servicenow

Cybercriminals are resilient. How about you?

Staying ahead of those agile bad actors

“

Often the right people aren't looking at the right data and aren't empowered to take the right action in a timely way.

Andrea Castillo
Practice Director, Security and Risk, Crossfuze

$10.5 trillion USD

THE COST OF GLOBAL CYBERCRIME ANNUALLY BY 2025

Source: Cyberwarfare in the C-Suite, Cybersecurity Ventures, 2020

400%

INCREASE IN RANSOMWARE ATTACKS YEAR ON YEAR

Source: Cyber security statistics 2020, IT Chronicles, 2021

How vulnerable is your organization to cybercrime?

Cybercrime continues to be a major issue and shows no signs of slowing down. In 2020, hackers uncovered many new opportunities to exploit vulnerabilities as organizations responded to the global pandemic. Among the initiatives that made organizations the ripe targets of bad actors were digital transformation projects such as the addition of public cloud services, new network devices, remote workforces, and SaaS applications. Trends show that ransomware attacks are increasing 400% year on year[1] and are expected to grow in 2021 across both public and private sectors.[2] It's no surprise that the cost of global cybercrime will reach $10.5 trillion USD annually by 2025.[3]

What makes cybercrime prevention so difficult

Simply put, security teams struggle to keep up with the cybercrime volume, with little time to see the big picture across the enterprise and respond in real time. They don't have the agility and resources to build a cyber-resilient organization where people, technology, and processes work seamlessly together.

What keeps security teams up at night? Well, here are a few highlights of what they faced in 2020[1]:

- **Every 40 seconds**, a new cyberattack starts
- There were **nearly 550,000 cyberattacks per day** involving ransomware
- **More than 25,000 different malicious applications** are detected and blocked every day
- Each day hackers attack **more than 30,000 websites**
- **More than 65% of organizations worldwide** have had at least one cyberattack against them
- Email is responsible for propagating **95% of all malware**

Building a cyber-resilient organization is tough with only point products

Trying to monitor all parts of enterprise environments is a tall order when you consider security teams need to maintain visibility into complex networks. These networks are continually expanding in the cloud and must accommodate a growing mobile workforce. Companies have traditionally implemented a myriad of security point products, but this strategy is not efficient, scalable, or effective at meeting cybercrime challenges.

And, even if security teams have developed and established cybercrime processes and responses with these point products, they still feel overwhelmed by daily, ever-increasing obstacles, including:

1. Too many potential security threats to address and prioritize

2. Too much data generated by so many different solutions

3. No way to understand the intent of cybercriminals when dealing with security incidents

The consequences? Security teams are constantly reactive rather than proactive. They lack the agility, the resources—and the resilience—to stay ahead of cybercriminals who are intent on doing harm.

Resilience: The ability to respond effectively to stress and adversity

IT and security teams: better together for cyber resilience

Creating agile, resilient enterprise security operations to counter cybercrime is not simply an issue of technology. Fostering a mindset of resilience and agility requires moving away from the traditional perspective where security teams operate in siloes. Instead, a cyber-resilient organization requires a change in culture. IT and security teams must work together in a much more harmonious way to combat today's relentless bad actors rather than each relying independently on spreadsheets and emails. Cybercriminals move fast—IT and security teams need to do the same!

Deploying the right security incident response strategies

Becoming agile and cyber resilient with collaborative security and IT teams doesn't mean replacing the security solutions that work for your organization and adding staff. Instead, the focus is on using solutions and teams optimally. Additionally, your teams must concentrate on cyber hygiene with effective and standardized security incident response processes.

