2019 CrowdStrike

Global Security Attitude Survey

VansonBourne

CROWDSTRIKE
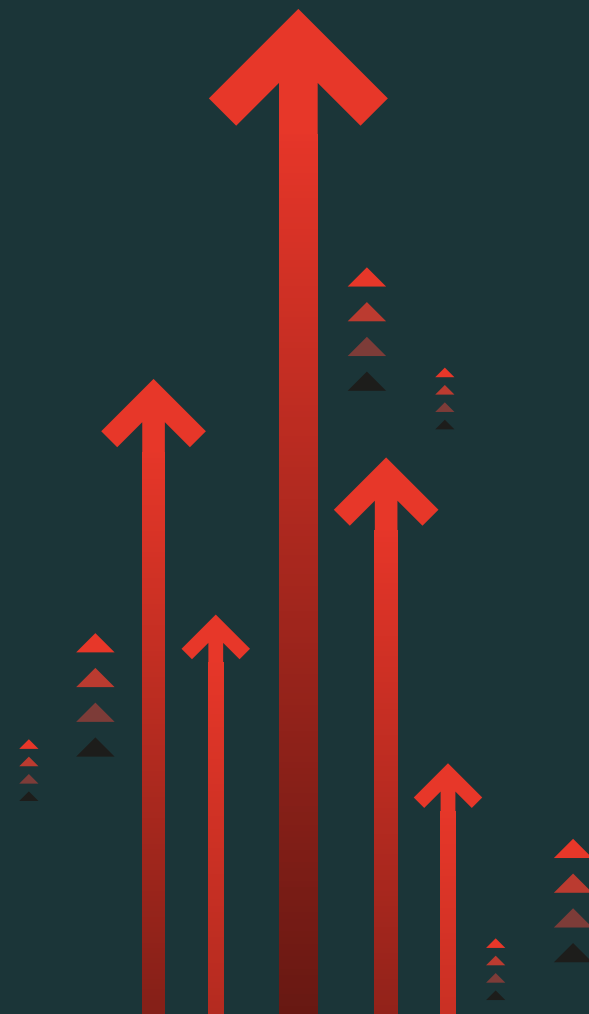
Introduction

For modern organizations, cyberattacks are simply unavoidable. There is no hiding from this fact. And if attacks are unavoidable, then the key to effective protection is speed and accuracy.

You need to react quickly when you are attacked in order to:

➔ Detect an incident as soon as possible

➔ Investigate it thoroughly and discover everything that you need to tackle it

➔ Contain it before it breaks out and causes significant damage

Organizations may believe in the critical importance of speed but be unsure of how that translates into metrics. The 1-10-60 rule provides useful guidelines: One minute to detect, 10 to investigate and 60 to contain and remediate. Organizations that strive to adhere to this rule are better prepared to defend against threats and successfully remediate cybersecurity incidents when they occur.

This begs the question: How far away from this ideal standard are organizations? This report explores the state of organizations' cybersecurity detection and containment capabilities, as well as their ability to understand the attackers themselves. Are they detecting threats fast enough? Do they know what is putting them at risk? Can they contain a threat before attackers reach their objectives?

And the biggest question: What happens to organizations that cannot detect, investigate and contain a threat fast enough?
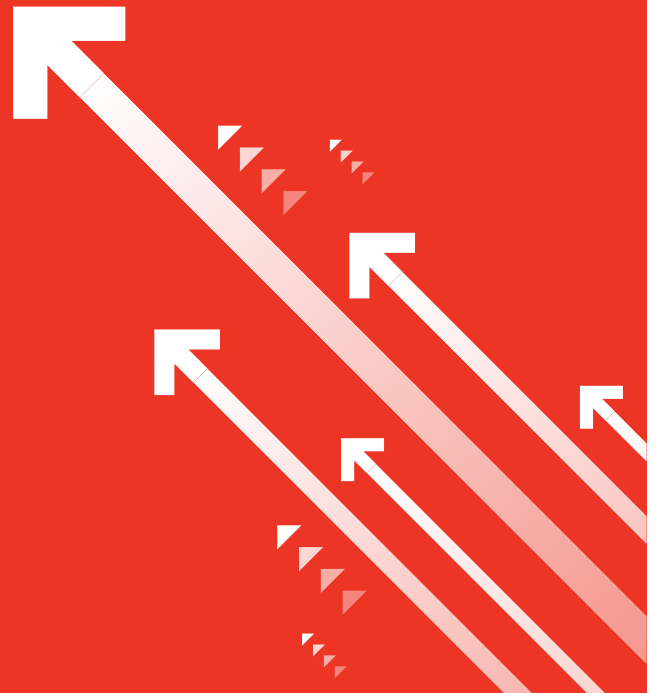
Key findings

95% of respondents cannot get close to the 1:10:60 industry ideal: 1 minute to detect, 10 minutes to understand, 60 minutes to contain

