INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-23 06:27 UTC

Verizon DBIR 2026: Vulnerability Exploitation Overtakes Stolen Credentials as Top Breach Entry Point

SECURITY ANALYSIS | CRITICAL

SCC Item ID	SCC-STY-2026-0153
Type	Security Analysis
Severity	CRITICAL
Affected Products	Industry-wide, no single product; all sectors with unpatched external-facing systems
Published	3 days ago
Discovery Source	Serper

Executive Summary

The 2026 Verizon Data Breach Investigations Report marks a structural shift in the threat landscape: vulnerability exploitation has overtaken stolen credentials as the leading initial access vector in confirmed data breaches for the first time in the DBIR's 19-year history. This finding signals that organizations relying on identity controls as their primary defense posture are now exposed to a gap that perimeter and endpoint controls must close. The convergence of AI-accelerated attack tooling with persistent patch management failures compresses disclosure-to-exploitation timelines that most security programs are not operationally designed to absorb.

Technical Analysis

The 2026 DBIR represents a measurable inflection point. For nearly two decades, stolen credentials held the top position among initial access vectors in Verizon's breach dataset, which is one of the largest empirical collections of confirmed breach data in the industry. This year, that ranking flipped: exploitation of public-facing applications (MITRE ATT&CK T1190) and client-side exploitation (T1203) collectively outpaced credential-based entry. The third technique flagged, software deployment tool abuse (T1072), reinforces that trusted internal channels are increasingly weaponized once external footholds are established.

The mechanism driving this shift is not new; it is the acceleration of known dynamics. Threat actors are operationalizing publicly disclosed CVEs faster than most organizations can test, approve, and deploy patches. The DBIR specifically identifies AI-driven attack tooling as compressing the window between vulnerability disclosure and active exploitation, which removes the informal 'patch grace period' that many patch management programs are implicitly built around.

Critical infrastructure sectors received specific callout in the report, with exploitation of unpatched external-facing systems enabling attackers to bypass perimeter controls entirely. This is consistent with patterns observed in CISA advisories from 2024-2025, where edge devices, VPN concentrators, firewalls, and industrial remote access gateways were targeted because they sit outside standard endpoint detection coverage and often run software on extended patch cycles.

The defensive gap the report exposes is not purely technical. It is operational: patch prioritization workflows that treat CVSS base scores as the primary risk signal are systematically under-responding to actively exploited vulnerabilities. CISA's Known Exploited Vulnerabilities catalog exists precisely to address this, but adoption as a mandatory prioritization input remains inconsistent outside federally regulated environments.

The AI-acceleration finding deserves specific attention. The DBIR does not claim AI is writing novel exploits from scratch; the more precise threat is AI-assisted reconnaissance, payload customization, and scaling of exploitation attempts, compressing the human labor cost of running broad exploitation campaigns. This changes the economics of opportunistic exploitation, making it viable against a wider target set than before.

Action Checklist

1. Step 1: Assess exposure, audit all external-facing systems (VPNs, firewalls, web application servers, remote access gateways, OT/ICS remote interfaces) for unpatched CVEs; cross-reference your open vulnerabilities against the CISA KEV catalog as the primary exploitation-confirmed prioritization signal
2. Step 2: Review patch management SLAs, if your patching timelines are driven by CVSS base scores alone, recalibrate immediately to use CISA KEV status and EPSS scores; establish a maximum 72-hour remediation SLA for any vulnerability appearing on the KEV catalog (NIST SI-2: Flaw Remediation; CIS 7.1, 7.2, 7.3, 7.4)
3. Step 3: Verify perimeter detection coverage, confirm EDR and network monitoring extend to edge devices and external-facing infrastructure; exploitation at T1190 frequently occurs in segments where endpoint agents are absent; review NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation) coverage for these assets
4. Step 4: Validate that identity controls are not your only fallback, the DBIR shift means an attacker exploiting a perimeter vulnerability bypasses credential controls entirely; verify network segmentation, least-privilege service account configurations (NIST AC-6; CIS 5.4), and lateral movement controls are functioning independently of MFA protections
5. Step 5: Incorporate AI-accelerated exploitation timelines into your threat model, update your incident response playbooks to reflect compressed disclosure-to-exploitation windows; the assumption that you have days to patch after a CVE is published is no longer operationally safe for critical-severity externally-facing flaws
6. Step 6: Communicate findings, brief leadership with the specific organizational risk: how many unpatched external-facing systems exist, what the CISA KEV overlap is, and what the business impact of a successful exploitation event would be; avoid generic 'patch faster' framing in favor of asset-specific risk language
7. Step 7: Monitor DBIR supplemental releases and CISA advisories, Verizon typically releases industry-vertical supplements post-DBIR; track for sector-specific findings relevant to your industry and correlate with any new KEV additions

