Level 4 Unified TDIR SOC tooling is fully integrated and a single pane of glass brings together detections, enrichment, investigations, automated response, containment, remediation, and threat eradication. Level 3 Enhanced insights and analytics Collect web and application server data, command line, PowerShell and file-level audit logs and focus on more specific capabilities such as fraud, insider threat, threat hunting, and OT/ICS requirements. Level 2 Data exploration and automation Increased data collection and volumes including workstation and endpoint/EDR, cloud infrastructures and services, DHCP and DNS data, and threat intelligence feeds. Level 1 Foundational data insights Collect basic security logs such as intrusion prevention and detection systems as well as server and EDR for critical infrastructure. A standard security taxonomy is applied. Asset and identity data is added. Description Milestones Challenges Data source Level 4
Automated malware analysis (Sandbox)
SDLC/DevOps specific data sources
DLP
Database query/transaction logs
Full email body
Chat
SWIFT/wire data logs (specific to fraud)
Physical security logs
Printer/copiers logs
3rd party forensics tools Level 3
Application servers
Web servers
Web application firewall (WAF)
Command line audit logs
PowerShell audit logs
File level audit logs
NAC
NDR (Network detection and response)
OT/ICS specific data sources Level 2
Desktops/workstations
Sysmon
Email servers/email gateways
EDR for endpoints/clients
EDR for all servers
VPN
Cloud infrastructure and services (IaaS/PaaS/SaaS)
DHCP
DNS
Threat intelligence feeds (TI) Level 1
Firewalls (and NextGen firewalls)
Intrusion prevention/detection systems
Vulnerability management (VM)
Windows servers
Linux/Unix servers
Asset and identity lists (from CMDB, AD, LDAP etc.)
Active directory/domain controllers
Anti-virus/malware
Proxy systems (Web proxies)
User authentication (SSO/PAM/IAM/SAML)
EDR for critical infrastructure Reference data
Good/bad app protocols and ports
Bad network traffic
Subnet/network locations

Blocked countries
Interesting processes
Interesting services
Service/non-human accounts
Admin/privileged accounts
VIP type users
Known user types and titles
Organizational units that contain critical assets
Known honeypots
Known vulnerability scanners Foundational data insights This level focuses on collecting machine data generated by the foundational components of your security infrastructure, including servers and security controls, and the gathering of assets and identities reference data. This data, along with the implementation of the Common Information Model (CIM) enables you to track systems and users on your network and to consume detection mechanisms for critical infrastructure. Even if you don ' t plan to stand up a formal SOC, normalized data will streamline investigations and improve the effectiveness of an analyst.
The foundation for the collection, storage, processing, and analysis of data has been established.
Analysts have the data necessary to enable a security specialist to perform basic investigations.
Data is mapped properly to the CIM. Common Information Model documentation
Search performance can be improved dramatically through the use of accelerated data models associated with the CIM.
Asset and user details are correlated to events in your security log platform. The foundational data you are collecting supports basic threat detection and investigation but lacks context and might contain indicators of compromise that are known to your peer organizations but lay undetected in your environment. Everything at this stage is predominantly manual and performed in an ad-hoc fashion with little to no event enrichment.
Firewalls (and NextGen Firewalls)
Intrusion Prevention / Detection Systems
Vulnerability Management (VM)
Windows Servers
Linux/Unix Servers
Asset and Identity Lists (from CMDB, AD, LDAP etc.)
Active Directory; Domain Controllers
Anti-Virus / Malware
Proxy Systems (Web Proxies)
User Authentication (SSO / PAM / IAM / SAML)
EDR for critical infrastructure Data exploration and automation The data sources at this level unlock a rich set of detection capabilities and the automation of simple response actions. Endpoint, cloud, and DNS data, along with threat intelligence feeds, improve visibility and contextual understanding while enhancing early threat detection and incident response capabilities. World-class threat hunters rely on DNS and advanced endpoint data to uncover and track adversaries dwelling in your network.
Opportunities to automate more routine tasks such as password resets/lockouts, malicious IP blocking etc. have been identified and implemented. The Splunk Common Information Model (CIM) is being utilized to normalize data to aid in the scale and speed of security event correlation.
Monitoring endpoint behavior allows early detection of suspicious activities and/or anomalies and provides valuable insights into user behavior and application usage.
Monitoring cloud environments provides visibility into atypical activities and potential threats in cloud-based applications and services.
Monitoring DNS traffic can help identify and block malicious activities at an early stage.
Integrating threat intelligence feeds enhances proactive threat prevention and incident response capabilities.
Simple automation capabilities such as the automated blocking of malicious IP addresses and the

