INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 06:36 UTC

AI-Accelerated Exploit Development Compresses Vulnerability Window, CrowdStrike and IBM X-Force Report

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0122
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Enterprise security tooling broadly; CrowdStrike Falcon Platform referenced as primary intelligence source
Discovery Source	Rss:T1 Threatintel

Executive Summary

AI-assisted tooling is collapsing the time between vulnerability disclosure and active exploitation from weeks to hours, a structural shift documented independently by CrowdStrike's 2026 Global Threat Report and IBM X-Force. CrowdStrike recorded a 42% year-over-year increase in zero-day exploitation and an 89% rise in AI-assisted adversary attacks, driven by purpose-built offensive AI datasets developed by both state-aligned and criminal groups. For CISOs and boards, this signals that existing patch prioritization timelines and mean-time-to-remediate benchmarks are no longer calibrated to the actual threat velocity adversaries now operate at.

Technical Analysis

The convergence documented in these two independent reports represents a structural change in attacker economics, not a one-cycle anomaly. CrowdStrike's 2026 Global Threat Report documents a 42% year-over-year increase in zero-day exploitation and an 89% rise in AI-assisted adversary attacks. IBM X-Force independently corroborates acceleration in exploitation timelines, with both vendors identifying the same underlying driver: adversaries are no longer relying solely on general-purpose coding models. IBM X-Force specifically flags active development of purpose-built offensive AI datasets by frontier labs, private groups, and adversarial nation-state actors. These datasets are trained to accelerate fuzzing, automated exploit generation, and infrastructure provisioning, the three most time-intensive phases of a traditional exploitation campaign.

The practical result is that the vulnerability window, historically measured in days to weeks, is compressing to hours. Memory safety vulnerabilities (CWE-119, CWE-787), improper input validation (CWE-20), and code

injection weaknesses (CWE-94) represent the primary exploitation surface being accelerated. These classes are not new, but the speed at which working exploits are now generated against them is. Adversaries are pairing AI-accelerated exploit development with automated infrastructure acquisition (T1583) and living-off-the-land execution via scripting interpreters (T1059) to reduce the human labor required per intrusion.

The MITRE ATT&CK techniques observed across attributed campaigns in this reporting period form a recognizable pattern: initial access via public-facing application exploitation (T1190) or phishing (T1566), privilege escalation (T1068), lateral movement via remote services (T1021), client-side exploitation (T1203), and exfiltration over command-and-control channels (T1071, T1020). The acquisition of offensive AI tooling (T1588.006) and development of exploitation capabilities (T1587.004) as distinct ATT&CK techniques now appear with measurable frequency in tracked campaigns.

Threat actors demonstrating AI-assisted tradecraft adoption include Russian GRU-aligned operations, North Korean state actors, and financially motivated criminal groups, as documented in CrowdStrike and IBM X-Force threat reporting. Their shared adoption of AI-assisted tradecraft suggests capability diffusion across the adversary ecosystem, not isolated experimentation by a single advanced actor. The implication for defenders is that AI-accelerated exploitation is no longer a threat reserved for targets of nation-state interest; it is becoming baseline criminal infrastructure.

Action Checklist

1. Step 1: Assess exposure, audit your organization's patch SLA policies against current mean exploitation timelines; if your SLA is measured in weeks, it is no longer aligned with a threat environment where exploitation can follow disclosure in hours
2. Step 2: Review controls, verify EDR coverage and detection rule freshness across all endpoints; confirm that vulnerability management tooling is ingesting threat intelligence feeds that include exploitation velocity data, not just CVSS scores; validate that memory-safety-class vulnerabilities (CWE-119, CWE-787) and input validation weaknesses (CWE-20) are prioritized in your scanning cadence
3. Step 3: Update threat model, incorporate AI-accelerated exploit development as a baseline adversary capability into your threat register; map state-aligned and financially motivated threat actor activity as a named threat if your sector or geopolitical exposure warrants it; map the T1190, T1059, T1068, T1021, and T1583 technique chain as a priority detection scenario
4. Step 4: Communicate findings, brief leadership on the documented trend from CrowdStrike and IBM X-Force: increasing zero-day exploitation and AI-assisted attack campaigns represent a quantified shift in threat velocity, not a qualitative warning; frame the ask around patch window compression and detection engineering investment rather than general AI risk
5. Step 5: Monitor developments, track CrowdStrike Global Threat Report follow-on advisories and IBM X-Force Threat Intelligence Index updates for published IOCs, actor-specific tooling indicators, and sector-targeted campaign data as this reporting cycle continues