You can't protect what you don't know about
THE POWER OF THE CMDB

You can't protect everything
RISK-BASED VULNERABILITY MANAGEMENT

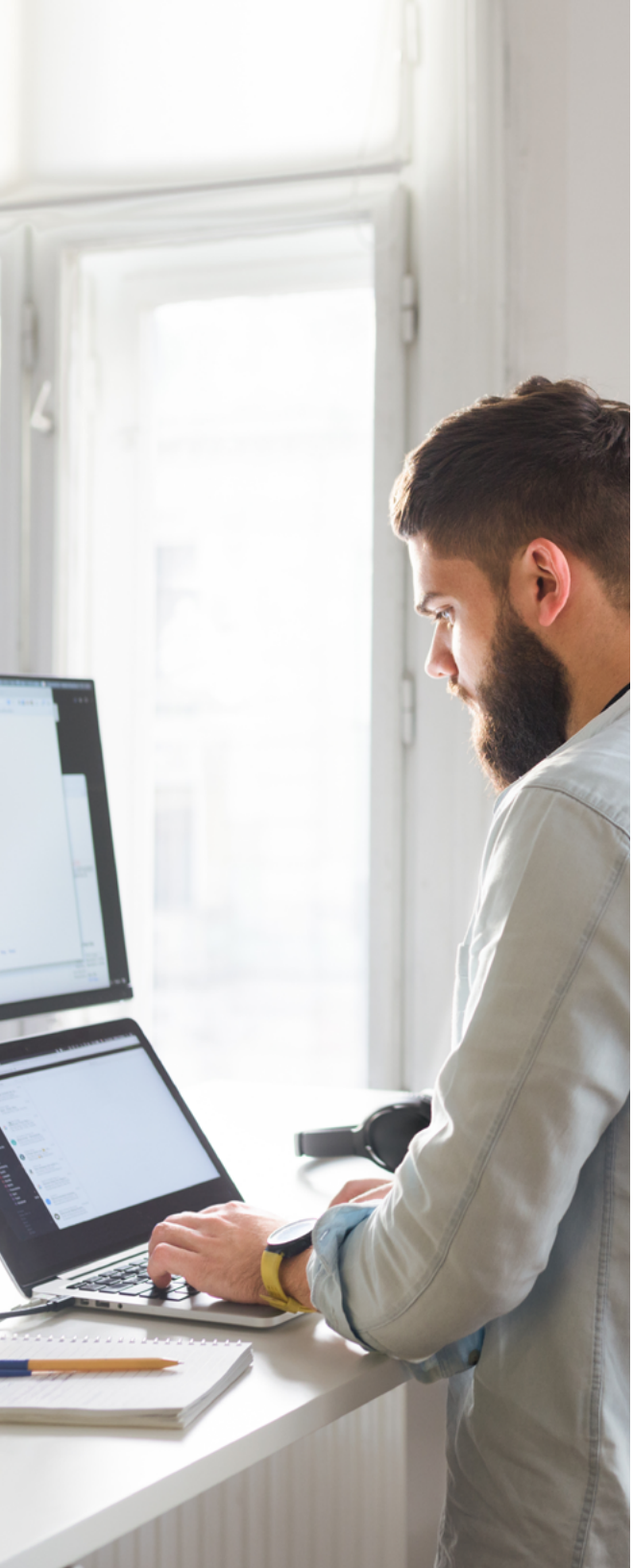
If you are (unfortunately almost inevitably) breached, you must minimize cost and impact
HAVE A GOOD SECURITY INCIDENT RESPONSE PROCESS IN PLACE

Build a system of action
BRING SECURITY & IT TEAMS TOGETHER

The ideal security incident response process

- Tools for detection and/or security information and event management will generate alerts
- Alert data is stored in a centralized, integrated system for analysis and action
- Additional information is harnessed from threat intelligence and vulnerability tools
- Security and IT teams work together to respond to prioritized incidents to address threats and adversaries quickly and effectively