19% Only the minority say that intruder detection is their primary IT security focus, despite the majority...
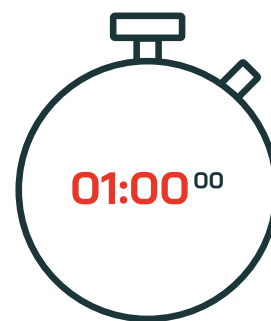
86% ...seeing one-minute detection as a cybersecurity "game-changer" for their organization

88% feel that their organization should be doing more to understand attackers

67% see a direct link between better understanding and more complete data protection

01:00⁰⁰

31 hours on average to contain a cybersecurity incident once it has been detected and investigated, a far cry from the 60 minute ideal in the 1-10-60 benchmark

162 hours to detect, triage, investigate and contain the average cyber incident - almost seven days of working around the clock
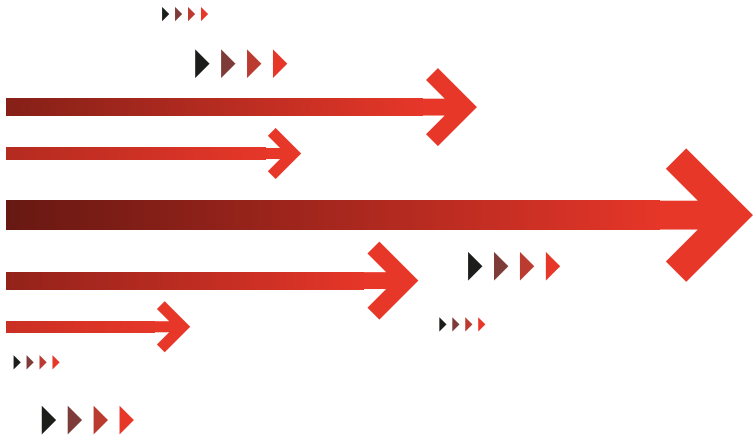
10:00⁰⁰

80% report that in the past 12 months they have been unable to prevent intruders on their networks from accessing their targeted data, with...

44% ...pointing the finger at slow detection as the cause

60:00⁰⁰

One minute to detect

Time is of the essence. If you are unable to prevent an intruder from gaining access to your network, you must be able to detect the intrusion as quickly as possible. However, this is not often the case, allowing intruders to stay on networks undetected for months at a time.

Only 11% of respondents estimate that their organization can detect an intruder on their networks within one minute. For security professionals — the ones on the front lines dealing with these intrusions — only 9% believe this to be true.

The reality is that for most, detection is taking much longer than one minute.

On average, respondents estimate that it takes their organization 120 hours to detect a cybersecurity incursion or incident.
That is the equivalent of five days working around the clock. Imagine the damage that can be done by a malicious threat actor that goes undetected for almost a week.

For many, the main focus of cybersecurity teams is not on detection. Only 19% believe that their organization considers detection to be their primary focus, half the number of those who report their primary focus is on preventing access (38%). While it is obviously important to proactively monitor and avoid attacks initially, there seems to be little defense for attacks that make it onto the network — something that could be considered unavoidable given the sophisticated tactics, techniques and procedures (TTPs) of today's adversaries.

Those who estimate that their organization can detect a cyber security incident within one minute
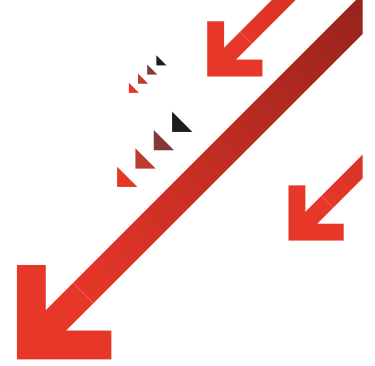
11%
All respondents

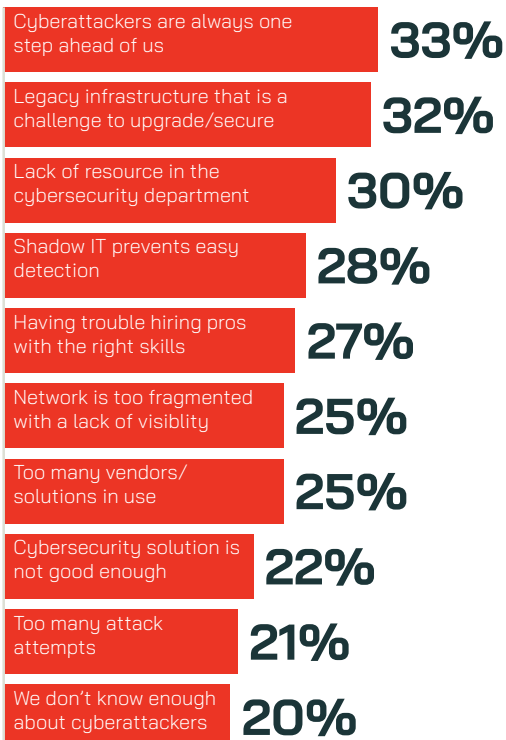**13%**
Senior IT decision makers

9%
IT security professionals

While this inability to detect quickly might appear to be a question of "will", for many organizations, it actually comes down to "skill" — they are just not equipped for faster detection. Almost a third (32%) are being slowed down by legacy infrastructure that is a challenge to upgrade and secure. Meanwhile, a lack of resources in the cybersecurity department (30%), shadow IT (28%), and/or a skills shortage (27%) were also cited among the most prevalent reasons for slow detection times.

