Protecting Major Events: An Incident Response Blueprint

By: Jerzy ‘Yuri’ Kramarz & Dr. Giannis Tziakouris

Updated October 15, 2024

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

Incident response (IR) readiness for major events — such as sport championships or political summits — requires long-term strategic planning on various organizational levels ahead of time to ensure the event is prepared for any cybersecurity scenario.

Organizers need a detailed plan to ensure they are prepared to handle several types of attacks before, during and after the event.

Cisco Talos Incident Response (Talos IR) has identified 13 focus areas that could help organizations and the geographic regions that host these events build appropriate security strategies ahead of time.

Organizing the cybersecurity of major events, whether they are related to sports, professional conferences, expos or inter-government meetings can be a time-consuming undertaking. It necessitates a multifaceted approach and the involvement of multiple entities, including the organizing committee, vendors, hospitality teams and service providers, to facilitate a uniform approach to cybersecurity across the event. Talos IR has successfully participated in several global events at the forefront and in supporting roles to ensure that events are secured, and threats are contained before causing any major disruptions.

BUILDING A SECURE ECOSYSTEM

Talos IR identified 13 areas of focus that typically need to be assessed and understood in preparation for effective cybersecurity by the hosting region's businesses and government agencies before any major event. These focus areas are not restricted to protecting the events' venues or organizational bodies but should also be considered for the broader ecosystem connected with the hosting regions. Core private and public entities working with key supply chains, businesses or utilities such as water, electricity, traffic management or public transportation all play a key role in the overall security of an event so this whitepaper is also applicable to them.

For each of the 13 identified areas, Talos IR provides a short checklist to ensure that different organizations and committees can ask the right questions to vendors, suppliers and other event participants. Although the checklist can serve as a useful starting point for most of our readers, the complexity of the problem and the diverse need of security requirements might require an in-depth analysis to identify all risk avenues. Talos IR also suggests that each of the areas should be assessed through simulated exercises like hypothetical tabletop scenarios prior to a major event taking place. This will help identify and address any gaps or limitations in advance and allow for able time to address any observed issues.

1. ATTACK SURFACE AND ASSET MANAGEMENT

One of the key aspects that organizations need to identify ahead of any major event is the attack surface exposed by applications, hosts and other devices that might be visible to adversaries looking to gain a foothold in the environment.

The attack surface exposed by internal and external systems will determine the likelihood and associated impact of a potential compromise.

A less obvious but crucial part of the environment that needs to be protected is the access granted to fan zones, vendor networks and generic hospitality entities supporting the event.

Risk is often introduced to organizations when they enable access to third parties, who themselves might also have other suppliers who could be compromised. They are also exposed when extending the network perimeter to greenfield operations to enable event operations. As such, detailed asset management, attack surface discovery and strict management over the network perimeter need to be executed in a controlled manner to reduce the risk of compromise through trust relationships granted during preparation for the event. Key considerations for this section are:

- Do we understand the exposed attack surface and key assets and processes that we are trying to protect?
- Do we have a map of internal and external assets that will become part of the event? Is there a priority assigned for these assets in the event of recovery?
- Do we know potential attack paths that adversaries might leverage to achieve their goals?
- How would we identify if an asset is actively exploited with our current logging and detection mechanisms? When was the last time we tested our detection capability?
- Do we know how to identify vulnerable components of the event hosting infrastructure? Did we do a penetration testing or other type of detailed assessment on the infrastructure and applications? How about code reviews for critical applications and functionality?
- Do we have any responsibility for third-party networks (i.e., vendors/hospitality partners)? Do we understand how these networks are connecting to the environment we are defending, and would there be any impact in an event of compromise?