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and initiate your IR plan immediately if: any KEV-listed CVE is confirmed unpatched on an external-facing asset AND anomalous inbound traffic, unexpected process execution, or new admin account creation is observed on that asset within the preceding 72 hours, OR if your organization operates in a CISA-designated critical infrastructure sector and KEV overlap exceeds 5 external-facing systems.
Recovery Notes	After patching KEV-matched vulnerabilities on external-facing systems, verify integrity of those systems before returning them to production: compare running process lists and scheduled tasks against a known-good baseline, audit all local administrator and service accounts for unauthorized additions (new accounts created during the exposure window are a primary persistence indicator for T1190 exploitation), and review outbound connection logs for the 30-day window preceding patch application for signs of data exfiltration or C2 beaconing that predates your detection. Maintain enhanced monitoring on patched assets for a minimum of 30 days post-remediation, specifically alerting on process lineage anomalies (web server or VPN process spawning shells) and new outbound connections to previously unseen external IPs. If your organization has regulatory breach notification obligations (HIPAA, PCI DSS, SEC cyber rules), preserve all log evidence from the exposure window under legal hold before any system changes.
Forensic Artifacts	CISA KEV JSON snapshot (dated): timestamped download of the KEV catalog cross-referenced against your asset inventory — establishes which KEV-listed CVEs were unpatched and for how long, critical for breach window reconstruction and regulatory notification scoping | Web server and reverse proxy access logs (Apache access_log, Nginx access.log, IIS W3C logs): review for exploit payload patterns in URI paths and POST bodies (path traversal, deserialization gadget strings, template injection sequences) during the exposure window — these logs survive even if the attacker cleans up post-exploitation artifacts on the host | VPN and remote access gateway authentication and session logs: look for successful authentication events immediately followed by configuration changes, new account creation, or privilege escalation — in T1190 exploitation of VPN appliances (e.g., Ivanti, Fortinet, Cisco ASA), attackers frequently create backdoor admin accounts within minutes of initial access | Network flow records (NetFlow, Zeek conn.log, or firewall session logs) for DMZ and perimeter segments: identify any new or anomalous outbound connections from perimeter devices to external IPs, particularly on non-standard ports or to cloud hosting ranges not in your expected egress baseline — C2 channels established post-exploitation are the most reliable indicator that exploitation preceded your detection | OS-level process creation and scheduled task logs on external-facing Linux/Windows systems: on Linux, `/var/log/auth.log`, `/var/log/secure`, and auditd logs with `execve` syscall recording; on Windows, Security Event Log Event ID 4688 (Process Creation) and Event ID 4698 (Scheduled Task Created) — web shell deployment and cron-based persistence are the canonical post-T1190 artifacts that survive patch application and should be hunted regardless of whether active exploitation is confirmed

Per-Action IR Details

Step 1: Assess exposure — audit all external-facing systems (VPNs, firewalls, web application servers, remote access gateways, OT/ICS remote interfaces) for unpatched CVEs; cross-reference your open vulnerabilities against the CISA KEV catalog as the primary exploitation-confirmed prioritization signal

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing and maintaining IR capability, asset visibility, and vulnerability posture before an incident occurs

Controls: NIST SI-2 (Flaw Remediation), NIST RA-3 (Risk Assessment), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run `nmap -sV --open -p 80,443,8080,8443,4443,10443,1194,500,4500 ` against your external IP ranges to enumerate exposed services; pipe output to a CSV and manually cross-reference each service/version against the CISA KEV catalog at https://www.cisa.gov/known-exploited-vulnerabilities-catalog (download the KEV JSON feed and grep for matching CPEs). For OT/ICS interfaces, use Shodan's free tier with `org:` query to identify inadvertently exposed SCADA/HMI panels. Document results in a shared spreadsheet with columns: asset, IP, port, service version, KEV match (Y/N), remediation owner.