Yet, if one-minute detection time could be achieved, IT leaders and security professionals alike can see the positive impact. Not only would it give the intruder less time to try to access their targeted data, but it also gives the organization a head start when it comes to investigating the incident and ultimately containing it. In fact, most (86%) see the ability to detect an intruder on their network within one minute as a "game-changer" for their organization's cybersecurity.

Reasons for slow detection

Reason	
Cyberattackers are always one step ahead of us	33%
Legacy infrastructure that is a challenge to upgrade/secure	32%
Lack of resource in the cybersecurity department	30%
Shadow IT prevents easy detection	28%
Having trouble hiring pros with the right skills	27%
Network is too fragmented with a lack of visiblity	25%
Too many vendors/ solutions in use	25%
Cybersecurity solution is not good enough	22%
Too many attack attempts	21%
We don't know enough about cyberattackers	20%

CROWDSTRIKE

Simply put, the faster you can detect, the greater the chance that you can stop an incident from growing into a breach. Attacks are likely to have interrelated steps: The sooner you can detect and identify one of these steps, the sooner you can take steps to nullify or contain the impact.

Many of the high-profile incidents and breaches featured in the media in recent years illustrate what CrowdStrike® refers to as "silent failure." This happens when security technologies are not able to detect intrusions and the attacker is free to move throughout the environment with impunity. Modern day approaches and platforms such as CrowdStrike Falcon® were designed to detect quickly and accurately, so that silent failures do not occur.

Click here to find out how CrowdStrike Falcon can help your organization detect intrusions more quickly and accurately.
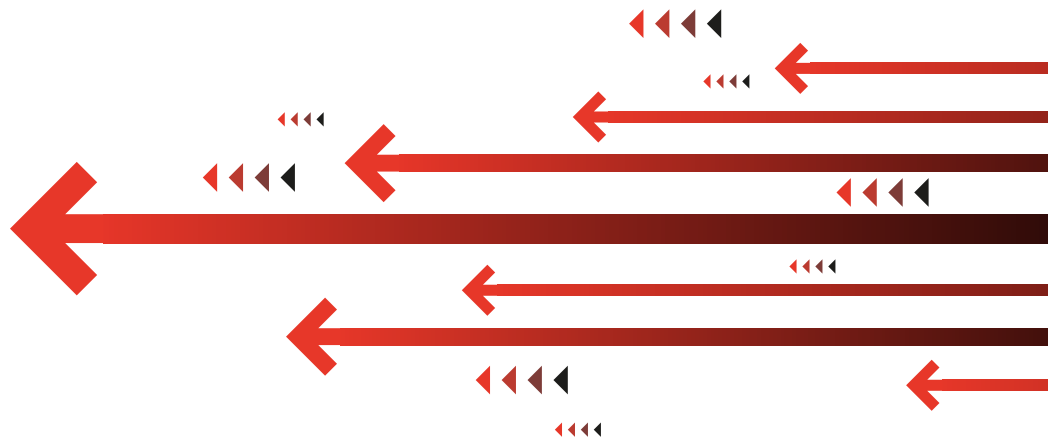
Ten minutes to investigate

What happens once a threat has been detected on an organization's network?

The next step is to investigate — to find out more about the attack and if possible, the attacker. After all, it is easier to stop someone if you know who they are, and importantly, what they want. Almost four in ten respondents see it as absolutely critical that when their organization is attacked, they find out the level of experience and expertise of the attacker (39%) and/or their motive (39%). Two-thirds (67%) of respondents believe that knowing more about an attacker helps them better protect the data and files the attacker is targeting.
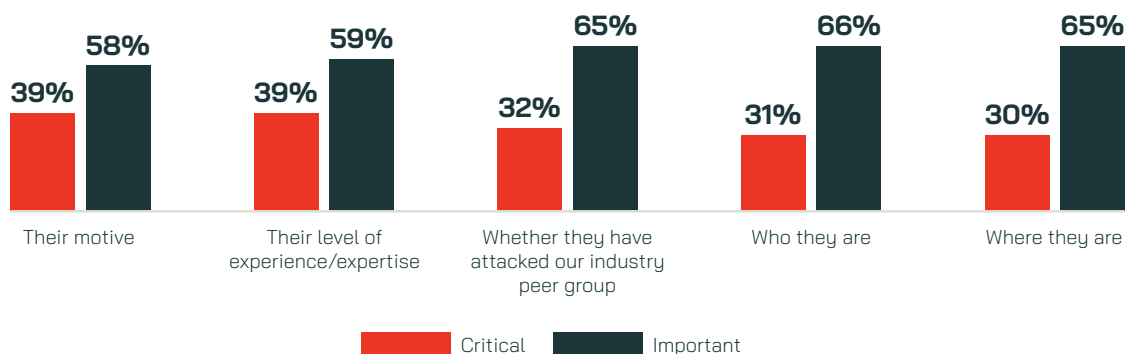
However, the study shows that it takes an average of five hours after detection before a threat can even be triaged and six to actually investigate it. Even then, the identity of the threat actor(s) is only discovered in 53% of cases, on average.
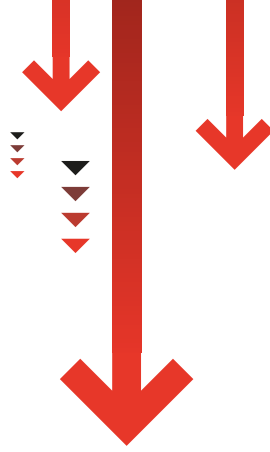
Two-thirds (67%) of respondents believe that knowing more about an attacker helps them better protect the data and files the attacker is targeting