2. NETWORK-BASED INTRUSION DETECTION, WIRELESS AND INTERNAL NETWORK SEGMENTATION

Another important aspect of cyber defense lies in the ability to identify potentially suspicious network traffic between the devices connected within venues, building control systems, generic IT, any other OT/ICS devices, and any other greenfield operations deployed. It is therefore recommended to ensure a network intrusion detection system (NIDS) is positioned at the choke point of the various segmented networks to maximize visibility into network traffic. Wireless networks typically deployed in fan zones and hosting venues should be segmented away from primary hosting infrastructure and monitored to ensure cybersecurity of the attendees. Client isolation is also a helpful feature that should be applied across wireless networks to stop adversaries from attempting to subvert other clients on the same network. Zero-trust architecture, segmentation and firewalling should be applied across the various organizations supporting the event and in the different venues that are part the of overall hosting infrastructure. Finally, the systems responsible for transmissions (satellite dishes, broadcasting equipment and other devices) need to be segmented away into control rooms to ensure uninterrupted network access. Key considerations for this section are:

- Do we know the network boundaries and network choke points within our environment?
- Do we have sufficient visibility and coverage to identify all networking assets?
- Do we know how our networks are segmented? Are we following principles of zero trust to segment away fans, key control, broadcast systems and venue controls?
- How do we plan to enable greenfield operations teams to access our resources during the event? Is this access secured and segmented to only specific applications?
- Do we have well-positioned detection devices in our environment that could detect command and control (C2) or adversary traffic?

3. REMOTE ACCESS, ADMINISTRATION AND LOGGING

Administrators and other key personnel might need access to critical assets and devices to enable operations, recovery and event broadcasting. As such, it is quite common for key staff supporting the event and wider IT operations across venues or supporting organizations to have high permissions on the equipment that venues, broadcasting centers or ticket systems deploy. Although a change freeze is typically enforced just before and during the event, it is important to log all the administrative actions so they can be reviewed by the Security Operational Center (SOC) team. This could include changes to GPO, key configuration files used by various applications, and security devices. Even simple integrity checks using various hashing algorithms such as SHA256 could be an effective way of tracking if any changes were introduced to the key configuration files. This is an important precaution for operational technology (ICS/OT) devices which often relies on configuration files to execute a sequence of checks across critical infrastructure. In a worst-case scenario, a tainted configuration file could result in unexpected behavior. Key considerations for this section are:

- Are we logging administrative actions? If so, how long are these logs stored and are they presented in a usable format?
- How often do we review performed administrative actions and can we identify anything that stands out from normal operations?
- Do we know if key configuration files for IT, ICS/OT, broadcast equipment and any other IOT devices were changed in the last 90 days?
- Have we observed any changes in device behavior or configuration during change freeze?
- When an administrator needs to access a high-privileged system, what security controls are in place to stop an adversary from having that access? Do we use Multi-Factor Authentication (MFA) or certificate as an additional authorization method?
- Do we correlate different logs to ensure a holistic understanding of different events and suspicious activities?

4. SECURITY AWARENESS TRAINING

Although copious amounts of money can be spent on state-of-the-art security tools, subject matter experts, and technology, security is as strong as its weakest link, which

is usually the end users. Adversaries are aware of this and often employ techniques such as social engineering (e.g., phishing, vishing, etc.) to target users and gain an initial foothold in an environment. As such, the organizing committees of major events need to ensure that key stakeholders and users remain vigilant and have in-depth knowledge of how to identify threats and operate in a secure and safe manner. Such awareness trainings need to be initiated at least one year before the start of an event to ensure that users have ample time to familiarize themselves with the best security practices for identifying and reporting suspicious activities such as phishing, vishing or baiting. Among other activities, it is critical that users and key stakeholders participate in different simulated attack scenarios that provide a better understanding of possible attack vectors. Internal phishing and vishing tests should be performed to assess the security awareness with timely feedback for potential improvement. Finally, users with high-level permissions should be trained in regular intervals on the potential cyber threats they could face. Key considerations for this section are:

- When was the last time we trained our employees on phishing, vishing and other types of social engineering attacks?
- Do we provide continuous security awareness training of users and key stakeholders?
- Do we have any metrics that can serve as a point of comparison for the performance of users and key stakeholders concerning security training progress?
- Do we have different security training courses for different users based on their technical expertise and capabilities? What about third parties that might operate on event infrastructure?

