Fostering a culture of security

In a strong security culture, employees are treated as part of the solution rather than the problem. Awareness of the role they play is key. This may be seen by regularly reporting phishing attempts, potential malware, and other incidents. Conversely, frequent security policy violations and workarounds are evidence of poor security culture.

Source: Cisco Security Outcomes Report Volume 3

Organizations that foster a culture of security see a 46% increase in resilience.

Have your resources in place

Maintaining excess internal staff and resources in order to better respond to unexpected cyber events makes a big difference. If maintaining extra staffing to handle unexpected events isn't feasible for your organization, firms that retain external incident response (IR) services show an 11% average improvement in security resilience. Consider getting those retainer contracts in place with a credible IR service provider so help is just a phone call away.

Organizations able to maintain excess resources achieve 15% higher security resilience scores on average than those without “flex” resources to tap into when needed.

Utilize threat intelligence as part of your detection and response capabilities

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose. No protection can ever provide complete cover, and we can’t fully anticipate how threats may change and evolve. Preparation is key. Ensuring that systems have no single points of failure helps ensure that operations can continue even if one component must be taken out of action due to a threat.

Organizations with these capabilities boasted a 45% better overall resilience score than those without a XDR solution.

There are two key pieces to a cohesive Extended Detection and Response (XDR) solution:

Automation/orchestration

Utilize threat intelligence as part of your detection and response capabilities

Cyber threat intelligence

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose. No protection can ever provide complete cover, and we can’t fully anticipate how threats may change and evolve. Preparation is key. Ensuring that systems have no single points of failure helps ensure that operations can continue even if one component must be taken out of action due to a threat.

Organizations with these capabilities boasted a 45% better overall resilience score than those without a XDR solution.

There are two key pieces to a cohesive Extended Detection and Response (XDR) solution:

Automation/orchestration

Cyber threat intelligence

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose. No protection can ever provide complete cover, and we can’t fully anticipate how threats may change and evolve. Preparation is key. Ensuring that systems have no single points of failure helps ensure that operations can continue even if one component must be taken out of action due to a threat.

Organizations with these capabilities boasted a 45% better overall resilience score than those without a XDR solution.

There are two key pieces to a cohesive Extended Detection and Response (XDR) solution:

Automation/orchestration

Cyber threat intelligence

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose. No protection can ever provide complete cover, and we can’t fully anticipate how threats may change and evolve. Preparation is key. Ensuring that systems have no single points of failure helps ensure that operations can continue even if one component must be taken out of action due to a threat.

Organizations with these capabilities boasted a 45% better overall resilience score than those without a XDR solution.

There are two key pieces to a cohesive Extended Detection and Response (XDR) solution:

Automation/orchestration

Cyber threat intelligence

Detect and Alert

Utilize threat intelligence as part of your detection and response capabilities

Cyber threat intelligence

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose. No protection can ever provide complete cover, and we can’t fully anticipate how threats may change and evolve. Preparation is key. Ensuring that systems have no single points of failure helps ensure that operations can continue even if one component must be taken out of action due to a threat.

Organizations with these capabilities boasted a 45% better overall resilience score than those without a XDR solution.

There are two key pieces to a cohesive Extended Detection and Response (XDR) solution:

Automation/orchestration

Cyber threat intelligence

Focus on simple to manage, flexible technologies

Security resilience is about taking the fear out of change, and planning for unexpected events. When you have security resilience, no accidental clicks can’t jeopardize your whole company. Or if suddenly you need to spin-up a branch office, it can be secure the moment it goes online.

So, what are the key steps towards security resilience?

Source: Cisco Security Outcomes Report Volume 3

To learn more, read our eBook:
Your guide to building security resilience,
with Cisco Secure

Cisco Secure is helping organizations everywhere prepare for the unexpected. Not so they can avoid it. But so they can face it, quickly adapt, and withstand it.