effectiveness and efficiency. Leveraging the organization's existing technical and psychosocial data sources, the platform performs stream data analytics to continuously monitor personnel for insider risk — at scale and according to model-defined logic.



Prioritized insider risk viewer, active case files, and case details

Analysts can focus their time on high-priority potential insiders — whether the threat is explicit or predictive. The solution's case management features allow teams to more efficiently review profiles, craft assessments, collaborate on case files, and create customized business intelligence dashboards to monitor and improve team performance.

Finally, Coglynt is a no-code platform. While our solution includes a foundation set of C-InT models informed by the SOFIT ontology¹, organizations can easily create or customize the behavioral models to support their data sources, policies, and behaviors they wish to counter.

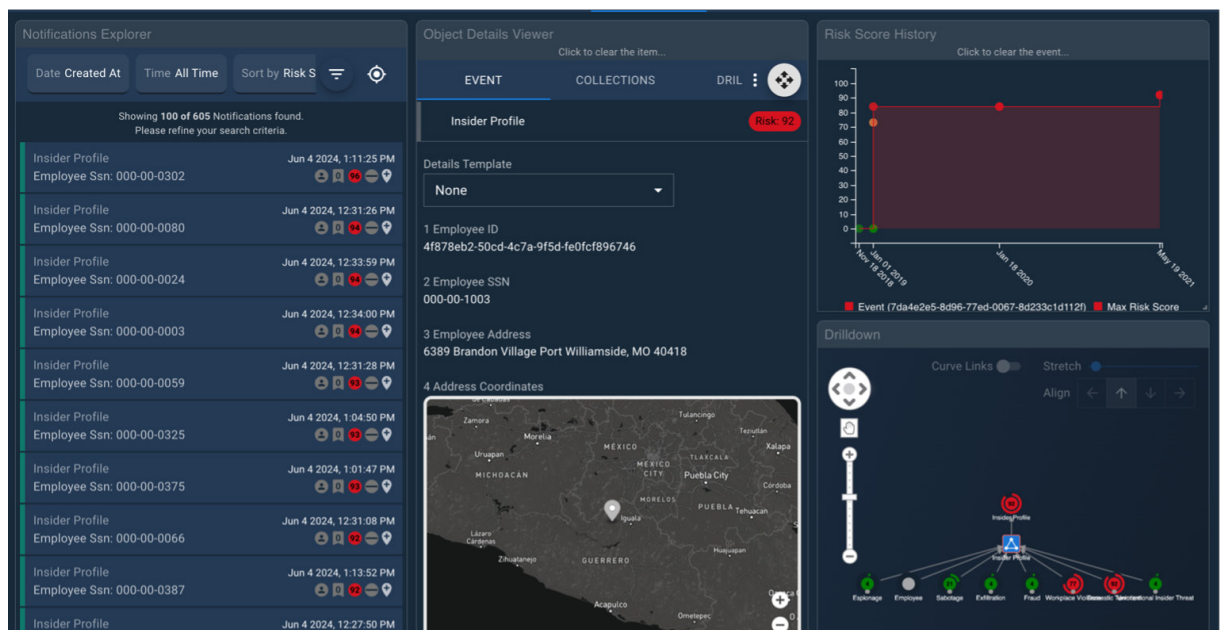
¹ Greitzer, FL, Purl, J, Leong, YM, and Becker DE. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Symposium on Security and Privacy Workshops*, 197-206

Behavioral Analytic

Instead of relying on analysts to search for information and piece it together to uncover insights and make insider risk inferences, Cogynt automatically and continuously processes all incoming data in real-time to identify findings, match technical and psychosocial risk indicator patterns, and provide actionable intelligence. By the time an analyst examines this information, its risk indicator data has already been scored and prioritized. This enables the insider threat team to focus their time and effort on high-priority threats. Additionally, Cogynt provides all underlying data that informed its risk score as part of each insider threat profile, so operations teams have the context and evidence they need to create an informed assessment with full auditability.

Workflow Management and Shared Situational Awareness

Cogynt's Analyst Workstation is designed to power the day-to-day operations for insider threat analysts. It's also versatile enough to configure a customized workflow that allows analysts to communicate, share information, and draft assessments in a collaborative manner with human resources, legal, and other participants. Cogynt's tagging system simplifies delegation and coordination between teams that contribute to the investigative process. Finally, Cogynt's custom fields, rich text editor, and report builder make it easy for analysts to draft assessments and for case file managers to review and hand off assessment determinations to decision makers and mitigation participants.



Custom dashboard: profiles, details, risk history, traceability

Simplified Effectiveness Measurement and Reporting

As an integrated solution, analyst interactions and case management are centrally tracked for auditing and performance measuring. End-to-end, real-time tracking combined with customizable business intelligence dashboards gives managers and stakeholders up-to-date insights into the operations team's performance. Finally, the process of creating and exporting performance reports is significantly streamlined as compared to other conventional C-InT approaches.

Facilitating Change Management

Switching toolsets is difficult for any organization. This is why Cogility offers robust customer support, training, and documentation to onboard C-InT operations team into the Cogility C-InT solution and phase out other tools. Since the Cogitynt platform offers flexible data ingestion, implementation is non-disruptive, allowing organizations to incorporate their existing technical security and psychosocial data sources. By identifying, presetting and phasing in data sources, organizations can adjust and expand insider risk models as needed, further easing transition efforts. Lastly, the solution allows for flexible data export into other workflow and auditing applications.

Conclusion

As a team leader, you have a critical responsibility to maintain a mature, efficient, and effective C-InT program. Essential ingredients of selecting a C-InT solution that meets or exceeds best practices is to implement methods and processes that transforms alerts and data into prioritized caseloads for the operations team, streamlines the day-to-day workflow, and tracks analyst actions for auditing and reporting purposes.

Cogility's C-InT solution, powered by our Cogynt continuous intelligence platform, was designed to achieve this by continuously processing technical and behavioral data across personnel to calculate whole-person risk scores and generate profiles. The whole person approach prioritizes analyst investigation, facilitates assessments, and provides real-time performance insights for stakeholders. It empowers the operations team with a customizable case management system. With its seamless deployment and end-to-end capabilities, Cogility modernizes C-InT programs and helps operations teams achieve a proactive posture to better protect the organization against insider risk and get left of harm.

A series of light blue, wavy, overlapping lines that create a sense of motion and depth, spanning the width of the page.

COGILITY

Visit www.cogility.com/counter-insider-threat to obtain more information and request an expert demo.

Cogility

15495 Sand Canyon Ave. #150
Irvine, CA. 92618

sales@cogility.com
+1 949.398.0015

01/25