Evidence: Before remediating, capture your current exposure baseline as forensic evidence of pre-remediation state: export your vulnerability scanner output (Nessus, OpenVAS, or equivalent) with timestamps; download a dated snapshot of the CISA KEV JSON feed (`curl -o kev_$(date +%Y%m%d).json https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`); record firewall/WAF rule sets and NAT configurations showing which internal assets are externally reachable. This establishes the window of exposure if a breach is later discovered to have preceded remediation.

Step 2: Review patch management SLAs — if your patching timelines are driven by CVSS base scores alone, recalibrate immediately to use CISA KEV status and EPSS scores; establish a maximum 72-hour remediation SLA for any vulnerability appearing on the KEV catalog (NIST SI-2: Flaw Remediation; CIS 7.1, 7.2, 7.3, 7.4)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: policy and process readiness including documented response procedures and remediation timelines that reflect the current threat environment

Controls: NIST SI-2 (Flaw Remediation), NIST PM-9 (Risk Management Strategy), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If your patch management tooling cannot ingest KEV or EPSS feeds natively, build a lightweight triage script: download the CISA KEV JSON and FIRST EPSS CSV daily via cron, join them against your open vulnerability list on CVE ID, and flag any item with KEV=true OR EPSS>0.50 as P1/72-hour. A two-person team can implement this in Python (~50 lines) using only standard library modules plus `requests`. For EPSS scores, query the FIRST API: `https://api.first.org/data/1.0/epss?cve=CVE-XXXX-XXXXX`. Document the revised SLA policy in writing and obtain sign-off — this is audit evidence that your program reflects exploitation-reality, not just CVSS theory.

Evidence: Capture the current state of your patch management policy document (version-controlled), your open vulnerability backlog with original CVSS-only priority assignments, and the date of your last patching cycle for all external-facing asset classes. This establishes whether a KEV-listed vulnerability was already in your backlog and deprioritized under old SLA criteria — critical if a breach occurs and you need to reconstruct the decision timeline for regulatory or legal purposes.

Step 3: Verify perimeter detection coverage — confirm EDR and network monitoring extend to edge devices and external-facing infrastructure; exploitation at T1190 frequently occurs in segments where endpoint agents are absent; review AU-2 (Event Logging) and AU-12 (Audit Record Generation) coverage for these assets

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: confirming that monitoring coverage is sufficient to detect adversary activity at initial access vectors, specifically at external-facing systems where T1190 exploitation occurs before any credential use

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), CIS 8.2 (Collect Audit Logs)

Compensating: For edge devices without EDR agent support (firewalls, VPN concentrators, load balancers), verify that syslog forwarding is active to a central collector — even a single rsyslog server. Deploy Zeek (formerly Bro) on a

network tap or span port at the DMZ boundary to generate connection logs, HTTP logs, and SSL logs for all inbound traffic to external-facing assets; Zeek's `weird.log` is particularly valuable for detecting exploitation anomalies like malformed protocol sequences. For Linux-based edge systems that do support agents, deploy osquery with the `process_events` and `socket_events` tables enabled. Write a Sigma rule targeting your web application server process spawning unexpected child processes (e.g., Apache/Nginx spawning bash or sh) — this is the canonical post-exploitation signal for T1190 web application attacks.

Evidence: Query web server access logs for anomalous HTTP methods, oversized request bodies, or URI patterns matching known exploit payloads (e.g., path traversal sequences `../../`, JNDI injection strings `${jndi:`, SQL meta-characters in GET/POST parameters). On VPN and firewall appliances, extract authentication logs and look for successful authentication events immediately preceding configuration changes or new admin account creation — this pattern indicates exploitation followed by persistence. Pull NetFlow or Zeek `conn.log` data for the 72-hour window preceding any suspected compromise to identify beaconing or unusual outbound connections from perimeter devices.

Step 4: Validate that identity controls are not your only fallback — the DBIR shift means an attacker exploiting a perimeter vulnerability bypasses credential controls entirely; verify network segmentation, least-privilege service account configurations (NIST AC-6; CIS 5.4), and lateral movement controls are functioning independently of MFA protections

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring defense-in-depth controls are operational and not dependent on a single control layer that perimeter exploitation renders irrelevant

Controls: NIST AC-6 (Least Privilege), NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Run `netstat -ano` (Windows) or `ss -tulpn` (Linux) on internal systems to enumerate listening services reachable from your DMZ — compare against intended architecture. Use `net localgroup administrators` (Windows) or `getent group sudo` (Linux) on all internal servers to audit which accounts hold elevated privileges; any service account with local admin rights that is also used by an external-facing application is a direct lateral movement path post-exploitation. Test VLAN segmentation by attempting ICMP and port scans from a DMZ host to internal segments using nmap — if successful, segmentation is not enforced. For OT/ICS, verify that remote interfaces are on isolated VLANs with explicit deny-all rules between OT and IT segments.