5. ENDPOINT PROTECTION AND HARDENING

At the core of the defense against adversarial activity is visibility into endpoints. If a new process is started, the SOC needs to see the command line, arguments and permissions of the user who started the process. A large percentage of infrastructure coverage should be reached with security products such as anti-virus (AV) or enterprise detection and response (EDR) solutions. The higher the percentage of coverage, the better chance an organization must detect adversarial activity that could affect the systems or serve as a prelude to wider compromise. With that comes the need to configure existing security stack to ensure optimal protection. Where possible, heuristics should be enabled in AV solutions to ensure optimal detection of new and emerging threats and other security options explored to ensure the best possible configuration of security products. Different operating systems come with their own protection mechanisms (e.g., SELinux, Windows Defender, various memory protection methods) which should also be integrated into the overall endpoint defense strategy.

With the deployment of security tools and increased visibility, hardening against common standards such as CIS should be considered to make sure that there are not easily exploitable vulnerabilities and misconfigurations that would give an adversary leeway to perform other attacks on the endpoint. Password management software and secure rules for login credentials should be set to a common secure standard to ensure that brute-force attacks and other related attacks are not easily performed. If systems are deployed in a cloud environment, consider hardening these deployments too, especially if you are hosting infrastructure there. Finally, deploying an MFA for key and critical servers and applications can be a straightforward way to hamper access to systems without explicit authorization.

The aforementioned activities might be straightforward to implement in conventional environments but put in the context of a major event, they make for a complex undertaking. It is not sufficient to perform such activities solely on the assets of the organizing team. Contractors, vendors and other external parties must also follow the same guidelines to ensure uniform security. Key considerations for this section are:

- What security standards do our suppliers, vendors and hospitality managers follow?
- Do we have a common hardening standard on our devices, based on guidance such as CIS?
- Do we enable new built-in memory protection mechanisms on our devices that could stop adversary exploits from working?
- What is the visibility into our infrastructure? Are EDR, AV and other security tools deployed across endpoints, servers and cloud devices?
- Do we have a list of allowed software and can we identify devices which have unapproved/unauthorized software installed?
- Is it possible to quickly access endpoint security tools remotely and are there the suitable dashboards to easily identify and manage threats? Can the same dashboards and access be leveraged to execute a threat hunt?

6. DATA STORAGE AND ACCESS PROTECTION

Attendees, country visitor, passports and ID data are considered prime targets for any type of threat actor, and as such, great efforts must be made to secure these assets. This is especially valid for large events which typically require registration, often including sensitive information, such as passport numbers and ID details, to issue a ticket. A starting point of securing this type of data is to ensure that they are stored securely at rest (storage) with strong encryption algorithms, such as AES-256, but also in transit via encryption over a secure medium (e.g., TLSv1.3). If there are financial limitations and it is impossible to perform the above for all data, priority should be put on personally identifiable (e.g., attendee, staff, collaborator data), confidential and sensitive data. In addition, it is imperative that only vetted authorized personnel can access such data to avoid the misuse of privileges. The number of administrators (e.g., local admin and service accounts) in the environment should also be minimized based on the need to know and least-privilege principles.

Recording detailed logs is necessary for enforcing security to ensure the quick identification of unauthorized access. Logs should, at a minimum, capture data modification, data creation and data deletion, access time and duration, and account that was used to access the data along with source IP address. In addition, cameras and smart gates should be installed in critical areas such as server rooms so the SOC can monitor physical access to key devices. That said, awareness needs to be raised around the use of these technologies where they can expose internal information. For example, a camera overlooking the screen of a system containing sensitive information could allow a remote

adversary to extract system details that can be used for further attacks.

Finally, MFA should be utilized through the environment (or at least to all systems storing sensitive data) to attest to the identity of the user and eliminate cases where an attacker is attempting to access data with stolen credentials. Key considerations for this section are:

- How is our data storage secured from third-party access?
- Do we store personally identifiable information (PII) on our servers? How are we going to dispose of this data after the event?
- Do we encrypt data at rest or use column-level encryption solutions for the databases?
- How would we plan on dealing with requests for data removal after the event is over? What is the planned retention length of different data types?
- Do we have a good handle on what physical controls are deployed in various venues? Are these controls positioned in such a way that they wouldn't disclose sensitive information if compromised?