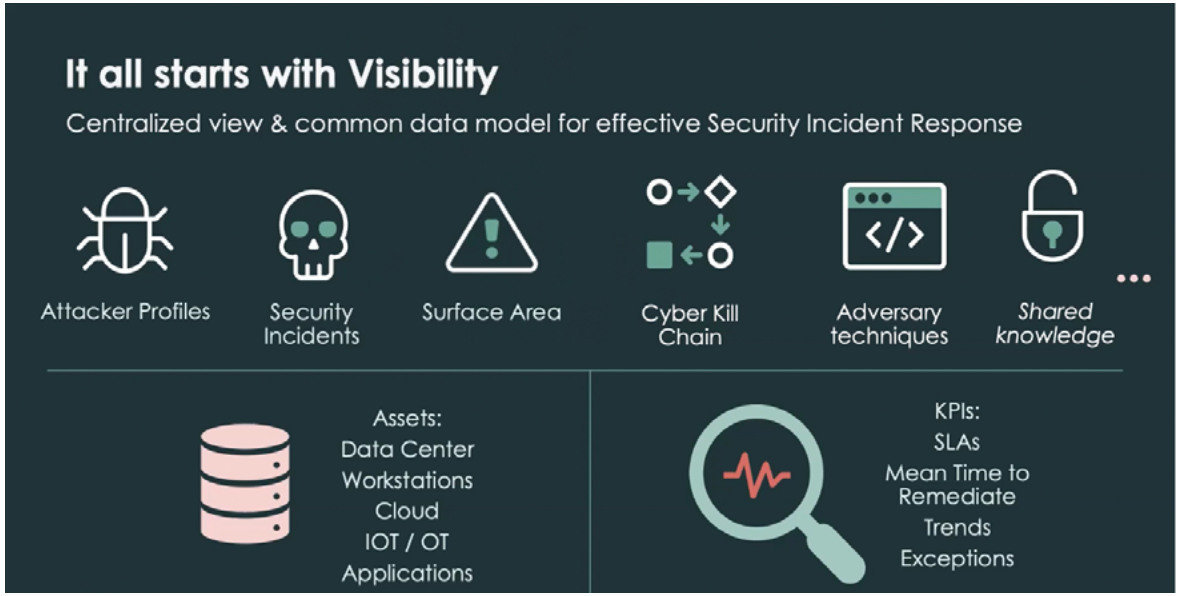
Ultimately, this direct and accelerated collaboration between IT and security teams for vulnerability and incident response is really what helps to prevent security breaches from impacting your business.



A better view of your adversaries

A key component of effective security incident response is a centralized, integrated system of data and action. This enterprise-grade system can be a game-changer in responding to cyberthreats by delivering a clear understanding of your adversaries.

It all starts with visibility into each incident to accurately determine the kinds of attacker capabilities threatening your organization. It's also important to have a precise view of your organization's attack surface, whether it's on premises, in your data center, or in your cloud environment.



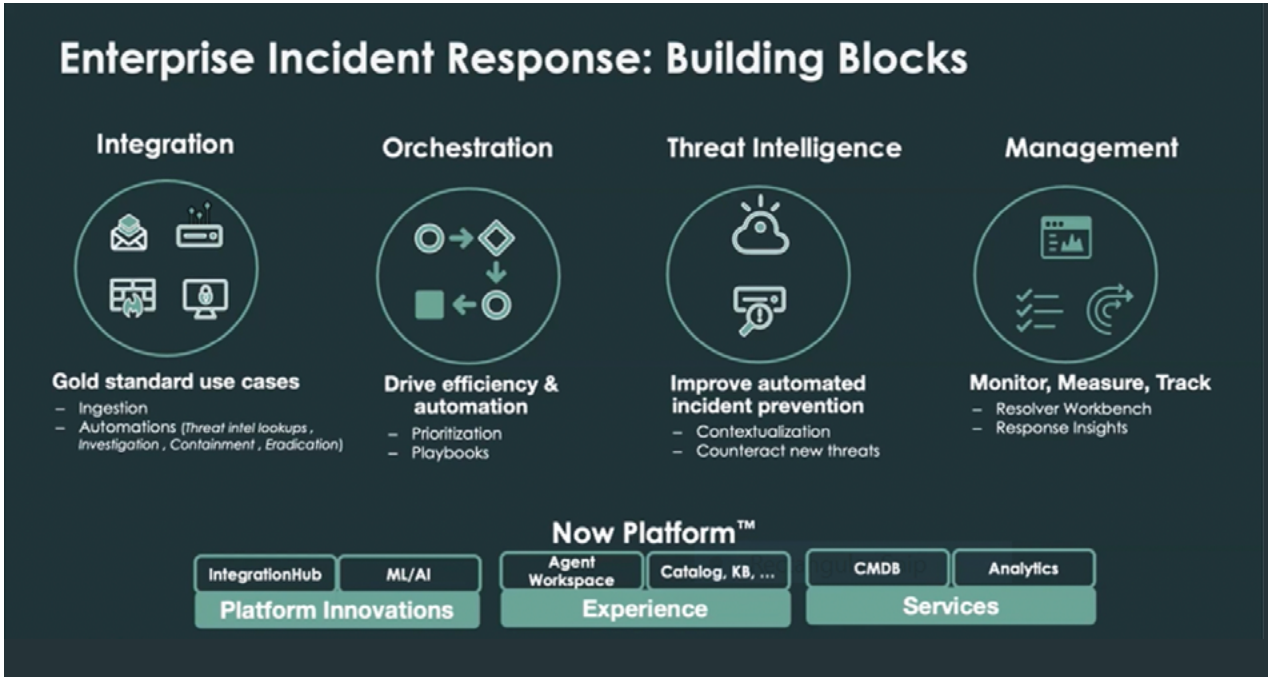
Your IT and security teams need to understand the techniques your adversaries use and what kind of detection capabilities are in place. With the right incident response platform, they can standardize, automate, and accelerate incident response to easily:

