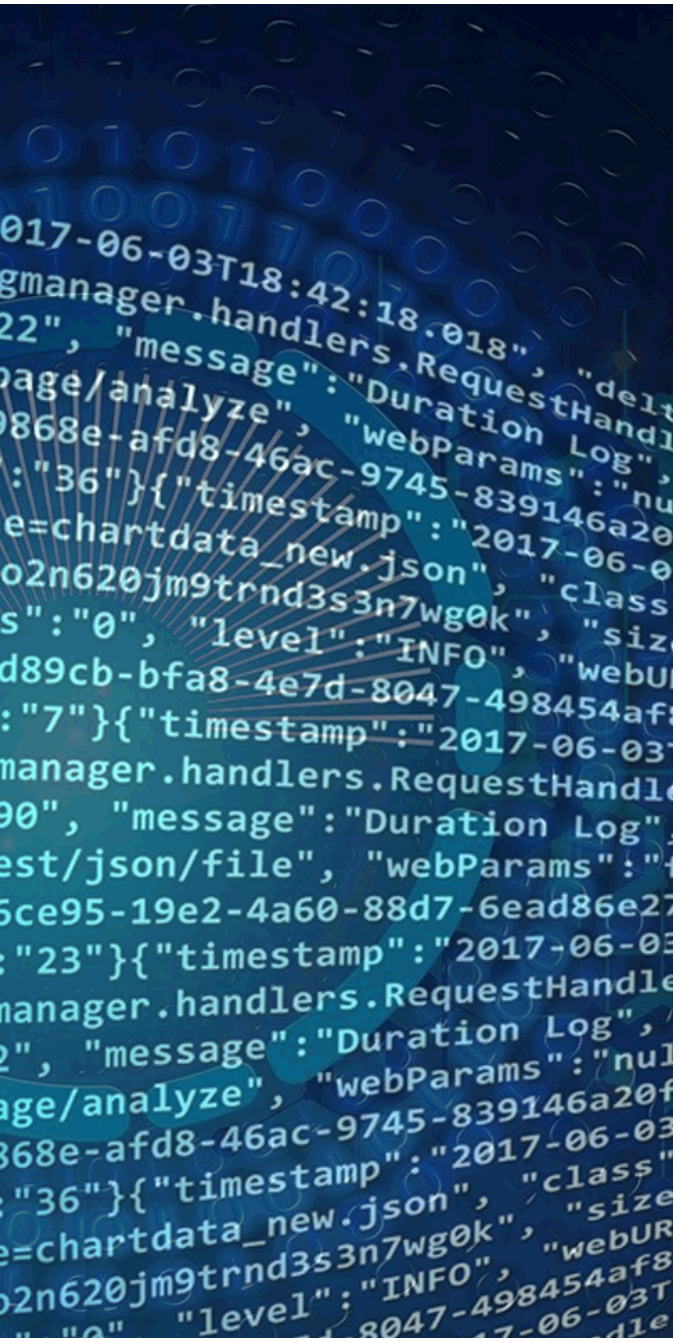
Why Every CISO Needs to Track Insider Threats More Proactively:

Counter Craft

Cyber Deception and the Rule of Three



Introduction

When it comes to looking at how to **deal effectively with insider risk**, not many security leaders will be thinking of deploying cyber deception to counter this problem. In fact, many leaders may think intuitively that the problem belongs in a different department (legal, internal investigations, etc.) and it is not part of their remit. However, every CISO needs to be part of the stakeholder group that deals with insider risk. In fact, Cyber Deception and "the rule of three" can help CISOs tackle the problem.

Cognitive Bias

When CISOs are developing their overall cybersecurity strategies what often gets overlooked is that cyber risk can and does originate from within their own organisations. This situation can often arise due to something that is deeply rooted in all of our decision-making processes: cognitive bias.

There are numerous types of cognitive biasses that have been identified by research. What is important to know is how this impacts a CISO's ability to objectively understand how his or her cybersecurity risk is distributed across the organisation, how much of that risk emanates from within their organisation and how much of it originates from cyberspace.