7. INCIDENT RESPONSE

Significant effort is required to ensure sufficient readiness to respond to emergencies. On the strategic side, an IR plan describing elements such as key stakeholder responsibilities, action plans, communication strategies and overall governance of the IR lifecycle, is necessary. IR Playbooks focusing on responding to specific types of threats such as ransomware, DoS or phishing should be clearly presented and provided to the SOC and IR. This will ensure the security practitioners that are part of the event can effortlessly use them as pre-approved guidelines when responding to threats inside their organizations and across various coordination centers. At minimum, IR playbooks containing procedures for the top three major incidents need to be present and available to responders and the wider IT staff.

Poor log coverage and quality, together with restricted visibility into the environment, have major effects on the speed and quality of response. Therefore, based on the threat model and threat landscape, sufficient logging should be put in place to ensure that the SOC and IR analysts are able to quickly identify a threat and perform the needed analysis to identify the root cause and potential impacts of a threat.

In terms of tactical planning, several well-trained Incident Responders and SOC analysts are required to monitor and effectively respond to any observed threats. Such employees need to not only be granted access to the venue and event data, but also to the systems of various hospitality vendors taking part in a major event to ensure holistic coverage and response to threats. It is also imperative that tested and verified forensic tools are readily available for the IR team to use in case of emergencies. The list of such tools typically includes forensic collectors for creating disk images and memory dumps, scripts for automated extraction of specific artefacts, forensic software for the analysis of forensic artefacts, etc. Where possible, SOC and IR activities should be automated (e.g., extraction of IPs or hashes from large log files, etc.) to ensure effective response. In cases of containment and eradication of large numbers of compromised systems, it is essential to be able to access such systems remotely and, if needed, push system changes on a large scale. Due to the implications of such massive remote access change, all actions performed with such high privileges should be logged. Finally, coordination with external bodies such as the Computer Emergency Response Team (CERT), national, security vendors and digital crime units is necessary to ensure that, in case of a critical emergency, the internal team can contact such organizations for emergency assistance. Key considerations for this section are:

- Do we have an IR Plan and IR Playbooks that cover a variety of scenarios that might be expected during large events?
- When was the last time we reviewed and tested our IR plan?
- Do we have contact details for the Internet Service Provider (ISP), national CERT and other vendors or public bodies we might need to contact to initialize some of the response steps? Where are these contact details saved and are they accessible to key staff? Who is authorized to request their services?
- Are our key employees aware of the IR plan and response procedures? When was the last time they were trained through a tabletop exercise?
- Can we deploy forensic collector software across multiple hosts and servers during the incident? Is there a tested and pre-approved method of doing so?
- Do we have cross-functional teams who can quickly triage specific cases to identify the root cause of an

incident? Are our tiger-teams working together and in good sync under management of incident commanders from different organizations?

- When was the last time that we had an assessment of our IR capabilities and processes via tabletop exercises or IR readiness assessments to ensure effectiveness of IR?

8. RISK MANAGEMENT

Risk management is a significant part of addressing security threats in a proactive fashion, especially in the setting of major, global events. A good starting point is the adoption of international, industry-leading standards such as NIST or ISO27001 across an organization. If an official certification process is not planned by the organization, at a minimum, required policies and procedures derived from these standards should be created for risk management. Such procedures should also include the risk for third parties and vendors accessing internal networks, given the unique environment of major events where many collaborators and attendees are introducing their own devices (e.g., mobile phones, point-of-sale devices, laptops, cameras, routers, communication devices, etc.) in their environment. Finally, as part of the wider risk management process, an investigation into cybersecurity insurance policies and procedures should be conducted with the internal legal team to ensure that, if insurance is purchased by the business, all the required frameworks are adhered to. Key considerations for this section are:

- Which cyber risk management framework are we following?
- When did we execute a threat modelling exercise to identify what risk management strategies should be deployed in different environments required when hosting large scale events?
- Which documents describe our defined baseline security standards that our organization should follow even if not certified by external bodies?

