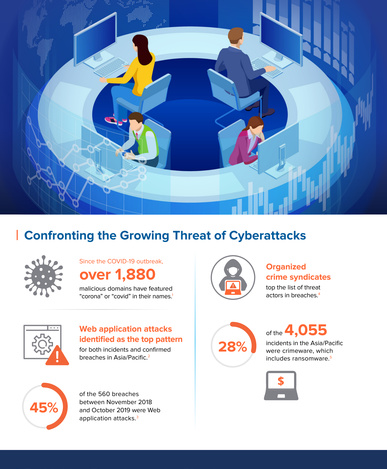
IDC INFOGRAPHIC

AUTOMATION & CLOUD POWERING SOC TRANSFORMATION

Cloud-enabled and automation-driven security solutions help transform Asia/Pacific enterprises' cyberdefense capabilities. This IDC Infographic looks at the rapidly growing role of analytics, automation, and cloud in optimizing the efficacy and resiliency of security operation centers (SOCs).



Confronting the Growing Threat of Cyberattacks

Since the COVID-19 outbreak,
over 1,880
malicious domains have featured "corona" or "covid" in their names.

Web application attacks identified as the top pattern for both incidents and confirmed breaches in Asia/Pacific.[1]

45% of the 560 breaches between November 2018 and October 2019 were Web application attacks.[1]

Organized crime syndicates top the list of threat actors in breaches.[1]

28% of the **4,055** incidents in the Asia/Pacific were crimeware, which includes ransomware.[1]

Rethinking Security on the Cloud

50% **Public cloud will account for 50% of Asia/Pacific (excluding Japan) enterprise IT infrastructure spending.**

Public cloud security fears remain, albeit largely perceptional or theoretical.

The shifting of workloads to the cloud is transforming consumption of security services.

In 2025, **35%** of managed security services (MSS) environments will be cloud-based.

1/4 **1/4 of enterprise IT applications will run on public cloud services in the next 2 – 3 years.**

Accelerated cloud usage amid the COVID-19 pandemic is set to drive cloud security.

Asia/Pacific (excluding Japan) security solutions and services spending
Almost $22 billion in 2024, a 5-year CAGR (2019-2024) of 15%

Cloud-based security solutions and services
2X CAGR

Paradigm Shift Away from 'Protect and Defend' to 'Quickly Detect, Contain and Respond'

Augmented with automation, analytics

Benefits

Better ROI

Enhanced security due to resource optimization, enabling security professionals to focus on critical functions such as communication, critical thinking, and complex trouble shooting.

IDC Predicts **50%** of legitimate security alerts will have an automated response, untouched by human analysts by 2022.

Use of AI and machine learning is not an option but an imperative

50% of Asia/Pacific organizations surveyed have reported experiencing **at least 1 security incident** that took **more that 3 days to resolve.**

IDC's take: Employing **new** technologies and approaches to security initiatives helps mitigate risks while ensuring:

Privacy · Confidentiality · Integrity · Availability

Percentage of SMEs (employee size of 500 to 999) surveyed that are researching, considering piloting, have a proof of concept, or have implemented enhanced security:

In Asia/Pacific:

71% **Security Analytics** for threat detection

63% **User Behavior Analytics** for threat detection

67% **Threat Intelligence**

50% **Threat Hunting**

Source: IDC Digital Trust and Cyber Security Economics Survey, n=156

Asia/Pacific Scorecard: Self-assessed level of automation in cyberthreat management

Automation and Cloud to Power the Modern SOC

SOC transformation and use of a managed security service provider (MSSP) bring key benefits:

- Addresses shortage of in-house IT security skills and rising wages.
- Transforms the security operation from a reactive approach to a proactive one.
- Quick remediation of incidents helps prevent a full-blown breach or data loss.
- Access to security expertise and the latest technologies.
- Build an effective cyber-risk strategy beyond conventional infrastructural layer monitoring.
- Vulnerability management assists in driving patch management to address newly discovered vulnerabilities.

AI and ML will help improve the ratio of level 1 to level 2 SOC analysts

Today 3:1 → **Future** 1.5:1

IDC Predicts **55%** IDC predicts by **2021**, **55%** of tier-1 SOC analysts will permanently elevate their productivity and improve operational security metrics by harnessing AI and ML.

IDC Essential Guidance

People & Partner

- Hire with diversity in mind. Problem solving in an SOC requires holistic analytical skills which are often found outside of traditional IT roles.
- Select a vendor that can scale with the business and support the organization's geographical expansion plans. The cloud may be global, but support may not be as ubiquitous.
- Make every effort to ensure technology partners can work together and be orchestrated.

Process

- Ensure IT security does not operate in a silo but in lockstep with a business use case, business user, or business metric.
- Look for a good playbook or use case libraries to learn about different options that unlock greater value from the SOC.
- Start with basic automation and grow the team's knowledge and skills to embrace AI/ML.
- Be aware of how this transition to an as-a-service model or cloud-based security solutions will impact finances. Costs may escalate faster than desired as requirements grow.

Technology

- Consider core technologies and tools used in the modern SOC, such as advanced detection and analytics techniques like ML, behavior analytics, NetFlow analysis, decryption, threat intelligence, and ongoing threat hunting.
- Adopt incident response orchestration services and automated containment.
- Extend monitoring to the cloud environment.

Source:
[1]Sophos Labs
[2] 2020 Verizon Data Breach Investigations Report

Sponsored by:

IDC ANALYZE THE FUTURE

RAPID7