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to CISO and legal counsel immediately if retrospective IOC matching (Step 5) or anomalous process-tree analysis (Step 2) reveals evidence of T1190 exploitation or T1021 lateral movement activity attributable to FANCY BEAR, FAMOUS CHOLLIMA, or SPIDER-cluster actors, or if any regulated data (PII, PHI, financial records) was accessible from systems showing indicators of compromise, triggering breach notification obligations under applicable regulations.
Recovery Notes	Because this threat documents AI-accelerated exploitation of CWE-119, CWE-787, and CWE-20 vulnerability classes — not a single patched CVE — recovery is a posture shift, not a one-time remediation: verify that revised patch SLAs and detection rules are operational before declaring recovery complete, and maintain elevated monitoring of internet-facing services, authentication logs (Windows Event ID 4624/4625), and process creation telemetry (Sysmon Event ID 1) for a minimum of 90 days given the documented persistence capabilities of FANCY BEAR and SPIDER-cluster actors. Validate that all CWE-119 and CWE-787 findings in your scanner output have been either patched or formally risk-accepted with documented compensating controls, and confirm that vulnerability management tooling is now ingesting exploitation-velocity data feeds rather than CVSS-only scoring before closing the remediation cycle.
Forensic Artifacts	Web server access logs (IIS W3C logs or Apache/nginx access.log) filtered for anomalous POST request patterns to API endpoints or file upload handlers consistent with T1190 exploitation — AI-generated exploits targeting CWE-20 input validation weaknesses frequently produce malformed Content-Type headers, oversized payloads, or URL-encoded shellcode patterns distinguishable from normal traffic | Sysmon Event ID 1 (Process Creation) entries where ParentImage is a network-facing service (e.g., w3wp.exe, httpd, java) and Image is cmd.exe, powershell.exe, or wscript.exe — this parent-child anomaly is the primary host artifact of successful CWE-119/CWE-787 memory corruption exploitation leading to code execution (T1059) | Windows Security Event Log Event ID 4673 (Privileged Service Called) and Event ID 4697 (Service Installed) within the same session as anomalous process creation — these are indicators of T1068 privilege escalation following initial exploitation, a technique explicitly mapped to FANCY BEAR and FAMOUS CHOLLIMA post-exploitation chains | Memory dump artifacts from the exploited process: if CWE-787 out-of-bounds write exploitation occurred, process memory will contain shellcode regions with executable permissions in non-standard memory segments — capture with ProcDump (`procdump.exe -ma `) and analyze with Volatility3 malfind plugin to identify injected shellcode consistent with AI-generated exploit payloads | DNS query logs and proxy logs for outbound connections from the exploited host occurring within 60 seconds of the anomalous Sysmon Event ID 1 alert — SPIDER-cluster and FANCY BEAR C2 callback patterns documented in CrowdStrike GTR show rapid beaconing after T1059 execution, often to newly registered domains or compromised legitimate infrastructure identified via passive DNS analysis

Per-Action IR Details

Step 1: Assess exposure — audit your organization's patch SLA policies against current mean exploitation timelines; if your SLA is measured in weeks, it is no longer aligned with a threat environment where exploitation can follow disclosure in hours

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability, policies, and readiness posture before incidents occur

Controls: NIST SI-2 (Flaw Remediation) — requires organizations to identify, report, and correct system flaws and test remediation effectiveness, NIST RA-3 (Risk Assessment) — mandates assessment of the likelihood and impact of threats given current threat intelligence, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) —

requires a documented vulnerability management process reviewed and updated to reflect current threat conditions, CIS 7.2 (Establish and Maintain a Remediation Process) — mandates a risk-based remediation strategy with defined SLA tiers that must be re-evaluated as exploitation velocity data changes

Compensating: Export your current patch SLA policy document and map each SLA tier (critical/high/medium) against the CrowdStrike-reported mean time-to-exploit metric of hours, not weeks. Use a simple spreadsheet: Column A = CVE severity tier, Column B = current SLA, Column C = CrowdStrike 2026 GTR mean exploitation window. For vulnerability scanning without commercial tooling, run OpenVAS (Greenbone Community Edition) on a weekly cron job targeting internet-facing assets first. Script a daily pull from CISA KEV (https://www.cisa.gov/known-exploited-vulnerabilities-catalog — human validation recommended) using curl and compare against your asset inventory to flag any actively exploited CVEs your current SLA would miss.

