LogRhythm®
The Security Intelligence Company

Threat Lifecycle Management™

A Framework for Rapidly Detecting and Responding to Cyber Threats (Without Adding More Staff)

The Modern Cyber Threat Pandemic

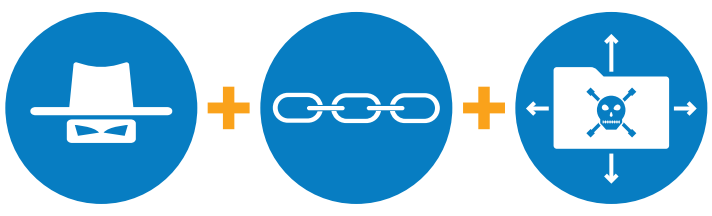
The number of records exposed by breaches aren't showing any signs of slowing.

96 million in 2010

736 million in 2015

That's an increase of 760% in just 5 years!

The risk of breaches continues to grow due to the combination of:



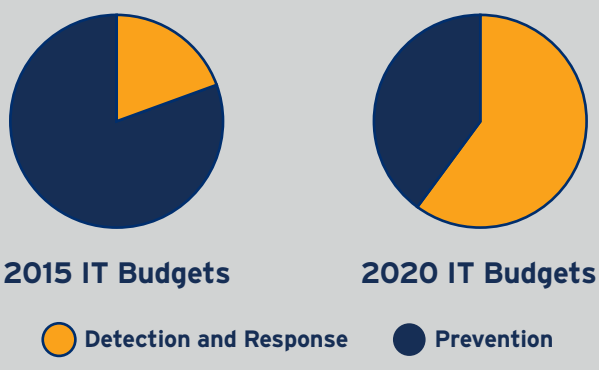
Motivated threat actors

An active cyber crime supply chain

A constantly expanding attack surface

Prevention-centric solutions aren't enough to keep attackers out.

In fact, the industry is seeing a strategic shift to detection and response. Gartner® predicts that by 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches—up from 20% in 2015.



2015 IT Budgets

2020 IT Budgets

Detection and Response

Prevention

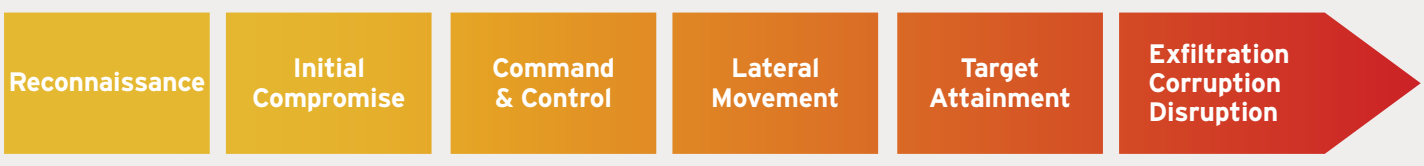
Faster detection and response isn't always easy.

There are many obstacles that keep your team from being able to detect and respond to a threat quickly—including:

The Cyber Attack Lifecycle

Today's cyber threats use your holistic attack surface to execute a compromise. An attacker begins with reconnaissance—finding their way in by manipulating users, compromising physical environments, etc.

If their initial compromise isn't detected, they will take increasing control over the environment and move laterally toward their target—taking over accounts and systems until the target is attained. This is where the biggest damage is done: exfiltration, corruption and disruption.



The Solution: The Threat Lifecycle Management™ Framework

The Threat Lifecycle Management (TLM) Framework is a series of aligned security operations capabilities. It begins with the ability to see broadly and deeply across your IT environment and ends with the ability to quickly mitigate and recover from security incidents.

The result? Reducing your mean time to detect (MTTD) and mean time to respond (MTTR) without adding staff to accomplish the job.

This is Not Effective

A combination of disparate, siloed technology systems makes it harder for your team to cut through the noise and correlate data—resulting in inefficiencies across people, processes, and technologies.

This is Effective

By combining each step of the TLM framework into a single UI, your team views end-to-end workflows through a single pane of glass.

End-to-End Threat Lifecycle Management Framework

Time to Detect → **Time to Respond**

Collect
- Security event data
- Log & machine data
- Forensic sensor data

Discover
- Search analytics
- Machine analytics

Qualify
- Assess threat
- Determine risk
- Is full investigation necessary?

Investigate
- Analyze threat
- Determine nature and extent of incident

Neutralize
- Implement countermeasures
- Mitigate threat & associated risk

Recover
- Clean up
- Report
- Review
- Adapt

LogRhythm®

To learn more, download our white paper