Evidence: Document the current network segmentation topology with firewall ACL exports before making changes — this is your pre-incident baseline. Enumerate all service accounts associated with external-facing applications (web servers, VPN services, API gateways) and record their privilege levels, password last-set dates, and whether they can authenticate to internal resources. If an exploitation event is later confirmed, this inventory establishes whether the compromised service account had privileges sufficient for lateral movement, which is critical for scoping the incident.

Step 5: Incorporate AI-accelerated exploitation timelines into your threat model — update your incident response playbooks to reflect compressed disclosure-to-exploitation windows; the assumption that you have days to patch after a CVE is published is no longer operationally safe for critical-severity externally-facing flaws

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: maintaining current IR playbooks and threat models that reflect the operational threat environment, including updated timelines driven by AI-accelerated weaponization of newly disclosed CVEs

Controls: NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST PM-16 (Threat Awareness Program), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Subscribe to CISA's free KEV RSS feed and configure an email or Slack alert for new additions — treat any KEV addition for an asset class you own as a potential active incident trigger, not just a patching task. Integrate EPSS score monitoring: any CVE with EPSS > 0.70 on an external-facing asset should trigger your 'possible active exploitation' detection playbook immediately, not after patch SLA review. Update your IR playbook to include a

'zero-day or rapid exploitation' decision branch that bypasses normal change management for emergency compensating controls (WAF virtual patching, temporary service isolation) when a CVE affecting your external stack appears on KEV within 48 hours of disclosure.

Evidence: Maintain a timestamped log of NVD/CVE disclosure dates versus KEV addition dates for vulnerabilities affecting your asset classes — this is your empirical evidence for the compressed exploitation window claim in your threat model. When briefing leadership or auditors, this data makes the AI-acceleration argument concrete rather than theoretical. Capture vendor advisory publication timestamps alongside KEV addition dates for your specific product stack to demonstrate the actual disclosure-to-KEV window your organization faces.

Step 6: Communicate findings — brief leadership with the specific organizational risk: how many unpatched external-facing systems exist, what the CISA KEV overlap is, and what the business impact of a successful exploitation event would be; avoid generic 'patch faster' framing in favor of asset-specific risk language

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: translating threat intelligence and incident findings into organizational risk communication that drives resource allocation and policy decisions at the leadership level

Controls: NIST IR-4 (Incident Handling), NIST PM-9 (Risk Management Strategy), NIST RA-3 (Risk Assessment), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Build a one-page risk brief using the KEV JSON feed output from Step 1: count KEV-matched vulnerabilities by asset class (VPN: X, web apps: Y, firewalls: Z), map each to the business process it supports (e.g., 'VPN gateway serves 800 remote employees and all M365 traffic'), and estimate breach impact using publicly available DBIR cost-per-incident figures for your industry vertical. Use the DBIR 2026 industry supplement data (when released) to contextualize your sector's specific exploitation frequency. This approach replaces abstract CVSS numbers with language leadership can act on: 'Our edge VPN has 3 KEV-listed unpatched CVEs; the DBIR shows this is the #1 confirmed breach vector this year; a successful exploit gives an attacker direct access to our internal network without needing credentials.'

Evidence: Attach the dated KEV overlap report from Step 1 as a supporting exhibit to your leadership brief — this is both the risk evidence and the paper trail demonstrating that the security team identified and communicated the risk. If a breach subsequently occurs, this document protects the organization by showing proactive risk identification and escalation. Retain the brief with version control and distribution records.