So how long should an investigation into a cybersecurity incident take?

It needs to be quick so that you can move onto the containment part of the response, given it is likely that a significant amount of time has already been lost to detection. However, investigations into attacker behavior and motivations must be conducted to find out as much information about the attacker as possible, so future targeting and attacks can be avoided.

Importance of discovering the following about cyberattackers

	Their motive	Their level of experience/expertise	Whether they have attacked our industry peer group	Who they are	Where they are
Critical	39%	39%	32%	31%	30%
Important	58%	59%	65%	66%	65%

Critical   Important

What if you could fully investigate and gain a complete understanding of an intruder/intrusion within 10 minutes?

Despite the vast majority (88%) of respondents seeing this as something that would revolutionize how their organization deals with cyberattacks, only 9% report that they have this capability. Most (88%) respondents are aware that they need to be doing more to understand cyberattacks and those that perpetrate them.

However, with detection taking so long, do organizations have the time to gain this valuable knowledge, and on the flip side, can they afford not to?

It is critical to understand the details of an attack: who is attacking you, what happened during the attack and its scope, and what motivated the attacker. This information can help you shape a necessary and effective response. If you don't do this step well, or take too long in doing it, you will continue to hand the advantage to the attacker and your organization will continue to be compromised.

Putting this idea into context: The CrowdStrike 2019 Global Threat Report found that Russian adversaries are the fastest of all cyber actors and can break out of their initial intrusion beachhead in under 19 minutes. This is why CrowdStrike recommends that understanding the adversary that is targeting your organization is key to driving your response strategy and tactics.

### Breakout time: a critical metric

The survey found that on average, it takes global respondents an average of 162 hours to detect, investigate and contain an attack — that is close to seven days, working around the clock to stop an incident. When battling today's sophisticated adversaries, 162 hours is unacceptable.

The statistics revealed in the survey are significant because they differ widely from the key metrics CrowdStrike believes organizations must observe to effectively respond to an attack. Chief among them is "breakout time," which CrowdStrike first revealed in the CrowdStrike Global Threat Report. Breakout time is the interval for an intruder to begin moving laterally, "breaking out" from the initial machine they have compromised to traverse and compromise other systems in your network.

The average breakout time depends on which adversary you are facing. Last year, CrowdStrike tracked the average breakout time of adversaries at 1 hour and 58 minutes.

This means that in order to stop a breach and contain an adversary before they "breakout" of the initial beachhead and get to critical resources within the network, a defender has to detect, investigate and remediate or contain the intrusion, on average, within roughly two hours. This is a tight window for organizations to be able to prevent an incident from turning into a breach.

CrowdStrike believes that the ability to respond within the 1-10-60 window is a critical factor in mounting an adequate defense against cyberattacks of any kind, including software supply chain attacks. With the Falcon platform, CrowdStrike accelerates time to investigate and understand threats by providing deep context, seamlessly integrated threat intelligence, and sophisticated visualizations. In turn, enterprises are able to automate the labor-intensive stages of incident investigations and dramatically speed response.
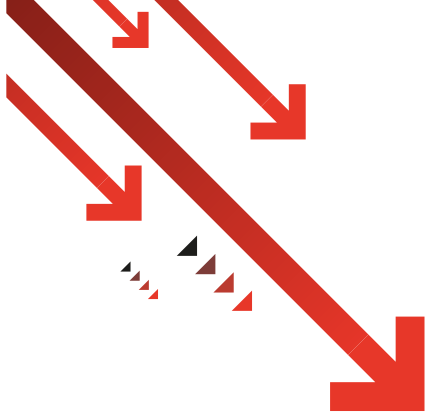
60 minutes to contain

Everything that has been discussed so far leads to the next step in the cybersecurity chain: containment. The threat has been detected and investigated, and now it is time for organizations to act.

Yet, with detection and investigation both taking much too long in most cases, how much time do organizations have to contain the threat? By that point, is it too late? And most importantly, can they contain it effectively?