Evidence: Before revising SLA policy, preserve the current state as a baseline artifact: export your existing patch SLA policy document with timestamps, pull a point-in-time report from your vulnerability scanner showing open findings older than your current SLA thresholds, and capture your vulnerability management tool's current threat feed configuration to document whether it ingests exploitation velocity data or only CVSS scores. This establishes the pre-remediation risk posture for post-incident review and audit evidence under NIST IR-5 (Incident Monitoring).

Step 2: Review controls — verify EDR coverage and detection rule freshness across all endpoints; confirm that vulnerability management tooling is ingesting threat intelligence feeds that include exploitation velocity data, not just CVSS scores; validate that memory-safety-class vulnerabilities (CWE-119, CWE-787) and input validation weaknesses (CWE-20) are prioritized in your scanning cadence

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring infrastructure, detection rule currency, and correlation of indicators aligned to current adversary capabilities

Controls: NIST SI-4 (System Monitoring) — requires monitoring of the system to detect attacks and indicators of potential attacks, NIST SI-5 (Security Alerts, Advisories, and Directives) — requires ingestion of external security alerts and advisories, including exploitation velocity data from CrowdStrike GTR and IBM X-Force Threat Intelligence Index, NIST AU-2 (Event Logging) — requires identification of event types the system is capable of logging to support detection of exploitation attempts targeting CWE-119, CWE-787, and CWE-20 vulnerability classes, CIS 7.3 (Perform Automated Operating System Patch Management) — ensures OS-level memory-safety vulnerabilities (CWE-119 buffer overflows, CWE-787 out-of-bounds writes) are addressed within an automated cadence, CIS 7.4 (Perform Automated Application Patch Management) — ensures application-layer input validation weaknesses (CWE-20) are patched through automated mechanisms

Compensating: For teams without commercial EDR: deploy Sysmon v15+ with the SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config — human validation recommended) which captures process creation (Event ID 1), network connections (Event ID 3), and memory allocation anomalies relevant to CWE-119/CWE-787 exploitation. To validate detection rule freshness against AI-accelerated exploit patterns, pull the SigmaHQ rule repository and filter for rules tagged 'exploit' and 'cwe-119' or 'cwe-787': `grep -r 'CWE-119\|CWE-787\|buffer.overflow\|out.of.bounds' sigma/rules/ --include='*.yml' -l`. For exploitation velocity intel without a commercial feed, subscribe to CISA KEV RSS and NVD's CVE JSON feed filtered by CWE-119, CWE-787, and CWE-20, then compare disclosure dates against KEV add dates to derive your own mean-time-to-exploitation metric for your asset classes.

Evidence: Capture the following before rule updates: export current EDR detection rule set with last-modified timestamps to document staleness; query your SIEM or Windows Event Log for the past 30 days of Event ID 4688 (Process Creation) entries where the spawning process is a network-facing service and the child process is cmd.exe, powershell.exe, or a known scripting interpreter — this baseline reveals whether AI-generated shellcode leveraging CWE-119/CWE-787 has already produced anomalous process trees; export your vulnerability scanner's current plugin/feed version and last-update timestamp to document whether CWE-119 and CWE-787 findings are being scored with exploitation-velocity weighting or CVSS-only.

Step 3: Update threat model — incorporate AI-accelerated exploit development as a baseline adversary capability into your threat register; add FANCY BEAR, FAMOUS CHOLLIMA, and financially motivated SPIDER-cluster actors as named threats if your sector or geopolitical exposure warrants it; map the T1190,

T1059, T1068, T1021, and T1583 technique chain as a priority detection scenario

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Threat modeling, actor profiling, and detection engineering as foundational IR readiness activities

Controls: NIST RA-3 (Risk Assessment) — requires assessment of threat likelihood incorporating current threat intelligence, explicitly including named actor groups and AI-assisted offensive capabilities, NIST IR-4 (Incident Handling) — requires an incident handling capability that includes preparation activities such as threat modeling and technique-level detection planning, NIST SI-5 (Security Alerts, Advisories, and Directives) — requires dissemination of threat intelligence to relevant personnel, including actor-specific TTPs from CrowdStrike GTR and IBM X-Force, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — threat model updates must feed back into vulnerability prioritization, particularly for T1190 (Exploit Public-Facing Application) which directly targets unpatched internet-exposed services

Compensating: Build the MITRE ATT&CK technique chain (T1190 → T1059 → T1068 → T1021 → T1583) as a Sigma rule chain using the SigmaHQ framework. Specific rule targets: T1190 — web server access logs for anomalous POST requests to known vulnerable endpoints; T1059 — Sysmon Event ID 1 filtering on powershell.exe or cmd.exe with encoded command-line arguments (`-enc`, `-e`, `IEX`); T1068 — Windows Security Event Log Event ID 4697 (service installed) or 4673 (privileged service called) following an anomalous process creation; T1021 — Event ID 4624 logon type 3 (network) or type 10 (remote interactive) from unexpected source IPs within minutes of the T1059 alert; T1583 (resource development, pre-compromise) — monitor passive DNS or threat intel feeds for newly registered domains typosquatting your organization's name or mimicking your vendor tooling, a documented FANCY BEAR and SPIDER-cluster pre-attack behavior.

