2021

Cybersecurity Conversations for the C-Suite

Securing the Post-COVID Paradigm Shift

HERJAVEC GROUP

"COVID Testing" Your Devices
The Process and Support Required to Manage, Detect & Respond to Emerging Threats

Refreshing Emergency Preparedness Plans
Why Incident Response Expertise is More Critical Now Than Ever

Re-Prioritizing Scanning and Testing Programs
Continuous Improvement Is Not Optional

A Message from Robert Herjavec

Founder & CEO, Herjavec Group

Welcome to 2021!

In last year's Cybersecurity Conversations report, we predicted it would be "the Year of Digital Transformation." We encouraged enterprises to take an integrated approach to cybersecurity by prioritizing three areas:

- Identity-Focused Digital Transformation Driven by Context
- Proactive & Customized Security Planning Through Threat Modelling
- Leveraging the Power of Security Orchestration, Automation & Response (SOAR)

While these transformations were critical, they were overshadowed by the mass accelerated moves to the cloud, and to remote work scenarios due to the COVID-19 Pandemic.

Over the last year we experienced complete change to our "every days" - from the immense pressures on our global healthcare system, to the way we travel, do business, and most importantly, connect with others. The very core of our humanity has been forced to evolve as we adapt to pandemic life. Almost overnight, enterprises sent employees home, supported by monitors, laptops, desktops, printers, and phones to be connected to unsecured personal environments. Phrases like "just get it done" and "do what you can to keep the lights on" became the mantras for many organizations (and unfortunately security programs) as we did our best to grapple with the dreaded "new normal."

Some of you thrived – you quickly rolled out your remote workforce, your SOC transitioned to work from home (as ours did), and for many, it almost felt too easy.

Let me be the first to say, ***it was.***

We got it done but did we proactively protect this transition as well as we could have? Think long and hard…

- What endpoint protection was in place before you sent those devices home?
- What was the frequency of your scanning program?
- What was your process for patch management and have you kept it up?
- How confident are you in your cyber visibility? In your ability to detect and contain an infected device?

- How would you feel if your entire team returned to work tomorrow and plugged into the enterprise network?
- Do you have the support required to address the infections that may follow another dramatic shift in the way we work?

To truly prepare for the security challenges we will face this year you need to be able to address the points above with complete confidence.

Just because 2020 is behind us, it doesn't mean we can sit back and relax. To put it frankly, we are in for a difficult year.

> I will go on the record confirming that 2021 will be the most profound year in cybersecurity in our global history.

This is going to be the year we look back to in terms of heightened impacts of nation-state attacks and emerging malware threats. Targeted attacks like those against the SolarWinds supply chain, and the total system disruption of UVM Health Network, are only the beginning of what we can expect to see. The challenges we will face as a cybersecurity community will be varied, continuous, and demanding.

With the COVID-19 vaccine being rolled out, enterprises will start heading back into the physical workspace, embracing a flexible, hybrid work model. We will reconnect the devices we sent home a year ago and be in for a world of hurt if the right processes, programs and support services are not in place.

As cybersecurity professionals, the pandemic drastically affected the way we detect, manage, respond, protect, and secure. I surveyed the Herjavec Group executive team to get their take on how enterprise leaders will need to adapt their security programs as a result.

This year Herjavec Group's Conversations for the C-Suite Report is dedicated to the conversations we recommend having with your executive teams in order to confront the paradigm shift resulting from the pandemic head on:

"COVID Testing" Your Devices
The Process and Support Required to Manage, Detect & Respond to Emerging Threats

Refreshing Emergency Preparedness Plans
Why Incident Response Expertise is More Critical Now Than Ever

Re-Prioritizing Scanning and Testing Programs
Continuous Improvement Is Not Optional

2020 proved to be a formidable adversary, bringing historic losses and challenges. If we have learned anything throughout the pandemic, it's that we as a people are resilient, adaptable, and industrious. The collaborative innovations, moments of compassion, and examples of sheer willpower that we bore witness to are undeniable proof that if we work together and support each other in moving forward towards our common goals, there is nothing we cannot overcome as a cyber community.

Here's to a (cyber) safe 2021…Let's keep the conversation going.