Two thirds (68%) of respondents admit that it takes too long for their organization to contain an intruder on their network. On average, the act of containment takes respondents' organizations 31 hours.

Once you factor in the time, on average, for detection, triaging, and investigating, there is another serious question to ask: How much damage could a proficient and experienced attacker do with 162 hours of unhindered access to your network?
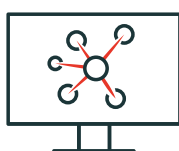
120
hours to
detect

5
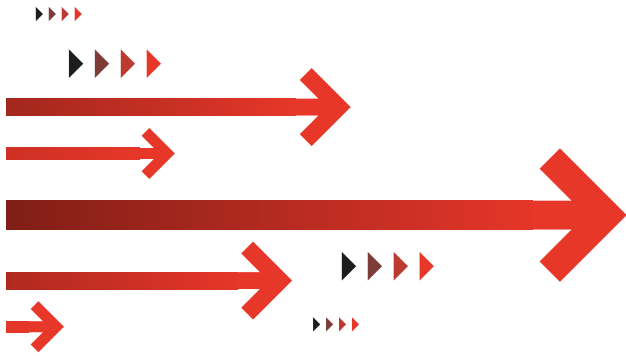hours to
triage

6
hours to
investigate

31
hours to
contain

162 hours in total

6+ days working around the clock

23+ working days (based on a seven hour working day)

Overall, only 5% of respondents feel confident that their organization can detect a cybersecurity incident within one minute, investigate it within 10 minutes, and contain it within 60 minutes
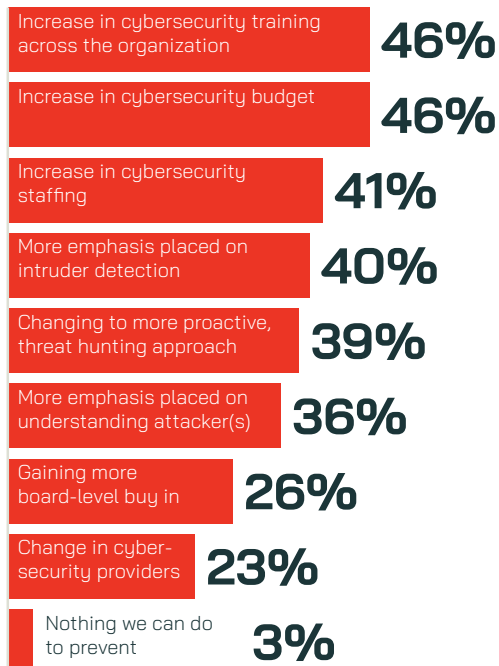
While a third (33%) of respondents feel that their organization could contain a cybersecurity intruder within one hour, is that really adequate, given how long the rest of the process takes? Or is it still a case of too little, too late?

Overall, only 5% of respondents feel confident that their organization can detect a cybersecurity incident within one minute, investigate it within 10 minutes, and contain it within 60 minutes.

The impact of this is that eight in ten (80%) experienced an incident where they were unable to prevent an intruder from obtaining their objective once they got onto the network. For close to half of the respondents (44%), detection taking too long was the root cause of this failure to contain. For nearly four in ten, a lack of resources (39%) and/or skills (36%) to detect, investigate and mitigate these attacks were to blame.

Yet something can be done to prevent the access to data once an intruder is on the network, as nearly all (97%) respondents are aware, whether it is an increase in budget (46%), training (46%) or staffing (41%). Four in ten would like to see more emphasis placed on intruder detection (40%), understanding the attacker (36%), and/or a change to a proactive "'threat hunting" approach (39%) in order to more successfully prevent this from happening.

Things that can be done to improve chances of containment

Increase in cybersecurity training across the organization	**46%**
Increase in cybersecurity budget	**46%**
Increase in cybersecurity staffing	**41%**
More emphasis placed on intruder detection	**40%**
Changing to more proactive, threat hunting approach	**39%**
More emphasis placed on understanding attacker(s)	**36%**
Gaining more board-level buy in	**26%**
Change in cyber-security providers	**23%**
Nothing we can do to prevent	**3%**

CROWDSTRIKE

CrowdStrike is laser focused on helping organizations stop breaches. Its success in protecting customers across the globe, across a wide-range of industries, is evidenced by the more than 35,000 breaches that will be successfully stopped in 2019.

It is a testament to the power and speed of the Falcon platform and its ability to rapidly detect, investigate and respond to incidents to stop them from becoming breaches.

To find out more, click on this link.

Conclusion

The gold standard for response to a cybersecurity incident — 1 minute to detect, 10 minutes to investigate and 60 minutes to contain — seems out of reach for all but 5% of organizations.

The vast majority of organizations struggle to detect active threats in their environments, investigate hackers and contain cyberattacks fast enough. Almost an entire week goes by before an organization even identifies that an attack is taking place, and another two days are gone by the time the attack is responded to effectively. The average amount of time to detect, triage, investigate and contain a cyberattack is 162 hours. The damage that can be done in that timeframe can be catastrophic to a business.

