Cognizant

What to Look for in an Advanced MSSP

Cognizant Cyber Threat Defense

Shop carefully before hiring a managed security service provider (MSSP) to meet your exploding security needs. An MSSP that just throws hundreds of thousands of alerts at your overworked staff can do more harm than good. Here is what an Advanced MSSP must provide to really protect your ever-growing landscape of digital devices and users. An Advanced MSSP must project your ever-growing landscape of digital devices and users. To help in your search for the right MSSP, below are the differences between a Legacy and an Advanced MSSP, and the technologies which support it.

1

Legacy MSSP
Floods internal security staff with lookalike alerts that lack context.

Advanced MSSP
Prioritizes alerts based on the likelihood they signal a threat, and the importance of the affected data and systems.

Advanced Technology
SIEM (Security Information & Event Management)
TI (Threat Intelligence)
MDR (Managed Detection Response)

Technology Adoption Rate
61% of global security technology decision-makers say that improving security analytics capabilities is a critical or high priority.

Forrester Analytics, Global Business Technographics® Security Survey, 2018

2

Legacy MSSP
Follow-up is left to the customer.

Advanced MSSP
Recommends detailed workflows for finding and fighting the most serious threats.

Advanced Technology
TI (Threat Intelligence)
SOAR (Security Orchestration, Automation and Response)

Technology Adoption Rate
43% of global network security decision-makers say that their firm has implemented or is expanding their implementation of a **Threat Intelligence Platform** (TIP).

Forrester Analytics, Global Business Technographics® Security Survey, 2018

3

Legacy MSSP
Reacts to security events, often based on static policies applied only to legacy systems.

Advanced MSSP
Proactively searches for the latest threats, tapping everything from AI to real-time device data.

Advanced Technology
MDR (Managed Detection Response)
TI (Threat Intelligence)
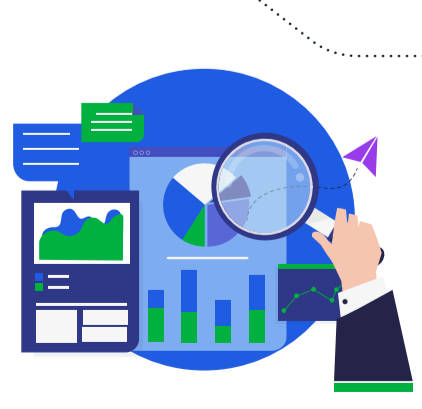UEBA (User Entity Behavior Analysis)

Technology Adoption Rate
63% of global client security decision-makers say that their firm has implemented or is expanding their implementation of **Endpoint Detection and Response** Technology (EDR).

Forrester Analytics, Global Business Technographics® Security Survey, 2018

4

Legacy MSSP
Focuses on the network perimeter, neglecting internal threats and not focused on the most critical assets.

Advanced MSSP
Focus on the business impact with tools and processes geared to the most critical systems and data.

Advanced Technology
SOAR (Security, Orchestration, Automation and Response)
VM (Vulnerability Management)

Technology Adoption Rate
51% of global network security decision-makers say that their firm has implemented or is expanding their implementation **Security Automation and Orchestration.**

Forrester Analytics, Global Business Technographics® Security Survey, 2018

5

Legacy MSSP

Standard, inflexible service models and pricing.

Advanced MSSP

Custom-configured tools and processes, guided by the MSSP's expertise, to prioritize protection of business-critical assets.

Advanced Technology

VM (Vulnerability Management)
SOAR (Security, Orchestration, Automation and Response)
SIEM (Security Information & Event management)

Technology Adoption Rate

55% of global network security decision-makers say that their firm has implemented or is expanding their implementation of Vulnerability Assessment in an 'as-a-service' security offering/approach.

Forrester Analytics, Global Business Technographics® Security Survey, 2018

6

Legacy MSSP

Scattershot collection and analysis of data from multiple security platforms.

Advanced MSSP

Comprehensive collection and correlated analysis of data from all security platforms and devices to find hidden threats.

Advanced Technology

SIEM (Security Information & Event management)
UEBA (User Entity Behavior Analysis)
TI (Threat Intelligence)
MDR (Managed Detection Response)

Technology Adoption Rate

68% of global security technology decision-makers say that their firm has implemented or is expanding their implementation of Security Analytics/SIM in an 'as-a-service' security offering.

Forrester Analytics, Global Business Technographics® Security Survey, 2018

7

Legacy MSSP

Guesses what activity is legitimate rather than signaling a possible breach.

Advanced MSSP

Quickly identifies possible security events through awareness of normal data flows, critical users and assets.

Advanced Technology

UEBA (User Entity Behavior Analysis)
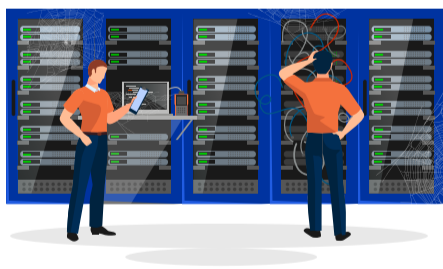MDR (Managed Detection Response)

Technology Adoption Rate

62% of global client security decision-makers say that their firm has implemented or is expanding their implementation of **Security User Behavior Analytics (SUBA)** in an 'as-a-service' security offering/approach.

Forrester Analytics, Global Business Technographics® Security Survey, 2018

8

Legacy MSSP

"Set and forget" configuration; only updates are pre-planned or in reaction to security events.

Advanced MSSP

Ongoing improvement to systems and processes based on security analytics, new threats and changes to the business.

Advanced Technology

TI (Threat Intelligence)
SOAR (Security Orchestration, Automation and Response)

Technology Adoption Rate

65% of global security technology decision-makers say their firm has implemented or is expanding their implementation of **Threat Intelligence** Capabilities in an 'as-a-service' security offering

Forrester Analytics, Global Business Technographics® Security Survey, 2018

To learn more about our Advanced MSSP – Cyber Threat Defense visit our webpage Click here

www.cognizant.com

Cognizant