Step 7: Monitor DBIR supplemental releases and CISA advisories — Verizon typically releases industry-vertical supplements post-DBIR; track for sector-specific findings relevant to your industry and correlate with any new KEV additions

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrating external threat intelligence and industry findings into continuous improvement of detection, response, and vulnerability management processes

Controls: NIST PM-16 (Threat Awareness Program), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Set up free threat intelligence feeds using RSS or API: CISA advisories (https://www.cisa.gov/cybersecurity-advisories — RSS available), CISA KEV JSON feed (daily pull via cron), and NVD CVE feed filtered to your product CPEs. For Verizon DBIR supplements, monitor the Verizon security blog and set a Google Alert for 'DBIR 2026 [your industry]'. Correlate new KEV additions weekly against your asset inventory using the Step 1 script — any new KEV addition affecting your stack should automatically create a tracked remediation ticket. Two-person teams can operationalize this with a weekly 30-minute 'threat intel sync' using only free feeds and a shared tracking spreadsheet.

Evidence: Maintain a running intelligence log that maps external advisories and DBIR findings to your internal asset inventory and open vulnerability backlog — date-stamp each entry. This log demonstrates continuous threat-informed risk management and is valuable evidence for compliance audits (demonstrating NIST SI-5 compliance) and for post-incident reconstruction showing whether your team was aware of a relevant threat actor or technique before a breach occurred.

Detection Guidance

The MITRE techniques flagged in this story point to three distinct detection surfaces that security teams should audit against current coverage.

For T1190 (Exploit Public-Facing Application): Review WAF and edge device logs for anomalous request patterns against authentication endpoints, admin interfaces, and known vulnerable paths, particularly for CVEs disclosed in the last 90 days. Look for successful authentication events from IP ranges with no prior organizational history immediately following a failed exploitation sequence. NIST AU-6 (Audit Record Review and Analysis) should be configured to flag these patterns on an accelerated review cycle for external-facing assets.

For T1203 (Exploitation for Client Execution): Monitor endpoint telemetry for unexpected child processes spawned from browser, email client, or document rendering processes. Correlate against file system modifications (NIST SI-7: Software, Firmware, and Information Integrity) to detect modification of system files following a suspicious parent-child process chain. If your EDR coverage has gaps on specific asset classes, prioritize closing those gaps on assets that handle inbound external content.

For T1072 (Software Deployment Tools): Audit software deployment infrastructure (SCCM, Ansible, remote management agents) for executions originating outside normal deployment windows or from accounts without a documented deployment role. NIST AC-2 (Account Management) monitoring should flag any privileged account accessing deployment tooling outside business hours or from unexpected source IPs.

Broader hunting hypothesis: Given the DBIR's emphasis on exploitation bypassing perimeter controls, run a query across your SIEM for any authentication event on internal systems that cannot be correlated back to a documented VPN or authorized remote access session in the preceding 30-minute window. Unexplained authenticated internal activity with no corresponding perimeter entry event is a high-signal indicator of successful exploitation as the initial access method.

Log sources to prioritize: edge device syslogs (VPN, firewall, load balancer), WAF access logs, authentication logs for privileged accounts, and deployment tool execution logs. If any of these sources are not currently ingested into your SIEM, that is the first gap to close; NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) require coverage across enterprise assets.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Verizon DBIR 2026 full report (verizon.com/about/news) for published indicators`	The DBIR is an aggregate empirical report, not a single-incident advisory; campaign-specific IOCs are not published in the report itself. Sector-specific threat intelligence correlated with DBIR findings should be sourced from CISA advisories and ISACs relevant to your industry vertical.	LOW

Framework Mappings

MITRE-ATTACK

- **T1072** — Software Deployment Tools
- **T1203** — Exploitation for Client Execution
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1072	Software Deployment Tools	Execution
T1203	Exploitation for Client Execution	Execution

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://www.verizon.com/about/news/breach-industry-wide-dbir-finds	T3
Vulnerability Exploitation Top Breach Entry Point, 2026	https://www.globenewswire.com/news-release/2026/05/19/3297614/0/en/...	T3
Vulnerability Exploitation Top Breach Entry Point, 2026 Industry ...	https://www.barchart.com/story/news/2015287/vulnerability-exploitat...	T3
Verizon DBIR finds vulnerability exploitation overtakes stolen ...	https://industrialcyber.co/reports/verizon-dbir-finds-vulnerability...	T3
Verizon DBIR 2026: Vulnerability Exploitation Overtakes Credential ...	https://www.reddit.com/r/cybersecurity/comments/1tjzt11/verizon_dbi...	T3

Generated 2026-05-23 06:27 UTC by TJS Security Command Center