To your success,

Robert Herjavec

"COVID Testing" Your Devices

The Process and Support Required to Manage, Detect & Respond to Emerging Threats

It's rare to have a conversation these days without referencing testing, contact tracing, quarantining or social distancing. Cyber professionals have noted similarities between the public health response to COVID-19 and security incident response processes – at minimum, the vocabulary is certainly related. With vaccines rolling out on a global scale, and enterprises planning their return to work scenarios, we would be wise to take note of the diligence and discipline demonstrated by our healthcare heroes in dealing with this infectious virus. With any transformation of this nature, it's imperative we pause and assess our security controls, and the potential impacts to business operation before initiating a change. Consider this – your employees have been primarily out of the corporate network over the last 11 months. How comfortable would you be for them to return tomorrow and simply plug back in?

Your answer likely depends on how prepared you were for the remote work transition in the first place. Your scenario will depend on:

Your Tools – Does your technology stack deliver the same level of security efficacy for remote employees as it does in the corporate environment?

Your Visibility – Endpoint Coverage, Regular Scanning Cadence, 24/7 Device Monitoring & Management

Your Degree of Control – Access to Contain and Configure Devices as Necessary, Patch Management

As we transitioned to the remote work environment, we saw many enterprises make compromises within their security programs, and rightly so. There's no such thing as perfect cybersecurity and we all had to make it work. You may have experienced the pain of overwhelmed Virtual Private Networks (VPN), accepted the risk of split tunnelling, and felt vulnerable to rising malware infections & viruses that often result from mixing personal and corporate traffic. The tiered policies you put in place to protect your weakest link (your employee base) against ransomware and phishing may not have scaled. ALL of your employees became "road warriors", requiring next generation endpoint protection, email gateway monitoring, cloud access and secure internal gateways.

In a perfect scenario, these tools would have been deployed company-wide, been logging to a Security Information Event Management (SIEM) platform and been monitored & managed 24/7 with expert level analysis and response. But we've already said, there's no such thing as perfect…

So where do we go from here? We've summarized our Office Essentials for your consideration.

The Move Back to the Office Essentials:

There will be no shortage of projects and cyber initiatives to take on this year but in order to ensure your enterprise network is protected as your team transitions to a hybrid work model, we recommend prioritizing these essential tasks:

1. Asset inventory

Take inventory of all devices coming back to your network to ensure visibility of all endpoints.

2. Test all devices

If you haven't already deployed cloud-based Endpoint Detection and Response, do so. This will be the best way to identify and respond to any malware or compromises on all devices coming back to the office. Respond to any infected devices appropriately to ensure they are safe to return to the office.

3. Quarantine devices that have yet to be tested or are infected

If a device is infected or hasn't been tested yet, quarantine these devices on a network segment that is isolated to avoid total corruption until the device can be properly treated.

4. Regularly test moving forward

Once your team is back to the office, continue to scan and monitor your EDR solution to ensure all devices remain safe. We highly recommend engaging Managed Detection and Response (MDR) support to ensure time to value, proactivity and automated blocks & updates.

EDR to MDR to XDR

There has been a lot of confusion surrounding the many forms of Detection and Response in the cybersecurity ecosystem. Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), and Extended Detection and Response (XDR) should be thought of as a continuum that has evolved in response to the needs of your enterprise.

First you need to be able to detect & respond at the device, and user level. This requires EDR coverage & support.

Endpoint Detection & Response (EDR)

Endpoint solutions that provide capabilities to detect and investigate security events, contain the attack, and produce guidance for remediation. Visibility and reporting of user and device activity are combined with direct intervention when abnormal activity is detected.

The next step is having a security expert take on the threat detection and response 24/7. This is where your Managed Detection & Response service comes into play.

Managed Detection & Response (MDR)

MDR service providers leverage a combination of technologies deployed at the host and network layers, as well as advanced analytics, threat intelligence and human expertise to deliver 24/7 monitoring, detection, and response to threats against customers.

XDR takes the protection and visibility beyond the endpoint, collating multiple sources of information including network, vulnerability and identity data, to provide a more holistic and robust escalation, and in turn, response.

Extended Detection & Response (XDR)

A vendor-specific, threat detection and incident response tool that unifies multiple security products into a security operations system.

