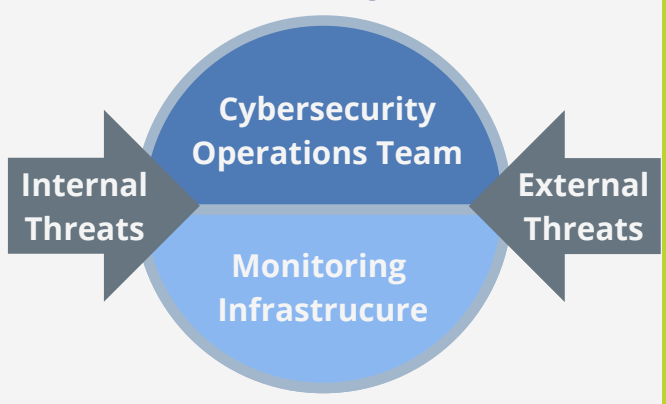
AXELLIO

Cybersecurity Challenges That Increase Your Risk!

Are you addressing the external and internal pressures that hinder effective threat mitigation?

Average Time to Identify and Contain a Security Breach [1]

Enterprise Cybersecurity Challenges



Operations Team Challenges:

- Only 26% of all attacks are detected, with only 9% of all attacks generating automatic alerts [3]
- Too much data that is difficult to correlate combined with too many tools complicates threat detection and leaves little time for comprehensive threat mitigation

Monitoring Infrastructure Challenges:

- Creating a scalable monitoring infrastructure that keeps up with traffic growth
- Extending the useful life of your monitoring infrastructure and delaying costly upgrades

External Pressures: Complexity Increases

- Increased volume and complexity of attacks
- Risks and costs of breaches
- Complexity of the infrastructure across networks, applications, services
- Traffic volume and complexity
- Number of vendors, tools, information, and events

Internal Pressures: Deliver on Expectations

- Reduce the risk along the IT delivery chain
- Protect and maintain the IT infrastructure
- Develop and execute a rapid response to minimize damage
- Stay within budget and resources

Not a Question of If But When!

- Over 900 weekly attacks for each corporation, an all-time peak in Q4 2021 [5]
- 50% annual increase in overall attacks per week in 2022, expected to grow further in 2022 [5]
- 94% of all malware is delivered via email, allowing for direct deployment by users with direct access to your most sensitive systems [2]
- Only 26% of all attacks are detected, only 9% create alarms – how many did you miss [6]
- Attackers spend an average of 212 days before being detected [6]

What is Needed?

- Broader and more reliable visibility – DDos attacks should not make you blind to attacks
- More relevant data – Events, logs, alarms provide too much data that is difficult to correlate and provide not enough information for threat detection
- More effective event data correlation – to shorten time to decision and resolution
- More cost-effective monitoring approach – to broaden visibility beyond the perimeter

References:

Source 1: "2019 Cost of a Data Breach Report" IBM Security
Source 2: 2019 Data Breach Investigations Report, Verizon
Source 3: Mandiant 2020: Security Effectiveness Report 2020, Mandiant
Source 4: 2022 Check Point Research: Cyber Attacks Increased 50% Year over Year, Check Point Software
Source 5: 2021 Cost of a Data Breach Report – IBM Security
Source 6: Mandiant – Security Effectiveness Report 2020

AXELLIO
www.Axellio.com
(800) 463-0297
2375 Telstar Dr. Suite 150 Colorado Springs, CO 80920