9. BACKUP AND RESTORE PROCEDURES

Backups can play a crucial role during major events in cases of high-severity attacks that can shut down critical services, such as broadcasting equipment, security systems, building management systems or any other standard IT devices. In such situations, a pre-configured golden backup image will speed up the recovery of key systems. In addition, backups of critical equipment (e.g., servers, databases) should be easily retrieved and readily available. Such copies should be stored safely in isolated environments both offline (cold storage) and online (hot storage) on a separate network. This guarantees redundancy and diminishes the risk of a potential loss or manipulation of backups in the event of an attack.

Furthermore, backups need to be tested regularly to ensure they are usable and virus-free. Attackers often purposefully infect backups as a last resort backdoor, which would re-introduce the threat to the environment. For the same reason, recovery operations should be conducted in a separate network zone which separates hosts that have been restored and confirmed to be clean of infection from newly restored and yet to be observed hosts. If the latter are reintroduced to the product environment too quickly, without ensuring the correct operation and health of the machine, this can lead to reinfection. Key considerations for this section are:

- How are our backups connected to the network? Are they offline or online?
- When was the last time we tested backup and restore procedures?
- What is the order of priority for backup and restore procedures? Do we have sufficient hardware and software to support the restoration process? Are our backups compatible with various hardware requirements?
- How often do we check if backups are not infected with malware to ensure clean recovery?
- What is our procedure to restore systems into an isolated network ahead of reconnection to the main network? Where is this procedure documented and is it tested at regular intervals? Can other vendors initialize system isolation too?

10. THREAT INTELLIGENCE AND AUTOMATION

The effectiveness of readiness and response speed is directly tied to the degree of automation implemented in core cybersecurity tasks, such as threat detection and isolation. For a robust defense strategy, it is essential to prioritize automated threat detection and intelligence. Technologies like Security Orchestration, Automation, and Response (SOAR) or data lakes can significantly enhance these efforts by processing critical information from threat hunting and detection perspectives. However, automated platforms require thorough optimization to develop processes that can be executed upon successful threat detection. Additionally, detailed detection engineering is necessary to identify key data points and visibility constraints that shape the overall automation process.

In terms of threat intelligence, it is crucial that the collected data is effectively processed and easily accessible to key security systems, aiding in detection and response while avoiding the common pitfall of underutilized intelligence. Important considerations for this section include:

- Do we have a threat intelligence feed which can be used, together with automated solutions, to speed up our detection and response? Is it usable and actionable by our automation platforms or SOC teams? When was the last time this integration was tested?
- Can we collect and process internal and external indicators of compromise (IOCs) coming from researchers, internal threat hunting platforms and third-party providers? How will vendors and third parties report their own threat intelligence to our organization?
- How often do we review our existing SOAR playbooks? Are our playbooks still up to date and do we consider the latest datapoints and threat intelligence?
- How can we detect tactics, techniques, and procedures (TTPs) along with hash and IP-based IOCs?
- How are we going to run and execute a threat intelligence program ahead of, and during, the major event? Will the engagement model change? Is it going to be outsourced threat intelligence, or run in-house by an internal team supporting the event?
- Do we perform threat intelligence checks for our own employees and vendors? Should we check if their corporate credentials are leaked in the dark web? If so, who will organize and perform these searches?
- Is there a central threat intelligence platform that allows us to search for specific IOCs to identify any managed systems which might be affected by these IOCs?

11. MAJOR EVENT MANAGEMENT & OPERATIONS

To ensure robust security at major events, particularly those involving multiple vendors or even competitors, effective vendor management is crucial. In any major operation, it is common that many vendors come together to support an event. Some vendors will be sharing responsibilities for specific aspects of the events such as networking, Wi-Fi or security, while others might have very specific responsibilities such as badge issuance and accreditation services. Seamless communication between all teams is essential. All relevant IT and security personnel should be physically co-located to facilitate real-time communication and rapid response. Additionally, collaboration can be further enhanced by sharing a detailed contact list that includes names, photos, company affiliations and key details. This ensures that requests for access, data or analysis are handled efficiently. Key security personnel, such as incident responders, threat intelligence analysts, and SOC analysts, should treat their involvement as an emergency response, maintaining 24/7 availability onsite or remotely.