*EDR, MDR and XDR definitions from Gartner (2021)

Your use of EDR, MDR or XDR will vary based on your organization's maturity and technology stack. We recommend at minimum deploying a best of breed EDR solution and having Managed Detection & Response (MDR) support, coupled with Incident Response expertise. Your comprehensive cybersecurity plan should protect against adversaries at a granular, device level, and requires practised, knowledgeable teams that have the capability to continuously monitor and respond to security incidents.

Adam Crawford, Herjavec Group's VP of Managed Security Services believes, "generally speaking, enterprise attacks are the result of a human unintentionally interacting with something malicious on their device. So, having more robust security on the endpoint with EDR acts as a first line of defense. When combined with SOAR technology, our team can stop the attack in its tracks. We can stop the script running or purge the malicious email from your inbox. We can take proactive actions to mitigate the attack." Managed Detection & Response (MDR) service support is key to identifying, disrupting, containing and remediating the onslaught of malware and emerging threats we are predicting in year.

> "Enterprise attacks are the result of a human unintentionally interacting with something malicious on their device. So, having more robust security on the endpoint with EDR acts as a first line of defense. When combined with SOAR technology, our team can stop the attack in its tracks.

ASK YOURSELF

- ☐ Can I reach remote devices today?
- ☐ Do I have a plan to "treat and quarantine" devices before they return to the office?
- ☐ To what degree is my existing cyber services provider supporting Managed Detection and Response?
- ☐ Do I have proactive, 24/7 support in hunting for emerging threats?
- ☐ Have my most impactful and repeatable processes been automated into playbooks?

When engaging a Managed Detection and Response services provider, Adam Crawford suggests you should expect the following:

24/7 Support

Around the clock Security Event Monitoring, Triage & Escalation.

Hands-on Expertise

Proactive pre-approved changes, Indicator of Compromise (IOC) identification, Investigation and Threat Hunting.

Threat Disruption Across Platforms

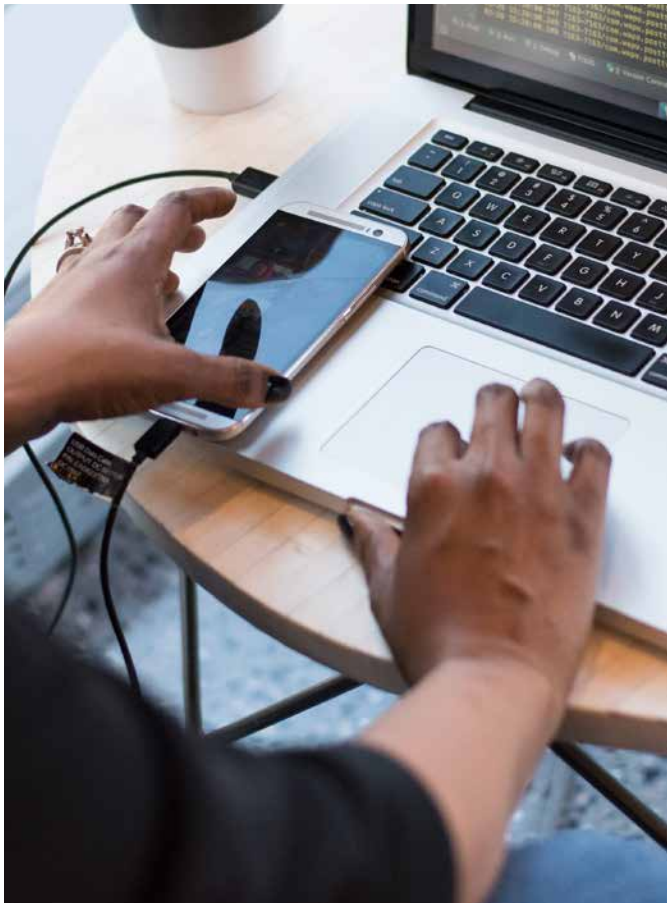
Network Security Monitoring coupled with Management of EDR or XDR solutions, cloud environments, and containers.

SOAR to Drive Security ROI

Automated, pre-approved, pre-defined playbooks and resolver group expertise.

Incident Response Expertise

Battle-tested Incident Commander level resources who bolster your team with state of the art networking, discovery and forensic tools to provide a faster, more effective response, when you need more than blocking or configuration support.