The survey shows that the vast majority of organizations recognize that they should place more emphasis on high-speed detection and attacker breakout prevention, as well as the ability to understand the threat actors themselves.

They appreciate the importance of these measures, and the value that success in these areas can bring to their organization's cybersecurity. It is not so much a case of "why" for them, but more "how." How do organizations move closer to the goal of the 1-10-60 rule? What changes must they make to do this? What benefits can their organization reap if they succeed?

Regardless of how organizations answer these questions, time is of the essence. Businesses cannot afford to be satisfied with the detection and containment capabilities they have currently. As attacks continue to grow in sophistication and threats fly in from an increasingly broad range of vectors, organizations must do more to act quickly enough to stop a breach.

Recommendations

The 2019 Global Security Attitude Survey reveals that organizations lack the expertise, processes and technology that they need to efficiently detect, triage and contain cyber threats to keep their critical data secure. Along with adopting proactive prevention techniques focused on identifying malicious behavior even when no malware "signatures" or known exploits are present, organizations need to close the security gaps that are making them vulnerable to attack. This requires, in addition to prevention, a focus on detection and response technologies.

The following are some recommendations aimed at helping organizations increase their security postures to avoid becoming a breach victim.
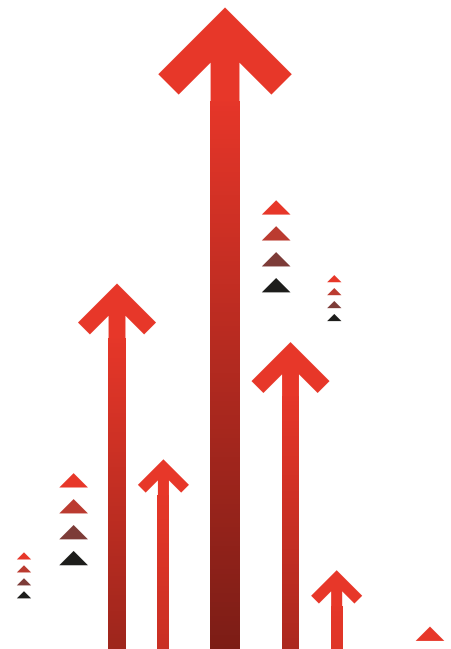
1

Employ solutions that integrate both threat hunting and threat intelligence

This year's survey indicates that the persistent nature of advanced threat actors and issues within the software supply chain continue to plague organizations. Companies that do not have a full deployment of effective endpoint security solutions across their entire network suffer from protracted detection and response times because they lack the comprehensive visibility necessary to defend against cyberattacks.

Solutions that integrate a threat hunting strategy not only collect detailed endpoint data but identify stealthy adversaries using TTP and evasion techniques. Forward-leaning organizations under threat from cyber actors should deploy threat hunting teams, whether staffed internally or via managed detection and response (MDR) services such as Falcon OverWatch™, to rapidly detect, investigate and remediate intrusions before the adversary can accomplish its objective and cause a data breach.

Threat intelligence is another informative solution to help you build out your security stack and illuminate important attacker motivations and behaviors. This helps security teams understand incidents more fully and make more informed decisions to get ahead of future attacks. Falcon X™, CrowdStrike's threat intelligence solution, provides industry-leading intelligence on threats detected using CrowdStrike Falcon® endpoint protection. This ensures that all new attacks in your environment are automatically analyzed and enriched with threat intelligence, giving you a complete picture of the threat and delivering all the context you need to predict future attacks and deploy proactive countermeasures.

2

Next-generation security solutions are key

As sophisticated attacks continue to evolve, organizations of all sizes must employ leading-edge techniques such as behavioral analytics, artificial intelligence (AI) and machine learning (ML). These next-generation security solutions go beyond malware to detect indicators of attack (IOAs), which focus on identifying attacker activity while an attack is in process, a key capability for getting ahead in the detection cycle. As the survey indicates, the global average to detect a cyber incident is 120 hours. Integrating a real-time endpoint detection and response (EDR) solution such as Falcon Insight™ is crucial for accelerating the detection cycle and operating at a pace that will disrupt the abilities and operations of adversaries.

Protecting your organization by employing a security platform that enables prevention and detection has become even more critical in today's threat landscape. However, defenders must also look for early warning signs that an attack may be underway. These early indicators include hands-on-keyboard activity, code execution, command and control activity, and lateral movement within a network. Contextual and behavioral analysis, when delivered in real time through ML, can help detect these warning signs and prevent attacks that legacy technologies often miss, giving defenders insight to prevent future attacks.

3

Proactive security is as critical as reactive

Preparing to deal with the next attack is an integral part of managing risk. Security professionals' knowledge can run deep and wide, but can never be comprehensive enough to encompass every unknown. That is why proactively preparing and testing a security plan on a continual basis is a necessity in the face of evolving attacker tradecraft.

