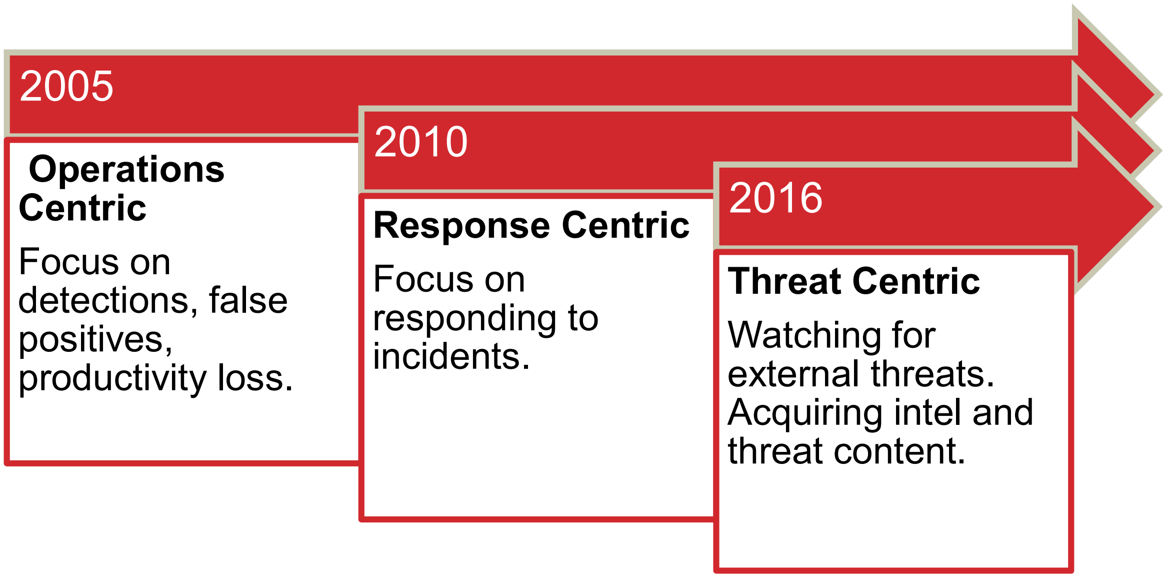
# THREAT MANAGEMENT

## THE MISSING PIECES IN YOUR INFOSEC PRACTICE

InfoSec teams like any other operations, just run. There is no time to stop, retrospect and change course. But once in a while the threat landscape changes so drastically, that you realize, you are not reaching anywhere. Let's look at some of the pieces, organizations have forgotten to add to their InfoSec practice.

## COORDINATED OPERATION

Coordinated operations approach to risk management, incident management and intel management is key to combat todays threats. Though it is in the wish list of every CSO, it is very difficult to achieve in today's eco system.



2005

**Operations Centric**

Focus on detections, false positives, productivity loss.

2010

**Response Centric**

Focus on responding to incidents.

2016

**Threat Centric**

Watching for external threats. Acquiring intel and threat content.

The way security operations have evolved, companies are left with a number of tools and processes around them. They mostly work in silos and the holistic view necessary is never there.

## COLLABORATION AND KNOWLEDGE SHARING

In today's world even the smallest companies have distributed teams and outsourcing to take advantage of global talent and cost benefits. Along with it, comes the challenge of keeping everybody in sync. Ticketing systems are just that. They facilitate the workflow involved in resolving an individual ticket. They are not meant to store artifacts for retrospective analysis or group people's actions in a timeline etc. So you end up with a separate collaboration system which cannot take advantage of the wealth of data in the ticketing system.

Collaboration outside your enterprise is a big challenge. In the age of ransomware and crime ware, sharing intel and incident data across organizations has become necessary. This is something very new and most organizations don't have tools to do it in a systematic way.

## TALENT SUPPLEMENT

Shortage of InfoSec talent is something companies of all sizes face these days. This has actually resulted in driving up the cost. Another aspect is the quality of talent required. Five or ten years back companies didn't have the requirement to analyze malicious documents or exploits in-house. They thought the AV or IDS is going to take care. The wonderful world of targeted attacks has changed this and put this additional burden on your InfoSec practice. A practical way to supplement your existing talent with additional specialized talent and at reasonable cost is something enterprises miss now.

## OPERATIONALIZING INTEL

Many organizations subscribe to intel feeds. But the tools and processes making sure these feeds reach the analysts in the team and put to proper use are missing. An analyst working on an incident should be able to export the latest IOC list and scan against the artifacts he collected or create an alert list for your next generation firewall. An analyst in the audit team should be able to look up the latest incident reports and get himself updated on latest techniques in the wild. An InfoSec manager may want to check if a particular malware was present in artifacts collected by his team in the last six months.

## ATTACK MODEL REPORTS

Creating an attack model and resolution summary at the end of every incident should be part of your playbook. The kill chain analysis, important IOCs collected, any information about the attacker, how your detection and protection system performed are important aspects to be tracked. This summary is ideal for sharing with external entities.

## SUMMARY

InfoSec leaders of enterprises should take the time to review their playbook and tools. Analyzing the big picture and having a forward looking understanding of what their practice needs and currently missing is essential to success.

Questions?

research@spellsecurity.com

## THREAT WORK BENCH

Threat Workbench is a next generation threat and intel management platform that allows collaboration and analysis of operational and threat intel data. It can derive the actionable data you need to stop the next big attack.

**SpellSecurity Inc**