The Fact Is Your Endpoint Protection is Only as Strong as your Identity Program

The remote work environment we experienced in 2020 and the impending hybrid workforce we expect to see in 2021 have forced cyber professionals to revisit and reinforce their Identity and Access Management strategies. When teams were working in the corporate office, it was easy to identify users and their devices as they were all using one secured network and keeping fairly predictable behavior patterns. Doug Chin, Herjavec Group's VP of Identity and Access Management explains that, "the way we approach Identity and Access Management governance hasn't changed, but the importance of implementing it in your cyber strategy has significantly shot up."

Human beings, devices and applications all have identities. It is imperative that your enterprise has a way of detecting anomalous behavior across all three categories. Remote work "at scale" has certainly complicated this effort as behavior patterns have shifted significantly as a result of the pandemic. People are logging on at all hours of the day, their kids are using their corporate devices, personal emails are being accessed… you get the picture.

One of the most frequent questions Doug has received from our clients is, ***"how do I keep my data and my employees secure now that we have deployed cloud operations?"*** His response is simple in theory but complex in execution: "Focus on identity – who is accessing your environment, at what time, from where, and for what reason. But take an adaptive approach, with behavior as the driver in your analysis."

Adaptive authentication recognizes behavior patterns at the user and device level, triggering security incidents when anomalies occur. The user is prompted to authenticate, and the security baselines continue to "adapt" based on those responses. At Herjavec Group we believe that analyzing and identifying behavioral anomalies is a key component to advancing your security posture. As Founder & CEO Robert Herjavec likes to say, "Behavior is where risk, vulnerability and identity converge".

Think of it this way… one of your analysts lives and works in New York. During the pandemic, she has generally logged on from her laptop on her personal home network early in the morning. You see her device "activate" daily. Today, your adaptive authentication system notifies your team that she has logged in to her account from Russia at 2:00 AM. Based on this anomaly, the adaptive authentication system would first present another form of authentication to her. Multi factor authentication kicks in and she's asked to provide her email, password and a corresponding key code before access is granted. If she fails this request for verification, the system will lock her out.

During our many years of incident response and Managed Security Services support, our Herjavec team has seen the "bad guy playbook" repeat itself: Lateral Movement. Get in and Escalate Privilege.

We know what you're thinking – if our ability to detect anomalous behavior at the device level is strong, then we should be covered right?

Wrong – your endpoint visibility and protection is only as strong as your identity program.

Start with Identity.

You won't be able to spot truly anomalous behavior across users, devices and applications without robust programs in Identity Governance, Access Control (including authentication) and Privileged Access Management.

> "Focus on identity – who is accessing your environment, at what time, from where, and for what reason. But take an adaptive approach, with behavior as the driver in your analysis.

Refreshing Emergency Preparedness Plans

Why Incident Response Expertise is More Critical Now Than Ever

Building and Reviewing Incident Response (IR) Plans in Hybrid Work Environments

Cybersecurity has never been a perfect science. As Robert Herjavec referenced in an interview with Cyber Defense Magazine, " You will get breached…Smart money is on how quickly you can contain it". That assertion has been reaffirmed over the course of the pandemic with the FBI reporting a 300% increase in cybercrimes in 2020 alone. Over the last year, the average cost of an enterprise data breach was $3.86 million. Phishing email scams accounted for 1 in every 4,200 emails sent in Q1 2020, and that only increased over the course of the last 8 months.

While most executives and infosec professionals have moved beyond the out-dated notion that preventing all cyber-attacks is possible - a step in the right direction - not all have sought out Incident Commander level expertise in proactively preparing for the security emergencies they will undoubtedly face. Emergency preparedness is critical in order to respond quickly & comprehensively to attacks, minimizing the cost and damage that results from a security incident.

Robert Herjavec explains, "the bottom line is, the worst time to decide how to respond to a cyber-attack is after the incident has occurred. Your enterprise needs a well thought out and properly equipped Incident Response plan to ensure you don't lose precious time figuring out what to do when an attack occurs. You have to approach a cyber incident in an organized and holistic manner."

Today's Incident Response plans involve executive level engagement, boots on the ground and communications support to ensure all elements and impacts of the incident are considered.

We recommend prioritizing a post-incident review to ensure your organization is continuously learning and improving upon your IR strategy.