The CrowdStrike Services team not only handles incident response and digital forensics in the wake of an attack, it also offers organizations proactive services such as tabletop exercises, red teaming, blue teaming and more. CrowdStrike Proactive Services can improve an organization's ability to withstand sophisticated targeted attacks. The Services team also offers Cybersecurity Maturity Assessments and Compromise Assessments that give customers an understanding of their current exposure and a roadmap for enhancing defenses.

Geopolitical cyberattacks and software supply chain cyberattacks

Two reasons why detection, investigation, and containment need to be taken more seriously

1. Nation-state-sponsored attacks

We live in uncertain times where nations orchestrating frequent, coordinated and sophisticated cyberattacks against both public and private entities is a reality, though these attacks often fly under the radar. Respondents confirm this, with over eight in ten (81%) reporting that nation-state sponsored cyberattacks are far more common than most people think. It's fair to say that five years' ago, relatively few organizations would readily admit that they were at risk of cyberattack by a nation-state. Today, only 5% feel they are not at risk.

Respondents are concerned that what their organization produces (73%), their industry itself (63%), high profile members of the leadership team (56%), and the country in which they are based (33%), could all place them in harm's way.

These types of attacks are on the rise and nation-states have far greater resources available to achieve their goals than your typical cybercriminal or hacktivist. With political tensions high, it's no wonder that almost three quarters (73%) of IT leaders and security professionals see nation-state sponsored attacks as having the potential to pose the single biggest threat to organizations like theirs in 2020.

While it's more understandable for the majority (82%) to see the clear and present danger from malicious or unfriendly countries, it's perhaps surprising that a similarly high proportion (80%) cannot rule out an intrusion by any government, including their own. With threats at home and abroad, no one should be taking nation-state sponsored cyberattacks lightly.

What might motivate a nation-state to attack?

73%	**63%**	**56%**	**56%**	**33%**	**5%**
What we do/ produce	Our industry	Individuals on our leadership team	Close ties to our government	The nation in which we're based	We would not be at risk

Organizations are becoming more aware of the threat of software supply chain attacks and are working on mitigating them, which are all positive signs. However, the bottom line is that these attacks are still increasing in volume

2. Software supply chain cyberattacks

Last year, research by CrowdStrike found that the software supply chain was proving to be the soft underbelly of many organizations. By many accounts, 2017 was the year of the supply chain cyberattack, but what about 2019 and what does the future potentially hold?

In 2019 over three quarters (77%) of respondents admit that their organization has experienced this attack type at least once at some point in time, a significant increase over 2018 (66%). In 2019 alone, 53% of respondents encountered this attack type — perhaps 2019 will someday be viewed as the year this attack type really accelerated.
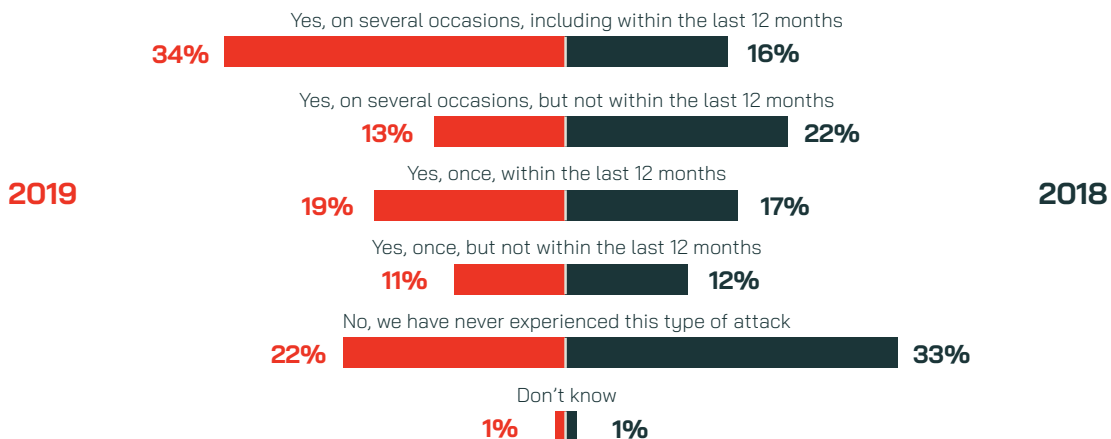
In addition, the number of respondents whose organizations have paid some form of ransom in the last 12 months to retrieve data encrypted in a software supply chain attack increased markedly (14% in 2018 up to 40% in 2019). These attacks are more frequent and more potent.

However, there is some good news: Over half (52%) of those hit by a software supply chain attack in 2019 had a comprehensive strategy in place at the time, compared to only just over a third (34%) 12 months ago. Additionally, the number of 2019 respondents' organizations that are vetting all suppliers, new or existing, in the past 12 months is over four in ten (45%), which is up from 32% who had done the same in the 12 months preceding last year's study.