Evidence: Before updating the threat register, document the current threat model state: export existing threat register entries to establish what actors and techniques were previously scoped in or out; pull MITRE ATT&CK Navigator layer exports for FANCY BEAR (G0007), FAMOUS CHOLLIMA (G1006), and representative SPIDER-cluster groups showing their current technique coverage against your existing detection rules; capture any prior threat intelligence reports referencing these actors in your sector to justify the scoping decision and provide audit evidence for NIST RA-3 compliance.

Step 4: Communicate findings — brief leadership on the specific metric: a 42% increase in zero-day exploitation and an 89% rise in AI-assisted attacks represent a quantified shift in threat velocity, not a qualitative warning; frame the ask around patch window compression and detection engineering investment rather than general AI risk

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned communication, reporting to leadership, and using threat intelligence to drive capability improvements

Controls: NIST IR-6 (Incident Reporting) — requires reporting of incident and threat information to organizational leadership and relevant personnel within defined timeframes, NIST IR-8 (Incident Response Plan) — requires the IR plan to include communication procedures to senior leadership with evidence-based metrics supporting resource and capability decisions, NIST RA-3 (Risk Assessment) — quantified threat metrics (42% zero-day increase, 89% AI-assisted attack rise from CrowdStrike 2026 GTR) constitute updated risk assessment inputs that must be communicated to risk owners, CIS 7.2 (Establish and Maintain a Remediation Process) — leadership brief must explicitly connect the CrowdStrike-reported exploitation velocity data to the need for revised patch SLA tiers and detection engineering investment

Compensating: Prepare a one-page brief using only publicly verifiable data points from CrowdStrike's 2026 Global Threat Report and IBM X-Force Threat Intelligence Index — do not interpolate or extrapolate beyond what those reports state. Structure the brief as: (1) current SLA vs. documented mean time-to-exploit gap, (2) specific technique chain (T1190, T1059, T1068, T1021, T1583) mapped to your current detection coverage gaps identified in Step 2, (3) concrete ask: funding for detection rule refresh cycle and patch SLA policy revision with defined new SLA targets. Attach the Step 1 SLA gap spreadsheet and Step 2 EDR rule staleness report as supporting evidence. This documentation also satisfies NIST AU-6 (Audit Record Review, Analysis, and Reporting) requirements for communicating analysis findings.

Evidence: Compile supporting evidence package before the brief: the Step 1 SLA gap analysis, Step 2 EDR coverage and rule-freshness report, and Step 3 threat register delta showing what actor/technique coverage was added. Preserve CrowdStrike 2026 GTR and IBM X-Force report PDFs with download timestamps as primary source citations — these are the evidentiary basis for the quantified metrics and must be retained as audit artifacts under NIST AU-11 (Audit Record Retention) to support any subsequent regulatory or board-level inquiry.

Step 5: Monitor developments — track CrowdStrike Global Threat Report follow-on advisories and IBM X-Force Threat Intelligence Index updates for published IOCs, actor-specific tooling indicators, and sector-targeted campaign data as this reporting cycle continues

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Continuous monitoring, CTI integration, and correlation of external intelligence with internal telemetry

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — requires ongoing receipt of external threat intelligence including actor-specific IOCs and campaign data from authoritative sources such as CrowdStrike and IBM X-Force, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — requires ongoing review and analysis of audit records for indications of threat activity, enriched by external CTI feeds, NIST IR-5 (Incident Monitoring) — requires tracking and documenting threat activity indicators, including FANCY BEAR, FAMOUS CHOLLIMA, and SPIDER-cluster campaign updates as they are published, CIS 8.2 (Collect Audit Logs) — continuous log collection must be validated as operational across all assets to ensure that when new IOCs from CrowdStrike or X-Force are published, retrospective log searches are possible