- Root out threats
- Watch for trends and anticipate what's next
- Improve your organization's ability to withstand a risk
- Put proper governance processes in place

The platform building blocks

An effective incident response platform should track and manage security incidents throughout the entire lifecycle through:

1. Seamless integration with your cybersecurity ecosystem, including devices protected by antivirus software, firewalls, and threat intelligence solutions
2. Efficient orchestration to better contextualize data, improve prioritization, and drive automation
3. Threat intelligence to provide a broad view of incidents that offers a more accurate perspective on what attackers are doing; this ensures security teams don't react from a silo, can aggregate multiple alerts into a single incident, and drive a deeper response while also counteracting new threats
4. Extensive management capabilities to provide a comprehensive analyst experience and draw insights from incident response, while monitoring trends and backlogs



Time to SOAR

When you have collaboration between IT and security teams, standardized security incident response processes, and an enterprise-grade incident response platform in place, then you can begin to fully explore security orchestration, automation, and response (SOAR) technology and tools.

Security Orchestration Automation and Response (SOAR)

- Effectively manage the evolving threats to your business
- Drive efficiencies and accelerate reaction time
- Proactively manage exposure
- Ensure cyber resilience

SOAR solutions help security teams become more agile and resilient in preventing cybercrime. Since processes such as security incident response or threat intelligence lookups are standardized and automated, security analysts can determine more quickly if an incident is real or false.

And, when blocking firewalls, quarantining hosts, and responding to phishing attacks are all automated tasks, your security teams aren't spending the bulk of their time on routine security activities. They have the time and resources to hunt for advanced threats.

SOAR facilitates security and IT collaboration

Automation and orchestration together facilitate collaboration between IT and security teams—helping them be proactive and scale faster to mitigate cyberattacks.

The financial benefit of SOAR is impressive: the average savings by companies with fully deployed, automated security solutions is $2.5 million.[4]

$2.5 million

Average cost of breach savings by companies with fully deployed automated security solutions[4]

What is the MITRE ATT&CK Framework:

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Source: Mitre Corp. [https://attack.mitre.org/]

