Threat management

A necessity for securing what matters

In today's ever-expanding threat landscape you need to adopt holistic threat management to protect against the reality of continuous advanced threats coming your way.

Cyberattacks are costing organizations millions of dollars in lost revenue due to downtime, and damage to brand value and reputation. The Ponemon Institute estimates that the average cost of a data breach globally is now $3.86 million. A "mega breach", ranging from 1 million to 50 million lost records, can cost organizations between $40 million and $350 million.

With the threat vista rapidly expanding it is impossible, both economically and practically, to have a sentry at every corner. A thinly-spread security strategy will not withstand this storm of attacks which are coming from all corners – from lone wolves and highly-organized, global cybercriminal gangs to nation states.

At the same time, cybercriminals are getting cleverer. Their methods and tools are becoming more sophisticated. A purely reactive solution built around traditional security defense systems is no longer sufficient to keep bad actors out.

Holistic threat management can help plug this gap. It provides a multi-layered proactive approach to your cyberdefenses, incorporating threat anticipation, threat detection and rapid incident response to comprehensively mitigate an attack, should it be successful.

Identifying threats that matter

Threat management is designed to defend against all cyberthreats, including the growing menace of advanced persistent threats (APT). Once just the problem of high-profile targets such as governments and large multinationals, APTs are now posing a significant threat to all organizations as the value of data rises. Cybercriminals are also using smaller organizations in the supply chain to leapfrog through to larger prey.

Robust and effective threat management stops these types of attacks before a large-scale breach can carry out catastrophic, widespread damage to your critical information assets and infrastructure.

Preparing for the unexpected

The question is no-longer whether your organization will be attacked, but when, where and how it will happen. It is therefore critical to have a threat management strategy in place that includes cybersecurity experts capable of handling known cyberthreats. This expertise needs to be coupled with proven processes to detect, analyze and remediate attacks together with proven security tools that can provide intelligence, intrusion detection, data analysis and event correlation.

196 days on average for organizations to detect a breach[1]

20%+ of malicious domains are used around a week after registration[2]

55% of all security alerts from antivirus software are false positives[3]

350% growth in ransomware attacks annually[4]

orange™ Business Services

1. The Ponemon Institute Hidden Cost of Data Breaches 2018
2. Cisco Annual Cybersecurity Report 2018
3. The Ponemon Institute State of Endpoint Security 2018
4. Cisco Annual Cybersecurity Report 2018

Minimizing the risk of attack

Organizations must overcome several significant threat management challenges, especially when it comes to advanced, coordinated attacks.

These challenges include lack of operational visibility, difficulty in turning unknown threats into known threats, lack of in-house skills to monitor for and mitigate sophisticated attacks, and too many alerts for security teams to process, analyze and prioritize within a practicable timeframe.

We recommend addressing threat management with three interlocked activities:

Detect: detecting new and mutating threats to stop or limit the impact of a breach. This includes continuous monitoring and qualifying risk levels. Managing and qualifying security alerts requires the right technology and threat intelligence to reduce false positives alongside experts that can qualify alerts and identify the course of action.

Respond: reacting rapidly to intrusions for effective incident response, including incident investigation and recovery. This includes access to digital forensics experts that can intervene on demand, if needed, remotely and on-site.

Anticipate: applying accurate threat intelligence, threat hunting and analysis to spot potential security vulnerabilities and prevent threats. A security outpost is needed beyond your IT environment to protect your brand by monitoring for rogue websites and apps, hacking of social media accounts and to identify any data leaks on the dark web for example.

Six steps to effective threat management

1. Run a risk assessment to understand the nature of your data which is at risk. You need a clear understanding of the scope of your assets and data. This includes its value, location and regulations that it may impact on such as the General Data Protection Regulation (GDPR). Allocate your security budget according to the value of your assets, in particular sensitive data.

2. Adopt an offensive strategy anticipating threats that combines people, processes and technology. Cybercriminals are increasingly sophisticated, persistent and data driven. Threat intelligence can help you build up a picture of who is targeting you, what they are targeting and their attack plan. This intelligence also allows you to build scenarios on how to mitigate such attacks.

3. Run a regular review that identifies significant events and incidents. This will help you to make adjustments in order to achieve the best performance from your detection capabilities. This will help spotlight entry points for the latest scourge, fileless malware, for example.

4. Create a comprehensive incident response plan. It is crucial that you have a detailed incident response plan that is specific to your organization, outlining steps for detection, investigation, containment, eradication, and recovery.

5. Threat intelligence sharing. Continuously tracking the evolving cyberthreat landscape is critical to preventing threats, but if you don't disseminate this intelligence it will have little impact on your security posture.

6. Surveillance within your own enterprise perimeter, and beyond into cyberspace. Surveillance monitoring of the deep, dark and clear web is paramount to protect an organization's brand from website fraud, phishing attacks and rogue apps amongst others.

Why Orange

- **1,500 plus multi-skilled cyber experts worldwide**
- **10 SOCs, 5 CyberSOCs and 4 CERTs**
- **Proprietary threat intelligence database and real-time data feeds**
- **24/7/365 follow the sun capabilities**
- **Independent CERT and Signal Intelligence and Behaviors Lab to qualify and remediate emerging threats**
- **1,600 multinationals and thousands of SME customers worldwide**

orange™ Business Services

To find out more information go to:
https://cyberdefense.orange.com/en/