automated response to detected threats on endpoints and servers. Classifying risk into categories and by particular risk objects can be a challenge. Knowing where your most critical assets are and protecting them with the appropriate detections is key to a healthy security program. Filtering the "noise" and focusing on the most important events leads to more success which is why classifying risk is so critical as it allows you to have higher fidelity analytics in your data.
Desktops / Workstations
Sysmon
Email Servers / Email Gateways
EDR for endpoints/clients
EDR for all servers
VPN
Cloud infrastructure and Services (IaaS / PaaS / SaaS)
DHCP
DNS
Threat Intelligence Feeds (TI) Enhanced insights and analytics The integration of these data sources enhances threat detection through improved visibility into application-layer activities, behavioral analysis, and the monitoring of broader attack surfaces. It enables the detection of insider threats, supports incident response and investigation with additional, detailed logs, and contributes to policy enforcement and compliance — especially in OT/ICS environments.
Monitoring application and web servers helps identify vulnerabilities and potential attack vectors in web applications.
Monitoring user activities and file access patterns through command line, PowerShell, and file-level audit logs aids insider threat detection, incident response, and forensic analysis.
NDR data improves the detection and response to network-based threats and supports quick mitigation of security incidents.
Monitoring and analysis of OT/ICS-specific data improves critical infrastructure security and prevents disruptions to industrial processes, equipment, and devices.
Analysts are able to quickly identify high-priority/high fidelity events because risk is fully understood and contextualized in the alerts. Capability gaps may exist, which can also introduce visibility gaps. Some pre-built solutions may exist to fill these gaps or more tailored detections/workflows will need to be created. Behavioral-based detections can be particularly challenging but are crucial in detecting deviations from "normal" user/asset activity. User behavior, network, and OT/ICS visibility has significantly improved and few gaps remain but SOC workflows have not yet been fully integrated or unified across DevSecOps.
Application Servers
Web Servers
Web Application Firewall (WAF)
Command Line Audit Logs
PowerShell Audit Logs
File Level Audit Logs
NAC
NDR (Network Detection and Response)
OT / ICS specific Data Sources Unified threat detection, investigation, and response workflows The availability of these data sources, along with more advanced automation, minimizes visibility gaps and enables the implementation of unified, risk-based threat detection, investigation and response (TDIR) workflows within the SOC and the software development life cycle.
Security measures are integrated throughout the software development life cycle enabling early detection of vulnerabilities.
Physical security logs provide insights into access control, surveillance, and other physical security measures.
Automation is present everywhere.
Artificial intelligence and machine learning are fully utilized to provide more augmentation to security analysts. Continued refinement of the TDIR lifecycle as well as ongoing automation and integration of

SOC workflows and processes. Equipping and evolving the SOC to continually detect and respond to the latest 0-day attacks is the biggest challenge. This is addressed through repetition and preparedness through activities such as attack simulation, tabletop exercises, and staying current with the ever-changing threatscape.
Automated Malware Analysis (Sandbox)
SDLC / DevOps specific Data Sources
DLP
Database Query/Transaction Logs
Full Email Body
Chat
SWIFT / wire data logs (specific to fraud)
Physical Security Logs
Printer/Copiers Logs
3rd party forensics tools