Compensating: For teams without a commercial threat intelligence platform: configure RSS/Atom feed monitoring for CrowdStrike Adversary Intelligence blog, IBM X-Force Exchange, and CISA Alerts (us-cert.cisa.gov/ncas/alerts — human validation recommended) using a free aggregator such as FreshRSS or Miniflux deployed on-premises. When new IOCs are published for FANCY BEAR, FAMOUS CHOLLIMA, or SPIDER-cluster tooling, convert them to YARA rules for file-based indicators and to osquery scheduled queries for host-based behavioral indicators (e.g., `SELECT * FROM processes WHERE name IN ('known_malware.exe') OR cmdline LIKE '%base64_encoded_payload%'`). For network IOCs (C2 domains, IPs), push them into your host firewall blocklist via a daily PowerShell script that reads from a local STIX/TAXII-formatted IOC file and updates Windows Firewall rules using `netsh advfirewall firewall`.

Evidence: Establish a threat intelligence log as a running artifact: maintain a timestamped record of each CrowdStrike and IBM X-Force advisory ingested, the IOCs extracted, and the date each IOC was added to detection tooling — this creates an audit trail for NIST IR-5 (Incident Monitoring) compliance and documents the organization's CTI-to-detection pipeline latency. Retroactively query 90 days of web proxy or DNS logs for any previously undetected domains or IPs that match newly published FANCY BEAR or SPIDER-cluster C2 infrastructure indicators, since AI-accelerated campaigns may have already established footholds before IOC publication.

Detection Guidance

Because this trend affects the pre-exploitation and early-intrusion phases most directly, detection focus should weight initial access and privilege escalation. Review web application and perimeter logs for unusual sequencing of reconnaissance probes followed by rapid exploitation attempts against known CVE classes, this compressed timing is itself a behavioral signal. Hunt for scripting interpreter execution (PowerShell, cmd, bash) spawned from unexpected parent processes, particularly web server processes or service accounts, consistent with T1059 post-exploitation. Monitor for new scheduled tasks, service installations, or registry run key modifications following any external-facing application activity. For AI-assisted infrastructure acquisition (T1583), watch for rapid provisioning of new cloud or VPS resources from unfamiliar IP ranges correlating with inbound attack activity. Audit privileged account usage for anomalous lateral movement patterns via RDP, SMB, or WMI (T1021). Detection engineering teams should prioritize rule coverage for the CWE-20 and CWE-94 exploitation classes, specifically, anomalous input patterns to web-facing APIs and unexpected process spawning from interpreted code execution. Given the speed compression documented, signature-based detection alone is

insufficient; behavioral baselines and anomaly detection on short time windows are necessary complements. Review threat intelligence integration to confirm your SIEM or XDR is ingesting exploitation velocity data so that newly disclosed vulnerabilities in the CWE-119/787 class trigger escalated monitoring automatically rather than waiting for scheduled scan cycles.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to CrowdStrike 2026 Global Threat Report for published indicators`	CrowdStrike's 2026 Global Threat Report references AI-assisted tooling and actor-specific infrastructure indicators; specific hashes, domains, and C2 addresses are published in the full report and associated Falcon intelligence advisories	LOW
TOOL	`Pending — refer to IBM X-Force Threat Intelligence Index for published indicators`	IBM X-Force documents offensive AI dataset development and associated campaign infrastructure; specific indicators are available through the X-Force Threat Intelligence portal and index report	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter
- **T1020** — Automated Exfiltration
- **T1588.006** — Vulnerabilities
- **T1587.004** — Exploits
- **T1566** — Phishing
- **T1068** — Exploitation for Privilege Escalation
- **T1021** — Remote Services
- **T1203** — Exploitation for Client Execution
- **T1071** — Application Layer Protocol
- **T1583** — Acquire Infrastructure

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **SI-10** — Information Input Validation
- **SI-16** — Memory Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1020	Automated Exfiltration	Exfiltration
T1588.006	Vulnerabilities	Resource-Development
T1587.004	Exploits	Resource-Development
T1566	Phishing	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Technique ID	Technique Name	Tactic
T1021	Remote Services	Lateral-Movement
T1203	Exploitation for Client Execution	Execution
T1071	Application Layer Protocol	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/tune-in-future-of-ai-powered...	T3
	https://www.crowdstrike.com/en-us/blog/crowdstrike-named-leader-gar...	T3
	https://www.crowdstrike.com/en-us/blog/announcing-threat-ai-industr...	T3
	https://www.ibm.com/think/x-force/understanding-future-of-offensive...	T3
The CrowdStrike Falcon® Platform | Unified Agentic Security	https://www.crowdstrike.com/en-us/platform/	T3

Generated 2026-05-12 06:36 UTC by TJS Security Command Center