Due to the sheer diversity of threat actors and threat types, the focus understandably always falls on who is trying to break into your organisation from cyberspace. This is where the cognitive bias kicks in and CISOs begin to focus very heavily on how to keep external attackers at bay and overlook the risk that actually sits within the organisation.

Insider Threat

An obvious place to start is to define clearly what is an insider threat. It is not limited to employees stealing data from your organisation. **An insider threat needs to include your supply chain, former employees and any individual that has inside information about security processes and practices**. It does not have to simply include employees that have a good technical understanding of how your network is defended. It can also include those who may simply know the frequency of password changes. Traditionally, insider threats are broken down into three distinct categories:

1 **Malicious insiders**

2 **Negligent insiders**

3 **Infiltrators**

Insider Threats: How big is the problem?

The Ponemon global report '[Cost of Insider Threats 2020]' provided some interesting data points that help to accurately quantify and qualify the insider issue:

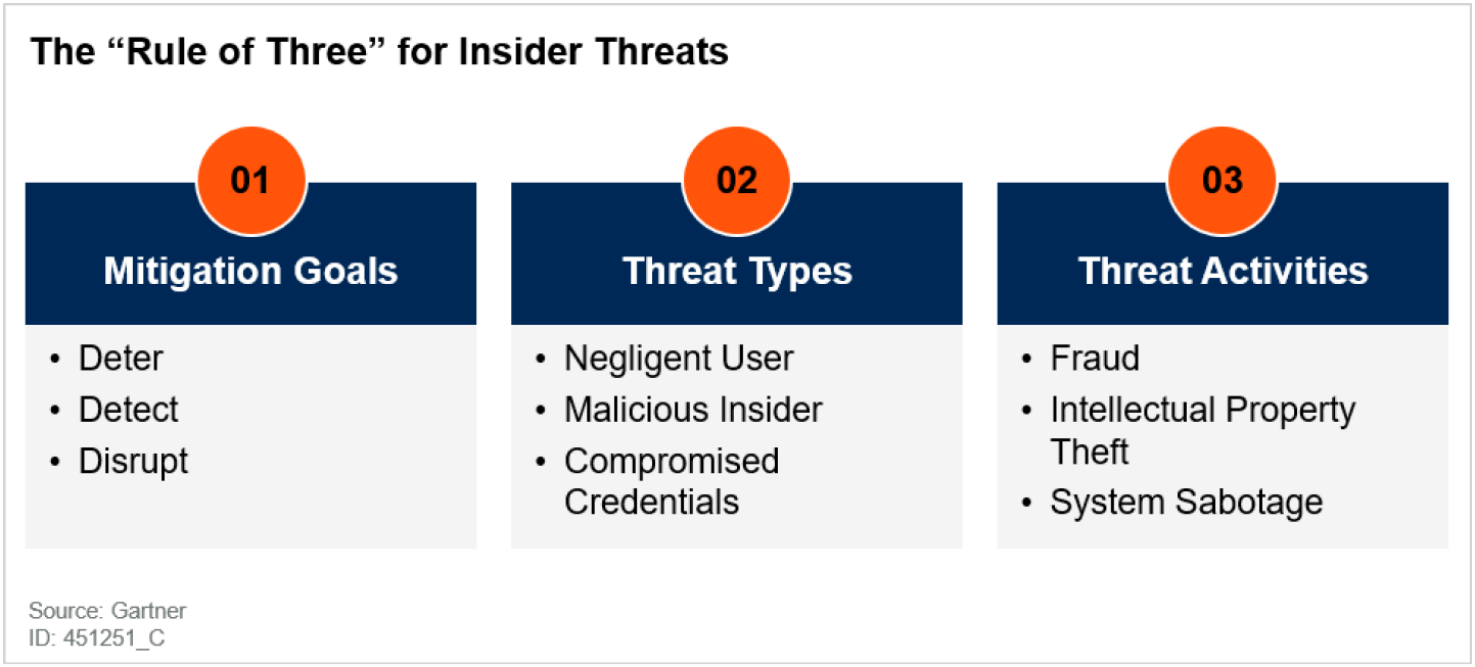
- 34% of business around the globe are impacted by insider threats
- During the last 2 years the number of insider incidents have increased by 47%
- The average annual cost of insider threats has increased by 31% to $11.45M over the last 2 years