Generally speaking, enterprises are all too quick to move on to the next cybersecurity challenge because, in most incidents, you're not going to get the attribution answer:

"Don't worry about attribution," Adam Crawford, HG's VP, Managed Services suggests. "The WHO isn't nearly as important as the HOW. How did they get in? Where did our defenses fail us? And what are we changing so this never happens again?"

Make sure your incident response partner will support you in answering these fundamental questions, and validate how this information advances your overall threat detection & response workflow, as part of your Managed Security Service, or Security Operations Center (SOC) program. Adam believes that, "enterprises need to create synergy between incident response, vulnerability management, threat intelligence, and adversary emulation teams for a well-rounded approach to their security operations and overall information security plan."

Incident Response 10-Point Plan

In Tony A. Gaskins Jr.'s book, The Road to Destiny he explains, "they say chance favors the prepared so get prepared and stay ready so that you don't have to get ready later on, when it is too late." We couldn't agree more.

If you're not sure where to begin with your enterprise Incident Response Plan, you can start by considering these 10 points.

1. **Be Prepared and Be Proactive –** Don't wait for an incident to occur to start building your Incident Response Strategy
2. **Know your Enterprise Essentials –** Identify and document where all critical components of your business are stored, how they're protected, and what the cost and impact would be if they were lost or stolen.
3. **Educate and Inform Your Team –** Engage employees across all levels of your organization in Security Awareness Training and provide policies and resources that encourage them to practice good cybersecurity hygiene in their daily lives.
4. **Develop and Communicate Internal Policies, Procedures, and Guidelines for Handling Cybersecurity Incidents –** Ensure all appropriate departments and organizations are engaged and connected to develop and properly document escalation and authority structures. Make sure to include legal departments, staff, law enforcement, and customers.
5. **Assess the Visibility of Your Information Security Environment –** Ensure you have visibility on all critical activity and behavior in your enterprise. Understand how your organization receives and processes data and which stakeholders receive, contribute, and/or action that information.
6. **Prioritize Incident Detection and Analysis in your Cybersecurity Strategy –** Since we know total breach prevention is not possible, implement the right layers of detection and analysis into your information security plan to mitigate the damage and time and effort spent on cyber-attacks.
7. **Develop and Understand your Enterprise's Capacity for Incident Response –** Cybersecurity is a complicated and vast undertaking. Building a team from a variety of sources – your internal staff, contractors, external firms, etc… - is one of the best ways to ensure that your cybersecurity response team's capabilities exceed the skill level and capacity of just your internal staff. Hire, contract, or allocate resources to individuals or groups that are qualified and have the necessary tools and experience in incident response.
8. **Practice and Continuously Improve -** Reviewing your plan on an annual basis and running practice drills like cyber-attack simulations and table top exercises with your team will ensure your strategy and team are reaching their maximum potential and ready to face the real attacks.
9. **Leverage Expert Advice and Guidance –** There are so many valuable and accessible resources to guide your IR Plan development including trusted security advisors, resources from reputable organizations like NIST's Computer Security Incident Handling Guide, and online courses like the SANS Institute's IR Training.
10. **Communicate Clearly and Regularly –** Connect early and often with your enterprise executives, staff, contractors, and all appropriate stakeholders about your IR plan, including your information security program's readiness, strategies for improvement, and capacity for response.

ASK YOURSELF

- ☐ Does my existing MSS or MDR provider offer Incident Response support including analysis, forensics and Incident Commander expertise?
- ☐ What logs would I be capable of providing to an Incident Responder?
- ☐ Does my incident response plan account for remote deployment of IR tools and processes?
- ☐ Am I leveraging SOAR playbook execution and automation to disrupt and block attacks and reduce mean time to detect & respond?
- ☐ Have I conducted a Tabletop exercise or Incident Response Readiness Assessment in the last 12 months?
- ☐ Does my incident response plan include Post-Incident Review?
- ☐ Have I secured an Incident Response provider on retainer in the event of a breach?

Re-Prioritizing Scanning and Testing Programs

Continuous Improvement Is Not Optional

While experts in cybersecurity have always urged enterprises to continuously test and improve their information security plans, in 2021 this will no longer be optional. Now is not the time to settle for "good enough". 2020 was the worst year on record in terms of the data breaches that occurred, according to Security Magazine (2020). A staggering 36 billion records were exposed, many of which were vulnerable due to poor hygiene, and a rise in social engineering threats. As we return to the physical workspace, particularly with a hybrid work model, we expect an onslaught of malware and threat activity.