Teams from different vendors should be able to work well together toward contextualizing findings and enhancing the work of others to reach common conclusions and present those to the core security team managing the security of a major event. This collaboration ensures that identified issues are smoothly handed off between vendors for further contextualization.

When determining access levels to security tools for vendors, two primary strategies can be considered. One option is to provide full access to all security tools across teams, enabling thorough investigations and incident tracking across the entire environment. This is particularly beneficial for rapid, cross-functional collaboration in addressing complex threats. Alternatively, access can be restricted by vendor, with the core security team retaining overall visibility and control. In this approach, vendors focus on their specific tools and provide insights to the core team, which integrates and completes the analysis. While this method may reduce data exposure risks, it could limit the depth of individual investigations.

Furthermore, it is vital that vendors maintain transparency across different teams regarding their security stack deployments. This includes sharing network maps, security tool lists, and coverage details to ensure a clear understanding of which vendors are responsible for which parts of the environment (IT and OT). With numerous third parties involved, organizers and participating vendors must clearly understand each other's roles and responsibilities supporting the event. They should also establish the quickest communication channels for incidents or outages. This ensures that vendors who detect suspicious behavior can promptly identify the appropriate parties and contact them for assistance and further investigation.

Key considerations for this section are:

- Are all security teams positioned for effective in-person communication? Are there lists with priorities and objectives for each team? How frequently can these objectives change?
- Are there any remote team(s) supporting and, if they are, can they directly escalate incidents or share data with the onsite team effectively?
- How is access to security tools managed, and does it support the event's overall security strategy? Are there network maps and a list of contacts with their respective coverage distributed to relevant security groups?
- Are there any approved and established out-of-band communication methods and processes in place?
- Is there a template for standup meetings with simple sections such as challenges faced, action point and observations sections available for all vendors?
- Is there a culture of feedback and looping feedback back to everyone so that every vendor and personnel is aware of ongoing objectives, deliverables and overall progress of the event?
- Is the security monitoring organized in 24x7 shifts? If so, when do we organize a brief meeting to summarize actions and observations for the end of a shift? What template is used to drive this meeting and ensure that each vendor or partner presents findings and report in a unified way?
- Do we treat major events as ongoing emergency work? Does our staffing support such a model?
- Is there a list of personnel available for each shift available along with email and phone number so they can reach out in the event of incident?
- Is there an enforced mechanism on how to deal with physical threats that might be related to venues or hospitality infrastructure? What about ransom emails that might be sent to vendors or third parties?

12. UNIFIED TICKETING PLATFORM

An incident ticketing platform should serve as the central point of reference for tracking and managing all incidents across various teams and vendors. It is essential that all relevant security and IT personnel have access to this system, with strict guidelines and training on what information should be included in a ticket and how to classify the severity of different threats. A threat that one vendor can consider as critical risk may be considered medium by another, so understanding how tickets should be created, assigned and managed is key to rapid response.

When creating a new ticket, analysts should always verify that no existing ticket(s) cover the same incident by searching for relevant keywords in the platform. If there is uncertainty about whether a new ticket is warranted, consulting with the incident commander and the core security team overseeing the event is advisable, to avoid unnecessary activities involving opening a ticket, validating the information and closing the ticket.

Lastly, given the sensitive information stored within ticketing platforms, robust security measures must be put in place. Multi-factor authentication should be strictly enforced, and access to the platform should be limited to authorized personnel only.

Key considerations for this section are:

- Is there an incident ticketing platform accessible to

all relevant security stakeholders for reporting and tracking incidents?

- Are all security stakeholders trained in the platform's use, with clear guidance on threat severity and ticket handling? Do they know how to log tickets, who should be assigned, or which team will perform follow-up triage on the ticket to ensure that findings are identified?
- Is the incident ticketing platform adequately secured with solutions such as MFA?