The scale of the problem is increasing year on year. Is this due to the fact that a cognitive bias exists? Irrespective of the root cause, **the result is insider threats are being overlooked and have led to an upward trend in both the number of incidents and the cost per incident**. Apart from being overlooked, the upward trend may point to the fact that the existing technology that is deployed to deal with insider threats is falling short of expectations. An excellent piece of research produced by Paul Furtado from Gartner, '[Strategies for Midsize Enterprises to Mitigate the Insider Threat]', highlights one very worrying trend that encompasses all insider threats. That trend is the length of time it is taking to detect the threats in question. Paul's research paper shows that *"over 70% of breaches that begin with an abuse of access are only ever discovered many months or years later".*

What Can be Done to Tackle the Problem?

In the same paper, Paul talks about the "*Rule of Three*" as a means to deal effectively with the insider problem. This is where deception technology comes into its own by allowing CISOs to ensure that they can align themselves accurately to the rule of three. What is the rule of three? It allows a CISO to address the problem of insider threats by deploying his or her constrained security budget far more effectively. Below is a pictorial representation of the rule of three.

Gartner



Cyber Deception and the Rule of Three

The first rule is that the technology that you deploy to deal with the insider threat must deter, detect, and disrupt. How is this done within the CounterCraft Cyber Deception Platform? The deterrence goal can be simply achieved by allowing it to be known that there is a deception environment deployed within the corporate network. What this does is shift the security paradigm. Now, instead of security toolsets having to detect the insider threat, the deception platform forces the insider to be right every time, and this creates doubt and indecision. This means we are disrupting the threat already even before any actual detection takes place. Finally, there is detection. Due to the way deception technology works, deceptive artifacts can be distributed throughout a large enterprise without generating false positives. The end user has high fidelity alerts that will detect that they have a potential insider with malicious intent within their network within seconds of an artifact being touched.

Time to Detection

Real-time detection of potential insider threats early on in the threat cycle will address one of the biggest pain points for organisations: the time to detection. Over 70% of breaches are only discovered many months or years later, by which time the business has suffered sustained harm in potentially lost data, intellectual property rights and schematics of how its security toolset has been distributed across its enterprise. The problem with traditional approaches such as analysing behaviour or monitoring data flows is that they have failed to identify or disrupt the insider threat.

This is borne out by the fact that over the last 2 years insider threats have increased by 47%. The data is demonstrating that now is the time for change in how we approach the problem of detecting, deterring, and disrupting insider threats.

There is this assumption that organisations have the ability to quantify and qualify the depth and breadth of their insider problem. Therefore, they know where to deploy their limited monitoring toolsets. What if you do not have this visibility? Do you assume you have no insider issue? If you assume you have one, how do you know where that resource constrained monitoring needs to be deployed? The CounterCraft automated deception platform will help you to answer this fundamental question. Not only that, it grows with you on your security journey, helping you to implement the rule of three as your maturity expands.

About CounterCraft

CounterCraft empowers organizations to strengthen their security posture more efficiently than ever before. Designed and developed by experts, CounterCraft is a pioneering provider of full-spectrum cyber deception and ground-breaking threat hunting and enterprise cyber counterintelligence to detect, investigate and control targeted attacks.

The CounterCraft Cyber Deception Platform fits seamlessly into existing security strategies and delivers personalized, actionable intelligence to facilitate early threat detection, accelerate incident response and significantly reduce security spend. Our award-winning solution combines powerful campaign automation with controlled synthetic environments to allow attackers to penetrate organizations without doing real damage.

CounterCraft is recognized worldwide for its radical contribution to the deception technology market and operates in more than 20 Fortune500 Index companies globally, including financial institutions, critical infrastructures, retail and telecommunication companies, governments and law enforcement agencies.

Download our latest documents at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com