In order to properly prepare your proactive defense, you must be able to assess your current state. Cyber leaders have relied on different approaches to provide indicators of coverage, control and overall security. Typically, this begins with a balance of **Vulnerability Management, Penetration Testing** and **Red Team Operations.**

"I like to think of Vulnerability Management as a camera, taking a snapshot in time," says Herjavec Group VP of Professional Services Eric Cowperthwaite. "You take your picture, understand the scenario, prioritize what needs to be addressed and then later on, take another picture." **Vulnerability Management Services** typically involve a network scanning program on a monthly or quarterly basis, supported by a stakeholder report summarizing the delta of prioritized vulnerabilities between scanning periods.

To continue the analogy, **Penetration Testing** takes another photo, a snapshot in time if you will, with the goal of testing specific controls. A network penetration test aims to find weaknesses in the defense capabilities before an adversary can take advantage through a combination of security expertise and best-of-breed technology. Security consultants identify exploitable flaws in the security architecture, detective controls,

Ask the Experts

If I Had 1 More Dollar to Spend on Security in 2021...

Adam Crawford
VP, Managed Services

"I would buy a packet of TUMS… Then with the money leftover I would invest in a Security or Vulnerability Management Workshop before jumping into an expensive, complex security tool or service engagement. Workshops are a great way to set priorities and provide visibility based on your business goals, cyber maturity, security controls, and risk profile."

Eric Cowperthwaite
VP, Professional Services

"I would prioritize Identity & Access Management, because in many organizations there's a lot of work to be done there. If you already have a robust identity program, which some do, then I would put that dollar into supply chain risk management. As we saw with the events of last year, when handled correctly you get a huge multiplier on that investment."

Doug Chin
VP, Identity & Access Management

"As a CISO, I would look at outsourcing security operations to a Managed Services provider. Instead of hiring for specific skillsets or responding to security incidents, this allows my team to focus on forward thinking such as establishing better controls and policies across the organization, managing shadow IT, and enabling the workforce. "

Robert Herjavec
Founder & CEO

"That dollar is best spent on visibility. A lot of organizations don't want to see everything, because they know they can't fix it all. But understanding what your business looks like from the eyes of an attacker, is critical. Put yourself in a position where you know your vulnerabilities, know the risks, and know what the exposure of the organization looks like."

> I like to think of Vulnerability Management as a camera, taking a snapshot in time. You take your picture, understand the scenario, prioritize what needs to be addressed and then later on, take another picture.

and preventative controls to help build strategies that effectively secure and protect the environment from malicious actors.

Red Team Operations in comparison are more complex, take more time and can be considered a more thorough exercise to proactively uncover weaknesses in control. They are typically objective-oriented, with the goal of gaining access to a specific folder or set of data, pre-determined by the client organization.

In order for any red team exercise to be successful, it is critical that only the key stakeholders at the client organization are aware of it. The rest of the IT and security teams must believe that the red team operation is a real adversary so that they can respond and defend their networks accordingly.

Herjavec Group believes balancing all three assessment types is critical and recommends adhering to industry specific requirements in terms of the cadence of your scanning and penetration testing practices. As we look forward, we foresee enterprise security mirroring the continuous improvement approach of Dev Ops, and Application Development. In fact, many next generation endpoint providers are already offering continuous monitoring at the device level. The argument that continuous monitoring and escalation offers greater visibility and threat detection versus a "snapshot" in time is sound, but should not change your practices entirely, as you continue to follow verticalized regulations and policies.

As you move to a model of continuous improvement, it is imperative that synergies exist between your Vulnerability Management Service, any Penetration Test or Red Team Operations outputs, your Security Operation Center service (SOC), and your Managed Detection and Response ability. We encourage you to align with your SOC operation, and/or existing service providers to log the appropriate engagement specific scans and data in order to ensure detection, assessment, investigation, and resolver group initiation of potential vulnerabilities before they become security incidents.

MITRE ATT&CK Framework

The Benchmark for Continuous Improvement

One means of measurement recognized industry-wide is the MITRE ATT&CK Framework. We view this as the benchmark for Continuous Improvement and encourage our enterprise customers to leverage Threat Modelling exercises against this framework to identify existing tool capabilities and gaps that need to be addressed, based on their log source coverage.