13. THREAT HUNTING-CENTRIC APPROACH TO SECURITY

Fostering a proactive threat hunting culture among cybersecurity personnel offers significant benefits. Regularly scheduled threat hunts for simulated threats of varying types and severity can build synergy among security team members and vendors. This ensures that when a major event begins, all teams are equipped to collaborate effectively, are familiar with the tools and hunting methodologies, and can correlate data across different vendors and security solutions.

Proactive threat hunts also allow security experts to identify visibility gaps or weaknesses in security measures, enabling them to address these issues before the event starts, ensuring comprehensive security and visibility. Starting a threat hunt a few weeks before major events take place can root out any problems that may arise with visibility or technology gaps.

Frequent threat hunts also cultivate a mindset of continuously searching for threats, a mentality that carries over into the event itself, with analysts maintaining vigilance and applying the same rigorous checks during the event.

Key considerations for this section are:

- How frequent should proactive threat hunts be conducted? What will be the objectives of the threat hunt?
- How will different vendors participate in the treat hunt if their systems might be a subject to the exercise? Will they need to provide special consent to perform an extended threat hunt across their estate?
- Is there a system in place to document successes and identify gaps, and are there processes for addressing these gaps before the event takes place?

ACHIEVING YOUR GOALS WITH CISCO TALOS INCIDENT RESPONSE

One of the key elements of the IR lifecycle is the preparation phase. During that phase, Talos IR aims to understand the long-term objectives, technology and security stack of the customer and the core business functions and assets that should be defended from adversaries. By understanding the core business and its operations, Talos IR can tailor engagements and deliverables to match the overall strategy that organizations and regions seek to achieve regarding cybersecurity for major events.

Typically, Talos IR begins by defining the attack surface exposed by event preparation and the various organizations and their role in the event. At this stage, Talos reviews the current policies and procedures that govern the participating organizations and supply chain vendors with the appropriate stakeholders. Starting from attack surface discovery through technical assessments, such as penetration testing and red & purple teaming, Talos IR uses these engagements to understand what security controls are missing or can be bypassed, and what are the potentially exploitable vulnerabilities that can cause an incident during or before a major event.

These engagements assist in better identifying exposed infrastructure or process gaps that might result in adversaries gaining a foothold within an organization by exploiting vulnerabilities. The next step in the event preparation journey would typically involve the completion of Talos Incident Response Readiness Assessment (IRRA) which determines the maturity level of an organization and maps weaknesses from people, processes and technology stacks against industry standards. While this service will not identify vulnerabilities, it will help identify process gaps

that can be addressed. In combination with a technical assessment, the IRRA contributes to the creation of a detailed image of the organization's security posture.

These first two steps would typically allow Talos IR to gain insight into the technical and procedural gaps that hosting organizations might have, and based on the results, establish an improvement roadmap. Such roadmaps often take a few years to complete and require a high degree of collaboration between Talos IR, Cisco and our customers to ensure well-informed, precise execution of the plan even when additional services and capabilities are introduced within different businesses supporting major events. Leading up to the event, Talos IR would typically shift focus to execution of a threat hunting and compromise assessment exercises to identify any adversarial activity across entities supporting the event, along with testing operational security through tabletop exercises to ensure that various teams are primed for incident handling. Talos IR has successfully delivered this model across several organizations participating in global events.

RISKS EXPECTED DURING MAJOR EVENTS

Over the years, Talos IR participated in several events across the globe and observed that some adversarial activity themes largely repeat themselves regardless of the event size or location.

Primarily, all kinds of malware can be expected in various forms such as malware on mobile phones, laptops and other devices carried by fans and attendees. In terms of malware attacks, Talos IR would anticipate two major types, namely ransomware and trojans. Ransomware attacks would aim at disrupting the availability of high-profile systems and key control devices, hence capitalizing such activities, whereas trojans would target gathering and potentially retaining access to key systems. Some adversary activity will be opportunistic in nature by targeting any system which can be found in relation to hosting organizations while other adversary activity might be targeted against systems exposed to the Internet to infiltrate the DMZ and move laterally across organization. This behavior is exemplified by the Olympic Destroyer malware example. Trojan-based attacks would typically start months ahead of the events to ensure that targeted environment is primed for adversary access and access can be sold via an initial access broker (IAB).