Organizations are becoming more aware of the threat of software supply chain attacks and are working on mitigating them, which are all positive signs. However, the bottom line is that these attacks are still increasing in volume.

As organizational cybersecurity improves — and it is improving — attackers are searching more intensely for that back door onto networks. If the software supply chain is vulnerable, then it is a route that is increasingly being taken. With attackers always able to find a new way onto networks, fast detection, investigation and containment become the only guaranteed way to protect your organization.

Experiences with software supply chain cyberattacks: 2019 vs. 2018

Yes, on several occasions, including within the last 12 months
34% **16%**

Yes, on several occasions, but not within the last 12 months
13% **22%**

2019 Yes, once, within the last 12 months **2018**
19% **17%**

Yes, once, but not within the last 12 months
11% **12%**

No, we have never experienced this type of attack
22% **33%**

Don't know
1% **1%**

Methodology

CrowdStrike commissioned independent market research specialist Vanson Bourne to undertake the research upon which this whitepaper is based. A total of 1,900 senior IT leaders and security professionals were interviewed in Fall 2019, with representation in the Americas, EMEA and APJ:

Country	Number of interviews
US	400
Canada	100
Mexico	100
UK	200
Germany	200
France	200
Middle East	100
India	300
Australia	100
Japan	100
Singapore	100

Respondents had to be from organizations with 250 or more employees and from a range of private and public sectors including engineering, manufacturing, financial services, retail and healthcare.

The interviews were conducted online and were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, the results discussed are based on the total sample.
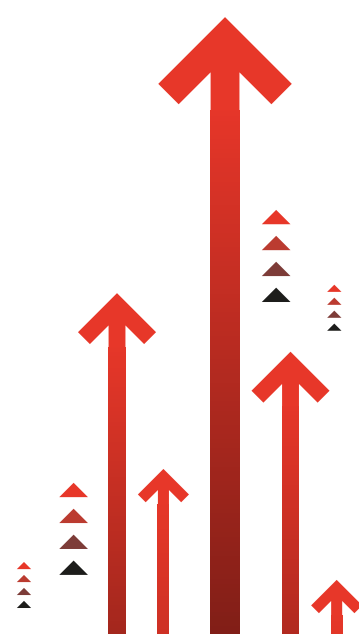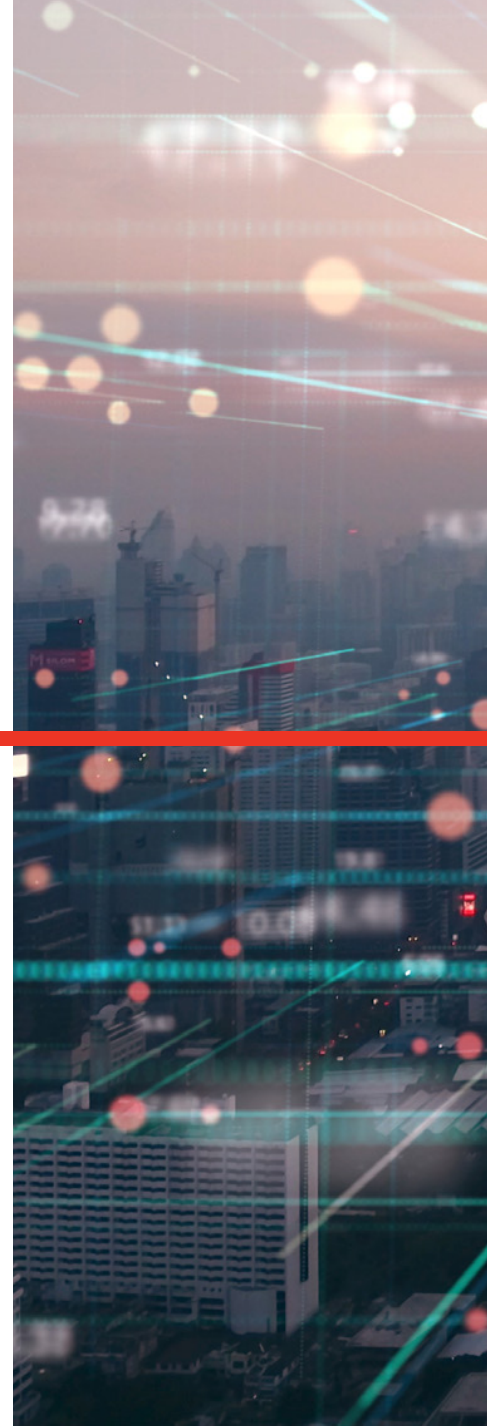
1,900
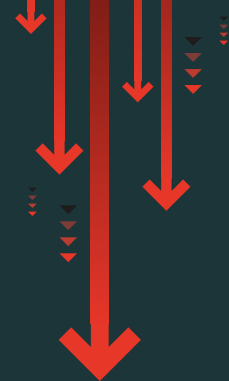
senior IT leaders and security professionals

3

regions: Americas, EMEA and APJ

250+

employee organizations

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit www.vansonbourne.com