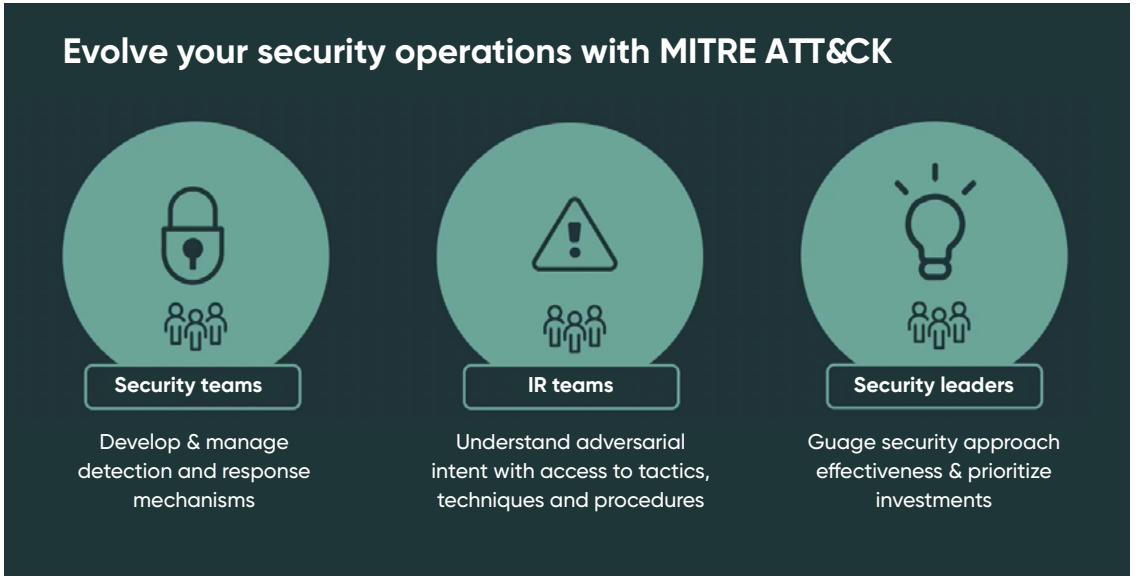
SOAR + Mitre Att&ck = highest evolution of security operations

As more organizations adopt SOAR technology to build cyber-resilience and agility, the next logical step is to couple their SOAR solution with the MITRE ATT&CK Framework for process automation and orchestration. Integration, automation, and orchestration can then help organizations add MITRE data to business, asset, risk, and threat context. This combination improves the efficacy and efficiency of security operations in areas like incident detection, assessment and engineering, cyber-threat intelligence analysis, and adversary emulation.

Combining SOAR and the MITRE ATT&CK framework enables security teams to:

- Proactively drive fast security responses
- Prioritize threats by business context
- Automate required actions to quickly triage and remediate incidents
- Reduce the overall attack surface

Teams will have true insight into an attacker's every move and can contextualize not only response capabilities but also detection functionalities.



The roadmap for building proactive, agile, cyber-resilient organizations

Cybersecurity has long been a top priority for IT leaders. Yet, despite increasing investments in security solutions, cyberattacks continue to proliferate. In June 2021 alone, there were 9.8 million breached records from publicly disclosed security incidents.[5] Many enterprises are still struggling to understand the scale and scope of the threat landscape—as well as the goals and objectives of cybercriminals.

However, if you're a security leader intent on building a proactive, agile, cyber-resilient organization, success is on the horizon. The goal is to facilitate collaboration between IT and security teams, introduce standardized security incident response processes, implement an enterprise-grade incident response platform, and begin to automate mundane and repetitive tasks. With this approach, people, technology, and processes will work seamlessly together so your teams understand how your adversaries operate and can establish a clear roadmap for investigations and resolution.

servicenow

For a deeper exploration of security operations solutions from ServiceNow, we recommend:

White paper: Using ServiceNow SOAR to operationalize MITRE ATT&CK

Webinar: The MITRE ATT&CK Framework and SOAR: Better together

Sources

1. Cyber security statistics 2020, IT Chronicles, May 27, 2021 (https://itchronicles.com/information-security/cyber-security-statistics-2020/
2. Global Risks Report 2020, World Economic Forum, 2020 (http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)
3. Cyberwarfare in the C-Suite, Cybersecurity Ventures, Nov. 2020 (https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/)
4. Cost of a Data Breach Report, Ponemon Institute, 2019
5. List of data breaches and cyberattacks in June 2021, IT Governance (https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2021-9-8-million-records-breached)