The second most common attack vector is denial-of-service (DoS) on government infrastructure (including critical infrastructure such as airports, electricity, transportation, or rail operations) or event infrastructure such as application programming interface (API) points used by mobile applications in ticket-taking operations. It is quite typical of major events to be targeted, with the goal to cause disruption to the event.

Finally, cyber criminals are expected to increasingly target visitors, athletes, or event officials via phishing and social engineering attacks to defraud or steal sensitive information related to the event or individuals.

Finally, the risk of remotely distributed and exposed internet of things (IoT) devices that can be disrupted by adversaries is a major security concern and has been seen as a threat in various global events.

LAST-MINUTE ADVICE

While drawing near to the start of the event, there are several steps that can be taken to better assess the external attack surface like performing a formal asset discovery. This exercise should highlight the systems that must have high availability and the potential impact in the case of a DoS or any other attack that would render such systems unavailable. The list of the identified critical assets and related risks will play a significant role in preparing an appropriate mitigation plan.

In addition, an assessment of an organization's most vulnerable systems from an adversary point of view should enable the SOC and IR teams to better anticipate any malicious activities and potential attacks. Such an assessment can take place by reviewing network diagrams, business products sites, public IP addresses, exposed Network address translation (NAT) addresses, database lists, system hosting details, IP Address Management (IPAM) and other available data sources.

Another action that organizers can do shortly before the start of the event is assess the impact of DDoS/DoS attacks on back-end systems such as databases, routers, and switches to determine the business impact. The findings should be used to draw a dependency tree and data flow mapping between exposed infrastructure and various back-end systems, and to understand the worst-case scenario in a potential cyber-attack. This mapping exercise should allow an organization to better understand the impact of a potential

full-scale attack and warrant better preparedness.

Weak systems that can become a single point of failure should be identified. Based on the previous steps of identifying dependencies and dataflow mappings, ensure that any systems identified as a single point of failure can be brought up from backup whenever needed. Test backups and restore procedures before the event to ensure easy restore. Where feasible, create a long-term strategic plan to migrate systems deemed as a single point of failure to a more resilient state.

Ensure that administrative actions performed against either IT or OT/SCADA devices are logged so that a quick triage of activities executed in the environment can be performed by the operational teams. The speed of response will often make a difference between being online and offline during a critical in-country event. Other network traffic records such as NetFlow can also be quickly reviewed to identify any signs of access to critical environments or attempted exfiltration.

If not in place already, establish a chain of command and escalation paths within the organization and external vendors supplying IT and OT systems. By establishing clear war room-like teams, the efficiency of communication is improved and, as a result, incident handling is faster. In many cases, there is also a need to coordinate some of the response steps with cybersecurity regulation bodies such as national CERT teams to comply with local regulations, so knowing their contact details and how to report an incident might need to be part of an overall incident response plan.

Ensuring that a few basic security measures are taken across an environment can play the catalyst between a fully compromised environment and a small compromise isolated to only a few systems. Environments that have a good network segmentation, MFA and low user privileges running on some key services such as web applications tend to pose a greater challenge to adversaries who attempt to execute malicious code or perform lateral movement.

POST-EVENT

Even after a major event has finished, cyber criminals will still target key stakeholders and digital assets used for the event. In fact, some adversaries will see this as an opportunity to launch an intensified attack as the risk of getting detected after an event is significantly lower due to more relaxed security measures.

Therefore, it is imperative that a similar effort in cybersecurity is made after the event's completion and maintained until all critical digital assets and sensitive data associated with the event have been dismantled safely and stored offline. As long as critical digital assets are in operation and sensitive data is in transit between different stakeholders, security measures and monitoring of such systems and data should remain vigilant for any IOCs or anomalous behaviour. A 90-day post-event monitoring of systems should be sufficient to identify any signs of malicious behaviour and attempted access to key data.