The objective is for you to assess your current detection and response capabilities against the threat vectors most commonly targeting your business and your industry peers.

Herjavec Group's Threat Modelling Approach involves:

- Identifying current tool capabilities
- Revealing gaps in coverage and ingestion based on MITRE ATT&CK Framework
- Developing strategic tool & risk based process plan
- Updating the enterprise capabilities on go forward basis

Following this exercise, you will understand your current detection ability, your available detections that are not currently logging, and any other existing gaps, in comparison to the prioritized threats your enterprise is facing. From there, we build a plan for continuous improvement that includes:

- Content development alignment
- Custom business specific use cases
- Log source coverage
- Technology investments
- Security service roadmap planning
- Continued maturity assessment against MITRE

Threat Modelling against the MITRE ATT&CK Framework has been a powerful measure of an enterprise's security posture. It translates extremely well into a board level presentation with clear, measurable outcomes and a proposed plan that includes technology, process, people and service needs. Once it is completed, progress against the framework can be evaluated quarterly, with the sole objective of measuring how far the needle is being moved forward, as we work to continuously improve the enterprise's security posture.

ASK YOURSELF

- ☐ If a new device appeared in my environment, how quickly could I discover it?
- ☐ Do I have a testing, diagnosing, and treatment plan for all devices coming back to my enterprise network?
- ☐ Do I have a Vulnerability Management Service in place? How frequently am I performing Penetration Tests and Red Team/Blue Team Operations? Am I meeting industry guidelines?
- ☐ Have I engaged my Managed Security Services provider to support the Threat Modelling of my detection and response capabilities?
- ☐ How am I benchmarking my organization's threat detection and response capabilities? How am I communicating this to my executive team and board?

HERJAVEC GROUP

Herjavec Group has been recognized as one of the world's most innovative cybersecurity operations leaders, and we excel in complex, multi-technology environments. We offer products and services to keep enterprise organizations secure while we help solve the industry's greatest challenge – a severe cybersecurity labor shortage. With 5 global Security Operations Centers, emerging technology partners and a dedicated team of security specialists, Herjavec Group is well positioned to be your organization's trusted advisor in cybersecurity.

Herjavec Group understands that technology alone cannot prevent today's cyber attacks. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity Services, Managed Security Services, Threat Management, and Incident Response.

MANAGED SECURITY SERVICES

- SOC Operations
- Managed Detection & Response
- Security Technology Engineering
- Threat Management
- Managed Phishing
- Vulnerability Management
- Incident Response

PROFESSIONAL SERVICES

- Security Workshops
- Advisory Services
- Privacy & Compliance Services
- Identity & Access Management
- Technology Architecture & Implementation
- Security Assessments & Testing

Recognized Industry-Wide

LEADER IN MANAGED SECURITY SERVICES — CYBER DEFENSE AWARDS

SECURITY COMPANY OF THE YEAR — CDM CYBER DEFENSE MAGAZINE

SECURITY SERVICES LEADER — IDC Analyse the Future

BEST IAM SERVICE — CYBER DEFENSE AWARDS

4 ON THE — MSSP Alert TOP 250 MSSPs

TOP HEALTHCARE CYBERSECURITY PROVIDER — FROST & SULLIVAN

Accelerate Your Cybersecurity Journey

- **COMPREHENSIVE SECURITY EXPERTISE**
  We offer Advisory, Implementation, Identity, Managed Security & Incident Response Services.
- **100% CYBERSECURITY FOCUSED**
  We are laser-focused on security & recognized as one of the world's most innovative cybersecurity players.
- **UNBIASED, VENDOR AGNOSTIC APPROACH**
  We partner with best of breed technology providers and are on the pulse of emerging technology trends, to design and protect your security stack.
- **SPEED & AGILITY IN MULTI-TECH ENVIRONMENTS**
  Our cyber experts support the world's largest banks, gaming companies and utility providers - offering customized and flexible solutions.
- **GLOBAL APPROACH WITH CROSS CLIENT LEARNINGS**
  We have expert knowledge of regional and industry directives. Threat intelligence and data enrichment across industry & region benefit our global clients.